Факултет техничких наука

КЊИГА ПРЕДМЕТА
Информациона безбедност

Нови Сад

2026.

Садржај

КЊИГА ПРЕДМЕТА - Информациона безбедност

Наставни предмет	Примењена криптографија и криптоанализа
Ознака предмета: 25.IB21	
Број ЕСПБ: 6	
Програм(и) у којем се изводи	E2B - Информациона безбедност (MAC), Обавезан предмет
УНО предмета	Телекомуникације и обрада сигнала
Наставници:	Лендак И. Имре, Ванредни професор Ковачевић Н. Младен, Ванредни професор

Број часова активне наставе (недељно)

Предавања	Аудиторне вежбе	Други облици наставе	СИР/СТИР/ИР/ПИР/НИР	Остали часови
3.00	0.00	2.00	0.00	0.00

Предмети предуслови: Нема

Услови:

1. Образовни циљ:

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.

2. Исходи образовања (Стечена знања):

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.

3. Садржај/структура 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.

4. Методе извођења наставе:

Предавања; Други облици наставе; консултације.

Оцене 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			
Присуство на вежбама	Да	5.00	Усмени део испита	Да	20.00

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
1	Савић, Г., & Сегединац, М.	Софтверска инфраструктура за управљање курикулумом у електронској настави	Нови Сад: Факултет техничких наука	2016
2	Ивановић, Д., & Милосављевић, Б.	Управљање дигиталним документима	Нови Сад: Факултет техничких наука	2015
3	Милосављевић, Г.	Развој пословних информационих система вођен моделима	Нови Сад: Факултет техничких наука	2017
4	Хајдуковић, М.	Оперативни системи: проблеми и структура	Нови Сад: Факултет техничких наука	2013
5	Новковић, М.	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

КЊИГА ПРЕДМЕТА - Информациона безбедност

Наставни предмет	Безбедност рачунарских система
Ознака предмета: 25.IB12	
Број ЕСПБ: 6	
Програм(и) у којем се изводи	DR1 - Дистрибуирано рачунарство и информациони инжењеринг (МАС), Изборни предмет E2B - Информациона безбедност (МАС), Обавезан предмет
УНО предмета	Примењене рачунарске науке и информатика
Наставници:	Петровић Б. Вељко, Доцент Кордић С. Славица, Ванредни професор

Број часова активне наставе (недељно)

Предавања	Аудиторне вежбе	Други облици наставе	СИР/СТИР/ИР/ПИР/НИР	Остали часови
3.00	0.00	2.00	0.00	0.00

Предмети предуслови: Нема

Услови:

1. Образовни циљ:

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

2. Исходи образовања (Стечена знања):

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.

3. Садржај/структура 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

4. 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.

Оцене знања (максимални број поена 100)

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

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
1	Diogenes, Y., & Oyakawa, D.	Cybersecurity – Attack and Defense Strategies: Infrastructure Security with Red Team and Blue Team tactics (2nd ed.)	Packt Publishing	2019
2	Hadnagy, C.	Social Engineering: The Science of Human Hacking, 2nd Edition	Wiley	2018
3	Li, S., & Xu, L. D.	Securing the Internet of Things	Rockland: Syngress	2017
4	Bramwell, P.	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	Bosworth, S., Kabay, M. E., & Whyne, E.	Cybersecurity	Wiley	2014
7	Bhunia, S., & Tehranipoor, M.	Hardware Security: A Hands-on Learning Approach 1st Edition	Springer	2017
8	Li, S., & Xu, L. D.	Securing the Internet of Things	Rockland: Syngress	2017

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
9	Плескоњић, Д., Мачек, Н., Ђорђевић, Б., & Царић, М	Сигурност рачунарских система и мрежа	Београд: Микро књига	2007

КЊИГА ПРЕДМЕТА - Информациона безбедност

Наставни предмет	Систем управљања безбедношћу информација
Ознака предмета: 25.IB32	
Број ЕСПБ: 6	
Програм(и) у којем се изводи	E2B - Информациона безбедност (МАС), Обавезан предмет
УНО предмета	Квалитет, ефективност и логистика
Наставници:	Делић М. Милан, Редовни професор Гостојић Л. Стеван, Редовни професор

Број часова активне наставе (недељно)

Предавања	Аудиторне вежбе	Други облици наставе	СИР/СТИР/ИР/ПИР/НИР	Остали часови
3.00	0.00	2.00	0.00	0.00

Предмети предуслови: Нема

Услови:

1. Образовни циљ:

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.

2. Исходи образовања (Стечена знања):

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.

3. Садржај/структура 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.

