ДОКУМЕНТАЦИЈА ЗА АКРЕДИТАЦИЈУ СТУДИЈСКОГ ПРОГРАМА:

ИНФОРМАЦИОНА БЕЗБЕДНОСТ

МАСТЕР АКАДЕМСКЕ СТУДИЈЕ

Нови Сад

2024.

Садржај

00. Увод 3

01. Структура студијског програма 4

02. Сврха студијског програма 6

03. Циљеви студијског програма 7

04. Компетенција дипломираних студената 8

05. Курикулум 9

5.1 Распоред предмета по семестрима и годинама студија . . . 9

5.2 Спецификација предмета . . . 15

Примењена криптографија и криптоанализа . . . 15

Безбедност рачунарских система . . . 16

Стратегије информационе безбедности . . . 17

Увод у истраживачки процес . . . 19

Статистичке методе и структурално моделовање у инжењерству . . . 20

Безбедност рачунарских мрежа . . . 22

Анализа и реакција на сајбер инциденте . . . 23

Систем управљања безбедношћу информација . . . 25

Безбедност софтвера . . . 26

Физичка безбедност и социјални инжењеринг . . . 27

Анализа ризика и безбедност информација . . . 28

Системи електронског плаћања . . . 29

Анализа података у информационој безбедности . . . 30

Интеграција информационих система и API менаџмент . . . 32

Безбедност рачунарства у облаку . . . 33

Управљање пројектима у информационој безбедности . . . 35

Увод у дигиталну форензику . . . 37

Безбедност критичних инфраструктура и индустријских система . . . 38

Системи менаџмента безбедношћу и приватношћу података о личности . . . 40

Друштвени аспекти информационе безбедности . . . 41

Безбедност и приватност Интернет ствари . . . 42

Садржај

Мастер рад - студијски истраживачки рад 44

Стручна пракса 45

Мастер рад - израда и одбрана 46

06. Квалитет, савременост и међународна усаглашеност студијског програма _____ 47

07. Упис студената _____ 48

08. Оцењивање и напредовање студената _____ 49

09. Наставно особље _____ 50

10. Организациона и материјална средства _____ 51

11. Контрола квалитета _____ 52

11.1 Листа чланова комисије за контролу квалитета 52

12. Студије на светском језику _____ 53

13. Заједнички студијски програм _____ 54

14. ИМТ програм _____ 55

15. Студије на даљину _____ 56

16. Студије у јединици без својства правног лица ван седишта установе _____ 57

Назив студијског програма	Информациона безбедност
Високошколска установа у којој се изводи студијски програм	Факултет техничких наука
Образовно-научно/образовно уметничко поље	ИМТ
Научна, стручна или уметничка област	ИМТ студије (Информационе технологије: Индустријско инжењерство и инжењерски менаџмент; Електротехничко и рачунарско инжењерство)
Врста студија	Мастер академске студије
Обим студија изражен ЕСПБ бодовима	60-62
Назив дипломе	Мастер инжењер информационих технологија, Маст. инж. инф. технол.
Дужина студија (у годинама)	1
Година у којој је започела реализација студијског програма	
Година када ће започети реализација студијског програма (ако је програм нов)	2021
Број студената који студирају по овом студијском програму	0
Планирани број студената који ће се уписати на овај студијски програм (у прву годину)	16
Планирани број студената који ће се уписати на овај студијски програм(на свим годинама)	16
Датум када је програм прихваћен од стране одговарајућег тела(навести ког)	13.03.2019 - Наставно Научно веће ФТН Нови Сад 25.04.2019 - Сенат Универзитета у Новом Саду
Језик на ком се изводи студијски програм	Српски и енглески језик
Година када је програм акредитован	2021 - Прва акредитација 2024 - Уверење о допуни
Веб адреса на којој се налазе подаци о студијском програму	http://www.ftn.uns.ac.rs

Стандард 00. Увод

Студијски програм мастер академских студија Информациона безбедност као ИМТ студијски програм из облсати електротехничког и рачунарског инжењерства и индустријског инжењерства и менаџмента се реализује у оквиру Департмана за рачунарство и аутоматику, Департмана за енергетику, електронику и телекомуникације и Департмена за индустријско инжењерство и менаџмент Факултета техничких наука Универзитета у Новом Саду.

Програм је конципиран да образује мастер инжењере који ће добити дубока теоријска знања и вештине за рад у пракси, а истовремено да омогући даљи наставак школовања на одговарајућим специјалистичким, односно докторским студијама.

Студијски програм Информациона безбедност који се акредитује, представља одговор на даљи, врло интензивни развој области информационих технологија, уз природно проширење кроз усвајање нових практичних и теоријских знања.

У току студија посебно се вреднује самосталан рад и мотивише учешће у конкретним стручним и развојним пројектима у оквиру појединих лабораторија. Потенцирају се и развијају способности за решавање сложених, инжењерских проблема. Поред неопходних теоријских знања и практичних вештина, добија се неопходан осећај личне сигурности и испуњености, који је неопходан за успешно интегрисање у професионално окружење.

Департман за рачунарство и аутоматику, Департман за енергетику, електронику и телекомуникације и Дапартман за индустријско инжењерство и менаџмент као одговорне организационе јединице за креирање и реализацију овог студијског програма, остварили су низ пројеката и других облика сарадње с реномираним светским компанијама и, кроз ту сарадњу, обезбедили савремену лабораторијску опрему. Неке од тих компанија су: Cirrus Logic, Imagination-MIPS, Sony, Philips, Nagra, Marvel, Onkyo, Pioneer, Google, Cisco, Ericsson, TTTech, Harman, Denso, Texas Instruments, Qualcomm, Leica, RT-RK и Schneider Electric. Студенти овог студијског програма имају прилику да, коришћењем те опреме, стекну савремена и високо тражена знања у које студијски програм детаљно покрива.

Стандард 01. Структура студијског програма

Назив студијског програма је Информациона безбедност. Академски назив који се стиче након завршених студија је Мастер инжењер информационих технологија (Маст. инж. инф. технол.).

Структура програма омогућава да се добију дубока знања и врхунске вештине из изабране области интересовања, односно да се добије знање које студентима омогућава коришћење стручне литературе, примену знања на сложене проблеме који се јављају у професији и, у случају да се студенти за то определе, наставак студија.

Кандидат да би се уписао мора да има завршене четворогодишње основне академске студије, одговарајућег смера, које су вредноване са најмање 240 ЕСПБ.

Процедуре пријављивања, рангирања и уписа пријављених кандидата, дефинисане су Правилником о упису на студијске програме усвојеним на нивоу Факултета техничких наука.

Студијски програм мастер академских студија Информациона безбедност траје једну годину и вреднује се са 60 ЕСПБ. Овим студијским програмом обухваћени су обавезни и изборни предмети, стручна пракса и мастер рад. Студијски програм детаљно покрива дисциплину информационе безбедности.

Студенти кроз изборне предмете, а на основу сопствених склоности и жеља, могу произвољно проширивати стечено знање.

Студирање на студијском програму Информационе безбедности омогућава стицање дубоких знања потребних за заштиту информационих система.

Изборни предмети се бирају из групе предложених предмета, али студенти имају могућност да, према сопственим склоностима и жељама и уз сагласност руководиоца студијског програма, одређени број предмета изаберу са Факултета техничких наука, Универзитета у Новом Саду или неког другог универзитета у земљи или иностранству. При томе морају бити испуњени предуслови који се прописују за похађање наставе из изабраног предмета.

Предност приликом избора предмета имају најбољи студенти, а руководство студијског програма има могућност да ограничи број студената по појединим предметима због рационалног коришћења постојећих ресурса.

Предмети на овом студијском програму су једносеместрални и при томе доносе одговарајући број ЕСПБ бодова. Стандардима је утврђено да један ЕСПБ бод одговара приближно 30 сати активности студента (предавања, вежбе, и припрема за полагање испита).

Настава се изводи кроз предавања и вежбе. У наставном процесу инсистира се на самосталном и истраживачком раду студента и његовом појачаном личном, активном укључивању у наставни процес.

На предавањима се, уз коришћење одговарајућих дидактичких средстава, излаже предвиђено градиво, али се том приликом студентима указује и на истраживачке трендове у дотичној области. На вежбама, које прате предавања, решавају се конкретни задаци и излажу примери који додатно илуструју градиво. На вежбама се дају и додатна објашњења градива које је изложено на предавањима. Вежбе могу да буду аудиторне, лабораторијске или рачунарске. Део вежби или истраживачког рада може се одвијати и у изабраним компанијама или другим институцијама.

Рад студената се прати и вреднује према Правилнику о извођењу наставе, методологији доделе ЕСПБ бодова, основама вредновања предиспитних обавеза и начину провере знања студената који је усвојен на нивоу Факултета техничких наука.

Сваки положени предмет доноси студенту одређени број ЕСПБ. Студије се сматрају завршеним када студент испуни све обавезе прописане студијским програмом и када оствари најмање 60 ЕСПБ (положи све предвиђене предмете, обави стручну праксу и одбрани мастер рад).

У зависности од карактера вежби, одређује се величина групе. Студентске обавезе на вежбама могу

садржавати и израду семинарских и домаћих радова, пројектних задатака и семестралних радова, при чему се свака активност студената током наставног процеса прати и вреднује према правилима која су усвојена на нивоу Факултета техничких наука. Број освојених бодова је исказан према јединственој методологији и одражава оптерећеност студента.

Стандард 02. Сврха студијског програма

Сврха студијског програма је образовање студената за професију мастер инжењера информационих технологија у информационој безбедности у складу са потребама друштва као и појединца.

Студијски програм Информациона безбедност конципиран је тако да обезбеђује стицање компетенција које су друштвено оправдане и корисне. Факултет техничких наука је дефинисао основне задатке и циљеве ради образовања високо компетентних кадрова у области технике. Сврха студијског програма Информациона безбедности потпуно је у складу са основним задацима и циљевима Факултета техничких наука.

Реализацијом овако конципираног студијског програма се школују мастер инжењери информационих технологија који поседују високу и препознатљиву компетентност у европским и светским оквирима.

Стандард 03. Циљеви студијског програма

Циљеви студијског програма могу се груписати у неколико категорија:

Техничко знање. Програм обезбеђује стицање дубоког познавања специјализоване дисциплине информационе безбедности.

Практичне способности и вештине. Стицање неопходних способности и вештина за формулисање проблема и пројеката, као и плана за њихово решавање коришћењем разнородних техничких метода и техника. То, поред осталог укључује и развој креативних способности разматрања проблема и способност критичког мишљења.

Комуникативност и тимски рад. Стицање неопходних способности за презентовање сопствених резултата стручној и широј јавности као и развијање способности за тимски рад.

Припреме за даље студије. Стицање неопходних знања, које ће омогућити даљи наставак школовања кроз специјалистичке и докторске студије.

Један од посебних циљева, који је у складу са циљевима образовања стручњака на Факултету техничких наука, је развијање свести код студената за потребом перманентног образовања, развоја друштва у целини и заштите животне средине.

Припреме за професионално ангажовање. Стицање дубоких знања и вештина и развијање свести о широком спектру сложених проблема и обавеза и који се јављају у професионалној пракси.

Оспособљеност студената да брину о општим аспектима сигурности, етике, екологије и економије.

Стандард 04. Компетенција дипломираних студената

Мастер инжењери информационих технологија, који заврше студијски програм Информациона безбедност компетентни су да решавају сложене проблеме из праксе и да наставе школовање уколико се за то определе.

Компетенције укључују, пре свега, развој способности критичког мишљења, способности анализе проблема и синтезе решења и предвиђање понашања одабраног решења са јасном представом шта су добре а шта лоше стране одабраног решења.

Савладавањем студијског програма стиче се дубоко познавање информационе безбедности уз оспособљавање студената за решавање конкретних проблема уз употребу стручних и научних метода и поступака.

Свршени студенти Информационе безбедности су способни да на одговарајући начин напишу и да презентују резултате свог рада.

Свршени студенти овог нивоа студија поседују компетенцију за примену знања у пракси и праћење и примену новина у струци, као и за сарадњу са локалним друштвеним и међународним окружењем.

Свршени студенти Информационе безбедности оспособљени су за тимски рад и развој професионалне етике.

По правилу компетенција студената се верификује и кроз барем један рад објављен на домаћим конференцијама.

