

**СТУДИСКА ПРОГРАМА ПО  
КОМПЈУТЕРСКА БЕЗБЕДНОСТ И ДИГИТАЛНА ФОРЕНЗИКА  
НА ФАКУЛТЕТОТ ЗА ИНФОРМАТИКА, УГД-ШТИП  
РЕЖИМ НА СТУДИРАЊЕ 1 ГОДИНА (60 ЕКТС)**

Студентот кој ќе заврши втор циклус на едногодишни студии, студиска програма Компјутерска безбедност и дигитална форензика, се стекнува со следното звање:

На македонски јазик: **Магистер по информатика – Компјутерска безбедност и дигитална форензика**

На англиски јазик: **Master of Computer Science - Computer Security and Digital Forensics**

**СТРУКТУРА НА СТУДИСКА ПРОГРАМА**

Реден број	Код на предметот	Назив на наставен предмет	Семестар	Неделен фонд на часови		Задолжителен	Изборен	ЕКТС
				П	В			
ПРВА ГОДИНА								
1	2FI200123	Методологија и организација на научно истражувачка работа	1	2	2	X		6
2	2FI201223	Криптографски алгоритми и протоколи	1	2	2	X		6
3	2FI200523	Дигитална форензика	1	2	2	X		6
4		Изборен наставен предмет	1	2	2		X	6
5		Изборен наставен предмет	1	2	2		X	6
6	2FI201023	Етичко хакирање и пенетрациско тестирање	2	2	2	X		6
7	2FI200323	Безбедност на компјутерски мрежи и веб безбедност	2	2	2	X		6
8		Изборен наставен предмет	2	2	2		X	6
9		Магистерски труд	2			X		12
<b>Вкупно часови (предавања/вежби) и ЕКТС за година</b>								<b>60</b>

**Листа на изборни предмети**

Реден број	Код	Назив на предметот	Семестар	Неделен фонд на часови		ЕКТС	Од која единица
				предавања	вежби		
1	2FI215223	Сајбер криминал и дигитална форензика	1	2	2	6	Правен факултет
2	2FI213523	Напредно скриптинг програмирање	1	2	2	6	Факултет за информатика
3	2FI211623	Дигитална стеганографија и стеганализа	1	2	2	6	Факултет за информатика
4	2FI211023	Безбедност на софтвер	1	2	2	6	Факултет за информатика

5	2FI213623	Наука за податоците и аналитика на големите податоци	1	2	2	6	Факултет за информатика
6	2FI211223	Вештачката интелигенција во компјутерската безбедност	1	2	2	6	Факултет за информатика
7	2FI210923	Безбедност на контролни системи и IoT	2	2	2	6	Факултет за информатика
8	2FI212723	Мобилна безбедност и форензика	2	2	2	6	Факултет за информатика
9	2FI212323	Интернет на нештата со безбедност	2	2	2	6	Факултет за информатика
10	2FI216623	Форензика и безбедност на мултимедија	2	2	2	6	Факултет за информатика

### 3 Општи и специфични дескриптори

Ниво во Националната рамка на високообразовните квалификации на која му припаѓа студиска програма Компјутерска безбедност и дигитална форензика, Факултет за информатика, Универзитет “Гоце Делчев”, согласно со уредбата за националната рамка на високообразовните квалификации

Ниво во Националната рамка на високообразовните квалификации	Високо образование	Ниво во Европската рамка на високообразовни квалификации
VIIA	Едногодишни академски студии од втор циклус, 60/120 ЕКСТ	7

**Квалификации кои означуваат успешно завршување на вториот циклус на студии (60 ЕКТС) се доделуваат на лице кое ги исполнува следните дескриптори на квалификациите:**

**За. Општи дескриптори на квалификации за втор циклус на едно/двогодишни студии со 60 ЕКТС, студиска програма Компјутерска безбедност и дигитална форензика, Факултет за информатика, согласно со Уредбата за националната рамка на високообразовните квалификации**

Тип на дескриптор	Опис
Знаење и разбирање	<ul style="list-style-type: none"> <li>Покажуваат знаење и разбирање за алгоритмите, базите на податоци, протоколите, дизајнот на софтвер, концептите на програмски јазици, компјутерската организација и архитектура, основите на мрежите и веб архитектурата, поврзани со безбедноста и дигиталната форензика, и кои се надградуваат врз првиот циклус на студирање.</li> <li>Покажуваат способност за употреба на проширено и продлабочено знаење и покажуваат високо ниво на професионална компетентност за компјутерските науки, како и свесност за нивната еволуција и динамичка природа.</li> <li>Ги разбираат професионалните, етичките, законските, безбедносните и социјалните импликации и одговорности.</li> </ul>

Примена на знаењето и разбирањето	<ul style="list-style-type: none"> <li>• Поседуваат вештини, знаење и професионално искуство неопходно за да се започне практична работа или истражување.</li> <li>• Показуваат способност за проектирање, верификување и документирање на софтверските и хардверските решенија.</li> <li>• Поседуваат способност за примена на концептите и принципите на современите информатички технологии за независно и креативно решавање на практични проблеми во работната околина, со одредена доза на оригиналност, во нови, непознати услови и во мултидисциплинарен контекст.</li> <li>• Поседуваат способност за критичко и независно оценување на квалитетот на предложените решенијата.</li> </ul>
Способност за проценка	<ul style="list-style-type: none"> <li>• Показуваат способност за идентификување, анализирање и справување со комплексни проблеми и прашања од работната околина, систематски и креативно, како и дефинирање на техничките и човечките барања кои се соодветни за решавање на тие проблеми.</li> <li>• Показуваат способност за синтетизирање и интегрирање на знаење.</li> </ul>
Комуникациски вештини	<ul style="list-style-type: none"> <li>• Демонстрираат способност за размена на заклучоци и предлози, аргументирано и со рационално поткрепување на истите, како со стручни, така и со нестручни лица, јасно и недвосмислено.</li> <li>• Демонстрираат способност за ефективна работа самостојно или како продуктивен член на тим, кој може да биде и мултидисциплинарен.</li> <li>• Преземаат значителна одговорност за заедничките резултати.</li> </ul>
Вештини на учење	<ul style="list-style-type: none"> <li>• Лесно се прилагодуваат и совладуваат нови технологии и поседуваат способност за евалуација и користење на современите софтверски развојни алатки.</li> <li>• Имаат способност за идентификација на лична потреба од понатамошно образование и постојан професионален развој, преку користење на стручна и научна литература, професионални обуки, членување во професионални организации, и тн.</li> <li>• Имаат способност за независно делување при стекнувањето нови знаења и вештини самостојно во рамките на општествениот контекст.</li> </ul>

**36. Специфични дескриптори на квалификации за вториот циклус на студии со 60 ЕКТС, студиска програма Компјутерска безбедност и дигитална форензика, Факултет за информатика, согласно со уредбата за националната рамка на високообразовните квалификации**

Тип на дескриптор	Опис
Знаење и разбирање	<ul style="list-style-type: none"> <li>• Оспособување на студентите на втор циклус за научно - истражувачка работа во областа на компјутерската безбедност и дигиталната форензика;</li> <li>• Знаење и разбирање на правните аспекти и законската регулатива на компјутерската безбедност и дигиталната форензика, како и разликување на различните видови на компјутерски криминал;</li> <li>• Знаење и разбирање на проблематиката и актуелната развојно-истражувачка работа: тековни и развојни концепти, принципи и теории, техники и алатки, релевантни за компјутерската безбедност и дигиталната форензика, со проширено и продлабочено знаење и разбирање надградено врз знаењето од претходното образование.</li> <li>• Специјализирано знаење во областа на компјутерската безбедност и дигиталната форензика;</li> <li>• Критичко знаење за најнапредните достигнувања во избраните области, што обезбедува основа за оригиналност при развивањето и примената на автономни идеи во аналитички и истражувачки контекст.</li> </ul>
Примена на знаењето и разбирањето	<ul style="list-style-type: none"> <li>• Применува теоретски знаења и практични техники и алатки во анализата на безбедноста на компјутерските системи и мрежи, веб апликациите и мобилните уреди;</li> <li>• Применува теоретски знаења и практични техники и алатки за етичко хакирање и пенетрациско тестирање;</li> <li>• Применува теоретски знаења и практични техники и алатки во форензичката анализа на компјутерските системи и мрежи, мобилните уреди, како и во идентификацијата, здобивањето и чувањето на дигиталните докази;</li> <li>• Примена на стекнатите знаења во дизајн и развој на нпви софтверски решенија за потребите на компјутерската безбедност и дигиталната форензика</li> <li>• Способност да соработува во проектни тимови без комуникациски бариери и изразена смисла за заедништво и желба за резултати и нови сознанија.</li> <li>• Способност за анализа и синтеза на сознанијата од повеќе дисциплини.</li> <li>• Способност за критичко мислење, за независно и креативно решавање на проблеми.</li> </ul>