4. Методе извођења наставе:

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

Оцене 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			

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
1	Бекер, И., & Радловачки, В.	Систем управљања безбедношћу информација - скрипта	Нови Сад: Истраживачки и технолошки центар	2012
2	Syngress Publishing, Inc.	Security + Study Guide & DVD Training System	Burlington: Syngress Media, Elsevier	2007
3	Tipton, H. F., & Krause, M. (Eds.)	Information Security Management Handbook (4th ed.)	CRC Press	2003
4	Andress, J.	The Basics of Information Security	Elsevier	2014
5	Talabis, C. D., & Jason, M.	Information Security Risk Assessment Toolkit	Elsevier	2013
6	Gardner, T. B., & Valerie	Building an Information Security Awareness Program	Elsevier	2014
7	Вулановић, В., Ходолич, Ј., Домазет, Д., & Марић, Б.	Методе и технике унапређења процеса рада	Нови Сад: Факултет техничких наука	2003

КЊИГА ПРЕДМЕТА - Информациона безбедност

Наставни предмет	Безбедан животни циклус софтвера
Ознака предмета: 25.ESI130	
Број ЕСПБ: 6	
Програм(и) у којем се изводи	E2B - Информациона безбедност (MAC), Изборни предмет
УНО предмета	Примењено софтверско инжењерство
Наставници:	Лендак И. Имре, Ванредни професор

Број часова активне наставе (недељно)

Предавања	Аудиторне вежбе	Други облици наставе	СИР/СТИР/ИР/ПИР/НИР	Остали часови
3.00	0.00	2.00	0.00	0.00

Предмети предуслови: Нема

Услови: Не постоје посебни услови за избор овог предмета.

1. Образовни циљ:

Циљ предмета је упознавање студената са различитим безбедносним изазовима у животном циклусу софтвера.

2. Исходи образовања (Стечена знања):

Студенти су упознати са кључним изазовима, односно различитим решењима у домену развоја безбедног софтвера.

3. Садржај/структура предмета:

Животни циклус безбедног софтвера; анализа ризика; руковање са рањивостима.

4. Методе извођења наставе:

Предавања и пројектни рад.

Оцене знања (максимални број поена 100)

Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Одбрана пројекта	Да	60.00	Усмени део испита	Да	40.00

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
1	Olmsted, A.	Secure Software Development	Packt Publishing	2024

КЊИГА ПРЕДМЕТА - Информациона безбедност

Наставни предмет	Безбедност рачунарских мрежа
Ознака предмета: 25.IB13	
Број ЕСПБ: 6	
Програм(и) у којем се изводи	E2B - Информациона безбедност (MAC), Изборни предмет
УНО предмета	Рачунарска техника и рачунарске комуникације
Наставници:	Поповић В. Мирослав, Редовни професор Башичевић Д. Илија, Редовни професор

Број часова активне наставе (недељно)

Предавања	Аудиторне вежбе	Други облици наставе	СИР/СТИР/ИР/ПИР/НИР	Остали часови
3.00	0.00	2.00	0.00	0.00

Предмети предуслови: Нема

Услови:

1. Образовни циљ:

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

2. Исходи образовања (Стечена знања):

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.

3. Садржај/структура предмета:

Увод у безбедност рачунарских мрежа, фазе и врста напада на рачунарске мреже, извиђање, скенирање, енумерација, прибављање приступа, малициозни софтвер, клијент-сервер аутентификација, преузимање сесије, уређаји за заштиту рачунарских мрежа, SQL напади, XSS напади, веб послужиоци и њихове рањивости, напади одбијањем услуге, безбедност мобилних уређаја, анонимност и приватност на Интернету, Tor систем, и напади на нивоу физичке архитектуре.

4. 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.

Оцене знања (максимални број поена 100)

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

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
1	Bejtlich, R.	The Practice of Network Security Monitoring: Understanding Incident Detection and Response	No Starch Press	2013
2	Douligeris, C., & Serpanos, D. N.	Network Security: Current Status and Future Directions		2007
3	Плескоњић, Д., Мачек, Н., Ђорђевић, Б., & Царић, М.	Сигурност рачунарских система и мрежа	Београд: Микро књига	2007
4	Башичевић, И., Поповић, М., & Ковачевић, В.	Основе рачунарских мрежа 1	Нови Сад: Факултет техничких наука	2017

КЊИГА ПРЕДМЕТА - Информациона безбедност

Наставни предмет	Друштвени аспекти информационе безбедности
Ознака предмета: 25.IB37	
Број ЕСПБ: 6	
Програм(и) у којем се изводи	E2B - Информациона безбедност (MAC), Изборни предмет
УНО предмета	Производни и услужни системи, организација и менаџмент
Наставници:	Бунчић М. Соња, Редовни професор

Број часова активне наставе (недељно)

Предавања	Аудиторне вежбе	Други облици наставе	СИР/СТИР/ИР/ПИР/НИР	Остали часови
3.00	0.00	2.00	0.00	0.00

Предмети предуслови: Нема

Услови:

1. Образовни циљ:

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.