Кључне компетенције студената су способност за имплементацију свих фаза и вођење пројеката заштите рачунарских система, рачунарских мрежа, софтверских система и информационих система.

Стандард 05. Курикулум

Курикулум мастер академских студија Информациона безбедност формиран је тако да задовољи све постављене циљеве. Структура студијског програма је обезбедила да изборни предмети буду заступљени са најмање 30% ЕСПБ бодова.

На мастер академским студијама студенти конкретизују проблематику информационе безбедности. Кроз изборне предмете студенти задовољавају своје афинитете који су се током основних академских студија профилисали.

Сви предмети су једносеместрални и носе одговарајући број ЕСПБ бодова при чему један бод одговара приближно 30 сати активности студента.

У курикулуму је дефинисан опис сваког предмета који садржи назив предмета, тип предмета, годину и семестар студија, број ЕСПБ бодова, име наставника, циљ предмета са очекиваним исходима, знањима и компетенцијама, предуслове за похађање предмета, садржај предмета, препоручену литературу (међу којом се налази један основни и више помоћних уџбеника), методе извођења наставе, начин провере знања и оцењивања и друге податке.

Студијски програм је усаглашен са европским стандардима у погледу услова уписа, трајања студија, услова преласка у наредну годину, стицања дипломе и начина студирања.

Саставни део курикулума информационе безбедности је стручна пракса и практичан рад у трајању од 90 часова, која се реализује у одговарајућим научноистраживачким установама, у организацијама за обављање иновационе активности, у организацијама за пружање инфраструктурне подршке иновационој делатности, у привредним друштвима и јавним установама.

Студент завршава студије израдом мастер рада који се састоји од студијског истраживачког рада, теоријско-методолошке припреме неопходне за продубљено разумевање области из које се мастер рад ради и израде самог рада.

Пре одбране самог рада кандидат полаже теоријско-методолошке основе по правилу пред комисијом која је одређена за одбрану. Коначна оцена мастер рада се изводи на основу оцене положене теоријско-методолошке припреме и оцене израде и одбране самог рада. Мастер рад се брани пред комисијом која се састоји од најмање три наставника при чему макар један мора да буде са другог департмана или факултета.

По правилу од студента се очекује барем један рад на домаћим конференцијама из области завршног мастер рада или, у изузетним случајевима, рад на међународним конференцијама, домаћим или страним часописима.

Стандард 05. - Курикулум

Стандард 05. - Курикулум

Табела 5.1 Распоред предмета по семестрима и годинама студија

Студијски програм: Информациона безбедност

Р.бр.	Шифра предмета	Назив предмета		С	Тип	Статус	Активна настава				Остали часови	ЕСПБ
							П	В	СИР	ДОН		
ПРВА ГОДИНА												
1	19.IB21	Примењена криптографија и криптоанализа		1	ТМ	О	3	0	0	3	0	8
2	19.IB01	Изборна група 1 (бира се 1 од 4)		1		ИБ	2-3	0	0-2	0-3	0	4-6
		19.IB12	Безбедност рачунарских система	1	ТМ	И	3	0	0	3	0	6
		19.IB22	Стратегије информационе безбедности	1	ТМ	И	3	0	0	3	0	6
		19.IB31	Увод у истраживачки процес	1	АО	И	3	0	0	3	0	6
		17.IZMI13	Статистичке методе и структурално моделовање у инжењерству	1	АО	И	2	0	2	0	0	4
3	19.IB02	Изборна група 2 (бира се 1 од 3)		1		ИБ	3	0	0	3	0	6
		19.IB13	Безбедност рачунарских мрежа	1	НС	И	3	0	0	3	0	6
		19.IB23	Анализа и реакција на сајбер инциденте	1	СА	И	3	0	0	3	0	6
		19.IB32	Систем управљања безбедношћу информација	1	НС	И	3	0	0	3	0	6
4	19.IB03	Изборна група 3 (бира се 1 од 3)		1		ИБ	3	0	0	3	0	6
		19.IB11	Безбедност софтвера	1	СА	И	3	0	0	3	0	6
		19.IB24	Физичка безбедност и социјални инжењеринг	1	СА	И	3	0	0	3	0	6
		19.IB33	Анализа ризика и безбедност информација	1	НС	И	3	0	0	3	0	6
5	19.IB04	Изборна група 4 (бира се 1 од 3)		1		ИБ	3	0	0	2-3	0	6
		17.E2501	Системи електронског плаћања	1	НС	И	3	0	0	2	0	6
		19.IB25	Анализа података у информационој безбедности	1	СА	И	3	0	0	3	0	6
		19.IB34	Интеграција информационих система и API менаџмент	1	ТМ	И	3	0	0	3	0	6
6	19.IB05	Изборна група 5 (бира се 1 од 3)		2		ИБ	3	0	0	3	0	6
		19.SEM022	Увод у дигиталну форензику	2	СА	И	3	0	0	3	0	6
		19.IB26	Безбедност рачунарства у облаку	2	СА	И	3	0	0	3	0	6
		19.IB35	Управљање пројектима у информационој безбедности	2	ТМ	И	3	0	0	3	0	6
7	19.IB06	Изборна група 6 (бира се 1 од 4)		2		ИБ	3	0-3	0	0-3	0	6
		19.SEM020	Безбедност и приватност Интернет ствари	2	СА	И	3	0	0	3	0	6
		19.IB27	Безбедност критичних инфраструктура и индустријских система	2	СА	И	3	0	0	3	0	6
		19.IB36	Системи менаџмента безбедношћу и приватношћу података о личности	2	ТМ	И	3	0	0	3	0	6
		19.IB37	Друштвени аспекти информационе безбедности	2	ТМ	И	3	3	0	0	0	6

Стандард 05. - Курикулум

Табела 5.1 Распоред предмета по семестрима и годинама студија

Студијски програм: Информациона безбедност

Р.бр.	Шифра предмета	Назив предмета	С	Тип	Статус	Активна настава				Остали часови	ЕСПБ
						П	В	СИР	ДОН		
8	19.IB51	Стручна пракса	2	СА	О	0	0	0	0	6	6
9	19.IB53	Мастер рад - студијски истраживачки рад	2	СА	О	0	0	8	0	0	6
10	19.IB54	Мастер рад - израда и одбрана	2	СА	О	0	0	0	0	4	6
Укупно часова (предавања+вежбе, ДОН, СИР, остали часови) и бодови на години						20-21	0-3	8-10	14-21	10	60-62
Укупно часова активне наставе на години						47-50					

Стандард 05. - Курикулум

Информациона безбедност

Мастер академске студије

Спецификација предмета

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	19.IB21 Примењена криптографија и криптоанализа
Наставник/наставници:	Лендак И. Имре, Ванредни професор Ковачевић Н. Младен, Ванредни професор
Статус предмета:	Обавезан
Број ЕСПБ:	8
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

Циљ предмета је стицање напредних знања о криптографским алгоритмима и системима. Упознавање са најновијим симетричним и асиметричним алгоритмима. Преглед модерних једносмерних функција. Стандарди на пољу криптографских система. Упоредна анализа предности и мана приказаних алгоритама. Успостављање безбедних комуникационих канала, креирање кључа сесије и perfect forward secrecy. Дискусија напредних техника за потписивање дигиталних садржаја. Упознавање са основама квантне и хомоморфне криптографије.

Исход предмета

Познавање напредних криптографских система, алгоритама и техника. Познавање релевантних стандарда и спецификација на пољу криптографије. Оспособљеност за анализу архитектуре система и избор одговарајућих криптографских техника у решавању инжењерских проблема на пољу информационе безбедности у инфраструктурним системима. Способност самосталне имплементације криптографских алгоритама и система.

Садржај предмета

Симетрични алгоритми. Асиметрични алгоритми. Једносмерне функције. Хомоморфни алгоритми. Упоредна анализа приказаних алгоритама. Успостављање комуникационих канала, размена кључева и кључеви сесија. Руковање са тајним кључевима. Дигитални потписи. Квантна криптографија. Криптографски системи у окружењима са ограниченим рачунским ресурсима.

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	Горан Савић, Милан Сегединац	Софтверска инфраструктура за управљање курикулумом у електронској настави	Нови Сад : Факултет техничких наука	2016
2,	Драган Ивановић, Бранко Милосављевић	Управљање дигиталним документима	Нови Сад : Факултет техничких наука	2015
3,	Гордана Милосављевић	Развој пословних информационих система вођен моделима	Нови Сад : Факултет техничких наука	2015
4,	Мирослав Хајдуковић	Оперативни системи (проблеми и структура)	Нови Сад : Факултет техничких наука	2013
5,	Момчило Новковић	Нелинеарни модели временских серија : допринос теорији и пракси	Нови Сад : Факултет техничких наука	2002
6,	Ferguson N.	Cryptography Engineering: Design Principles and Practical Applications	Wiley	2010
7,	Martin K.M.	Everyday Cryptography: Fundamental Principles and Applications	Oxford University Press	2012
8,	Singh S.	The Code Book: The Secret History of Codes and Code-breaking	Fourth Estate	2010

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	3	0	3	0	0

Методе извођења наставе

Предавања; Други облици наставе; консултације.

Оцена знања (максимални број поена 100)

Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Предметни пројекат	Да	50.00	Писмени део испита - комбиновани задаци и теорија	Да	20.00
Присуство на предавањима	Да	5.00	Усмени део испита	Да	20.00
Присуство на вежбама	Да	5.00			

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	19.IB12 Безбедност рачунарских система
Наставник/наставници:	Гајић Б. Душан, Ванредни професор Петровић Б. Вељко, Доцент
Статус предмета:	Изборни
Број ЕСПБ:	6
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

Стицање знања потребног за разумевање неопходних техника за вршење напада на и одбрану рачунарских система.

Исход предмета

Након успешно завршеног курса студент (1) разуме природу рањивости рачунарских система, (2) разуме природу напада на рачунарске систем и зна како да их спроведе у лабораторијском окружењу (3) оспособљен је за имплементацију решења у оквиру рачунарских система који минимизују успех напада.

Садржај предмета

(1) увод у безбедност (2) историја безбедности рачунарских система, (3) архитектура рачунарског система у ширем смислу као извор безбедности, (4) интернет ствари као технологија рањивих архитектура, (5) безбедност у оперативним системима, (6) слабост у менаџменту меморијом и (7) малициозни софтвер

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	Yuri Diogenes, Diogenes Oyakza	Cybersecurity – Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics	Packt Publishing	2018
2,	Christopher Hadnagy	Social Engineering: The Science of Human Hacking, 2nd Edition	Wiley	2018
3,	Shancang Li Li Da Xu	Securing the Internet of Things	Syngress	2017
4,	Phil Bramwell	Hands-On Penetration Testing on Windows: Unleash Kali Linux, PowerShell, and Windows debugging tools for security testing and analysis	Packt Publishing	2018
5,	Monnappa K A	Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware	Packt Publishing	2018
6,	Seymour Bosworth, M. E. Kabay, Eric Whyne	Seymour Bosworth, M. E. Kabay, Eric Whyne	Wiley	2014
7,	Swarup Bhunia, Mark Tehranipoor	Hardware Security: A Hands-on Learning Approach 1st Edition	Springer	2017
8,	Li, Shancang	Securing the Internet of Things	Rockland: Syngress	2017
9,	Драган Плескоњић, Немања Мачек, Борислав Ђорђевић и Марко Царић	Сигурност рачунарских система и мрежа	Микро књига	2007

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	3	0	3	0	0

Методе извођења наставе

Настава се одвија кроз предавања, додатне облике наставе и консултације. Теоријске основе се изучавају на предавањима. Продубљивање знања и стицање практичних вештина остварује се кроз додатне облике наставе. Интерактивни рад са студентима се остварује кроз консултације.

Оцена знања (максимални број поена 100)

Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Предметни пројекат	Да	50.00	Усмени део испита	Да	50.00

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	19.IB22 Стратегије информационе безбедности
Наставник/наставници:	Ковачевић Н. Младен, Ванредни професор Варга Д. Ервин, Ванредни професор
Статус предмета:	Изборни
Број ЕСПБ:	6
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

Циљ курса је да научи студенте да самостално приступе изради свеобухватне стратегије информационе безбедности у организацијама различите величине. За постизање тог циља ће студенти научити технике управљања ресурсима, анализе ризика, буџетирања и израде политике безбедности. Студенти ће се упознати и са релевантним стандардима и оквирима у информационој безбедности и њиховим односима са стратегијом информационе безбедности.