Способност за проценка	<ul style="list-style-type: none"> <li>• Способност за синтетизирање и интегрирање на знаењата во избраните области;</li> <li>• Способност за прибирање, анализирање, интерпретирање и користење на податоци и информации; донесување исправни проценки и изведување квалитетни толкувања и заклучоци, со почит на законската регулатива и етичките концепти;</li> <li>• Способност за пребарување, идентификување, и анализирање на проблеми, пред се од областа на компјутерската безбедност и дигиталната форензика, и идентификување и дефинирање на компјутерските барања кои се соодветни за решавање на тие проблеми;</li> <li>• Способност за идентификација и здобивање на дигиталните докази;</li> <li>• Демонстрираат свесност за примената на новите технологии и способност за евалуација и користење на современите софтверски развојни алатки.</li> </ul>
Комуникациски вештини	<ul style="list-style-type: none"> <li>• Способност за јасно и недвосмислено презентирање заклучоци, факти, состојби и резултати од анализи, истражувања, пред стручната јавност во орална или пишана форма и способност за прилагодување на стилот и формата на изразување пред нестручната јавност.</li> <li>• Способност за јасно и недвосмислено презентирање на резултатите од форензичка анализа, скенирање на ранливости, етичко хакирање и пенетрациско тестирање пред засегнатата страна.</li> <li>• Ефективно учество во мултидисциплинарни тимови, во својство на водач или експерт.</li> <li>• Вештини за управување со информации (прибирање, анализирање и употребување на информации од различни извори).</li> <li>• Користење на усни и писмени комуникациски вештини за ефективно, ефикасно и аргументирано презентирање на идеи и позиции.</li> <li>• Способност за соработка со експерти во сродни полиња.</li> <li>• Интерперсонални вештини, способност за дијалогска размена и презентирање на идеи, мислења, убедувања и заклучоци.</li> </ul>
Вештини на учење	<ul style="list-style-type: none"> <li>• Способност за идентификација на сопствените потреби од понатамошна едукација и самостојно стекнување на нови знаења и вештини од соодветната област;</li> <li>• Способност за анализа на стручна и научна литература.</li> <li>• Способност за генерирање на нови идеи (креативно размислување и соодветно практикување).</li> <li>• Вештини за истражување, подготвување, дизајнирање и управување со проекти и проектни циклуси.</li> </ul>

Прилог бр.3		Предметна програма втор циклус на студии			
1.	Наслов на наставниот предмет	Методологија и организација на научноистражувачката работа			
2.	Код	2FI200123			
3.	Студиска програма	Компјутерска безбедност и дигитална форензика			
4.	Организатор на студиската програма (единица, односно институт, катедра, оддел)	Факултет за информатика			
5.	Степен (прв, втор, трет циклус)	Втор циклус			
6.	Академска година / семестар	Прва година/прв семестар	7.	Број на ЕКТС кредити	6
8.	Наставник	Проф. Владо Гичев			
9.	Предуслови за запишување на предметот	нема			
10.	Цели на предметната програма (компетенции): Стекнува вештини за избор на правилна методологија за решавање на одреден инженерски проблем. Правилно ги организира постапките при решавање на проблемот од почеток до крај.				
11.	Содржина на предметната програма: Вовед. Математички модел наспроти експеримент. Организација и дизајн на експеримент, изведување на експеримент, интерпретација на резултати, публикација; Математички модели. Фуриевии редови и трансформации. Примена на Фуриевата анализа во процесирање на податоци. Спектрална густина. Конволуција и корелација. Моделирање на податоци. Лапласова трансформација. Примена на eigen проблем во решавање системи линеарни хомогени диференцијални равенки. Решавање на системи нелинеарни алгебарски равенки.				
12.	Методи на учење: Проектни задачи, семинарски работи, предавања, консултации.				
13.	Вкупен расположив фонд на време	6 ЕКТС x 30 часа = 180 часа			
14.	Распределба на расположивото време	30+30+30+30+60 = 180 часа (2+2+1)			
15.	Форми на наставните активности	15.1	Предавања- теоретска настава	30 часови	
		15.2	Вежби (лабораториски, аудиториски), семинари, тимска работа	30 часови	
16.	Други форми на активности	16.1	Проектни задачи	30 часови	
		16.2	Самостојни задачи	30 часови	
		16.3	Домашно учење	60 часови	
17.	Начин на оценување				
	17.1.	Проектна задача		30 поени	
	17.2.	Семинарска работа (презентација: писмена и усна)		40 поени	

	17.3.	Активност и учество				30 поени
18.	Критериуми за оценување (бодови/ оценка)			до 50 бода	5 (пет) (F)	
				од 51 до 60 бода	6 (шест) (E)	
				од 61 до 70 бода	7 (седум) (D)	
				од 71 до 80 бода	8 (осум) (C)	
				од 81 до 90 бода	9 (девет) (B)	
				од 91 до 100 бода	10 (десет) (A)	
19.	Услов за потпис и полагање на завршен испит	Редовност во извршување на активностите				
20.	Јазик на кој се изведува наставата	Македонски				
21.	Метод на следење на квалитетот на наставата	Самоевалуација				
22.	Литература					
22.1.	Задолжителна литература					
	Ред. број	Автор	Наслов	Издавач	Година	
	1.	R.D. Jarrard	“SCIENTIFIC METHODS” an online book © Richard D. Jarrard 2001	Dept. of Geology and Geophysics, University of Utah, jarrard@mines.utah.edu	2001	
	2.	E. Kreyszig	“Advanced Engineering Mathematics”, 8 <sup>th</sup> Edition	John Wiley & Sons, Inc.	1999	
	3.	Press, W.H., Teukolsky, S.A., Veterling, W.T., Flannery, B.P.	"Numerical Recipes in FORTRAN 77: The art of Scientific Computing", 2 <sup>nd</sup> Edition	Cambridge University Press.	2003	
	Дополнителна литература					
22.2	Ред. број	Автор	Наслов	Издавач	Година	

Ред. Број:2

Прилог бр.3		Предметна програма од прв, втор и трет циклус на студии
1.	Наслов на наставниот предмет	Криптографски алгоритми и протоколи
2.	Код	2FI201223
3.	Студиска програма	Компјутерска безбедност и дигитална форензика
4.	Организатор на студиската програма (единица, односно институт, катедра, оддел)	Факултет за информатика
5.	Степен (прв, втор, трет циклус)	Втор степен

6.	Академска година / семестар	Прва година/ прв семестар	7.	Број на ЕКТС кредити	6
8.	Наставник	проф. д-р Александра Милева			
9.	Предуслови за запишување на предметот	нема			
10.	Цели на предметната програма (компетенции): Цел на овој курс е студентите да се стекнат со напредни знаења од криптографијата и криптографските алгоритми и протоколи, како и основни знаења од криптоанализата.				
11.	Содржина на предметната програма: Перфектна тајност, шифра на Вернам, проточни шифри, Trivium, Edon-80, генератори на случајни броеви; Блок шифри, модови на операција, псевдо-случајни пермутации и функции, напади; Линеарна и диференцијална криптоанализа; Интегритет на пораки, кодови за автентикација на пораки (MAC); Хеш функции и напади; Автентикациска енкрипција и напади; Криптографија со јавни клучеви: математички основи, Diffie-Hellman размена на клучеви, ElGamal и Cramer-Shoup крипто системи, RSA, Rabin, Goldwasser-Micali крипто системи; Напади на крипто системите со јавни клучеви; Алгоритми за факторизација и пресметување на дискретни логаритми; Дигитални потписи, инфраструктура за јавни клучеви (PKI); Криптографски протоколи				
12.	Методи на учење: Предавања, дискусии, лабораториски вежби, електронско учење, семинарска работа, проект, консултации.				
13.	Вкупен расположив фонд на време	6 ЕКТС x 30 часа = 180 часа			
14.	Распределба на расположивото време	30+30+30+30+60 = 180 часа (2+2+1)			
15.	Форми на наставните активности	15.1.	Предавања- теоретска настава	30 часови	
		15.2.	Вежби, дискусии	30 часови	
16.	Други форми на активности	16.1.	Проектни задачи	30 часови	
		16.2.	Самостојни задачи	30 часови	
		16.3.	Домашно учење	60 часови	
17.	Начин на оценување				
	17.1.	Тестови			50 бодови
	17.2.	Семинарска работа/ проект ( презентација: писмена и усна)			30 бодови
	17.3.	Активност и учество			20 бодови
18.	Критериуми за оценување (бодови/ оценка)	до 50 бода		5 (пет) (F)	
		од 51 до 60 бода		6 (шест) (E)	
		од 61 до 70 бода		7 (седум) (D)	
		од 71 до 80 бода		8 (осум) (C)	
		од 81 до 90 бода		9 (девет) (B)	
		од 91 до 100 бода		10 (десет) (A)	
19.	Услов за потпис и полагање на завршен испит	60% успех од сите предиспитни активности т.е. 42 бодови од двата колоквиуми, семинарската, редовноста на предавања и вежби			
20.	Јазик на кој се изведува наставата	Македонски			
21.	Метод на следење на квалитетот на наставата	Самоевалуација			

22.	Литература				
	22.1.	Задолжителна литература			



	Ред. број	Автор	Наслов	Издавач	Година
	2.	S. Vaudenay	A Classical Introduction to Cryptography: Applications for Communications Security	Springer Science+ Business Media, Inc.	2006
	3.	D. R. Stinson	Cryptography: theory and practice, 3 <sup>rd</sup> edition	Chapman & Hall/CRC	2005
22.2.	Дополнителна литература				
	Ред. број	Автор	Наслов	Издавач	Година
	1.	N. Smart	Cryptography: An Introduction, 3 <sup>rd</sup> Edition	McGraw Hill	2004
	2.	A. J. Menezes, P. Van Oorschot, S. A. Vanstone	Handbook of Applied Cryptography	CRC Press	1997
	3.		Листа на трудови		