2. Исходи образовања (Стечена знања):

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.

3. Садржај/структура 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 инфорамционе технологије и електронску управу.Сарадња јавног и приватног сектора у области информационе безбедности. Злоупотреба информационих технологија и високо технолошки криминал у сајбер простору.

4. 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.

Оцене 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	Да	20.00			

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
1	Прља, Д., Рељановић, М., & Ивановић, З.	Интернет право	Београд: Правни факултет	2012
2	Savin, A.	EU Internet Law	Elgar European Law series	2020
3	Talimonchik, V. P.	Legal Aspects of International Information Security	Intech Open	2018
4	Шаркић, Н., Прља, Д., Дамњановић, К., Марић, В., Живковић, В., Водинелић, В, & Мрвић Петровић, Н.	Право информационих технологија	Београд: Правни факултет Универзитета Унион: Службени гласник	2012

КЊИГА ПРЕДМЕТА - Информациона безбедност

Наставни предмет	Анализа ризика и безбедност информација
Ознака предмета: 25.IB33	
Број ЕСПБ: 6	
Програм(и) у којем се изводи	E2B - Информациона безбедност (MAC), Изборни предмет
УНО предмета	Производни и услужни системи, организација и менаџмент
Наставници:	Рикаловић М. Александар, Редовни професор

Број часова активне наставе (недељно)

Предавања	Аудиторне вежбе	Други облици наставе	СИР/СТИР/ИР/ПИР/НИР	Остали часови
3.00	0.00	2.00	0.00	0.00

Предмети предуслови: Нема

Услови:

1. Образовни циљ:

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.

2. Исходи образовања (Стечена знања):

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

3. Садржај/структура 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.

4. 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.

Оцене 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			

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
1	Рикаловић, А.	Анализа ризика и безбедности информација: електронска скрипта	Нови Сад: Факултет техничких наука	2019
2	Antonucci, D.	The Cyber Risk Handbook	Willey	2019
3	Peltier, T. R.	Information Security Risk Analysis	Taylor & Francis Group	2005
4	Whitman, M. E., & Mattord, H. J.	Management of Information Security	Management of Information Security	2016
5	Lambert, P.	A Users Guide to Data Protection	London: Bloomsbury Professional	2018
6	Manning, C., Raghavan, P., & Schütze, H.	An Introduction to Information Retrieval	Cambridge University Press	2009
7	O'Brien, J. A.v	Management Information Systems	Boston: McGraw-Hill Irwin	2009
8	Vincenzo, M.	Big data and analytics	Cham [Switzerland]: Springer	2015
9	Susanto, H., & Almunawar, M. N.	Information Security Management Systems: A Context-Aware Systems Approach	Apple Academic Press	2018

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
10	Бајагић, М.	Улога и значај техничког метода у прикупљању обавештајних информација	Војнотехнички институт	2011

КЊИГА ПРЕДМЕТА - Информациона безбедност

Наставни предмет	Информациона безбедност у инфраструктурним системима
Ознака предмета: 25.ESI096	
Број ЕСПБ: 6	
Програм(и) у којем се изводи	E2B - Информациона безбедност (MAC), Изборни предмет ES0 - Примењено софтверско инжењерство (MAC), Изборни предмет
УНО предмета	Примењено софтверско инжењерство
Наставници:	Лендак И. Имре, Ванредни професор

Број часова активне наставе (недељно)

Предавања	Аудиторне вежбе	Други облици наставе	СИР/СТИР/ИР/ПИР/НИР	Остали часови
3.00	3.00	0.00	0.00	0.00

Предмети предуслови: Нема

Услови:

1. Образовни циљ:

Циљ предмета је стицање основних знања о претњама и безбедносним мерама којима се штите инфраструктурни системи. Упознавање са најновијим трендовима и претњама у физичком и дигиталном домену. Развој решења за аутентификацију и контролу приступа. Упознавање са основама развоја безбедног софтвера. Решавање специфичних безбедносних проблема у домену инфраструктурних система.

2. Исходи образовања (Стечена знања):

Познавање историјата и најчешћих проблема на пољу информационе безбедности инфраструктурних система. Способност примене адекватних безбедносних мера у физичком и дигиталном домену. Способност разликовања различитих типова претњи у кибер простору. Способност развоја решења за аутентификацију и контролу приступа. Оспособљеност за сагледавање могућих претњи и развој безбедног изворног кода.