Исход предмета

Студенти ће бити оспособљени да оцене комплексне утицаје и значај стратегија информационе безбедности на циљеве организација. Биће оспособљени за израду безбедносних политика, процеса и акција које омогућавају постизање пословних циљева у сајбер простору. Поседоваће знање за процену потреба, креирање одговарајућих сајбер стратегија за подршку пословних циљева.

Садржај предмета

Дефиниција сајбер простора. Стратегије сајбер безбедности. Безбедност и сајбер простору. Управљање ресурсима у контексту информационе безбедности. Управљање ризицима. Управљање комплексним односима у сајбер простору. Стандарди и оквири у информационој безбедности. Управљање информационом безбедношћу. Актуелни конфликти у сајбер простору. Планирање и израда политике безбедности. Планирање и израда буџета. Заштита људских права. Заштита података. Физичка безбедност, ризици и догађаји у физичком окружењу.

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	Војин Грковић и Александар Јовановић	Термоенергетска постројења - пројектовање технологије рада и управљање ризицима	Нови Сад : Факултет техничких наука	2015
2,	Гордана Милосављевић	Развој пословних информационих система вођен моделима	Нови Сад : Факултет техничких наука	2015
3,	Филип Кулић, Александар Ристић, Милан Рапаић	Основи система аутоматског управљања	Нови Сад : Факултет техничких наука	2013
4,	Велимир Чонградац, Илија Каменко, Филип Кулић, Никола Јорговановић	Управљање процесима рачунаром кроз решене примере	Нови Сад : Факултет техничких наука	2013
5,	Драган Кукољ	Системи засновани на рачунарској интелигенцији	Нови Сад: Факултет техничких наука	2007
6,	Timothy Shimeall, Jonathan Spring	Introduction to Information Security: A Strategic-Based Approach	Syngress	2013
7,	Yuri Diogenes, Erdal Ozkaya	Cybersecurity – Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics	Packt Publishing	2018
8,	Mike Chapple, James Michael Stewart, Darril Gibson	(ISC)2 CISSP Certified Information Systems Security Professional Study Guide 2018: : With 150+ Practice Questions	Sybex	2018
9,	Douglas W. Hubbard, Richard Seiersen	How to Measure Anything in Cybersecurity Risk	Wiley	2016
10,	Gregory J. Touhill, C. Joseph Touhill	Cybersecurity for Executives: A Practical Guide	Wiley-AIChE	2014

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	3	0	3	0	0

Методе извођења наставе

Предавања; други облици наставе; консултације.

Стандард 05. - Курикулум

Оцена знања (максимални број поена 100)					
Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Предметни пројекат	Да	50.00	Тест	Да	20.00
Присуство на предавањима	Да	5.00	Усмени део испита	Да	20.00
Присуство на вежбама	Да	5.00			

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	19.IB31 Увод у истраживачки процес
Наставник/наставници:	Мирковић Р. Милан, Редовни професор
Статус предмета:	Изборни
Број ЕСПБ:	6
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

Циљ предмета представља овладавање основним знањима у подручју истраживачког процеса, односно стицање компетенција које ће омогућити студентима да самостално дефинишу истраживачки проблем на адекватан начин, да дизајнирају истраживачки нацрт пратећи прихваћену методологију која обезбеђује транспарентност и поновљивост истраживања, да спроведу истраживање ослањајући се на одговарајуће методе прикупљања података, те да прикупљене податке анализирају употребом валидних статистичких метода и да на основу резултата анализе извуку релевантне и квалитетне закључке који могу бити представљени како академској тако и стручној заједници на адекватан начин.

Исход предмета

Студенти ће по завршетку курса бити оспособљени за самостално планирање, дизајнирање и извођење истраживачких подухвата. Очекује се да ће студенти стећи компетенције за формулисање релевантних истраживачких питања, идентификацију битних фактора и одабир адекватних метода истраживања за његово успешно спровођење. Коначно, студенти ће стећи вештине неопходне за приказ резултата истраживања стручној јавности, употребом савремених софтверских алата.

Садржај предмета

Уводни концепти, теоријске поставке и принципи истраживачког процеса, дефинисање истраживачког проблема, зависне, независне и интервенишуће варијабле у истраживању, нивои и начини мерења, посредна и непосредна мерења, поузданост, тачност и грешке мерења, нацрти истраживања, улога контролних група, методе и принципи узорковања у истраживању, закључивање на основу резултата истраживања, обликовање и извештавање о резултатима истраживања, алати за помоћ у истраживању и обликовању приказа истраживања, претраживање и референцирање извора.

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	Ристић, Ж.	О истраживању, методу и раду	Институт за педагошка истраживања	2006
2,	Williamson, K.; Johanson, G.	Research Methods: Information, Systems, and Contexts	Elsevier Science and Technology	2017
3,	Patten, M.; Newhart, M.	Understanding Research Methods: An Overviev of the Essentials	Taylor & Francis	2018
4,	Мирковић, М.	Увод у истраживачки процес, електронска скрипта	Факултет техничких наука	2019

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	3	0	3	0	0

Методе извођења наставе

Настава на предмету обухвата предавања уз осврт на практичне примере. Вежбе су потпуно рачунарске и на њима студенти кроз практичан рад примењују знања стечена на предавањима, а обавезним пројектним задатком се подстиче рад у групама.

Оцена знања (максимални број поена 100)

Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Предметни(пројектни)задатак	Да	30.00	Усмени део испита	Да	60.00
Присуство на предавањима	Да	10.00			

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	17.IZMI13 Статистичке методе и структурално моделовање у инжењерству
Наставник/наставници:	Иветић Б. Јелена, Ванредни професор
Статус предмета:	Изборни
Број ЕСПБ:	4
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

Оспособљавање студената на апстрактно мишљење и стицање основних знања из области Статистичких метода и структуралног моделовања у инжењерству. Циљ предмета је да код студента развије посебан начин размишљања при проучавању масовних појава у области информатике. Карактер предмета је апликативни, стога се даје значај знањима која могу појаснити квантитативни приступ проблемима из области студирања. Уз то студенти се оспособљавају за коришћење статистичког пакета Р. Циљ је оспособити студенте да знају одабрати одговарајуће статистичке методе, израдити статистичку анализу и суштински је образлижити. То знање је темељ за боље разумевање стручне литературе и за успешан напредак у студијама.

Исход предмета

Стечена знања студент треба да користи у даљем образовању и у стручним предметима прави и решава математичке моделе користећи се сазнањима стеченим у овом предмету. Овладавањем теоријским сазнањима из подручја Статистичких метода и структуралног моделовања у инжењерству која се изучавају у овом предмету те вештина израчунавања и тумачења израчунатих статистичких показатеља.

Садржај предмета

Бројне карактеристике - дисперзија, коваријанса, корелација. Граничне теореме. Параметарске и непараметарске хипотезе и тестови значајности, интерпретација статистичких закључака. Анализа варијанси. Регресиона анализа: линерана, нелинеарна и логистичка регресија. Визуализација статистичких података. Статистички модели у рачунарству . Статистички пакет Р. Структурално моделовање.

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	Rand Wilcox	Introduction to Robust Estimation and Hypothesis Testing 3rd Edition	Elsevier, Amsterdam	2012
2,	Његић, Радмила Жижић, Милева	Основи статистичке анализе	Савремена администрација	1979
3,	Жижић, Милева Ловрић, Миодраг	Методи статистичке анализе	Центар за издавачку делатност Економског факултета	2005
4,	Бошковић, Олгица	Методи статистичке анализе - збирка решених задатака	Центар за издавачку делатност Економског факултета	2005
5,	Хаџић, О.	Нумеричке и статистичке методе у обради експерименталних података	Институт за математику, Нови Сад	1989
6,	Стојаковић, М.	Вероватноћа, статистика и случајни процеси	Symbol, Нови Сад	2007
7,	Стојаковић, М.	Вероватноћа и случајни процеси	Факултет техничких наука, Нови Сад	2017
8,	Стојаковић, Мила Аџић, Невенка	Збирка решених задатака са писмених испита из вероватноће и математичке статистике	Универзитет у Новом Саду, Научно образовни институт за примењене основне дисциплине	1992

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	2	0	0	2	0

Методе извођења наставе

Предавања; Нумеричко рачунске вежбе и рачунарске вежбе(из статистике). Консултације. Предавања се изводе комбиновано. На предавањима се излаже теоретски део градива пропраћен карактеристичним примерима ради лакшег разумевања градива. На вежбама, која прате предавања, раде се карактеристични задаци и продубљује се изложено градиво са предавања. Поред предавања и вежби редовно се одржавају и консултације. Део градива, који чини логичку целину, може се полагати и у току наставног процеса у облику следећа 2 модула (први модул: статистика, други модул: структурално моделовање).

Стандард 05. - Курикулум

Оцена знања (максимални број поена 100)					
Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Тест	Да	40.00	Писмени део испита - комбиновани задаци и теорија	Да	60.00

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	19.IB13 Безбедност рачунарских мрежа
Наставник/наставници:	Поповић В. Мирослав, Редовни професор Башичевић Д. Илија, Редовни професор
Статус предмета:	Изборни
Број ЕСПБ:	6
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

Стицање знања потребног за примену технологија заштите рачунарских мрежа и разумевање проблема сигурности мрежа.

Исход предмета

Након успешно завршеног курса студент (1) разуме проблеме угрожавања безбедности рачунарских мрежа, (2) разуме основне концепте заштите рачунарских мрежа и (3) има потребна знања за примену технологија заштите рачунарских мрежа.

Садржај предмета

(1) увод у безбедност рачунарских мрежа, (2) фазе и врста напада на рачунарске мреже, (3) напади одбијањем услуге, (4) SQL напади, (5) уређаји за заштиту рачунарских мрежа, (6) анонимност на Интернету и (7) напади на нивоу физичке архитектуре.

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	Richard Bejtlich	The Practice of Network Security Monitoring: Understanding Incident Detection and Response	No starch press	2013
2,	C.Douligeris, D.N. Serpanos	Network Security: Current Status and Future Directions		2007
3,	Драган Плескоњић, Немања Мачек, Борислав Ђорђевић и Марко Царић	Сигурност рачунарских система и мрежа	Микро књига	2007
4,	Илија Башичевић, Мирослав Поповић и Владимир Ковачевић	Основе рачунарских мрежа 1	Факултет техничких наука	2017

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	3	0	3	0	0

Методе извођења наставе

Настава се одвија кроз предавања, додатне облике наставе и консултације. Теоријске основе се изучавају на предавањима. Продубљивање знања и стицање практичних вештина остварује се кроз додатне облике наставе. Интерактивни рад са студентима се остварује кроз консултације.

Оцена знања (максимални број поена 100)

Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Предметни пројекат	Да	50.00	Усмени део испита	Да	50.00

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	19.IB23 Анализа и реакција на сајбер инциденте
Наставник/наставници:	Ковачевић Н. Младен, Ванредни професор Селаков Ж. Александар, Ванредни професор
Статус предмета:	Изборни
Број ЕСПБ:	6
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

Циљ овог курса је студентима пренесе знања потребна за дизајн и изградњу тимова за реакцију на инциденте. Овај циљ ће бити постигнут детаљним приказом и анализом претњи, рањивости, типова напада, односно техника за моделирање напада у сајбер простору. Биће дат и преглед релевантног законског оквира.

Исход предмета

Студенти су оспособљени да наведу типове претњи и рањивости у сајбер простору. Оспособљени су да направе детаљну анализу и моделирање напада. Студенти су стекли неопходна знања за анализу узорака малвера. Студенти разликују различите типове тимова за реакцију на инциденте и упознати су са методологијом развоја и управљања центрима за надзор информационе безбедности. Упознати су са релевантним законским актима и етичким аспектима у домену анализе и реакције на инциденте.

Садржај предмета

Принципи сајбер безбедности и приватности. Претње и слабости система. Различите категорије напада, модели понашања нападача. Моделирање фаза сајбер напада. Увод у анализу малвера – концепти и методологија. Категорије инцидената, реакције на инциденте и правовременост реакције. Организација и управљање оперативним центрима за надзор информационе безбедности. Типови тима за реакцију на инциденте, нпр. војни, национални, на нивоу компанија. Закони, подзаконски акти, стандарди, политике и етика у сајбер безбедности и приватности.