Ред. Број: 3

Прилог бр.3		Предметна програма од прв, втор и трет циклус на студии			
1.	Наслов на наставниот предмет	Дигитална форензика			
2.	Код	2FI200523			
3.	Студиска програма	Компјутерска безбедност и дигитална форензика			
4.	Организатор на студиската програма (единица, односно институт, катедра, оддел)	Факултет за информатика			
5.	Степен (прв, втор, трет циклус)	Втор степен			
6.	Академска година / семестар	Прва година/прв семестар	7.	Број на ЕКТС кредити	8
8.	Наставник	проф. д-р Митко Богдановски			
9.	Предуслови за запишување на предметот	нема			
10.	Цели на предметната програма (компетенции): Цел на овој курс е студентите да се стекнат со напредни знаења, концепти и техники од дигиталната форензика, како и да научат да ги користат повеќето форензички алатки и да извршат основна форензичка анализа на Windows и Linux компјутерски систем и на Андроид мобилен телефон.				
11.	Содржина на предметната програма: Основи на дигиталната форензика, гранки на дигиталната форензика Поим на дигитален доказ, идентификација, собирање и чување на дигитални докази Карактеристики на мемориски уреди и податочни системи Бесплатни и комерцијални форензички алатки Windows и Linux артефакти Форензика во живо и dead-box форензика на Windows и Linux системи Форензика на бази на податоци Форензика на мобилни телефони Форензика на мрежа Криптовалуту и можности за форензика Техники на анти-форензика				
12.	Методи на учење: Предавања, дискусии, лабораториски вежби, електронско учење, семинарска работа, проект, консултации.				
13.	Вкупен расположив фонд на време	6 ЕКТС x 30 часа = 180 часа			

14.	Распределба на расположивото време		30+30+30+30+60 = 180 часа (2+2+1)	
15.	Форми на наставните активности	15.1.	Предавања- теоретска настава	30 часови
		15.2.	Вежби, дискусии	30 часови
16.	Други форми на активности	16.1.	Проектни задачи	30 часови
		16.2.	Самостојни задачи	30 часови
		16.3.	Домашно учење	60 часови
17.	Начин на оценување			
	17.1.	Тестови		50 бодови
	17.2.	Семинарска работа/ проект ( презентација: писмена и усна)		30 бодови
	17.3.	Активност и учество		20 бодови
18.	Критериуми за оценување (бодови/ оценка)		до 50 бода	5 (пет) (F)
			од 51 до 60 бода	6 (шест) (E)
			од 61 до 70 бода	7 (седум) (D)
			од 71 до 80 бода	8 (осум) (C)
			од 81 до 90 бода	9 (девет) (B)
			од 91 до 100 бода	10 (десет) (A)
19.	Услов за потпис и полагање на завршен испит		60% успех од сите предиспитни активности т.е. 42 бодови од двата колоквиуми, семинарската, редовноста на предавања и вежби	
20.	Јазик на кој се изведува наставата		Македонски	
21.	Метод на следење на квалитетот на наставата		Самоеваулација	

22.	Литература					
	22.1.	Задолжителна литература				
		Ред. број	Автор	Наслов	Издавач	Година
		1.	J. Sammons	The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, 2 <sup>nd</sup> Edition	Syngress	2014
		2.	C. Altheide, H. Carvey	Digital Forensics with Open Source Tools, 1 <sup>st</sup> Edition	Syngress	2011
	3.	J. Sammons	Digital Forensics: Threatscape and Best Practices 1 <sup>st</sup> Edition	Syngress	2015	
	22.2.	Дополнителна литература				
		Ред. број	Автор	Наслов	Издавач	Година
		1.		Листа на трудови и туторијали		
		2.				
3.						

Ред. Број:4

<b>Предметна програма од прв, втор и трет циклус на студии</b>	
--	--

1.	Наслов на наставниот предмет	Сајбер криминал и дигитална форензика			
2.	Код	2FI215223			
3.	Студиска програма	Компјутерска безбедност и дигитална форензика			
4.	Организатор на студиската програма (единица, односно институт, катедра, оддел)	Факултет за информатика			
5.	Степен (прв, втор, трет циклус)	Втор циклус			
6.	Академска година / семестар	Прва година / I семестар	7.	Број на ЕКТС кредити	6
8.	Наставник	Вонреден проф. д-р Олга Кошевалиска			
9.	Предуслови за запишување на предметот	/			
10.	Цели на предметната програма (компетенции): стекнување на знаење за правните аспекти на информатичката технологија, компјутерскиот криминал и дигиталните докази				
11.	Содржина на предметната програма: Сајбер криминалитет, анализа на меѓународни извори на сајбер криминалитетот и меѓународното дефинирање, Анализа на законодавство на РСМ од аспект на сајбер криминалот, Сајбер криминалитет, анализа на меѓународни извори на сајбер криминалитетот и меѓународното дефинирање, Анализа на законодавство на РСМ од аспект на сајбер криминалот, Кражби и измами, Измама со кредитни картички и хартии од вредност, Кражба на идентитетот, Попречување, присвојување и вмешување во компјутерски и телекомуникациски услуги, Компјутерска шпионажа – анализа на случаи и пресуди, Злоупотреба на лични податоци, Оштетување и неовластено навлегување во компјутерски систем, Правење и внесување на компјутерски вируси, Компјутерска измама – анализа на случаи од пракса, Производство и дистрибуција на детска порнографија преку компјутерски систем, - анализа на случаи и анализа на докази за извршено дело, Компјутерски фалсификат, Казнени дела чиј објект на заштита е интелектуалната сопственост – анализа на случаи, Поим за компјутерска форензика: Еволуција на форензиката, Собирање дигитални докази, обезбедување на дигиталните докази, Анализа на дигиталните докази, изведување на дигитални докази пред суд – практична настава, Доказната вредност на дигиталните докази според нов ЗКП – анализа на случаи од пракса. Собирање дигитални докази, обезбедување на дигиталните докази, Анализа на дигиталните докази, изведување на дигитални докази пред суд – практична настава,				
12.	Методи на учење: предавања и вежби, посета на МВР и одделението за крим техника, консултации; изработка на самостојна семинарска работа; case study; консултации.				
13.	Вкупен расположив фонд на време	4 ЕКТС x 30 часа = 120 часа			
14.	Распределба на расположивото време	30+15+15+30+30=120			
15.	Форми на наставните активности	15.1	Предавања- теоретска настава	30 часа	
		15.2	Вежби - семинари, тимска работа	15 часа	
16.	Други форми на активности	16.1	Проектни задачи	15 часа	
		16.2	Самостојни задачи	30 часа	

		16.3	Домашно учење	30 часа	
17.	Начин на оценување				
	17.1.	Тестови		30 поени	
	17.2.	Проектна задача (презентација: писмена и усна)		50 поени	
	17.3.	Активност и учество		20 поени	
18.	Критериуми за оценување (бодови/ оценка)		до 50 бода	5 (пет)	F
			од 51 до 60 бода	6 (шест)	E
			од 61 до 70 бода	7 (седум)	D
			од 71 до 80 бода	8 (осум)	C
			од 81 до 90 бода	9 (девет)	B
			од 91 до 100 бода	10 (десет)	A
19.	Услов за потпис и полагање на завршен испит		60% успех од сите предиспитни активности.		
20.	Јазик на кој се изведува наставата		Македонски и англиски јазик		
21.	Метод на следење на квалитетот на наставата		Самоевалуација		

22	Литература					
	22.1.	Задолжителна литература				
		Ред. број	Автор	Наслов	Издавач	Година
		1.	Rohit Arvind Jain	Cyber-crime and laws: An overview on Securing cyber space	Kindle Edition	2018
		2.	Angus M. Marshall	Digital Forensics, Digital Evidence in Criminal Investigation	JohnWiley & Sons	2008
		3.	John R. Vacca	Computer Forensics: Computer Crime Scene Investigation	Volume 1, Cengage Learning	2005
		4.	Jyoti Rattan	Cyber Laws & Information Technology	Kindle Edition	2018
	22.2.	Дополнителна литература				
		Ред. број	Автор	Наслов	Издавач	Година
		1.	Reyes , A.	Cyber Crime Investigations: Bridging the Gaps Between, Security Professionals, Law Enforcement, and Prosecutors	Elsevier	2007

			Кошевалиска, О.	„Приватноста versus безбедноста во размената на податоци во кривичните предмети“ – докторска дисертација	Докторска дисертација на Правен факултет „Јустинијан Први“ – Скопје, Универзитет Св.Кирил и Методиј, казнено правна катедра	2013
			Council of Europe	Convention on cybercrime	Council of Europe	2001
			Buzarovska, Lazetik, G., Koshevaliska, O.	Digital evidence in criminal proceedings,	Balkan Social Science Review (BSSR), Vol.II, Faculty of Law in the University “Goce Delcev” Stip	2013
			Koshevaliska Olga	<a href="#">Human security of migrants in the on-line world</a>	Editoriale Scientifica, Naples, Italy,	2021
			Buzarovska – Lazetik, G., Koshevaliska, O.	Protection of personal data in criminal legislation in Macedonia vs. its protection in EU	Annals of the Bucharest University – The Law Series, Bucharest	2013

