EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Vybrané části žádosti o akreditaci určené ke zveřejnění v Databázi výstupů projektů OP VVV

Označení příjemce:	Vysoké učení technické v Brně
Název projektu:	Vytvoření double-degree doktorského studijního programu Elektronika a informační technologie a vytvoření doktorského studijního programu Informační bezpečnost
Reg. č. projektu	CZ.02.2.69/0.0/0.0/16_018/0002575
Studijní program	Informační bezpečnost (DPC-IBE)

Následující dokument zahrnuje části A a B žádosti o akreditaci doktorského studijního programu Informační bezpečnost (DPC-IBE). Slouží ke zveřejnění dílčích výstupů uvedených v příloze projektové žádosti Přehled klíčových výstupů k naplnění indikátorů projektu ESF.

- Profil studijního programu na str. 2 (poslední odstavec)
- Klíčové výsledky učení na str. 3 (část Cíle studia ve studijním programu)
- Profesní profil absolventů na str. 3 (část Profil absolventa studijního programu)
- Přehled studijních povinností na str. 5
- Struktura předmětů na str. 6 – 13
- Detailní informace o předmětech na str. 6 – 13

A-I – Základní informace o žádosti o akreditaci

Název vysoké školy:

Vysoké učení technické v Brně

Název součásti vysoké školy:

Fakulta elektrotechniky a komunikačních technologií

Název spolupracující instituce:

Název studijního programu:

Informační bezpečnost

Typ žádosti o akreditaci:

udělení akreditace

Schvalující orgán:

Rada pro vnitřní hodnocení VUT

Datum schválení:

0

Odkaz na elektronickou podobu žádosti:

https://www.vutbr.cz/www_base/vutdisk.php?i=166501a2ec, heslo PhD2021_IBE

Odkazy na relevantní vnitřní předpisy:

https://www.vutbr.cz/uredni-deska/akreditace

ISCED F a stručné zdůvodnění:

0688 Interdisciplinární programy a kvalifikace zahrnující informační a komunikační technologie (ICT)
Studijní program je orientován do oblastí návrhu nových bezpečnostních zařízení a systémů určených především pro drátové a bezdrátové komunikační a mobilní technologie se zaměřením na zpracování dat, ochrany a zabezpečení přenášených informací, návrhu a použití kryptografických systémů a problematiku kybernetické bezpečnosti.

B-I – Charakteristika studijního programu

Název studijního programu	Informační bezpečnost		
Typ studijního programu	doktorský		
Profil studijního programu			
Forma studia	prezenční i kombinované studium		
Standardní doba studia	4		
Jazyk studia	čeština		
Udělovaný akademický titul	Ph.D.		
Rigorózní řízení	ne	**Udělovaný akademický titul**	
Garant studijního programu	Koton Jaroslav, doc. Ing., Ph.D.		
Zaměření na přípravu k výkonu regulovaného povolání	ne		
Zaměření na přípravu odborníků z oblasti bezpečnosti České republiky	ne		
Uznávací orgán			

Oblast(i) vzdělávání a u kombinovaného studijního programu podíl jednotlivých oblastí vzdělávání v %

Elektrotechnika 100%, Bez tematického okruhu, 100%

Cíle studia ve studijním programu

Doktorand se naučí tvůrčím způsobem využívat nabyté teoretické znalosti při návrhu nových bezpečnostních zařízení a systémů. Orientuje se ve zpracování dat, v návrhu a použití kryptografických systémů a v problematice kybernetické bezpečnosti. Vyzná se v telekomunikačních systémech, v zabezpečení přenosu proti chybám, v synchronizaci sítí. Umí připravovat nové služby a technicky řešit problémy s tím spojené.

Profil absolventa studijního programu

Studijní obor je zaměřen na vědeckou výchovu doktorandů s hlubokými znalostmi teorie sdělování, přenosu informací, jejich zabezpečení, principy kryptografie a systémové bezpečnosti. Hlavní části studia tvoří předměty aplikované matematiky, teorie sdělování, uchování dat, a telekomunikační techniky. Absolvent má široké znalosti komunikačních a informačních technologií, datových přenosů a jejich zabezpečení, včetně užití i návrhu software s tím spojeným. Je schopen se orientovat v moderních šifrách a kryptografických protokolech, ověřit jejich bezpečnost a navrhnout jejich konkrétní využití v komunikačních systémech. Na aplikační úrovni se velmi dobře orientuje v problematice operačních systémů, databázových systémů, metod statistické analýzy, distribuovaných aplikací apod. Na vysoké úrovni zvládá algoritmizaci úloh. Je schopen navrhovat nová technologická řešení komunikačních, informačních a podpůrných služeb s ohledem za zajištění vysoké míry bezpečnosti. Je schopen porozumět a sám navrhovat moderní komunikační systémy zajišťující kybernetickou bezpečnost.