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	Срђан Попов, Ђорђе Ћосић, Тања Новаковић, Љиљана Поповић	Моделовање и симулација у управљању ризиком	Нови Сад : Факултет техничких наука	2016
2,	Гордана Милосављевић	Развој пословних информационих система вођен моделима	Нови Сад : Факултет техничких наука	2015
3,	Војин Грковић и Александар Јовановић	Термоенергетска постројења - пројектовање технологије рада и управљање ризицима	Нови Сад : Факултет техничких наука	2015
4,	Бранислав Атлагић	Софтвер са критичним одзивом : пројектовање SCADA система	Нови Сад : Факултет техничких наука	2015
5,	Велимир Чонградац, Илија Каменко, Филип Кулић, Никола Јорговановић	Управљање процесима рачунаром кроз решене примере	Нови Сад : Факултет техничких наука	2013
6,	Eric C. Thompson	Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents	Apress	2018
7,	N.K. McCarthy, Matthew Todd, Jeff Klaben	The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk	McGraw-Hill Education	2012
8,	Monnappa K A	Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware	Packt Publishing	2018
9,	Scott N. Schober	Hacked Again	ScottSchober.com Publishing	2016
10,	André Årnes	Digital Forensics (1st Edition)	Wiley	2017

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	3	0	3	0	0

Методе извођења наставе

Предавања; други облици наставе; консултације.

Стандард 05. - Курикулум

Оцена знања (максимални број поена 100)					
Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Предметни пројекат	Да	50.00	Тест	Да	20.00
Присуство на предавањима	Да	5.00	Усмени део испита	Да	20.00
Присуство на вежбама	Да	5.00			

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	19.IB32 Систем управљања безбедношћу информација
Наставник/наставници:	Делић М. Милан, Редовни професор
Статус предмета:	Изборни
Број ЕСПБ:	6
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

Предмет Систем управљања безбедношћу информација изучава се у циљу стицања основних знања неопходних за управљање безбедношћу информација. Изучавају се захтеви стандарда ISO/IEC 27001 са активностима потребним за његову имплементацију, управљање ресурсима, преиспитивање од стране руководства и обезбеђење интегритета информација у систему.

Исход предмета

Кандидат се упознаје са основним појмовима и принципима управљања безбедношћу информација у процесима рада. Ова знања су, у контексту потреба која намеће тржишта данашњице, неопходна сваком менаџеру за успешно овбављање свог посла, а најмање у обиму који је неопходан да би се сагледали најзначајнији аспекти система за управљање безбедношћу информација у неком пословном систему и њихов утицај на управљање пословањем.

Садржај предмета

Место и улога безбедности информација у организацији; Основни појмови; Систем за управљање безбедношћу информација - ISMS; Одговорност руководства, интерне провере; Преиспитивање и унапређење система; Анализа ризика и документовање система; Стандард ISO/IEC 27002 - механизми управљања безбедношћу информација; Писање изјаве о безбедности информација; Перформансе система.

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	Бекер, И., Радловачки, В.	Систем управљања безбедношћу информација - скрипта	ИИС-Истраживачки и технолошки центар Нови Сад	2012
2,	Syngress Publishing, Inc.	Security + Study Guide & DVD Training System	Syngress Publishing, Inc., Elsevier, Burlington, MA, USA	2007
3,	Harold F. Tipton, Micki Krause, editors	Information security management handbook	CRC Press LLC, Danvers, MA, USA	2003
4,	Andress, Jason	The Basics of Information Security	Elsevier	2014
5,	Talabis, Christopher D.; Martin, Jason	Information Security Risk Assessment Toolkit	Elsevier	2013
6,	Gardner, Bill Thomas, Valerie	Building an Information Security Awareness Program	Elsevier	2014
7,	Вулановић, Војислав, ет. ал.	Методе и технике унапређења процеса рада	Факултет техничких наука, Департман за индустријско инжењерство и менаџмент	2012
8,	Вулановић, Војислав, ет. ал.	Систем менаџмента квалитетом	Факултет техничких наука, Департман за индустријско инжењерство и менаџмент	2012

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	3	0	3	0	0

Методе извођења наставе

Предавање. Аудиторне вежбе. Консултације. Оцена се формира на основу успеха из лабораторијских вежби, групних задатака, испитног задатка и усменог дела испита.

Оцена знања (максимални број поена 100)

Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Предметни пројекат	Да	40.00	Писмени део испита - комбиновани задаци и теорија	Да	50.00
Присуство на предавањима	Да	5.00			
Присуство на вежбама	Да	5.00			

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	19.IB11 Безбедност софтвера
Наставник/наставници:	Сладић С. Горан, Редовни професор
Статус предмета:	Изборни
Број ЕСПБ:	6
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

Оспособљавање студената за примену техника за дизајнирање, имплементацију и тестирање безбедносних аспеката софтверских система.

Исход предмета

Након успешно завршеног курса, студенти су стекли теоријска и практична знања о инжењерингу безбедног софтвера, укључујући разумевање безбедносних претњи, напада који реализују претње и метода за спречавање напада. Студенти су у стању да дизајнирају безбедне архитектуре софтвера, имплементирају код без рањивости и тестирају софтвер да верификују његову безбедност, резултујући у конструкцији безбедног софтвера.

Садржај предмета

Увод у инжењеринг безбедног софтвера: дефиниција (предмет интересовања), основни појмови, безбедносни захтеви. Анализа токова података: анализа граница поверења, минимизација токова података, анализа и редукција површине за напад. Моделовање претњи: поглед ресурса, поглед нападача, поглед софтвера. Безбедносни дизајн: принципи безбедног дизајна, шаблони безбедног дизајна, вишеслојна заштита. Веб безбедност: претње, напади, рањивости, митигације. Безбедносно тестирање: тестирање безбедносних захтева, тестирање митигација, алати за безбедносно тестирање, пенетрационо тестирање.

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	Ross J. Anderson	Security Engineering: A Guide to Building Dependable Distributed Systems, Second Edition	Wiley	2008
2,	James Ransome, Anmol Misra	Core Software Security: Security at the Source	CRC Press	2013
3,	Adam Shostack	Threat modeling: Designing for security	Wiley	2014
4,	Brook Schoenfield	Securing Systems: Applied Security Architecture and Threat Models	CRC Press	2015
5,	Роберт Мартин	Јасан код - Приручник за писање јасних програма	Микро књига	2020
6,	Роберт Ц. Мартин	Чиста архитектура	Компјутер библиотека	2020
7,	Monnappa, KA	Заштита од злонамерних програма	Компјутер библиотека	2019

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	3	0	3	0	0

Методе извођења наставе

Предавања; Други облици наставе; Консултације. Испит је усмени. Оцена испита се формира на основу успеха са одбране пројекта и усменог испита.

Оцена знања (максимални број поена 100)

Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Предметни пројекат	Да	70.00	Усмени део испита	Да	30.00

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	19.IB24 Физичка безбедност и социјални инжењеринг
Наставник/наставници:	Лендак И. Имре, Ванредни професор
Статус предмета:	Изборни
Број ЕСПБ:	6
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

Циљ предмета је стицање знања о претњама и безбедносним мерама којима се штите физичке тачке приступа, односно које омогућавају изградњу едуковане и лојалне радне снаге. Остваривање горе наведеног циља је значајно, јер у су физички домен и људски ресурси најслабије карике у контексту информационе безбедности.

Исход предмета

Упознатост са детаљима најпознатијих напада злоупотребама физичких тачака приступа, односно људских ресурса. Способност развоја и примене ефективних мера физичке безбедности. Познавање релевантних стандарда, закона и спецификација на пољу физичке безбедности. Упознатост са методима изградње лојалне радне снаге која је свесна софистицираних техника потенцијалних нападача.

Садржај предмета

Дизајн безбедних рачунарских центара и постројења. Екстерне мере заштите, расвета, ограде и баријере. Прозори, врата, браве и сефови. Картице и биометријски сензори. Физичко обезбеђивање рачунарских система. Технике надзора у физичком домену. Стандарди у домену физичке безбедности. Познати случајеви хакерских напада злоупотребом људског елемента. Имперсонација. Изградња лојалне и безбедносно-едуковане радне снаге. Континуални тренинзи у домену информационе безбедности.

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	Владимир Остојић, Татјана Лончар-Турукало	Практикум за рачунарске вежбе из дигиталне обраде слике	Нови Сад : Факултет техничких наука	2016
2,	Радош Радивојевић	Социологија технике	Нови Сад : Факултет техничких наука	2015
3,	Ана Петровић	Физика : Основи примењене физике	Нови Сад : Факултет техничких наука	2003
4,	Игор Пешко	Технологија извођења грубих грађевинских радова	Нови Сад, Факултет техничких наука	2016
5,	Милан Инић	Безбедност друмског саобраћаја	Нови Сад : Факултет техничких наука	2004
6,	Lawrence J. Fennelly	Effective physical security	Butterworth-Heinemann	2013
7,	Cristopher Hadnagy	Social Engineering – The science of human hacking	Wiley	2018
8,	Will Gragido, John Pric	Cybercrime and espionage	Syngress	2011
9,	Драган Плескоњић, Немања Мачек, Борислав Ђорђевић, Марко Царић	Сигунорст рачунарских система и мрежа	Микро књига	2007

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	3	0	3	0	0

Методе извођења наставе

Предавања; други облици наставе; консултације.

Оцена знања (максимални број поена 100)

Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Предметни пројекат	Да	50.00	Тест	Да	20.00
Присуство на предавањима	Да	5.00	Усмени део испита	Да	20.00
Присуство на вежбама	Да	5.00			

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	19.IB33 Анализа ризика и безбедност информација
Наставник/наставници:	Рикаловић М. Александар, Ванредни професор
Статус предмета:	Изборни
Број ЕСПБ:	6
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

Циљ предмета представља овладавање основним знањем из анализа ризика и безбедности информација у сврху свеобухватне заштите поверљивости информација система (предузећа). Основни циљ предмета је да мастер инжењер информационе безбедности стекне компентенције за управљање претњама по информациону безбедност система што подразумева:
- идентификацију претњи
- анализу рањивости
- дефинисање утицаја и процена вероватноће њихових појава
- планирање активности за минимизовање утицаја и вероватноће потенцијалних претњи и рањивости система.

Исход предмета

Студенти ће бити оспособљени за примену напредних статистичких и математичких метода за потребе Анализа ризика и безбедност информација.

Садржај предмета

Уводна разматрања. Изазови информационе безбедности у Индустрији 4.0. Анализа ризика и безбедности информација. Идентификација ризика. Праћење ризика. SWOT анализа и безбедности информација. Прогноза и предвиђање ризика. Напредне методе процене ризика. Управљање ризиком. Примери добре праксе.

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	Александар Рикаловић	Анализа ризика и безбедности информација - Електронска скрипта	ФТН, УНС	2019
2,	Domenic Antonucci	The Cyber Risk Handbook	Willey	2019
3,	Thomas R. Peltier	Information Security Risk Analysis	Taylor & Francis Group	2005
4,	Michael E. Whitman, Herbert J. Mattord	Management of Information Security	Management of Information Security	2016
5,	Lambert Paul	A user"s guide to data protection	London: Bloomsbury Professional	2018
6,	Maning. Christopher D.	An Introduction to Information Retrieval	Cambridge University Press	2009
7,	O"Brien, James A.	Management information systems	Boston: McGraw-Hill Irwin	2009
8,	Moeabito Vincenzo	Big data and analytics	Cham [Switzerland]: Springer	2015
9,	Heru Susanto, Mohammad Nabil Almunawar	Information Security Management Systems	Apple Academic Press	2018
10,	Бајагић, Младен	Улога и значај техничког метода у прикупљању обавештајних информација	Београд: Војнотехнички институт	2011

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	3	0	3	0	0

Методе извођења наставе

Настава на предмету обухвата предавања и рачунарске вежбе. Током семестра студент је обавезан да уради пројекат где ће применити стечена знања из области из анализа ризика и безбедности информација.

Оцена знања (максимални број поена 100)

Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Предметни пројекат	Да	40.00	Теоријски део испита	Да	50.00
Присуство на предавањима	Да	5.00			
Присуство на вежбама	Да	5.00			

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	17.E2501 Системи електронског плаћања
Наставник/наставници:	Сладић С. Горан, Редовни професор Видаковић П. Милан, Редовни професор
Статус предмета:	Изборни
Број ЕСПБ:	6
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

Упознавање студената са моделима и технологијама системима за електронско плаћање. Стицање знања и вештина за пројектовање одржавање система за електронско плаћање.