Ред. Број: 5

Прилог бр.3		Предметна програма од прв, втор и трет циклус на студии			
1.	Наслов на наставниот предмет	Напредно скриптинг програмирање (Advanced Scripting Programming)			
2.	Код	2FI213523			
3.	Студиска програма	Компјутерска безбедност и дигитална форензика			
4.	Организатор на студиската програма (единица, односно институт, катедра, оддел)	Факултет за информатика			
5.	Степен (прв, втор, трет циклус)	Втор степен			
6.	Академска година / семестар	Прва/ I семестар	7.	Број на ЕКТС кредити	6
8.	Наставник	Доц. д-р Душан Биков			
9.	Предуслови за запишување на предметот	нема			
10.	Цели на предметната програма (компетенции): Студентите да ги разберат концептите на напредното скриптинг програмирање, со посебен осврт на пишувањето на скрипти, тестирањето, имплементацијата и подготвувањето на				

	документацијата, како и запознавање со различните скриптинг јазици, како на пример, PERL и Python. Други вклучени теми се синтаксата на одреден програмски јазик за скриптирање и структурата на датотеките, работа со влезно/излезни уреди, графички кориснички интерфејси и сл.			
11.	Содржина на предметната програма: <ul style="list-style-type: none"> <li>• Контролни структури, податочни структури и објекти во програмскиот јазик. Примери со ГУИ програмирање и работа со интерфејси со оперативниот систем.</li> <li>• Програмирање на веб прегледувачи</li> <li>• Изработка на скрипти за серверска страна на веб апликации</li> <li>• ГУИ програмирање – улогата на скриптинг јазици како лепак јазици се користи и за програмирање на графички кориснички интерфејси</li> <li>• Програмирање на апликации</li> <li>• Контрола на работа или командни јазици или шелови</li> <li>• Намена и користење на PowerShell</li> <li>• Примена во етичкото хакирање</li> </ul>			
12.	Методи на учење: Предавања, дискусии, лабораториски вежби, електронско учење, семинарска работа, проект, консултации.			
13.	Вкупен расположив фонд на време		6 ЕКТС x 30 часа = 180 часа	
14.	Распределба на расположивото време		30+30+30+30+60 = 180 часа (2+2+1)	
15.	Форми на наставните активности	15.1.	Предавања- теоретска настава	30 часови
		15.2.	Вежби, дискусии	30 часови
16.	Други форми на активности	16.1.	Проектни задачи	30 часови
		16.2.	Самостојни задачи	30 часови
		16.3.	Домашно учење	60 часови
17.	Начин на оценување			
	17.1.	Тестови		30 бодови
	17.2.	Семинарска работа/ проект (презентација: писмена и усна)		50 бодови
	17.3.	Активност и учество		20 бодови
18.	Критериуми за оценување (бодови/ оценка)	до 50 бода		5 (пет) (F)
		од 51 до 60 бода		6 (шест) (E)
		од 61 до 70 бода		7 (седум) (D)
		од 71 до 80 бода		8 (осум) (C)
		од 81 до 90 бода		9 (девет) (B)
		од 91 до 100 бода		10 (десет) (A)
19.	Услов за потпис и полагање на завршен испит		60% успех од сите предиспитни активности т.е. 42 бодови од двата колоквиуми, семинарската, редовноста на предавања и вежби	
20.	Јазик на кој се изведува наставата		Македонски	
21.	Метод на следење на квалитетот на наставата		Самоеваулација	

22.	Литература				
	22.1.	Задолжителна литература			
		Ред. број	Автор	Наслов	Издавач

		1.	Tom Christiansen, brian d foy, Larry Wall, Jon Orwant	Programming Perl: Unmatched power for text processing and scripting, 4th Edition	O'Reilly Media	2012	
		2.	Mark Pilgrim	Dive into Python 3	Apress	2009	
		3.	Richard Blum, Christine Bresnahan	Linux Command Line and Shell Scripting Bible	Wiley	2011	
		4.		Листа на трудови од областа			
	22.2.	Дополнителна литература					
		Ред. број	Автор	Наслов	Издавач	Година	
		1.	Рендал Л.Шварц, Том Финикс	Научете Perl	Ад вербум	2009	
		2.	Sean-Philip Oriyano	Certified Ethical Hacker Version 9 Study Guide 3rd Edition	Wiley Publishing	2016	
		3.	Adam Bertram	PowerShell for Sysadmins:Workflow Automation Made Easy	No Starch Press	2020	

Ред. Број: 6

Прилог бр.3		Предметна програма од прв, втор и трет циклус на студии			
1.	Наслов на наставниот предмет	Дигитална стеганографија и стеганализа			
2.	Код	2FI211623			
3.	Студиска програма	Компјутерска безбедност и дигитална форензика			
4.	Организатор на студиската програма (единица, односно институт, катедра, оддел)	Факултет за информатика			
5.	Степен (прв, втор, трет циклус)	Втор степен			
6.	Академска година / семестар	Прва година/прв семестар	7.	Број на ЕКТС кредити	6
8.	Наставник	проф. д-р Александра Милева			
9.	Предуслови за запишување на предметот	нема			
10.	Цели на предметната програма (компетенции): Цел на овој курс е студентите да се стекнат со напредни знаења за криење на податоци во аудио, видео, текстуални и извршни датотеки, мрежни протоколи, апликации на мобилни телефони, IoT, и сл, како и за истражување за нивна соодветна примена и стеганализа				
11.	Содржина на предметната програма: Поим за стеганографски систем и стеганограм, скриен канал (covert channel), типови на скриени канали Мрежна стеганографија - криење на податоци во мрежните протоколи од TCP/IP складот на податоци, категоризација на техники Криење на податоци во слики и видеа, текстуални датотеки и аудио датотеки Скриени канали кај мобилни телефони Криење на податоци кај IoT Техники на стеганализа				
12.	Методи на учење: Предавања, дискусии, лабораториски вежби, електронско учење, семинарска работа, проект, консултации.				
13.	Вкупен расположив фонд на време	6 ЕКТС x 30 часа = 180 часа			
14.	Распределба на расположивото време	30+30+30+30+60 = 180 часа (2+2+1)			

15.	Форми на наставните активности	15.1.	Предавања- теоретска настава	30 часови
		15.2.	Вежби, дискусии	30 часови
16.	Други форми на активности	16.1.	Проектни задачи	30 часови
		16.2.	Самостојни задачи	30 часови
		16.3.	Домашно учење	60 часови
17.	Начин на оценување			
	17.1.	Тестови		50 бодови
	17.2.	Семинарска работа/ проект ( презентација: писмена и усна)		30 бодови
	17.3.	Активност и учество		20 бодови
18.	Критериуми за оценување (бодови/ оценка)	до 50 бода		5 (пет) (F)
		од 51 до 60 бода		6 (шест) (E)
		од 61 до 70 бода		7 (седум) (D)
		од 71 до 80 бода		8 (осум) (C)
		од 81 до 90 бода		9 (девет) (B)
		од 91 до 100 бода		10 (десет) (A)
19.	Услов за потпис и полагање на завршен испит	60% успех од сите предиспитни активности т.е. 42 бодови од двата колоквиуми, семинарската, редовноста на предавања и вежби		
20.	Јазик на кој се изведува наставата	Македонски		
21.	Метод на следење на квалитетот на наставата	Самоеваулација		

22.	Литература					
	Задолжителна литература					
		Ред. број	Автор	Наслов	Издавач	Година
	22.1.	1.	Ingemar J. Cox Matthew L. Miller Jeffrey A. Bloom Jessica Fridrich Ton Kalker	Digital Watermarking and Steganography	Morgan Kaufmann Publishers 2nd edition	2008
		2.	W. Mazurczyk, S. Wendzel, S. Zander, A. Houmansadr, K. Szczypiorski	Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures	IEEE Press Series on Information and Communication Networks Security, IEEE Press-Wiley	2016
		3.		Листа на трудови		
	Дополнителна литература					
		Ред. број	Автор	Наслов	Издавач	Година
	22.2.	1.				
		2.				
3.						