3. Садржај/структура предмета:

Увод и историјат информационе безбедности инфраструктурних система. Физичка безбедност. Безбедан људски елемент и социјални инжењеринг. Основни криптографски алгоритми и стандарди. Симетрични алгоритми. Асиметрични алгоритми. Једносмерне функције. Хомоморфни алгоритми. Упорена анализа приказаних алгоритама. Руковање са тајним кључевима. Дигитални потписи. Основе кванте криптографије. Идентификација, аутентификација и контрола права приступа. Безбедни комуникациони системи. Злонамеран софтвер. Основе моделирања претњи и развоја безбедног софтвера. Приватности правни аспекти информационе безбедности.

4. Методе извођења наставе:

Предавања; рачунарске вежбе; консултације.

Оцене знања (максимални број поена 100)

Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Одбрањене рачунарске вежбе	Да	25.00	Писмени део испита - комбиновани задаци и теорија	Да	20.00
Одбрањене рачунарске вежбе	Да	25.00			
Присуство на предавањима	Да	5.00	Теоријски део испита	Да	20.00
Присуство на рачунарским вежбама	Да	5.00			

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
1	Pfleeger, C., & Pfleeger, S.L.	Security in Computing	Prentice Hall	2015
2	Knapp, E. D., & Langill, J. T.	Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems	Elsevier	2015
3	Dooley, J. F.	History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms (History of Computing)	Springer	2018
4	Bhunia, S., & Tehranipoor, M.	Hardware Security: A Hands-on Learning Approach	Springer	2017
5	Donaldson, S., Siegel, S., Williams, C. K., & Aslam, A.	Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats	Apress	2015
6	Ransome, J., & Misra, A	Core Software Security : Security at the Source	Auerbach Publications	2013
7	Fisher, R. P.	Information systems security	Prentice-Hall	1984

КЊИГА ПРЕДМЕТА - Информациона безбедност

Наставни предмет	Системи електронског плаћања
Ознака предмета: 25.E2501	
Број ЕСПБ: 6	
Програм(и) у којем се изводи	E20 - Рачунарство и аутоматика (МАС), Изборни предмет E2B - Информациона безбедност (МАС), Изборни предмет
УНО предмета	Примењене рачунарске науке и информатика
Наставници:	Сладић С. Горан, Редовни професор Видаковић П. Милан, Редовни професор

Број часова активне наставе (недељно)

Предавања	Аудиторне вежбе	Други облици наставе	СИР/СТИР/ИР/ПИР/НИР	Остали часови
3.00	0.00	2.00	0.00	0.00

Предмети предуслови: Нема

Услови:

1. Образовни циљ:

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

2. Исходи образовања (Стечена знања):

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.

3. Садржај/структура 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. Безконтактне картице и NFC: принципи рада безконтактних картица и NFC. EVM стандард: намена, организација, фајл систем smart картица, представљање података, EMV трансакција. Онлине плаћања: опште карактеристике, 3D Secure. Мобилна плаћања: мобилни платни системи, модели плаћања, EMV мобилни стандард. Крипто валуте: настанак, врсте, технологије, опште карактеристике, blockchain, bitcoin, консензус, децентрализованост, дистрибуираност, трансакције, mining, безбедност. Типови и генерације blockchain технологија, принципи рада и намена.

4. Методе извођења наставе:

Предавања, рачунарске вежбе и консултације. Пројекат у оквиру кога се дизајнирају и имплементирају функционалности електронског плаћања за специфицирано софтверско решење. Испит је усмени. Оцена испита се формира на основу успеха пројекта и усменог испита.

Оцене знања (максимални број поена 100)

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

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
1	Mahony, D.O., Peirce, & M., Tewari, H.	Electronic Payment Systems for E-Commerce, 2nd edition	Artech House	2001
2	Rankl, W.	Smart Card Handbook, 2nd edition	Wiley and Sons	2004
3	EMVCo	EMV Specifications	EMVCo	2025
4	Antonopoulos, A.	Mastering Bitcoin: Programming the Open Blockchain	Sebastopol, CA: O'Reilly	2017
5	Narayanan, A.	Bitcoin and Cryptocurrency Technologies	Princeton: Princeton University Press	2016
6	Zheng, G.	Ethereum Smart Contract Development in Solidity	Singapore: Springer	2021
7	Grupa autora	Blockchain	Harvard Business Review	2024

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
8	Раденковић, Б., Деспотовић-Зракић, М., Богдановић, З., Бараћ, Д., & Лабус, А.	Електронско пословање	Београд: Факултет организационих наука	2015
9	Amus, S.	Bitkoin Standard	Best Practice	2024

КЊИГА ПРЕДМЕТА - Информациона безбедност

Наставни предмет	Системи менаџмента безбедношћу и приватношћу података о личности
Ознака предмета: 25.IB36	
Број ЕСПБ: 6	
Програм(и) у којем се изводи	E2B - Информациона безбедност (MAC), Изборни предмет
УНО предмета	Квалитет, ефективност и логистика
Наставници:	Делић М. Милан, Редовни професор

Број часова активне наставе (недељно)

Предавања	Аудиторне вежбе	Други облици наставе	СИР/СТИР/ИР/ПИР/НИР	Остали часови
3.00	0.00	3.00	0.00	0.00

Предмети предуслови: Нема

Услови:

1. Образовни циљ:

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.