Исход предмета

Након успешно завршеног курса студент је у стању да примењује принципе, технологије и стандарде из области електронског плаћања у пројектовању и развоју различитих софтверских система електронског плаћања, као и да унапређује постојеће системе електронског плаћања.

Садржај предмета

Платни промет: организација, инструменти платног промета, домаћи и међународни платни промет, мреже за финансијску размену (TARGET, SWIFT), средства електронског платног промета. Платне картице: врсте, асоцијације за платне картице, поступак плаћања картицама, стандарди платних картица. Магнетне картице: стандарди, структура, садржај, коришћење, PIN кодови, напади на картице. Smart картице: структура, врсте, стандарди, организација, модули, фајл систем, кључеви, комуникација са картицом, Java smart картице, напади на картице. EVM стандард: намена, организација, фајл систем smart картица, представљање података, EMV трансакција. Крипто валуте: настанак, врсте, технологије, blockchain, консензус, дистрибуираност, трансакције, mining, безбедност. Онлине плаћања: опште карактерстике, 3D Secure. Мобилна плаћања: мобилни платни системи, модели плаћања, EMV мобиле стандард. Дигиталне валуте: опште карактеристике, типови и технологије криптовалута. Преваре у системима електронског плаћања: онлине преваре, еволуција, врсте превара, учесници у преварама, управљање превенцијом и заштитом од превара, технике за превенцију превара.

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	D. OMahony, M. Peirce, H. Tewari	Electronic Payment Systems for E-Commerce, 2nd edition	Artech House	2001
2,	C. Radu	Implementing Electronic Card Payment Systems	Artech House	2002
3,	W. Rankl	Smart Card Handbook, 2nd edition	Wiley and Sons	2004
4,	D. Montague	Essentials of Online Payment Security and Fraud Prevention	John Wiley and Sons	2011
5,	Bruce Schneier	Примењена криптографија: протоколи, алгоритми и изворни код на језику Ц, превод другог издања	Микро књига	2007
6,	EMVCo	EMV Specifications	EMVCo	2008
7,	Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder	Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction	Принцетон Университу Пресс	2016
8,	Andreas M. Antonopoulos	Mastering Bitcoin - Programming the Open Blockchain, 2nd eddition	OReilly	2017
9,	Gilberto Najera-Gutierrez, Juned Ahmed Ansari	KALI LINUX Тестирање непробојности веба III издање	КОМПЈУТЕР БИБЛИОТЕКА	2018

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	3	0	2	0	0

Методе извођења наставе

Предавања; Рачунарске вежбе; Консултације.
Испит је усмени. Оцена испита се формира на основу успеха са лабораторијских вежби и усменог испита.

Оцена знања (максимални број поена 100)

Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Одбрана пројекта	Да	50.00	Усмени део испита	Да	50.00

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	19.IB25 Анализа података у информационој безбедности
Наставник/наставници:	Варга Д. Ервин, Ванредни професор Лендак И. Имре, Ванредни професор
Статус предмета:	Изборни
Број ЕСПБ:	6
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

Циљ предмета Анализа података у информационој безбедности је да припреми студенте за успешно извођење радних задатака аналитичара информационе безбедности виших нивоа (Л2/Л3). Велика је потражња за експертима са знањем у овој области у различитим индустријама, нпр. финансијске инфраструктуре (нпр.. банке, оператори система кредитних картица), велике мултинационалне компаније, министарства и разни тимови за реакцију на инциденте.

Исход предмета

Студенти ће се упознати са различитим типовима података који се прикупљају у процесу надзора. Изучиће технике за прикупљање, иницијалну обраду и складиштење података. Упознаће се са решењима за анализу и визуелизацију података. Детаљно ће се упознати са разним техникама и изазовима у процесу детекције аномалија. Студенти ће се упознати са процесом рада модерних оперативних центара за надзор информационе безбедности.

Садржај предмета

Типови података у надзору система и мрежа. Пресретање мрежног саобраћаја. Редуковани, текстуални описи мрежног саобраћај. Подаци о комуникационим сесијама. Логови оперативних система и апликација. Дојаве о новим типовима инцидената. Механизми детекције и индикатори инцидената. Анализа података базирана на правилима и репутацији. Детекција аномалија статистичким методима. Детекција аномалија машинским учењем. Тимови за реакцију на инциденте. Анализа података и аутоматизација процеса у оперативним центрима за надзор информационе бебзедност.

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	Владимир Остојић, Татјана Лончар-Турукало	Практикум за рачунарске вежбе из дигиталне обраде слике	Нови Сад : Факултет техничких наука	2016
2,	Дарко Чапко, Срђан Вукмировић, Дубравка Бојанић	Одабрана поглавља из моделовања и симулације система у Матлабу	Нови Сад : Факултет техничких наука	2016
3,	Марин Гостимировић	База података обрадних процеса	Нови Сад : Факултет техничких наука	2013
4,	Драган Кукољ	Системи засновани на рачунарској интелигенцији	Нови Сад , Факултет техничких наука	2007
5,	Момчило Новковић	Нелинеарни модели временских серија : допринос теорији и пракси	Нови Сад : Факултет техничких наука	2002
6,	Chris Sanders, Jason Smith	Applied network security monitoring	Syngress	2014
7,	Leslie F. Sikos	AI in Cybersecurity	Springer	2018
8,	Clarence Chio, David Freeman	Machine Learning and Security: Protecting Systems with Data and Algorithms	OReilly Media	2018
9,	Sumeet Dua, Xian Du	Data mining and machine learning in cybersecurity	Auerbach Publications	2016
10,	Soma Halder	Hands-on Machine Learning for Cybersecurity	Packt Publishing	2018

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	3	0	3	0	0

Методе извођења наставе

Предавања; други облици наставе; консултације.

Стандард 05. - Курикулум

Оцена знања (максимални број поена 100)					
Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Предметни пројекат	Да	50.00	Тест	Да	20.00
Присуство на предавањима	Да	5.00	Усмени део испита	Да	20.00
Присуство на вежбама	Да	5.00			

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	19.IB34 Интеграција информационих система и API менаџмент
Наставник/наставници:	Вучковић С. Теодора, Доцент
Статус предмета:	Изборни
Број ЕСПБ:	6
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

Циљ предмета Интеграција информационих система и API менаџмент јесте овладавање основним знањем неопходним за разумевање потреба за интеграцијама великих система и значаја управљања програмима у процесима њиховог интегрисања, као и методама за спровођење тих процеса.

Исход предмета

Студенти ће се упознати са основним принципима и појмовима везаним за интеграције информационих система и, по завршетку курса, биће оспособљени да самостално испројектују комуникацију између више система програмирањем јединственог интерфејса који дефинише начин на који апликације размењују информације. Такође, студенти ће овладати коришћењем савремених алата за пројектовање интеграција и програмирање API-ја.

Садржај предмета

Основни појмови везани за интеграције, XML – eXtensible Markup Language, JSON – JavaScript Object Notation, RESTful веб сервиси, RAML – Representational State Transfer, Животни циклус API-ја, Упознавање са Anypoint Platformom и Anypoint Studiom, Прављење апликација у Anypoint Studiu, MEL – Mule Expression Language, Структурирање Mule апликација, Организација Mule апликација, Комуникација са веб сервисима, Обрада и праћење грешака, Управљање токовима порука, DataWeave транформације, Конектовање на додатне/екстерне ресурсе.

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	Лолић, Т., Стефановић, Д.	Интеграција информационих система и API менаџмент – уџбеник у припреми	ФТН	2020
2,	Лолић, Т., Стефановић, Д.	Интеграција информационих система: основни концепти – електронска скрипта	ФТН	2019
3,	Лолић, Т, Стефановић, Д.	Животни циклус API-ја – електронска скрипта	ФТН	2019
4,	SOA Software, Inc.	Building Successful APIs	SOA Software, Inc.	2012
5,	Dossot, D., C'Emic, J., Romero, V.	Mule in Action, 2nd edition	Manning	2014
6,	Carter, R.	Getting started with Mule Cloud Connect	OReilly	2012

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	3	0	3	0	0

Методе извођења наставе

Настава на предмету обухвата предавања са примерима развоја интеграција информационих система и објашњењима свих концепата који су саставни део процеса интегрисања. Вежбе су током целог периода извођења подржане рачунаром и кроз практичан, интерактиван рад на заједничком примеру, студенти примењују знања стечена на предавањима. Обавезним пројектним задатком студенти показују способност за самосталну практичну примену стеченог знања.

Оцена знања (максимални број поена 100)

Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Предметни(пројектни)задатак	Да	40.00	Практични део испита - задаци	Да	30.00
Тест	Да	30.00			

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	19.IB26 Безбедност рачунарства у облаку
Наставник/наставници:	Лендак И. Имре, Ванредни професор Селаков Ж. Александар, Ванредни професор
Статус предмета:	Изборни
Број ЕСПБ:	6
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

Циљ предмета је упознавање са новим изазовима на пољу информационе безбедности система која су у целости или делимично мигрирана у cloud, са посебним нагласком на специфичне проблеме употребе cloud-базираних решења у инфраструктурним системима. Сагледавање проблема на пољу безбедности података и сервиса у рачунарском облаку. Упознавање са правним оквиром и релевантним стандардима. Упознавање са функционисањем и активностима тела која учествују у развоју области информационе безбедности cloud-базираних система.

Исход предмета

Студенти су упознати са разликама на пољу информационе безбедности између традиционалних и cloud-базираних информационих система. Способност моделирања претњи у cloud окружењу. Стицање неопходног знања за развој безбедносне архитектуре cloud-базираних система. Способност одабира и примене одговарајућих мера у заштити података и сервиса у рачунарству у облаку. Познавање релевантних организација, стандарда и спецификација на пољу cloud-базираних система. Познавање међународног правног оквира који регулише активности чиниоца cloud-базираних система, нпр. пружаоца рачуарских услуга у облаку. Познавање напредних техника за управљање у рачунарским системима у облаку.

Садржај предмета

Основни концепти и развој безбедносне архитектуре cloud-базираних система. Заштита cloud дата центара. Платформа и инфраструктура. Безбедност података и сервиса. Управљање операцијама у cloud-базираном окружењу. Сигурност као сервис. Међународни правни оквир у регулисању приватности и безбедности cloud-базираних система. Релевантне организације, стандарди и спецификације у домену рачунарства у облаку.

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	Живко Бојовић, Јелена Шух, Емил Шећеров	Рачунарске мреже засноване на Интернет протоколу : практикум за лабораторијске вежбе	Нови Сад : Факултет техничких наука	2017
2,	Илија Башичевић, Мирослав Поповић, Владимир Ковачевић	Основе рачунарских мрежа 1	Нови Сад : Факултет техничких наука	2017
3,	Растислав Струхарик	Пројектовање сложених дигиталних система : рачунарске вежбе	Нови Сад : Факултет техничких наука	2017
4,	Гордана Милосављевић	Развој пословних информационих система вођен моделима	Нови Сад : Факултет техничких наука	2015
5,	Мирослав Хајдуковић	Оперативни системи (проблеми и структура)	Нови Сад : Факултет техничких наука	2013
6,	Samani R. & Reavis J.	CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security	Syngress	2014
7,	Beyer B., Jones C., Petoff J. and Murphy N.R.	Site Reliability Engineering (SRE)	OReilly	2016
8,	Krutz R.L. & Vines R.D.	Cloud Security: A Comprehensive Guide to Secure Cloud Computing	Wiley	2010

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	3	0	3	0	0

Методе извођења наставе

Предавања; Други облици наставе; консултације.