Ред. Број: 8



Прилог бр.3		Предметна програма од прв, втор и трет циклус на студии			
1.	Наслов на наставниот предмет	Безбедност на софтвер			
2.	Код	2FI211023			
3.	Студиска програма	Компјутерска безбедност и дигитална форензика			
4.	Организатор на студиската програма (единица, односно институт, катедра, оддел)	Факултет за информатика			
5.	Степен (прв, втор, трет циклус)	Втор степен			
6.	Академска година / семестар	Прва година/први семестар	7.	Број на ЕКТС кредити	6
8.	Наставник	доц. д-р Александар Велинов			
9.	Предуслови за запишување на предметот	нема			
10.	Цели на предметната програма (компетенции): Студентите да го разберат процесот на развој на безбеден софтвер, вклучувајќи дизајнирање на безбедни апликации, пишување на безбеден код, обезбедување на бази на податоци, како и тестирање и проценка на безбедноста. Исто така целта е студентите да се запознаат со вообичаените безбедносни ранливости, грешки и закани при развивањето на софтвер.				
11.	Содржина на предметната програма: Модел на закани, безбедносни цели и принципи на дизајн; Злонамерен код: анализа и одбрана Вообичаени грешки во имплементацијата: Преполнување на бафер, ранливости со форматирање на стринг, надминување на рангот кај целите броеви, хип ранливости и корупција на меморијата; Конкурентност, race conditions и TOCTOU; Безбедност специфична за програмските јазици: “небезбедни” C/C++ и одбрана (ASLR, DEP, одбрана во време на извршување, интегритет на контрола на тек, софтверски-базирана изолација на грешки, SSured), return-ориентирано програмирање; Практики на безбедно програмирање; Безбедност на бази на податоци; Основи на теорија на типови; Information flaw; Статичка анализа на код; Верификација на програми; Тестирање: регресија и fuzzing Проблеми со имплементирањето на криптографските примитиви				
12.	Методи на учење: Предавања, дискусии, лабораториски вежби, електронско учење, семинарска работа, проект, консултации.				
13.	Вкупен расположив фонд на време	6 ЕКТС x 30 часа = 180 часа			
14.	Распределба на расположивото време	30+30+30+30+60 = 180 часа (2+2+1)			
15.	Форми на наставните активности	15.1.	Предавања- теоретска настава	30 часови	
		15.2.	Вежби, дискусии	30 часови	
16.	Други форми на активности	16.1.	Проектни задачи	30 часови	
		16.2.	Самостојни задачи	30 часови	
		16.3.	Домашно учење	60 часови	
17.	Начин на оценување				
	17.1.	Тестови			30 бодови
	17.2.	Семинарска работа/ проект (презентација: писмена и усна)			50 бодови
	17.3.	Активност и учество			20 бодови
18.	Критериуми за оценување (бодови/ оценка)	до 50 бода		5 (пет) (F)	
		од 51 до 60 бода		6 (шест) (E)	
		од 61 до 70 бода		7 (седум) (D)	

		од 71 до 80 бода	8 (осум) (C)
		од 81 до 90 бода	9 (девет) (B)
		од 91 до 100 бода	10 (десет) (A)
19.	Услов за потпис и полагање на завршен испит	60% успех од сите предиспитни активности т.е. 42 бодови од двата колоквиуми, семинарската, редовноста на предавања и вежби	
20.	Јазик на кој се изведува наставата	Македонски	
21.	Метод на следење на квалитетот на наставата	Самоеваулација	

22.	Литература					
	22.1.	Задолжителна литература				
		Ред. број	Автор	Наслов	Издавач	Година
		1.	Michael Howard, David LeBlanc and John Viega	The 24 Deadly Sins of Software Security	McGraw-Hill	2009
		2.	Hassan A. Afyouni	Database Security and Auditing: Protecting Data Integrity and Accessibility	Course Technology	2005
	3.		Листа на трудови од безбедност на софтвер			
	22.2.	Дополнителна литература				
		Ред. број	Автор	Наслов	Издавач	Година
		1.	Ross J. Anderson	Security Engineering, 2 <sup>nd</sup> Edition	Wiley	2008
		2.	Theodor Richardson, Charles N. Thies	Secure Software Design	Jones & Bartlett Publisher	2013
3.	James Ransome, Anmol Misra	Core Software Security: Security at the Source	CRC Press	2013		

Ред. Број: 8

<b>Прилог бр.3</b>		<b>Предметна програма од прв, втор и трет циклус на студии</b>				
1.	Наслов на наставниот предмет	Наука за податоците и аналитика на големите податоци				
2.	Код	2FI213623				
3.	Студиска програма	Компјутерска безбедност и дигитална форензика				
4.	Организатор на студиската програма (единица, односно институт, катедра, оддел)	Факултет за информатика				
5.	Степен (прв, втор, трет циклус)	Втор степен				
6.	Академска година / семестар	Прва година / I	7.	Број на ЕКТС кредити	6	
8.	Наставник	Проф. Д-р Зоран Здравев				
9.	Предуслови за запишување на предметот	Нема				
10.	Цели на предметната програма (компетенции): Овој предмет студентите ги воведува во областа на големи податоци и во животниот циклус на аналитика на податоците како алатка за решавање на деловните предизвици кои се потпора на големите податоци. Со предметот се стекнува основата за основните и напредните аналитички методи и вовед во технологиите и алатките за аналитика на големи податоци.					
11.	Содржина на предметната програма:					

	Дефинирање и преглед на големите податоци, состојба во практика на аналитика, улогата на научните податоци, и аналитиката за големи податоци во индустријата. Објаснување на различните фази на еден типичен животниот циклус на аналитиката - откривање, подготовка на податоци, планирање на модели, креирање на модели, резултати од комуникација и наоди, и употребливост. Основни методи кои се користат од страна на научниците, вклучувајќи и селекција на кандидати со користење на Naive Bayesian Classifier, категоризација со користење на K-means групирање и здружување на правила, предвидливо моделирање со користење на дрва на одлучување, линеарна и логичка регресија, анализа на временски серии и анализа на текст. Аналитичките алатки за неструктурирани податоци, како што се MapReduce и Hadoop екосистемот. Аналитика на базата на податоци со SQL екстензии и други напредни SQL техники и MADlib функции за аналитика на базата на податоци. Примена на методи на визуелизација.			
12.	Методи на учење: Предавања, лабораториски вежби, нумерички вежби, електронско учење, семинарска работа, тимска работа, консултации			
13.	Вкупен расположив фонд на време	180 часа		
14.	Распределба на расположивото време	$2*15+2*15+2*15+30+60=180$		
15.	Форми на наставните активности	15.1	Предавања- теоретска настава	30 часа
		15.2	Вежби (лабораториски, аудиториски), семинари, тимска работа	30 часа
16.	Други форми на активности	16.1	Проектни задачи	30 часа
		16.2	Самостојни задачи	30 часа
		16.3	Домашно учење	60 часа
17.	Начин на оценување			
	17.1.	Проектна задача		25 бодови
	17.2.	Семинарска работа (презентација: писмена и усна)		25 бодови
	17.3.	Активност и учество		50 бодови
18.	Критериуми за оценување (бодови/ оценка)	до 50 бода		5 (пет) (F)
		од 51 до 60 бода		6 (шест) (E)
		од 61 до 70 бода		7 (седум) (D)
		од 71 до 80 бода		8 (осум) (C)
		од 81 до 90 бода		9 (девет) (B)
		од 91 до 100 бода		10 (десет) (A)
19.	Услов за потпис и полагање на завршен испит	60% успех од редовноста на предавања, вежби и друга форма на активност		
20.	Јазик на кој се изведува наставата	Македонски јазик		
21.	Метод на следење на квалитетот на наставата	Самоевалуација		

22.	Литература					
	22.1.	Задолжителна литература				
		Ред. број	Автор	Наслов	Издавач	Година
		1.	Jay Liebowitz	Big Data and Business Analytics	Auerbach Publications	2013
2.	Thomas A. Runkler	Data Analytics: Models and Algorithms for	Vieweg+Teubner Verlag	2012		

				Intelligent Data Analysis		
	3.	Bing Liu		Web Data Mining. Exploring Hyperlinks, Contents and Usage Data	Springer	2007
22.2.	Дополнителна литература					
	Ред. број	Автор	Наслов	Издавач	Година	
	1.	Thomas Hill, Pawel Lewicki	Statistics, Methods and Applications	StatSoft	2006	
	2.	Daniel T. Larose	Data Mining Methods and Models -	Wiley-IEEE Press	2006	
	3.					

Ред. Број: 9

Прилог бр.3		Предметна програма од прв, втор и трет циклус на студии			
1.	Наслов на наставниот предмет	Вештачката интелигенција во компјутерската безбедност			
2.	Код	2FI211223			
3.	Студиска програма	Компјутерска безбедност и дигитална форензика			
4.	Организатор на студиската програма (единица, односно институт, катедра, оддел)	Факултет за информатика			
5.	Степен (прв, втор, трет циклус)	Втор степен			
6.	Академска година / семестар	Прва/ I семестар	7.	Број на ЕКТС кредити	6
8.	Наставник	Проф. д-р Цвета Мартиновска Банде			
9.	Предуслови за запишување на предметот	нема			
10.	Цели на предметната програма (компетенции): Студентите стекнуваат знаење од областа на вештачката интелигенција, како техники за претставување на знаење и механизми за резонирање, машинско учење, решавање на проблеми и пребарување кои се применливи во областа на компјутерската безбедност и дигиталната форензика.				
11.	Содржина на предметната програма: Апликации на вештачка интелигенција во компјутерска безбедност и форензика. Приоди во вештачката интелигенција. Формализми за репрезентација на знаење и резонирање. Пребарување на простор на состојби: BFS, DFS, Best First Search, Hill climbing, A* алгоритам. Проблеми кои се решаваат со задоволување на ограничувања. Техники на машинско учење: класификација, кластерирање. Баесов класификатор. Дрва на одлучување. Машини со носечки вектори (SVM). Линеарна и сигмоидална регресија. Градиентно спуштање. Учење со поттикнување (reinforcement learning). Маркови процеси на одлучување. Роботика и планирање на движење. Геометриска визија. Невронски мрежи и длабинско учење. Моделирање на неизвесност. Баесови мрежи. Непрецизирана логика (fuzzy logic).				
12.	Методи на учење: Предавања, лабораториски вежби, семинарска работа, тимска работа, консултации.				
13.	Вкупен расположив фонд на време	6 ЕКТС x 30 часа = 180 часа			
14.	Распределба на расположивото време	30+30+30+30+60 = 180 часа (2+2+1)			
15.	Форми на наставните активности	15.1.	Предавања- теоретска настава (15 недели x 2 часа = 30 часа)		30 часа