2. Исходи образовања (Стечена знања):

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.

3. Садржај/структура 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.

4. 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.

Оцене 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			

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
1	Бекер, И., & Радловачки, В.	Систем управљања безбедношћу информација - скрипта	Нови Сад: Истраживачки и технолошки центар	2012
2	Делић, М.	Интерне провере – Практикум за систем менаџмента безбедношћу информација – SRPS/ISO/IEC 27001:2014	Нови Сад: ИИС-Истраживачки и технолошки центар	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

КЊИГА ПРЕДМЕТА - Информациона безбедност

Наставни предмет	Анализа података у информационој безбедности
Ознака предмета: 25.IB25	
Број ЕСПБ: 6	
Програм(и) у којем се изводи	E2B - Информациона безбедност (МАС), Изборни предмет
УНО предмета	Примењено софтверско инжењерство
Наставници:	Лендак И. Имре, Ванредни професор

Број часова активне наставе (недељно)

Предавања	Аудиторне вежбе	Други облици наставе	СИР/СТИР/ИР/ПИР/НИР	Остали часови
3.00	0.00	3.00	0.00	0.00

Предмети предуслови: Нема

Услови:

1. Образовни циљ:

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.

2. Исходи образовања (Стечена знања):

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.

3. Садржај/структура 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.

4. Методе извођења наставе:

Предавања; други облици наставе; консултације.

Оцене 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			

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
1	Остојић, В., & Лончар-Турукало, Т.	Практикум за рачунарске вежбе из дигиталне обраде слике	Нови Сад: Факултет техничких наука	2016
2	Чапко, Д., Вукмировић, С., & Бојанић, Д.	Одабрана поглавља из моделовања и симулације система у Матлабу	Нови Сад: Факултет техничких наука	2016
3	Гостимировић, М.	База података обрадних процеса	Нови Сад: Факултет техничких наука	2013
4	Кукољ, Д.	Системи засновани на рачунарској интелигенцији	Нови Сад: Факултет техничких наука	2007
5	Новковић, М.	Нелинеарни модели временских серија: допринос теорији и пракси	Нови Сад: Факултет техничких наука	2002
6	Sanders, Ch., & Smith, J.	Applied Network Security Monitoring	Amsterdam; Boston: Syngress, an Imprint of Elsevier	2014
7	Sikos, L. F.	AI in Cybersecurity	Springer	2018
8	Chio, C., & Freeman, D.	Machine Learning and Security: Protecting Systems with Data and Algorithms	O Reilly Media	2018
9	Sumeet Dua, S., & Du, X.	Data Mining and Machine learning in Cybersecurity	Auerbach Publications	2016

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
10	Halder, S.	Hands-on Machine Learning for Cybersecurity	Packt Publishing	2018

КЊИГА ПРЕДМЕТА - Информациона безбедност

Наставни предмет	Дигитална форензика
Ознака предмета: 25.RVO05T	
Број ЕСПБ: 6	
Програм(и) у којем се изводи	E20 - Рачунарство и аутоматика (МАС), Изборни предмет E2B - Информациона безбедност (МАС), Изборни предмет
УНО предмета	Примењене рачунарске науке и информатика
Наставници:	Гостојић Л. Стеван, Редовни професор

Број часова активне наставе (недељно)

Предавања	Аудиторне вежбе	Други облици наставе	СИР/СТИР/ИР/ПИР/НИР	Остали часови
3.00	0.00	3.00	0.00	0.00

Предмети предуслови: Нема

Услови:

1. Образовни циљ:

Стицање општих знања о концептима, принципима и процесу дигиталне форензике. Стицање посебних знања о концептима, техникама и алатима појединачних области дигиталне форензике. Упознавање са етичким и правним начелима дигиталне форензике.

2. Исходи образовања (Стечена знања):

Након успешно завршеног курса студент је у стању да користи стандардне методе и алате за форензику рачунара, рачунарских мрежа, мобилних телефона и мултимедијалних записа и способан је да као стручњак из области информационих технологија учествује у кривичном поступку.

3. Садржај/структура предмета:

Теоријска настава
Основни концепти и принципи дигиталне форензике. Процес дигиталне форензике. Форензика рачунара (форензика масовне меморије, форензика радне меморије, форензика оперативних система и форензика апликација). Форензика рачунарских мрежа. Форензика мобилних телефона. Форензика мултимедијалних записа. Форензика криптовалута. Доказне радње за прикупљање и извођење дигиталних доказа.