Стандард 05. - Курикулум

Оцена знања (максимални број поена 100)					
Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Предметни пројекат	Да	50.00	Писмени део испита - комбиновани задаци и теорија	Да	20.00
Присуство на вежбама	Да	5.00	Усмени део испита	Да	20.00
Присуство на вежбама	Да	5.00			

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	19.IB35 Управљање пројектима у информационој безбедности
Наставник/наставници:	Ћирић Лалић Д. Данијела, Доцент
Статус предмета:	Изборни
Број ЕСПБ:	6
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

Образовни циљ предмета представља овладавање основним знањем у подручју управљања пројектима. Предмет разматра концепте и знања о формалним поступцима управљања пројектима и примену великог броја алата, метода и техника потребних за ефективно и ефикасно управљање пројектом како би се резултати пројекта остварили у планирано време и са планираним средствима. Циљ предмета јесте и упознавање студената са концептом стратешког управљања пројектима и управљања стратегијом предузећа помоћу пројеката како би се оспособили за координацију и усмеравање пројеката у складу са постављеним захтевима и стратешким циљевима предузећа.
Циљ предмете је да дипломирани инжењер информационих технологија стекне компетенције за управљање пројектима информационе безбедности уз примену напредних алата и техника за управљање пројектима.

Исход предмета

Студенти који реализују предиспитне обавезе и положе испит ће бити оспособљени да: (1) разумеју значај управљања пројектима за остварење пословних циљева, (2) разумеју значај примене различитих алата и техника у управљању пројектима, (3) да буду оспособљени за примену великог броја алата, метода и техника потребних за ефективно и ефикасно управљање пројектом како би се резултати постигли у планирано време и са планираним средствима, (4) разумеју стратегију управљања предузећем помоћу пројеката, и да (6) прате и контролишу пројектни тим, буду флексибилност у превазилажењу потешкоћа, прилагођавању променама и да спроводе контролу над оствареним резултатима.

Садржај предмета

Основни појмови у управљању пројектима. Савремено управљање пројектима. Стандарди за управљање пројектима. Разлике између пројеката, програма и портфеља. Повезивање пројеката са стратегијом предузећа.Управљање интеграцијом.Управљање обимом. Управљање временом. Управљање трошковима. Управљање квалитетом. Управљање ресурсима. Управљање комуникацијом. Управљање ризицима. Управљање интересним странама. Преглед савремених алата и техника са подручјем примене у управљању пројектима.

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	Група аутора	Водич кроз корпус знања за управљање пројектима (PMBOK водич) четврто издање	PMBOK / ФТН	2010
2,	John M. Nicholas, Herman Steyn	Project Management for Business, Engineering, and Technology: Principles nad Practices	Elseiver	2008
3,	Project Management Institute, Group of Authors	A Guide to the Project Management Body of Knowledge (PMBOK Guide)	A Guide to the Project Management Body of Knowledge (PMBOK Guide)	2017
4,	Џеф Сатерланд	SCRUM-Уметност постизања дупло више за упола мање времена	Финеса	2018
5,	Livia Dana Beju	Project management	Faculty of Technical Sciences	2015
6,	Albert Lester	Project management, planning and control	Butterworth-Heinemann	2017
7,	David Cleden	Managing Project Uncertainty	Managing Project Uncertainty	2016
8,	Harvey Maylor	Project management	Pearson Education	2010

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	3	0	3	0	0

Методе извођења наставе

Настава на предмету обухвата предавања, интерактивног типа, на којима се дефинишу основни појмови у области управљања пројектима и даје теоријска подлога за примену напредних алата и техника у различитим подручјима примене у управљању пројектима. У оквиру вежби студенти раде на анализи студије случаја, симулацијама процеса управљања пројектима, групним дискусијама. Подстиче рад у групама и учење кроз игру.
Целокупне вежбе се одвијају уз помоћ рачунара.

Стандард 05. - Курикулум

Оцена знања (максимални број поена 100)					
Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Домаћи задатак	Да	10.00	Практични део испита - задаци	Да	30.00
Предметни(пројектни)задатак	Да	50.00			
Присуство на предавањима	Да	5.00			
Присуство на вежбама	Да	5.00			

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	19.SEM022 Увод у дигиталну форензику
Наставник/наставници:	Гостојић Л. Стеван, Редовни професор
Статус предмета:	Изборни
Број ЕСПБ:	6
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

(1) упознавање са основним концептима високотехнолошког криминала, дигиталне форензике и е-открића (2) стицање знања и вештина потребних за идентификацију, прикупљање, чување, анализу и презентацију дигиталних доказа коришћењем стандардизованих метода и софтверскинг алата и (3) упознавање са етичким начелима и прописима релевантним за дигиталну форензику и е-откриће.

Исход предмета

Након успешно завршеног курса студент (1) разуме основне концепте високотехнолошког криминала, дигиталне форензике и е-открића, (2) у стању је да као стручњак из области информационих технологија учествује у откривању, кривичном гоњењу и суђењу за кривична дела високотехнолошког криминала, (3) у стању је да користи стандардне методе и софтверске алате за форензику података, рачунарских комуникација, софтвера, мобилних уређаја и мултимедијалних записа и е-откриће и (6) разуме етичке аспекте дигиталне форензике и е-открића.

Садржај предмета

(1) преглед високотехнолошког криминала, дигиталне форензике и е-открића, (2) правни аспекти дигиталне форензике и е-открића, (3) форензика података (хардверски интерфејси, disk images, memory dumps, и криптоанализа), (4) форензика рачунарских комуникација (TCP/IP, HTTP, SMTP/POP3/IMAP, VoIP, бежичне рачунарске мреже), (5) форензика софтвера (системски софтвер, апликативни софтвер, СУБП), (6) форензика мобилних уређаја (хардвер мобилних уређаја, системски софтвер мобилних уређаја, мобилне апликације, SIM картице и мобилне комуникације), (7) форензика мултимедијалних записа (фотографије, звучни записи и видео записи), (8) е-откриће, (9) етички аспекти дигиталне форензике и е-открића и (10) примери из судске праксе.

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	Дражен Драгичевић	Компјутерски криминалитет и информацијски сустави	Информатор, Загреб	1999
2,	André Årnes	Digital Forensics	John Wiley & Sons Ltd	2018
3,	Quick, D., Martini, B., Choo, K.K.R.	Cloud Storage Forensics	Elsevier	2014
4,	Shiva V.N. Parasram	Digital Forensics with Kali Linux	Packt Publishing	2017
5,	Gerard Johansen	Digital Forensics and Incident Response	Packt Publishing	2017
6,	Sammons, J.(ed.)	Digital Forensics	Elsevier	2016

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	3	0	3	0	0

Методе извођења наставе

Облици извођења наставе су предавања, други облици наставе и консултације. На предавањима се излаже теоријски део градива уз стимулисање активног учествовања студената. Практични део градива студенти савлађују кроз друге облике наставе решавајући обавезне задатке уз помоћ извођача наставе. На консултацијама се студентима дају додатна објашњења садржаја излаганих на предавањима и вежбама.

Оцена знања (максимални број поена 100)

Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Одбрана пројекта	Да	50.00	Усмени део испита	Да	50.00

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	19.IB27 Безбедност критичних инфраструктура и индустријских система
Наставник/наставници:	Лендак И. Имре, Ванредни професор
Статус предмета:	Изборни
Број ЕСПБ:	6
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

Циљ предмета је стицање напредних знања о претњама и безбедносним мерама којима се штите инфраструктурни и индустријских системи. Анализа реалних напада на инфраструктурне системе. Упознавање са индустријским протоколима и техникама њиховог обезбеђивања. Упознавање са релевантним стандардима на пољу безбедности инфраструктурних система. Развој напредних решења за аутентификацију и контролу приступа. Развоје архитектуре информационе безбедности и безбедносног плана.

Исход предмета

Упознатост са детаљима најпознатијих напада на инфраструктурне системе. Способност развоја архитектуре информацине безбедности и примене адекватних безбедносних мера. Познавање релевантних стандарда на пољу безбедности инфраструктурних и индустријских система. Способност сопственог развоја дистрибуираних информационих система са применом напредних техника аутентификације и контроле приступа. Способност обезбеђивања комуникационих канала.

Садржај предмета

Приказ и анализа Stuxnet напада на нуклеарна постројења. Приказ и анализа кибер напада на електродистрибутивна предузећа у Украјини. Приказ и анализа осталих напада на инфраструктурне системе. Преглед релевантних стандарда на пољу информационе безбедности. Безбедност индустријских комуникационих протокола. Моделирање претњи у инфраструктурним системима. Архитектура информационе безбедности.

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	Дарко П. Марчетић, Марко А. Гецић, Борис П. Марчетић	Програмабилни логички контролери и комуникациони протоколи у електроенергетици	Нови Сад : Факултет техничких наука	2014
2,	Владимир Стрезоски	Систем регулације напона радијалних дистрибутивни мрежа	Нови Сад : Стулос	1997
3,	Страхил Ј. Гушавац	Основни принципи пројектовања у мрежама средњег и ниског напона	Нови Сад : Факултет техничких наука	2014
4,	Велимир Чонградац, Илија Каменко, Филип Кулић, Никола Јорговановић	Управљање процесима рачунаром кроз решене примере	Нови Сад : Факултет техничких наука	2013
5,	Владо Поробић	Програмабилни логички контролери и комуникациони протоколи у електроенергетици : примери са решењима	Нови Сад : Факултет техничких наука	2017
6,	Al-Sakib Khan Pathan	Securing Cyber-Physical Systems	CRC Press	2015
7,	Robert S. Radvanovsky, Allan McDougall	Critical Infrastructure: Homeland Security and Emergency Preparedness	CRC Press	2013
8,	George Loukas	Cyber-Physical Attacks: A Growing Invisible Threat	Butterworth-Heinemann	2015
9,	Scott Donaldson, Stanley Siegel, Chris K. Williams, Abdul Aslam	Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats	Apress	2015
10,	Clint Bodungen, Bryan Singer, Aaron Shbeeb, Kyle Wilhoit, Stephen Hilt	Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions	McGraw-Hill Education	2016

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	3	0	3	0	0

Методе извођења наставе

Предавања; други облици наставе; консултације.

Стандард 05. - Курикулум

Оцена знања (максимални број поена 100)					
Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Предметни пројекат	Да	50.00	Писмени део испита - комбиновани задаци и теорија	Да	20.00
Присуство на предавањима	Да	5.00	Усмени део испита	Да	20.00
Присуство на вежбама	Да	5.00			

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	19.IB36 Системи менаџмента безбедношћу и приватношћу података о личности
Наставник/наставници:	Делић М. Милан, Редовни професор Тасић З. Немања, Ванредни професор
Статус предмета:	Изборни
Број ЕСПБ:	6
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

Циљ предмета представља овладавање кључним знањима у подручју концепата система менаџмента безбедношћу и приватношћу података о личности, разумевање повезаности тих концепата са међународном и домаћом законском регулативом и водећим организационо-управљачким стандардима из области разматране проблематике, разумевање прилаза, метода и техника у обезбеђивању и очувању приватности података о личности, као и развој одговарајућих експертиза и компетенција код студената, у циљу интерпретације поменутих елемената, у контексту захтева, које организација мора да испуни, уз осврт на практичне аспекте метода и техника, планирања, имплементације, управљања, и развоја система, на организационом нивоу.

Исход предмета

Студенти ће бити оспособљени за пројектовање система мапирања података о личности, који укључује и идентификацију токова података, облика и начина појаве података о личности у организацији, уз осврт на принципе, методе и технике документовања поменутог. Коначно, студенти ће бити оспособљени и за пројектовање одговарајућих организационо-управљачких механизама заштите података о личности, узимајући у обзир захтеве законске регулативе и међународних организационо-управљачких стандарда из поменуте проблематике.

Садржај предмета

Уводни концепти, теоријске поставке и принципи система менаџмента безбедношћу и приватношћу података о личности, захтеви међународне законске регулативе, захтеви домаће законске регулативе, захтеви организационо-управљачких стандарда, иницирање и планирање имплементације система менаџмента безбедношћу и приватношћу података о личности у организацији, развој и имплементација поменутог система у организацији, развој и имплементација механизама управљања и контроле поменутог система, уз осврт на механизме континуалног побољшавања.

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	Бекер, И., Радловачки, В.	Систем управљања безбедношћу информација - скрипта	ИИС-Истраживачки и ехнолошки центар Нови Сад	2012
2,	Делић, М.	Интерне провере – Практикум за систем менаџмента безбедношћу информација – SRPS/ISO/IEC 27001:2014	ИИС-Истраживачки и технолошки центар Нови Сад	2017
3,	Voigt, P., Bussche, A.V.D.	The EU General Data Protection Regulation (GDPR) – A practical guide	Springer	2017
4,	EU - IT Governance Privacy Team	EU General Data Protection Regulation (GDPR) An Implementation and Compliance Guide	IT Governance Publishing	2017

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	3	0	3	0	0

Методе извођења наставе

Настава на предмету обухвата предавања наставне материје из области разматране проблематике, уз осврт на практичне примере у вези са начинима, методама и техникама имплеметације механизама мапирања, документовања, обезбеђивања, контроле и континуираног побољшавања система заштите података о личности. Обавезним пројектним задатком подстиче рад у групама, односно, тимски рад на имплементацији система менаџмента безбедношћу и приватношћу података о личности, на примеру одабране организације, од стране студентата, односно, чланова групе који раде на изради пројектног задатака.