		15.2.	Вежби (лабораториски, аудиториски), семинари, теренска и тимска работа (15 недели x 2 часа = 30 часа)	30 часа
16.	Други форми на активности	16.1.	Проектни задачи	60 часа
		16.2.	Самостојни задачи	30 часа
		16.3.	Домашно учење	30 часа
17.	Начин на оценување			
	17.1.	Тестови		70 бодови
	17.2.	Индивидуална работа/ проект ( презентација: писмена и усна)		10 бодови
	17.3.	Активност и учество		20 бодови
18.	Критериуми за оценување (бодови/ оценка)		до 50 бода	5 (пет) (F)
			од 51 до 60 бода	6 (шест) (E)
			од 61 до 70 бода	7 (седум) (D)
			од 71 до 80 бода	8 (осум) (C)
			од 81 до 90 бода	9 (девет) (B)
			од 91 до 100 бода	10 (десет) (A)
19.	Услов за потпис и полагање на завршен испит	60% од бодовите на предиспитните активности: 42 бодови од два колоквиуми, семинарска работа, редовност на предавања и вежби		
20.	Јазик на кој се изведува наставата	македонски/ англиски		
21.	Метод на следење на квалитетот на наставата	самоевалуација		

22.	Литература					
	22.1.	Задолжителна литература				
		Ред. број	Автор	Наслов	Издавач	Година
		1.	Stuart Russell and Peter Norvig	Artificial Intelligence: A Modern Approach, 3 ed.	Prentice Hall (преводи од Влада на РМ, 2 изд.)	2014
		2.	Kevin Warwick	Artificial Intelligence, The basics	Routledge	2012
	3.	Patrick Winston	<i>Artificial Intelligence</i>	Addison-Wesley	1992	
	22.2.	Дополнителна литература				
		Ред. број	Автор	Наслов	Издавач	Година
		1.	Christopher Bishop	Pattern Recognition and Machine Learning	Springer Science and Business Media	2006
		2.	Tom Mitchell	Machine Learning	McGraw-Hill	1997
3.						

Ред. Број: 10

Прилог бр.3	Предметна програма од прв, втор и трет циклус на студии
-------------	---

1.	Наслов на наставниот предмет		Етичко хакирање и пенетрациско тестирање		
2.	Код		2FI201023		
3.	Студиска програма		Компјутерска безбедност и дигитална форензика		
4.	Организатор на студиската програма (единица, односно институт, катедра, оддел)		Факултет за информатика		
5.	Степен (прв, втор, трет циклус)		Втор степен		
6.	Академска година / семестар		Прва/ II семестар	7.	Број на ЕКТС кредити
8.	Наставник		Доц. д-р Душан Биков		
9.	Предуслови за запишување на предметот		нема		
10.	Цели на предметната програма (компетенции): Студентите да запознаат со најразличните алатки за хакирање, со чија помош се извршуваат најразлични компјутерски напади, како и пенетрациско тестирање на системот. Другата цел добивање на компетенции за тоа како да го заштитат компјутерскиот системот од методите кој се користат за напади, добивање на пристап и експлоатирање на системот.				
11.	Содржина на предметната програма:  Вовед во етичкото хакирање; Клучни прашања поврзани со безбедноста на информациите, процесот на управување со инциденти и пенетрациско тестирање; Различни типови на footprinting, footprinting алатки и контрамерки; Техники за скенирање на мрежата и контрамерки; Техники за енумерација и контрамерки; Методологија на хакирање, прикривање на траги; Малициозен софтвер вируси, тројанци, компјутерски црви, процедури за анализа и контрамерки; Техники за душкање на пакети и заштита од душкање; Безжична енкрипција, методологија на безжично хакирање, алатки за хакирање и безбедносни алатки; Различни cloud computing концепти, закани, напади и безбедносни алатки и техники; Различни типови на пенетрациско тестирање, безбедносна ревизија, оценка на ранливоста;				
12.	Методи на учење: Предавања, дискусии, лабораториски вежби, електронско учење, семинарска работа, проект, консултации.				
13.	Вкупен расположив фонд на време		6 ЕКТС x 30 часа = 180 часа		
14.	Распределба на расположивото време		30+30+30+30+60 = 180 часа (2+2+1)		
15.	Форми на наставните активности	15.1.	Предавања- теоретска настава	30 часови	
		15.2.	Вежби, дискусии	30 часови	
16.	Други форми на активности	16.1.	Проектни задачи	30 часови	
		16.2.	Самостојни задачи	30 часови	
		16.3.	Домашно учење	60 часови	
17.	Начин на оценување				
	17.1.	Тестови		30 бодови	
	17.2.	Семинарска работа/ проект (презентација: писмена и усна)		50 бодови	
	17.3.	Активност и учество		20 бодови	
18.	Критериуми за оценување (бодови/ оценка)		до 50 бода		5 (пет) (F)
			од 51 до 60 бода		6 (шест) (E)

		од 61 до 70 бода	7 (седум) (D)
		од 71 до 80 бода	8 (осум) (C)
		од 81 до 90 бода	9 (девет) (B)
		од 91 до 100 бода	10 (десет) (A)
19.	Услов за потпис и полагање на завршен испит	60% успех од сите предиспитни активности т.е. 42 бодови од двата колоквиуми, семинарската, редовноста на предавања и вежби	
20.	Јазик на кој се изведува наставата	Македонски	
21.	Метод на следење на квалитетот на наставата	Самоеваулација	

22.	Литература					
	22.1.	Задолжителна литература				
		Ред. број	Автор	Наслов	Издавач	Година
		1.	Allen Harper, Daniel Regalado, Ryan Linn, Stephen Sims, Branko Spasojevic, Linda Martinez, Michael Baucom, Chris Eagle, Shon Harris	Gray Hat Hacking The Ethical Hacker's Handbook, Fifth Edition	McGraw-Hill	2018
		2.	Sean-Philip Oriyano	Certified Ethical Hacker Version 9 Study Guide 3rd Edition	Wiley Publishing	2016
	3.		Листа на трудови од областа етичко хакирање и пенетрациско тестирање			
	22.2.	Дополнителна литература				
		Ред. број	Автор	Наслов	Издавач	Година
		1.	Patrick Engebretson	The Basics of hacking and penetration Testing Ethical hacking and penetration Testing Made Easy	Elsevier	2011
		2.	Abhinav Singh	Metasploit Penetration Testing Cookbook	Packt Publishing	2012
3.						

Ред. Број: 11

<b>Прилог бр.3</b>		<b>Предметна програма од прв, втор и трет циклус на студии</b>			
1.	Наслов на наставниот предмет	Безбедност на компјутерски мрежи и веб безбедност			
2.	Код	2FI200323			
3.	Студиска програма	Компјутерска безбедност и дигитална форензика			
4.	Организатор на студиската програма (единица, односно институт, катедра, оддел)	Факултет за информатика			
5.	Степен (прв, втор, трет циклус)	Втор степен			
6.	Академска година / семестар	Прва година/втор семестар	7.	Број на ЕКТС кредити	6
8.	Наставник	проф. д-р Александра Милева			

9.	Предуслови за запишување на предметот	нема			
10.	Цели на предметната програма (компетенции): Студентите да се стекнат со комплетна база од безбедност на мрежи и веб безбедност соодветна за оние кои сакаат да истражуваат во оваа област, или се интересираат за безбедноста и мрежите и веб апликациите				
11.	Содржина на предметната програма: Модел на закани, безбедносни цели и принципи на дизајн; Злонамерен код; Безбедносни проблеми во мрежните протоколи; Одбивање на сервиси (DoS и DDoS); Безбедност на безжични мрежи; Безбедност на мобилни мрежи; Безбедносни протоколи (SSL/TLS, SSH, IPSec, и др); Скенирање на мрежа; Анализа на сообраќај; Веб безбедносен модел; Автентикација, автентикациски протоколи и управување со сесија; Веб напади и одбрана, OWASP; Бот мрежи; Honeypots; Fishing; Спам и скам; Огнени сидови; Системи за детекција и превенција на упади во мрежи.				
12.	Методи на учење: Предавања, дискусии, лабораториски вежби, електронско учење, семинарска работа, проект, консултации.				
13.	Вкупен расположив фонд на време	6 ЕКТС x 30 часа = 180 часа			
14.	Распределба на расположивото време	30+30+30+30+60 = 180 часа (2+2+1)			
15.	Форми на наставните активности	15.1.	Предавања- теоретска настава	30 часови	
		15.2.	Вежби (лабораториски, аудиториски), семинари, теренска и тимска работа	30 часови	
16.	Други форми на активности	16.1.	Проектни задачи	30 часови	
		16.2.	Самостојни задачи	30 часови	
		16.3.	Домашно учење	60 часови	
17.	Начин на оценување				
	17.1.	Тестови			30 бодови
	17.2.	Семинарска работа/ проект ( презентација: писмена и усна)			50 бодови
	17.3.	Активност и учество			20 бодови
18.	Критериуми за оценување (бодови/ оценка)	до 50 бода		5 (пет) (F)	
		од 51 до 60 бода		6 (шест) (E)	
		од 61 до 70 бода		7 (седум) (D)	
		од 71 до 80 бода		8 (осум) (C)	
		од 81 до 90 бода		9 (девет) (B)	
		од 91 до 100 бода		10 (десет) (A)	
19.	Услов за потпис и полагање на завршен испит	60% успех од сите предиспитни активности т.е. 42 бодови од двата колоквиуми, семинарската, редовноста на предавања и вежби			
20.	Јазик на кој се изведува наставата	Македонски			
21.	Метод на следење на квалитетот на наставата	Самоеваулација			