Практична настава
Методе и алати за прикупљање, прегледање и анализу дигиталних трагова ускладиштених или преношених у дигиталном облику.

4. Методе извођења наставе:

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

Оцене знања (максимални број поена 100)

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

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
1	Милосављевић, М. & Грубор, Г.	Дигитална форензика рачунарског система	Београд: Сингидунум	2009
2	Årnes, A.	Digital Forensics: An Academic Introduction	John Wiley & Sons	2018
3	Kävrestad, J., Birath, M., & Clarke, N.	Fundamentals of Digital Forensics: A Guide to Theory, Research and Applications (Third Edition)	Springer	2024
4	Parasram, S.	Digital Forensics with Kali Linux	Packt Publishing	2017
5	Johansen, G.	Digital Forensics and Incident Response	Packt Publishing	2017

КЊИГА ПРЕДМЕТА - Информациона безбедност

Наставни предмет	Безбедност рачунарства у облаку
Ознака предмета: 25.IB26	
Број ЕСПБ: 6	
Програм(и) у којем се изводи	E2B - Информациона безбедност (MAC), Изборни предмет
УНО предмета	Примењено софтверско инжењерство
Наставници:	Јелачић П. Бојан, Доцент

Број часова активне наставе (недељно)				
Предавања	Аудиторне вежбе	Други облици наставе	СИР/СТИР/ИР/ПИР/НИР	Остали часови
3.00	0.00	3.00	0.00	0.00

Предмети предуслови: Нема

Услови:

1. Образовни циљ:

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.

2. Исходи образовања (Стечена знања):

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.

3. Садржај/структура 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.

4. Методе извођења наставе:

Предавања; Други облици наставе; консултације.

Оцене 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			
Присуство на вежбама	Да	5.00	Усмени део испита	Да	20.00

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
1	Бојовић, Ж., Шух, Ј., & Шеђеров, Е.	Рачунарске мреже засноване на Интернет протоколу: практикум за лабораторијске вежбе	Нови Сад: Факултет техничких наука	2017
2	Башичевић, И., Поповић, М., & Ковачевић, В.	Основе рачунарских мрежа 1	Нови Сад: Факултет техничких наука	2017
3	Струхарик, Р.	Пројектовање сложених дигиталних система: рачунарске вежбе	Нови Сад: Факултет техничких наука	2017
4	Милосављевић, Г.	Развој пословних информационих система вођен моделима	Нови Сад: Факултет техничких наука	2015
5	Хајдуковић, М.	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

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
7	Beyer, B., Jones, C., Petoff, J. & 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

КЊИГА ПРЕДМЕТА - Информациона безбедност

Наставни предмет	Методе и технике научног рада
Ознака предмета: 25.IB38	
Број ЕСПБ: 6	
Програм(и) у којем се изводи	E2B - Информациона безбедност (MAC), Изборни предмет
УНО предмета	Квалитет, ефективност и логистика
Наставници:	Делић М. Милан, Редовни професор Гостојић Л. Стеван, Редовни професор

Број часова активне наставе (недељно)

Предавања	Аудиторне вежбе	Други облици наставе	СИР/СТИР/ИР/ПИР/НИР	Остали часови
3.00	0.00	3.00	0.00	0.00

Предмети предуслови: Нема

Услови:

1. Образовни циљ:

Циљ предмета је да се студенти практично оспособе за научно-истраживачки рад. Студентима се пружају практична знања у вези са методама, техникама и поступцима претраге база података, индексних база и агрегатора електонских часописа, летимичног и детаљног прегледа, читања и анализирања разних облика стручних и академских публикација, као и синтезе тих публикација у циљу идентификације и уочавања трендова, кључних питања и мишљења, како академске, тако и стручне јавности. Поред тога, студент се упозаје са појмом, значајем и практичним аспектима примене основних метода прикупљања истраживачких података, математичке статистике и статистичког закључивања у научно-истраживаком процесу. Закључно, студент се упознаје са етичким пинципима научног и истраживачког рада.

2. Исходи образовања (Стечена знања):

Након одслушаног предмета и положеног испита, студент ће бити у стању да дефинише циљ истраживања, потребу за истраживањем, истраживачки проблем, истраживачки оквир и модел истраживања. Студент ће бити у стању да, уз примену основних метода математичке статистике поменуте елементе анализира, статистички закључује и пружи одговоре на постављена истраживачка питања.