Оцена знања (максимални број поена 100)

Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Предметни(пројектни)задатак	Да	40.00	Писмени део испита - комбиновани задаци и теорија	Да	50.00
Присуство на предавањима	Да	5.00			
Присуство на вежбама	Да	5.00			

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	19.IB37 Друштвени аспекти информационе безбедности
Наставник/наставници:	Бунчић М. Соња, Редовни професор Гостојић Л. Стеван, Редовни професор
Статус предмета:	Изборни
Број ЕСПБ:	6
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

Циљ предмета представља овладавање кључним знањима у области регулаторног и институционалног оквира информационе безбедности, што подразумева упознавање са међународним и националним нивом регулисања и успостављеног интитуционалног система информационе безбедности који значајно утичу на обликовање друштвених односа.

Исход предмета

Студенти ће стећи знања о настанку и развоју регулаторног и институционалног оквира на међународном, европском и националном нивоу, те оспособљени да прате степен усаглашености националног регулаторног/правног оквира информационе безбедности. Такође студенти ће бити оспособљени да индетификују законске оквире и институције овлашћене за систем информационе безбедности.

Садржај предмета

Увод у друштвени значај и историјски развој информационе безбедности.Општи оквир друштвених аспеката информационих система и мрежа.Интелектуална својина и правна заштита ауторских права у сајбер простору.Општи појмови и регулатрони оквир информационе бзбедности.Стратегија развоја информационе безбедности, међународни регулаторни и институционални оквир информационе безбеднсти .Европски правни и институционални оквир за регулисање информационе безбедност (најзначајније Директиве и стандарди). Национални регулаторни оквир ИБ, закон о информационој безбедности и његова примека.Подзаконски акти , уредбе , правилници, стандарди. Национална институционална структура-Центар за безбедност ИКТ система. Канцеларија за информационе технологије и електронску управу.Сарадња јавног и приватног сектора у области информационе безбедности. Злоупотреба информационих технологија и високо технолошки криминал у сајбер простору.

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	Прља Д, Релјановић М, Ивановић З	Интернет право	Правни факултет, Београд	2012
2,	Andrej Savin	EU Internet Law	Elgar European Law series	2020
3,	Petrovna Talimonchik V.	Legal Aspects of International Information Security	Intech Open	2018
4,	Група аутора	Право информационих технологија	Правни факултет, Службени Гласник, Београд	2012

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	3	3	0	0	0

Методе извођења наставе

Настава на предмету обухвата аудиторна предавања, уз примену нормативно-правног метода и активно учествовање студената у савладавању методских јединица применом интерактивног методом. Студије случајева.тимске презентације и дискусије обрађују се применом правно-аналитичког метода.

Оцена знања (максимални број поена 100)

Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Присуство на предавањима	Да	5.00	Писмени део испита - комбиновани задаци и теорија	Да	70.00
Присуство на вежбама	Да	5.00			
Пројектни задатак	Не	20.00			

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	19.SEM020 Безбедност и приватност Интернет ствари
Наставник/наставници:	Сладић С. Горан, Редовни професор
Статус предмета:	Изборни
Број ЕСПБ:	6
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

Оспособљавање студената за примену метода и техника за моделовање и имплементацију безбедносних аспеката система Интернет ствари уз заштиту и очување приватности коришћених података.

Исход предмета

Након успешно завршеног курса студенти су стекли теоријска и практична знања о инжењерингу безбедносних система Интернет ствари, заштити и очувању приватности коришћених података. Студенти су у стању да дизајнирају, имплементирају и евалуирају најсавременије безбедносне технике које се користе на уређајима од којих су сачињени IoT системи. Такође, студенти су у стању да разумеју различите безбедносне претње по системе Интернет ствари и методе за њихову детекцију, спречавање и ремедијацију.

Садржај предмета

Увод у инжењеринг безбедносних система Интернет ствари: дефиниција (предмет интересовања), основни појмови, безбедносни захтеви, типови уређаја и архитектура. Врсте напада: бежично прикупљање информација и мапирање, физички напади на уређаје, напади на протоколе, апликативни напади. Принципи безбедног инжењеринга у IoT: уграђивање безбедносних аспеката у дизајн и имплементацију, моделовање претњи, усклађеност са стандардима, надгледање система, пенетрационо тестирање, безбедносни тренинзи и едукација. Криптографија у IoT: алгоритми за енкрипцију, декрипцију, хеш функције, дигитални потписи, криптографске контроле уграђене у IoT комуникационе протоколе и протоколе за размену порука, размена кључева. Управљање идентитетом и контрола приступа у IoT: регистрација и животни циклус регистрованог уређаја, аутентификациони механизми, IoT IAM (Identity and Access Management) инфраструктура, шеме контроле приступа, модели веровања. Заштита података и очување приватности у IoT: изазови и захтеви за остваривање приватности података у IoT, процена утицаја дизајна на приватност података, шеме за заштиту приватности. Безбедно рачунарство у облаку намењено IoT: сервиси у облаку за IoT, безбедносне контроле сервиса у облаку за IoT, нови приступи у интеграцији рачунарства у облаку и Интернет ствари.

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	Edward Ashford Lee, Sanjit Arunkumar Seshia	Introduction to embedded systems: A cyber-physical systems approach	MIT Press	2017
2,	Knapp, E.D., Samani, R.	Applied Cyber Security and the Smart Grid	Elsevier	2013
3,	Brian Russell, Drew Van Duren	Practical Internet of Things Security	Packt Publishing	2016
4,	Tyson Macaulay	RIoT Control: Understanding and Managing Risks and the Internet of Things	Morgan Kaufmann - Elsevier	2016
5,	Li, S., Xu, L.D.	Securing the Internet of Things	Elsevier	2017
6,	Rosner, G.	Privacy and the Internet of Things	O Reilly	2017
7,	Knapp, E.D., Langill, J.T.	Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems	Elsevier	2015
8,	Wendell Odom	CCNA 200-301 Званични водич за сертификат, књига 1	КОМПЈУТЕР БИБЛИОТЕКА	2020
9,	Džejms Foršou	НАПАДИ НА МРЕЖНЕ ПРОТОКОЛЕ ХАКЕРСКИ ВОДИЧ	МИКРО КЊИГА	2018
10,	Dogan Ibrahim	RASPBERRY PI 3	АГЕНЦИЈА ЕХО	2014

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	3	0	3	0	0

Методе извођења наставе

Предавања; Рачунарске вежбе; Консултације. Испит је усмени. Оцена испита се формира на основу успеха са лабораторијских вежби и усменог испита.

Стандард 05. - Курикулум

Оцена знања (максимални број поена 100)					
Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Одбрана пројекта	Да	50.00	Усмени део испита	Да	50.00

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	19.IB53 Мастер рад - студијски истраживачки рад
Наставник/наставници:	-, -
Статус предмета:	Обавезан
Број ЕСПБ:	6
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

Примена основних, теоријско методолошких, научно-стручних и стручно-апликативних знања и метода на решавању конкретних проблема у оквиру изабраног подручја. У оквиру овог дела мастер рада студент изучава проблем, његову структуру и сложеност и на основу спроведених анализа изводи закључке о могућим начинима његовог решавања. Проучавајући литературу студент се упознаје са методама које су намењене за решавање сличних задатака и инжењерском праксом у њиховом решавању. Циљ активности студената у оквиру овог дела истраживања огледа се у стицању неопходних искустава кроз решавања комплексних проблема и задатака и препознавање могућности за примену претходно стечених знања у пракси.

Исход предмета

Оспособљавање студената да самостално примењују претходно стечена знања из различитих подручја које су претходно изучавали, ради сагледавања структуре задатог проблема и његовој системској анализи у циљу извођењу закључака о могућим правцима његовог решавања. Кроз самостално коришћење литературе, студенти проширују знања из изабраног подручја и проучавању различитих метода и радова који се односе на сличну проблематику. На тај начин, код студената се развија способност да спроводе анализе и идентификују проблеме у оквиру задате теме. Практичном применом стечених знања из различитих области код стуедената се развија способност да сагледају место и улогу инжењера у изабраном подручју, потребу за сарадњом са другим струкама и тимским радом.

Садржај предмета

Формира се појединачно у складу са потребама израде конкретног мастер рада, његовом сложеношћу и структуром. Студент проучава стручну литературу, дипломске и мастер радове студената који се баве сличном тематиком, врши анализе у циљу изналажења решења конкретног задатка који је дефинисан задатком мастер рада. Део наставе на предмету се одвија кроз самостални студијски истраживачки рад. Студијски рад обухвата и активно праћење примарних сазнања из теме рада, организацију и извођење експеримената, нумеричке симулације и статистичку обраду података, писање и/или саопштавање рада на конференцији из уже научно наставне области којој припада тема мастер рада.

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	група аутора	Одговарајући материјал неопходан за решавање конкретних проблема.		нема

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	0	0	0	8	0

Методе извођења наставе

Ментор мастер рада саставља задатак рада и доставља га студенту. Студент је обавезан да рад изради у оквиру задате теме која је дефинисана задатком мастер рада, користећи литературу предложену од ментора. Током израде мастер рада, ментор може давати додатна упутства студенту, упућивати на одређену литературу и додатно га усмеравати у циљу израде квалитетног мастер рада. У оквиру студијског истраживачког рада студент обавља консултације са ментором, а по потреби и са другим наставницима који се баве проблематиком из области теме самог рада. У оквиру задате теме, студент по потреби врши и одређена мерења, испитивања, бројања, анкете и друга истраживања, статистичку обраду података, ако је то предвиђено задатком мастер рада.

Оцена знања (максимални број поена 100)

Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Семинарски рад	Да	50.00	Усмени део испита	Да	50.00

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	19.IB51 Стручна пракса
Наставник/наставници:	-, -
Статус предмета:	Обавезан
Број ЕСПБ:	6
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

Стицање непосредних сазнања о функционисању и организацији предузећа и институција које се баве пословима у оквиру струке за коју се студент оспособљава и могућностима примене претходно стечених знања у пракси.

Исход предмета

Оспособљавање студената за примену претходно стечених теоријских и стручних знања за решавање конкретних практиних инжењерских проблема у оквиру изабраног предузећа или инситуције. Упознавање студената са делатностима изабраног предузећа или институције, начином пословања, управљањем и местом и улогом инжењера у њиховим организационим структурама.

Садржај предмета

Формира се за сваког кандидата посебно, у договору са руководством предузећа или институције у којима се обавља стручна пракса, а у складу са потребама струке за коју се студент оспособљава.

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	група аутора	Одговарајући материјал неопходан за решавање конкретних проблема		нема

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	0	0	0	0	6

Методе извођења наставе

Консултације и писање дневника стручне праксе у коме студент описује активности и послове које је обављао за време стручне праксе

Оцена знања (максимални број поена 100)

Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Домаћи задатак	Да	70.00	Теоријски део испита	Да	30.00

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм:	Информациона безбедност
Назив предмета:	19.IB54 Мастер рад - израда и одбрана
Наставник/наставници:	-, -
Статус предмета:	Обавезан
Број ЕСПБ:	6
Услов:	Нема
Предмети предуслови:	Нема

Циљ предмета

Циљ израде и одбране мастер рада је да студент покаже самосталан и креативан приступ у примени стечених практичних и теоријских знања из одговарајуће области у пракси у информационој безбедности. Оспособљавање студената за праћење литературе и истраживачки рад.

Исход предмета

Израдом и одбраном мастер рада студенти који су завршили студије треба да буду компетентни да решавају реалне проблеме из праксе као и да наставе школовање уколико се за то определе.
Мастер студент стиче темељно познавање и разумевање свих дисциплина информационе безбедности, као и способност решавања конкретних проблема уз употребу научних метода и поступака. Мастер студенти су способни да на одговарајући начин напишу и да презентују резултате свог рада. Свршени студенти овог нивоа студија поседују компетенцију за праћење и примену новина у струци, као и за сарадњу са локалним социјалним и међународним окружењем.