22.	Литература				
	22.1.	Задолжителна литература			
		Ред. број	Автор	Наслов	Издавач



22.2.	1.	J. M. Kizza	A Guide to Computer Network Security	Springer-Verlag London	2009
	2.	Michael Howard, David LeBlanc and John Viega	The 24 Deadly Sins of Software Security	McGraw-Hill	2009
	3.		Листа на трудови од безбедност на мрежи и веб безбедност		
	Дополнителна литература				
	Ред. број	Автор	Наслов	Издавач	Година
	1.	Dafydd Stuttard, Marcus Pinto	The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition	Wiley	2011
	2.	Ross J. Anderson	Security Engineering, 2 <sup>nd</sup> Edition	Wiley	2008
	3.				

Ред. Број: 12

Прилог бр.3		Предметна програма од прв, втор и трет циклус на студии			
1.	Наслов на наставниот предмет	Безбедност на контролни системи и ПоТ			
2.	Код	2F1210923			
3.	Студиска програма	Компјутерска безбедност и дигитална форензика			
4.	Организатор на студиската програма (единица, односно институт, катедра, оддел)	Факултет за информатика			
5.	Степен (прв, втор, трет циклус)	Втор степен			
6.	Академска година / семестар	Прва година/втор семестар	7.	Број на ЕКТС кредити	6
8.	Наставник	проф. д-р Александра Милева			
9.	Предуслови за запишување на предметот	нема			
10.	Цели на предметната програма (компетенции): Студентите да се стекнат со основите на автоматизацијата на процеси, контролните системи и концептот на ПоТ, но и да се стекнат со напредни знаења за проценка на безбедност, експлоатација и пенетрациско тестирање на ваквите системи и уреди.				
11.	Содржина на предметната програма: Вовед во автоматизација на процеси, контролни системи и ПоТ (PLC, RTI, IED, SCADA DCS, типови на ICS интерфејси, и сл) Преглед на архитектурата на поголемите ICS и смарт грид системи Purdue модел на контролни системи Преглед на протоколи кај ICS и ПоТ – fieldbus протоколи, контролни протоколи, протоколи за сериска и RF комуникација Вовед во ControlThings платформата и NESCOR методологијата за пенетрациско тестирање Проценка на безбедност и експлоатација на контролери Проценка на безбедност и експлоатација на ICS комуникациските протоколи – методологија на пенетрациско тестирање на традиционални мрежи, снимање и анализа на мрежен сообраќај, работа со непознати протоколи и нивно реверсно инженерство, фазинг на протоколи Проценка на безбедност и експлоатација на сериска комуникација и RF комуникација Проценка на безбедност и експлоатација на ICS вгнездена електроника – работа со EEPROM вгнездена меморија				
12.	Методи на учење: Предавања, дискусии, лабораториски вежби, електронско учење, семинарска работа, проект, консултации.				

13.	Вкупен расположив фонд на време		6 ЕКТС x 30 часа = 180 часа	
14.	Распределба на расположивото време		30+30+30+30+60 = 180 часа (2+2+1)	
15.	Форми на наставните активности	15.1.	Предавања- теоретска настава	30 часови
		15.2.	Вежби (лабораториски, аудиториски), семинари, теренска и тимска работа	30 часови
16.	Други форми на активности	16.1.	Проектни задачи	30 часови
		16.2.	Самостојни задачи	30 часови
		16.3.	Домашно учење	60 часови
17.	Начин на оценување			
	17.1.	Тестови		30 бодови
	17.2.	Семинарска работа/ проект ( презентација: писмена и усна)		50 бодови
	17.3.	Активност и учество		20 бодови
18.	Критериуми за оценување (бодови/ оценка)		до 50 бода	5 (пет) (F)
			од 51 до 60 бода	6 (шест) (E)
			од 61 до 70 бода	7 (седум) (D)
			од 71 до 80 бода	8 (осум) (C)
			од 81 до 90 бода	9 (девет) (B)
		од 91 до 100 бода	10 (десет) (A)	
19.	Услов за потпис и полагање на завршен испит		60% успех од сите предиспитни активности т.е. 42 бодови од двата колоквиуми, семинарската, редовноста на предавања и вежби	
20.	Јазик на кој се изведува наставата		Македонски	
21.	Метод на следење на квалитетот на наставата		Самоеваулација	

22.	Литература					
	22.1.	Задолжителна литература				
		Ред. број	Автор	Наслов	Издавач	Година
		1.	Clint Bodungen	Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions	McGraw Hill	2016
		2.	Keith Stouffer Victoria Pillitteri Suzanne Lightman Marshall Abrams Adam Hahn	Guide to Industrial Control Systems (ICS) Security	NIST Special Publication 800-82 Revision 2	2015
	3.		Листа на трудови од безбедност на контролни системи и ПоТ			
	22.2.	Дополнителна литература				
		Ред. број	Автор	Наслов	Издавач	Година
		1.	Charles J. Brooks, Philip A. Craig Jr.	Practical Industrial Cybersecurity: ICS, Industry 4.0, and IIoT	Wiley	2022
		2.				

		3.				
--	--	----	--	--	--	--

Ред. Број: 13

Прилог бр.3		Предметна програма од прв, втор и трет циклус на студии				
1.	Наслов на наставниот предмет	Мобилна безбедност и форензика				
2.	Код	2F1212723				
3.	Студиска програма	КОМПЈУТЕРСКА БЕЗБЕДНОСТ И ДИГИТАЛНА ФОРЕНЗИКА				
4.	Организатор на студиската програма (единица, односно институт, катедра, оддел)	Факултет за информатика				
5.	Степен (прв, втор, трет циклус)	Втор циклус на студии				
6.	Академска година / семестар	Прва/ II	7.	Број на ЕКТС кредити	6	
8.	Наставник	Проф. Сашо Коцески				
9.	Предуслови за запишување на предметот	нема				
10.	Цели на предметната програма (компетенции): Овој курс има за цел да ги запознае студентите основите на мобилната безбедност и форензика.					
11.	Содржина на предметната програма: Вовед во форензика на мобилни и преносни уреди. Мобилни уреди од аспект на форензичка анализа. Форензички софтвер – цели и употреба. Форензика на мобилни телефони и СИМ картички. Форензика на мобилни мрежи. Избор на алатки за форензичка обработка. Уреди кои се користат во мобилната форензика. Изолирање на мобилни телефони. Пронаоѓање на мобилни податоци.					
12.	Методи на учење:Предавања, лабораториски вежби, нумерички вежби, електронско учење, семинарска работа, тимска работа, консултации.					
13.	Вкупен расположив фонд на време	156				
14.	Распределба на расположивото време	2+2+1				
15.	Форми на наставните активности	15.1	Предавања- теоретска настава	2		
		15.2	Вежби (лабораториски, аудиториски), семинари, тимска работа	2		
16.	Други форми на активности	16.1	Проектни задачи	/		
		16.2	Самостојни задачи	1		
		16.3	Домашно учење	/		
17.	Начин на оценување					
	17.1	Тестови	30 бодови			
	17.2	Семинарска работа/ проект ( презентација: писмена и усна)	50 бодови			
	17.3	Активност и учество	20 бодови			
18.	Критериуми за оценување (бодови/ оценка)	до 50 бода		5 (пет) (F)		

		од 51 до 60 бода	6 (шест) (E)
		од 61 до 70 бода	7 (седум) (D)
		од 71 до 80 бода	8 (осум) (C)
		од 81 до 90 бода	9 (девет) (B)
		од 91 до 100 бода	10 (десет) (A)
19.	Услов за потпис и полагање на завршен испит	60% успех од сите предиспитни активности	
20.	Јазик на кој се изведува наставата	Македонски	
21.	Метод на следење на квалитетот на наставата	Самоеваулација	

<b>Литература</b>						
22.	22.1.	<b>Задолжителна Литература</b>				
		Ред. број	Автор	Наслов	Издавач	Година
		1.	Rohit Tamma, Oleg Skulkin, Heather Mahalik, Satish Bommisetty	Practical Mobile Forensics – Fourth edition	Packt Publishing	2020
		2.	Oleg Afonin, Vladimir Katalov	Mobile Forensics - Advanced Investigative Strategies	Packt Publishing	2016
	3.	Eamon P. Doherty	Digital Forensics for Handheld Devices	CRC Press	2013	
	22.2.	<b>Дополнителна Литература</b>				
		Ред. број	Автор	Наслов	Издавач	Година
		1.	Eoghan Casey	Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet	Academic Press	2011
		2.				
	3.					