3. Садржај/структура предмета:

Увод у метод научног рада, основни појмови, дефинисање појма циља истраживања, потребе за истраживањем и истраживачкг проблема, врсте и типови истраживачких, научних и стручних публикација, методе и технике претраге база података, индексних база и агрегатора електонских часописа, методе и технике летимичног и детаљног прегледа, читања и анализирања стручних и академских публикација, синтеза стручних и академских публикација, примена основних метода математичке статистичке и статисичког закључивања у истраживањима, структура и начини приказивања резултата истраживања, структура и писање истраживачких публикација. Осврт на етичке принципе при писању и публиковању истраживачких публикација.

4. Методе извођења наставе:

Предавања, студијски и истраживачки рад, консултације. Оцена се формира на основу успеха из испитног задатка и усменог дела испита.

Оцене знања (максимални број поена 100)

Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Предметни пројекат	Да	50.00	Завршни испит	Да	50.00

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
1	Petticrew, M., & Roberts, H.	Systematic Reviews in the Social Sciences: A Practical Guide	Blackwell Publishing	2006
2	Jesson, J. K., Matheson, L., & Lacey, F.M.	Doing Your Literature Review: Traditional and Systematic Techniques	SAGE Publications Ltd	2011
3	Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E.	Multivariate Data Analysis	Pearson Prentice Hall	2010
4	Cargill, M., & O`Conor, P.	Writing Scientific Research Articles: Strategy and Steps	John Wiley & Sons	2009
5	Делић, М	Менаџмент квалитетом и примена информационих технологија: Комбиновани утицај на перформансе организације	Нови Сад: Факултет техничких наука	2017
6	Ристић, Ж.	Квантитативна, квалитативна и мешовита истраживања: методолошки аспекти	Нови Сад: Универзитет у Новом Саду	2011

КЊИГА ПРЕДМЕТА - Информациона безбедност

Наставни предмет	Реаговање на безбедносне инциденте
Ознака предмета: 25.E2544	
Број ЕСПБ: 6	
Програм(и) у којем се изводи	E20 - Рачунарство и аутоматика (МАС), Изборни предмет E2B - Информациона безбедност (МАС), Изборни предмет
УНО предмета	Примењене рачунарске науке и информатика
Наставници:	Гостојић Л. Стеван, Редовни професор

Број часова активне наставе (недељно)

Предавања	Аудиторне вежбе	Други облици наставе	СИР/СТИР/ИР/ПИР/НИР	Остали часови
3.00	0.00	3.00	0.00	0.00

Предмети предуслови: Нема

Услови:

1. Образовни циљ:

Стицање општих знања о концептима, принципима и процесу реаговања на безбедносне инциденте. Стицање посебних знања и вештина потребних за коришћење метода и алата у реаговању на безбедносне инциденте. Упознавање са етичким и правним начелима дигиталне форензике.

2. Исходи образовања (Стечена знања):

Након успешно завршеног курса студент је у стању да користи стандардне методе и алате за реаговање не безбедносне инциденте и способан је да као стручњак из области информационих технологија учествује у реаговању на безбедносне инциденте.

3. Садржај/структура предмета:

(1) увод у управљање инцидентима нарушавања информационе безбедности (основни појмови, дефиниција и циљ, процес и етички принципи), (2) профили нападача, (3) прописи и стандарди, (4) припрема и планирање реаговања на инциденте, (5) модели реаговања на инциденте, (6) категоризација инцидената, (7) реаговање на инциденте – идентификација и детекција инцидента, (8) реаговање на инциденте – прекид пропагације инцидента, (9) реаговање на инциденте – ерадикација и опоравак система, (10) анализа малвера у реаговању на инциденте, (11) реаговање на инциденте у облаку и (12) ,,.лов на претње".

4. Методе извођења наставе:

Облици извођења наставе су: предавања, други облици наставе (рачунарске вежбе) и консултације. На предавањима се излажу садржаји предмета уз стимулисање активног учествовања студената. Практични део градива студенти савлађују кроз друге облике наставе решавајући задатке уз помоћ извођача наставе или самостално. На консултацијама се студентима дају додатна објашњења садржаја излаганих на предавањима и кроз друге облике наставе.

Оцене знања (максимални број поена 100)

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

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
1	Johansen, G.	Digital Forensics and Incident Response	Packt Publishing	2017
2	Martinez, R.	Incident Response with Threat Intelligence: Practical insights into developing an incident response capability through intelligence-based threat hunting	Packt Publishing	2022
3	Thompson, E. C.	Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents	Apress	2018
4	Brown, R., & Roberts, S. J.	Intelligence-Driven Incident Response	O'Reilly Media	2023
5	Ozkaya, E.	Incident Response in the Age of Cloud: Techniques and best practices to effectively respond to cybersecurity incidents	Packt Publishing	2021

КЊИГА ПРЕДМЕТА - Информациона безбедност

Стручна пракса	Стручна пракса
Ознака предмета: 25.IB51	
Број ЕСПБ: 6	
Програм(и) у којем се изводи	E2B - Информациона безбедност (МАС), Обавезан предмет
УНО предмета	Информационо-комуникациони системи Примењене рачунарске науке и информатика
Наставници:	

Број часова активне наставе (недељно)

Предавања	Аудиторне вежбе	Други облици наставе	СИР/СТИР/ИР/ПИР/НИР	Остали часови
0.00	0.00	0.00	0.00	6.00

Предмети предуслови: Нема

Услови:

1. Образовни циљ:

Стицање увида у функционисање предузећа/институција и примену стечених знања у реалном окружењу.