Садржај предмета

Информациона безбедност.

Литература

Р.бр.	Аутор	Назив	Издавач	Година
1,	група аутора	Одговарајући материјал неопходан за решавање конкретних проблема.		нема

Број часова активне наставе	Теоријска настава	Практична настава			Остало
		Вежбе	ДОН	СИР	
	0	0	0	0	4

Методе извођења наставе

Ментор за израду и одбрану мастер бира један од понуђених предмета из којег ће студент да ради дипломски-мастер рад и формулише тему са задацима за израду мастер рада. Кандидат у консултацијама са ментором самостално ради на проблему који му је задат. Након израде рада и сагласности ментора да је успешно урађен рад, кандидат брани рад пред комисијом која се састоји од најмање три члана од којих бар је један са другог департмана или факултета.

Оцена знања (максимални број поена 100)

Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Израда мастер рада	Да	50.00	Одбрана мастер рада	Да	50.00

Стандард 06. Квалитет, савременост и међународна усаглашеност студијског програма

Студијски програм је усаглашен са савременим светским научним токовима и стањем струке, а упоредив је са сличним програмима на иностраним високошколским установама.

Студијски програм Информациона безбедност, конципиран на дати начин, целовит је и свеобухватан и пружа студентима најновија научна и стручна знања из ове области.

Студијски програм Информациона безбедност је упоредив и усклађен са:
1. ETH (Switzerland): Masters Program in Information Security,
2. UCL (UK): Information Security M.Sc. и
3. Berkeley (USA), Master of Information and Cybersecurity.

Наставници, сарадници и студенти активно од 2011. године успешно учествују у европским пројектима за размену наставника, сарадника и студената у циљу подршке студирања у иностранству, као што је текући програм Еразмус+, који обухвата мрежу универзитета из Европске уније и земаља које се јој се придружују.

Стандард 07. Упис студената

Факултет техничких наука, расписује конкурс за упис кандидата на студијски програм мастер академских студија Информациона безбедност у складу са друштвеним потребама, својим слободним ресурсима и одобреним бројем студената. Број студената који ће бити уписани и начин финансирања њихових студија (буџет или самофинансирање) дефинише се сваке године посебном одлуком Наставно-научног већа Факултета техничких наука.

На конкурс за упис могу се пријавити кандидати који су завршили одговарајуће основне четворогодишње академске студије и које вреде најмање 240 ЕСПБ, што је и дефинисано у Правилнику о упису студената на студијске програме.

За све пријављене кандидате Комисија за квалитет студијског програма мастер академских студија Информациона безбедност врши вредновање студијског програма које су претходно завршили и доноси одлуку да ли је одговарајући за упис или не.

Кандидати који су, према мишљењу комисије, завршили одговарајући студијски програм стичу право уписа на мастер академске студије. Комисија за квалитет доноси одлуку да ли кандидати који су стекли право на упис полажу пријемни испит. Ако Комисија за квалитет донесе одлуку о полагању пријемног испита, тада кандидати полажу пријемни испит: Провера знања из области студијског програма.

Коначна ранг листа кандидата за упис се формира на основу успеха током претходног школовања, дужине трајања студија и постигнутог успеха на пријемном испиту, како је и дефинисано Правилником о упису студената на студијске програме.

Комисија, у складу са Правилником о упису студената на студијске програме, има право да одобри упис кандидатима који нису завршили одговарајуће основне академске студије у четворогодишњем трајању, а које вреде минимум 240 ЕСПБ, и то само у случају да остане слободних места након уписа свих кандидата који испуњавају услове постављене Конкурсом (одговарајуће основне академске студије, положен пријемни испит итд.). Кандидатима који, према стручном мишљењу Комисије, нису завршили одговарајући студијски програм основних академских студија може се одобрити упис уколико положе пријемни испит. Комисија у том случају одређује, за сваког кандидата посебно, разлику испита са основних академских студија које треба да положи. Збир ЕСПБ предмета који су одређени разликом не сме да прелази 30 (тридесет).

Чланови Комисије за квалитет су руководилац датог студијског програма и шефови свих катедри којима припадају предмети са датог студијског програма, или наставници које шефови тих катедри одреде, у складу са Правилником о упису студената на студијске програме.

Стандард 08. Оцењивање и напредовање студената

Коначна оцена на сваком од курсева овог програма се формира континуалним праћењем рада и постигнутих резултата студената током школске године и на завршном испиту.

Студент савлађује студијски програм полагањем испита, чиме стиче одређени број ЕСПБ бодова, у складу са студијским програмом. Сваки појединачни предмет у програму има одређени број ЕСПБ бодова који студент остварује када са успехом положи испит.

Број ЕСПБ бодова утврђен је на основу радног оптерећења студента у савлађивању одређеног предмета и применом јединствене методологије Факултета техничких наука за све студијске програме. Успешност студената у савлађивању одређеног предмета континуирано се прати током наставе и изражава се поенима. Максимални број поена које студент може да оствари на предмету је 100. Студент стиче поене на предмету кроз рад у настави и испуњавањем предиспитних обавеза и полагањем испита. Минимални број поена које студент може да стекне испуњавањем предиспитних обавеза током наставе је 30, а максимални 70.

Сваки предмет из студијског програма има јасан и објављен начин стицања поена. Начин стицања поена током извођења наставе укључује број поена које студент стиче по основу сваке појединачне врсте активности током наставе или извршавањем предиспитне обавезе и полагањем испита. Укупан успех студента на предмету изражава се оценом од 5 (није положио) до 10 (одличан). Оцена студента је заснована на укупном броју поена које је студент стекао испуњавањем предиспитних обавеза и полагањем испита, а према квалитету стечених знања и вештина.

Да би студент из датог предмета положио испит, мора да оствари најмање 51 поен.

Додатни услови за полагање испита су дефинисани посебно за сваки предмет. Напредовање студента током школовања је дефинисано Правилима студирања на мастер академским студијама.

Са изменом курикулума школске 2002/2003. године, уведен је и овакав начин оцењивања, који према нашим подацима обезбедио веома високу пролазност.

Стандард 09. Наставно особље

За реализацију студијског програма Информациона безбедност обезбеђено је наставно особље са потребним стручним и научним квалификацијама.

Број наставника одговара потребама студијског програма и зависи од броја предмета и броја часова на тим предметима. Укупан број наставника је довољан да покрије укупан број часова наставе на студијском програму, тако да наставник остварује просечно 180 часова активне наставе (предавања, консултације, вежбе и практичан рад) годишње, односно 6 часова недељно. Од укупног броја потребних наставника, преко 90% је у сталном радном односу са пуним радним временом.

Број сарадника одговара потребама студијског програма. Укупан број сарадника на студијском програму је довољан да покрије укупан број часова наставе на том програму, тако да сарадници остварују просечно 300 часова активне наставе годишње, односно 10 часова недељно.

Научне и стручне квалификације наставног особља одговарају образовно научном пољу и нивоу њихових задужења. Сваки наставник има најмање пет референци из уже научне, односно стручне области из које изводи наставу на студијском програму.

Величина групе за предавања је до 180 студената, групе за вежбе до 32 студената и групе за лабораторијске вежбе до 16 студената.

Ни један наставник није оптерећен више од 12 часова недељно. Сви подаци о наставницима и сарадницима (CV, избори у звања, референце итд.) су доступни јавности.

Стандард 10. Организациона и материјална средства

За извођење студијског програма обезбеђени су одговарајући људски, просторни, техничко-технолошки, библиотечки и други ресурси који су примерени карактеру студијског програма и предвиђеном броју студената. Настава на студијском програму Информациона безбедност се изводи у две смене тако да је по једном студенту обезбеђен минимум од 2 м2 простора.

Настава се изводи у амфитеатрима, учионицама и специјализованим лабораторијама.

Библиотека поседује више од 100 библиотечких јединица које су релевантне за извођење студијског програма Информациона безбедност. Сви предмети студијског програма Информациона безбедност су покривени одговарајућом уџбеничком литературом, училима и помоћним средствима који су расположиви на време и у довољном броју за нормално одвијање наставног процеса. При томе је обезбеђена и одговарајућа информациона подршка.

Факултет поседује библиотеку и читаоницу и обезбеђује за сваког студента место у амфитеатру, учионици и лабораторији.

Департман за рачунарство и аутоматику, Департман за енергетику, електронику и телекомуникације и Департман за индустријско инжењерство и менаџмент као одговорне организационе јединице за креирање и реализацију овог студијског програма, остварили је низ пројеката и других облика сарадње с реномираним светским компанијама и, кроз ту сарадњу, обезбедила савремену лабораторијску опрему. Неке од тих компанија су: Cirrus Logic, Imagination-MIPS, Sony, Philips, Nagra, Marvel, Onkyo, Pioneer, Google, Cisco, Ericsson, TTTech, Harman, Denso, Texas Instruments, Qualcomm, Leica, RT-RK и Schneider Electric. Студенти овог студијског програма имају прилику да, коришћењем те опреме, стекну савремена и високо тражена знања у областима информационе безбедности које студијски програм детаљно покрива.

Стандард 11. Контрола квалитета

Провера квалитета студијског програма се спроводи редовно и систематично путем самовредновања и спољашњом провером квалитета. Треба истаћи вишедеценијску праксу анкетирања студената.

Провера квалитета студијског програма се спроводи:
- анкетирањем студената на крају наставе из датог предмета;
- анкетирањем дипломираних студената при додели диплома о квалитету студијског програма и подршци студијама. Осим тога се процењује и комфор студирања (пре свега чистоћа и уредност учионица); и
- анкетирањем наставног и ненаставног особља о квалитету студијског програма и подршци студијама. У овој анкети се оцењује рад деканата, студентске службе, библиотеке, и осталих служби факултета.

За праћење квалитета студијског програма постоји комисија коју чине сви шефови катедри које учествују у реализацији студијског програма, један члан из ненаставног особља и бар један студент.

Стандард 11. - Контрола квалитета

Табела 11.1 Листа чланова комисије за контролу квалитета

Р.бр.	Име и презиме	Звање
1	Имре Лендак	Ванредни професор
2	Немања Тасић	Ванредни професор
3	Стеван Гостојић	Редовни професор
4	Братислав Радумило	Ненаставно особље
5	Мина Медић	Студент

Стандард 12. Студије на светском језику

Факултет поседује људске и материјалне ресурсе који омогућују да се наставни садржај _мастер академских студија на студијском програму Информациона безбедност може остварити у складу са стандардима на енглеском језику.

Наставници и ментори на академским студијама имају одговарајуће компетенције за извођење наставе на енглеском језику.

За извођење наставе на енглеском језику Факутет је обезбедио више од 100 библиотечких јединица на енглеском језику. Такође, Факултет поседује наставне материјале и учила прилагођена енглеском језику.

Студентске службе Факултета су оспособљене за давање услуга на енглеском језику.
Факултет обезбеђује да се све јавне исправе и административну документацију издају на обрасцима који се штампају двојезично, на српском језику ћириличним писмом и на енглеском језику.

Студенти који уписују мастер академске студије на студијском програму Информациона безбедност на енглеском језику морају поседовати задовољавајуће језичке компетенције из енглеског језика. Студент које се уписује на студије на енглеском језику приликом уписа потписује изјаву да има адекватно познавање енглеског језика. Овај навод се не доказује и не проверава посебно, али последице нетачности ове изјаве сноси сам студент.

Стандард 13. Заједнички студијски програм

-

Стандард 14. ИМТ програм

Студијски програм мастер академских студија Информациона безбедност су интердисциплинарне студије у оквиру техничко-технолошког поља.

Мултидисциплинарност овог студијског програма се огледа кроз предмете из области Електротехничко и рачунарско инжењерство и Индустријско инжењерство и инжењерски менаџмент.

Мултидисциплинарност је могуће остварити и кроз избор изборних предмета на овоме студијском програму, а поред тога студенту је уз сагласност руководиоца студијског програма, омогућено да изабере и слуша два предмета са било којег студијског прогарама Факултета техничких наука или неког другог факултета Универзитета у Новом Саду.

Стандард 15. Студије на даљину

-

Стандард 16. Студије у јединици без својства правног лица ван седишта установе

-