Ред. Број: 14

<b>Прилог бр.3</b>		<b>Предметна програма од прв, втор и трет циклус на студии</b>
1.	Наслов на наставниот предмет	Интернет на нештата со безбедност
2.	Код	2FI212323
3.	Студиска програма	Компјутерска безбедност и дигитална форензика
4.	Организатор на студиската програма (единица, односно институт, катедра, оддел)	Факултет за информатика
5.	Степен (прв, втор, трет циклус)	Втор степен

6.	Академска година / семестар	Прва година/втор семестар	7.	Број на ЕКТС кредити	6
8.	Наставник	доц. д-р Александар Велинов			
9.	Предуслови за запишување на предметот	нема			
10.	Цели на предметната програма (компетенции): <ul style="list-style-type: none"> <li>- Разгледување на концептот на интернет на нештата</li> <li>- Стекнување знаење за најважните протоколи кои се користат кај интернет на нештата</li> <li>- Стекнување на знаења за CoAP протоколот и симулаторот Cooja</li> <li>- Стекнување на знаења за MQTT протоколот (верзија 3.1.1 и верзија 5.0)</li> <li>- Разгледување на брокери кои се користат кај интернет на нештата</li> <li>- Развивање на MQTT клиент-брокер апликации</li> <li>- Утврдување на напади и ранливости кај интернет на нештата</li> <li>- Разгледување на скриени канали кај интернет на нештата</li> <li>- Утврдување на безбедносни мерки кај интернет на нештата</li> </ul>				
11.	Содржина на предметната програма: <ul style="list-style-type: none"> <li>- Вовед во концептот за интернет на нештата</li> <li>- Архитектура кај интернет на нештата и протоколи на апликациско ниво (CoAP, MQTT v.3.1.1, MQTT v.5.0, XMPP, AMQP)</li> <li>- Протоколот CoAP и изведување на експерименти со симулаторот Cooja</li> <li>- Протоколот MQTT (верзија 3.1.1 и верзија 5.0)</li> <li>- Брокери кои се користат кај MQTT протоколот</li> <li>- Развивање на MQTT клиент-брокер апликации</li> <li>- Напади и ранливости кај интернет на нештата</li> <li>- Мрежни скриени канали и нивни шеми</li> <li>- Скриени канали кај CoAP, MQTT v.3.1.1 и MQTT v.5.0</li> <li>- Заштита на приватноста и безбедносни мерки кај интернет на нештата</li> </ul>				
12.	Методи на учење: Предавања, дискусии, лабораториски вежби, електронско учење, семинарска работа, проект, консултации.				
13.	Вкупен расположив фонд на време	6 ЕКТС x 30 часа = 180 часа			
14.	Распределба на расположивото време	30+30+30+30+60 = 180 часа (2+2+1)			
15.	Форми на наставните активности	15.1.	Предавања- теоретска настава	30 часови	
		15.2.	Вежби, дискусии	30 часови	
16.	Други форми на активности	16.1.	Проектни задачи	30 часови	
		16.2.	Самостојни задачи	30 часови	
		16.3.	Домашно учење	60 часови	
17.	Начин на оценување				
	17.1.	Тестови		30 бодови	
	17.2.	Семинарска работа/ проект (презентација: писмена и усна)		50 бодови	
	17.3.	Активност и учество		20 бодови	
18.	Критериуми за оценување (бодови/ оценка)	до 50 бода		5 (пет) (F)	
		од 51 до 60 бода		6 (шест) (E)	
		од 61 до 70 бода		7 (седум) (D)	
		од 71 до 80 бода		8 (осум) (C)	
		од 81 до 90 бода		9 (девет) (B)	
		од 91 до 100 бода		10 (десет) (A)	
19.	Услов за потпис и полагање на завршен испит	60% успех од сите предиспитни активности т.е. 42 бодови од двата колоквиуми, семинарската, редовноста на предавања и вежби			

20.	Јазик на кој се изведува наставата	Македонски
21.	Метод на следење на квалитетот на наставата	Самоеваулација

22.	Литература					
	22.1.	Задолжителна литература				
		Ред. број	Автор	Наслов	Издавач	Година
		1.	Dr Kamlesh Lakhwani, Dr Hemant Kumar Gianey, Joseph Kofi Wireko, Kamal Kant Hiran	Internet of Things (IoT): Principles, Paradigms and Applications of IoT	BPB Publications	2020
		2.	Chuan-Kun Wu	Internet of Things Security	Springer Nature	2021
	3.		Листа на трудови од интернет на нештата			
	22.2.	Дополнителна литература				
		Ред. број	Автор	Наслов	Издавач	Година
		1.	Andy King	Programming the Internet of Things	O'Reilly Media, Inc.	2021
		2.	Banafa, Ahmed	Secure and Smart Internet of Things (IoT)	River Publishers	2018
3.	Cristina Alcaraz	Security and Privacy Trends in the Industrial Internet of Things	Springer	2019		

Ред. Број: 15

<b>Прилог бр.3</b>		<b>Предметна програма од прв, втор и трет циклус на студии</b>			
1.	Наслов на наставниот предмет	Форензика и безбедност на мултимедија			
2.	Код	2FI216623			
3.	Студиска програма	Компјутерска безбедност и дигитална форензика			
4.	Организатор на студиската програма (единица, односно институт, катедра, оддел)	Факултет за информатика			
5.	Степен (прв, втор, трет циклус)	Втор степен			
6.	Академска година / семестар	Прва година/ втор семестар	7.	Број на ЕКТС кредити	6
8.	Наставник	Насловен доц. д-р Светлана Кордумова Трајанова			
9.	Предуслови за запишување на предметот	нема			
10.	Цели на предметната програма (компетенции): Студентите да се здобијат со напредни знаења од полето на форензиката и безбедноста на мултимедијата и да можат да се справат со различни предизвици и проблеми, како на пример, да се дознае дали одредена слика или видео е генерирано со помош на модел со Вештачка Интелигенција, или пак е вистинска/веродостојна, или пак Противничко машинско учење (Adversarial machine learning) кое се користи за да ги прелаже машините со измамени влезни податоци.				
11.	Содржина на предметната програма: <ul style="list-style-type: none"> <li>• Длабинско Учење, основи и модели</li> <li>• Конволуциски Модели од Длабинско учење за проблеми од Компјутерска Визија</li> </ul>				

	<ul style="list-style-type: none"> <li>• Процесирање на слики со Длабинско Учење</li> <li>• Процесирање на видеа со Длабинско Учење</li> <li>• Видови на невронски мрежи од длабинско учење</li> <li>• Deep Fake – што е како да се препознае</li> <li>• Модели за генерирање на Deep Fake мултимедијален контент</li> <li>• Модели од Вештачка Интелигенција за генерирање на нови слики, текст</li> <li>• Авторски права (Intellectual Property Rights - IPR), Управување со дигитални авторски права (Digital Rights Management - DRM)</li> <li>• Етичка Вештачка Интелигенција, што е и како да се запази</li> </ul>			
12.	Методи на учење: Предавања, дискусии, лабораториски вежби, електронско учење, истражување, проект, консултации.			
13.	Вкупен расположив фонд на време	6 ЕКТС x 30 часа = 180 часа		
14.	Распределба на расположивото време	30+30+30+30+60 = 180 часа (2+2+1)		
15.	Форми на наставните активности	15.1.	Предавања- теоретска настава	30 часови
		15.2.	Вежби, дискусии	30 часови
16.	Други форми на активности	16.1.	Проектни задачи	30 часови
		16.2.	Самостојни задачи	30 часови
		16.3.	Домашно учење	60 часови
17.	Начин на оценување			
	17.1.	Тестови		30 бодови
	17.2.	Семинарска работа/ проект (презентација: писмена и усна)		50 бодови
	17.3.	Активност и учество		20 бодови
18.	Критериуми за оценување (бодови/ оценка)		до 50 бода	5 (пет) (F)
			од 51 до 60 бода	6 (шест) (E)
			од 61 до 70 бода	7 (седум) (D)
			од 71 до 80 бода	8 (осум) (C)
			од 81 до 90 бода	9 (девет) (B)
			од 91 до 100 бода	10 (десет) (A)
19.	Услов за потпис и полагање на завршен испит	60% успех од сите предиспитни активности т.е. 42 бодови од двата колоквиуми, семинарската, редовноста на предавања и вежби		
20.	Јазик на кој се изведува наставата	Македонски		
21.	Метод на следење на квалитетот на наставата	Самоевалуација		

22.	Литература					
	22.1.	Задолжителна литература				
		Ред. број	Автор	Наслов	Издавач	Година
		1.	Book by David Forsyth and Jean Ponce	Computer Vision: A Modern Approach	Pearson; 2nd edition	2011
2.	Richard Szeliski (Author)	Computer Vision: Algorithms and Applications	Springer	2010		

			Loveleen Gaur	DeepFakes Creation, Detection, and Impact	CRC Press	2022
		3.		Листа на трудови од областа		
	22.2.	Дополнителна литература				
		Ред. број	Автор	Наслов	Издавач	Година
		1.				
		2.				
		3.				