2. Исходи образовања (Стечена знања):

Развијање способности примене теоријских и стручних знања при решавању практичних инжењерско-менаџерских задатака. Упознавање са организацијом, делатношћу и улогом инжењера у пракси.

3. Садржај/структура предмета:

Дефинише се индивидуално, у сарадњи са предузећем/институцијом у којој се пракса реализује.

4. Методе извођења наставе:

Практичан рад, консултације и израда дневника праксе.

Оцене знања (максимални број поена 100)

Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Домаћи задатак	Да	50.00	Теоријски део испита	Да	50.00

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
1	Сви аутори / Група аутора	Одговарајући материјал неопходан за решавање конкретних проблема		-
2	All authors / Author group	Appropriate material necessary to solve specific problems		-

КЊИГА ПРЕДМЕТА - Информациона безбедност

Предмет завршног рада	Мастер рад - студијски истраживачки рад
Ознака предмета: 25.IB53	
Број ЕСПБ: 6	
Програм(и) у којем се изводи	E2B - Информациона безбедност (МАС), Обавезан предмет
УНО предмета	Информационо-комуникациони системи Примењене рачунарске науке и информатика
Наставници:	

Број часова активне наставе (недељно)

Предавања	Аудиторне вежбе	Други облици наставе	СИР/СТИР/ИР/ПИР/НИР	Остали часови
0.00	0.00	0.00	8.00	0.00

Предмети предуслови: Нема

Услови:

1. Образовни циљ:

Примена основних, теоријско-методолошких, научно-стручних и стручно-апликативних знања и метода на решавању конкретних проблема у оквиру изабране области. Студент анализира проблем, његову структуру и сложеност, и на основу спроведених анализа изводи закључке о могућим начинима његовог решавања.

2. Исходи образовања (Стечена знања):

Оспособљавање студента за самосталну примену стечених знања у системској анализи проблема и дефинисању могућих решења. Развијање способности анализе, идентификације проблема и препознавања улоге инжењера у пракси.

3. Садржај/структура предмета:

Формира се у складу са темом завршног рада. Студент проучава литературу, радове и примере и врши анализу ради проналажења решења.

4. Методе извођења наставе:

Ментор формулише задатак, даје смернице и врши праћење напретка. По потреби студент изводи мерења, истраживања или анкете.

Оцене знања (максимални број поена 100)

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

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
1	Сви аутори / Група аутора	Актуелни часописи свих година издавања и одбрањени завршни радови из дате области		-
2	All authors / Author group	Current journals of all years of publication and defended final theses in the given field		-

КЊИГА ПРЕДМЕТА - Информациона безбедност

Завршни рад	Мастер рад - израда и одбрана
Ознака предмета: 25.IB54	
Број ЕСПБ: 6	
Програм(и) у којем се изводи	E2B - Информациона безбедност (МАС), Обавезан предмет
УНО предмета	Информационо-комуникациони системи Примењене рачунарске науке и информатика
Наставници:	

Број часова активне наставе (недељно)

Предавања	Аудиторне вежбе	Други облици наставе	СИР/СТИР/ИР/ПИР/НИР	Остали часови
0.00	0.00	0.00	0.00	4.00

Предмети предуслови: Нема

Услови:

1. Образовни циљ:

Pokazivanje sposobnosti primene teorijskih i praktičnih znanja u realnom okruženju.

2. Исходи образовања (Стечена знања):

Razvijanje sposobnosti rešavanja problema, kritičkog mišljenja, analize i sinteze, kao i primene IKT alata u stručnoj oblasti.

3. Садржај/структура предмета:

Formira se pojedinačno u skladu sa tematikom. Rad se priprema u saradnji sa mentorom i brani javno.

4. Методе извођења наставе:

Mentor definiše temu i zadatke. Student radi samostalno uz konsultacije, a rad se brani pred komisijom.

Оцене 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

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
1	Сви аутори / Група аутора	Актуелни часописи свих година издавања и одбрањени завршни радови из дате области		-
2	All authors / Author group	Current journals of all years of publication and defended final theses in the given field		-