Pravidla a podmínky pro tvorbu studijních plánů

Studium doktoranda probíhá podle individuálního studijního plánu (dále jen ISP), který zpracuje v úvodu studia školitel doktoranda ve spolupráci s doktorandem. Individuální studijní plán je pro doktoranda závazný. Jsou v něm specifikovány všechny povinnosti stanovené v souladu se Studijním a zkušebním řádem VUT, které musí doktorand k úspěšnému ukončení studia splnit. Tyto povinnosti jsou časově rozvrženy do celého období studia, jsou bodově ohodnoceny a v pevně daných termínech probíhá kontrola jejich plnění. Průběžné bodové hodnocení všech aktivit doktoranda je vedeno v dokumentu „Celkové bodové hodnocení doktoranda“ a je součástí ISP. Při zahájení dalšího roku studia pak školitel do ISP zaznamená případné změny. Nejpozději do 15. 10. každého roku studia odevzdává doktorand vytištěný a podepsaný ISP na vědeckém oddělení fakulty ke kontrole a založení.
Během prvních čtyř semestrů skládá doktorand zkoušky z povinných, povinně volitelných anebo volitelných předmětů pro splnění bodových limitů ze Studijní oblasti, a současně se intenzivně zabývá vlastním studiem a analýzou poznatků v oboru stanoveném tématem disertační práce a průběžným publikováním takto získaných poznatků a vlastních výsledků. V dalších semestrech se doktorand již více soustřeďuje na výzkum a vývoj, který souvisí s tématem disertační práce, na publikování výsledků své tvůrčí práce a na vlastní zpracování disertační práce.
Do konce druhého roku studia skládá doktorand státní doktorskou zkoušku, kterou prokazuje široký rozhled a hluboké znalosti v oboru, souvisejícím s tématem disertační práce. K této zkoušce se musí přihlásit nejpozději do 30. dubna ve druhém roce svého studia. Státní doktorské zkoušce předchází zkouška z anglického jazyka.
Ve třetím a čtvrtém roce svého studia provádí doktorand potřebnou výzkumnou činnost, publikuje dosažené výsledky a zpracovává svoji disertační práci. Součástí studijních povinností v doktorském studijním programu je absolvování části studia na zahraniční instituci nebo účast na mezinárodním tvůrčím projektu s výsledky publikovanými nebo prezentovanými v zahraničí nebo jiná forma přímé účasti studenta na mezinárodní spolupráci, což je nutné doložit nejpozději při odevzdání disertační práce.
Doktorandi ve čtvrtém roce studia předkládají do konce zimního zkouškového období svému školiteli rozpracovanou disertační práci, který ji ohodnotí. Disertační práci doktorand odevzdává do konce 4. roku studia.
Student prezenční formy doktorského studia je v průběhu studia povinen absolvovat pedagogickou praxi, tj. působit v procesu výuky. Zapojení doktoranda do pedagogické činnosti je součástí jeho vědecké přípravy. Pedagogickou praxí doktorand získává zkušenosti v předávání poznatků a zdokonaluje prezentační dovednosti. Skladbu pedagogických aktivit (cvičení, laboratorní cvičení, vedení projektů apod.) určí doktorandovi vedoucí daného ústavu po dohodě se

školitelem. Povinnost pedagogické praxe se nevztahuje na doktorandy-samoplátce a na doktorandy v kombinované formě studia. Zapojení do výuky v rámci pedagogické praxe potvrdí po jejím splnění školitel v IS VUT.

Podmínky k přijetí ke studiu

Podmínkou přijetí ke studiu je řádné ukončení magisterského studijního programu stejného nebo příbuzného oboru. Základními předpoklady k přijetí jsou zájem a schopnosti k vědecké práci, znalost anglického jazyka a velmi dobré studijní výsledky dosažené v magisterském studijním programu. V rámci žádosti zájemce předkládá tzv. Applicant Statement, ve kterém především popisuje svůj zájem o téma studia, své předešlé aktivity (zkušenosti z praxe, vlastní výzkum, účast na projektech, apod.) v dané oblasti, očekávané výsledky. Applicant Statement je psán anglickém jazyce v rozsahu 1 až 2 strany A4.
Přijímací zkouška probíhá formou ústního pohovoru, kterým se ověřují předpoklady pro doktorské studium, kdy zájemce prokazuje a obhajuje především svůj zájem o zvolené téma studia, teoretické znalosti v oboru, znalost anglického jazyka, dosavadní tvůrčí činnost.
Přijímací komise hodnotí kvalitu uchazeče v rámci 100 bodové stupnice ve čtyřech oblastech:
- Zaměření studia, přehled z oboru disertace, motivace (max 30b)
- Obecně teoretický přehled (max 30b)
- Obsah dosavadní tvůrčí činnosti (max 20b)
- Znalost anglického jazyka (max 20b)

kdy pro přijetí studenta musí být z každé kategorie, kromě „Obsah dosavadní tvůrčí činnosti“, hodnocen alespoň polovinou bodů. V případě více zájemců o shodné téma, kdy všichni splňují minimální požadavky v rámci dílčích kategorií, o návrhu k přijetí jednoho ze zájemců rozhoduje komise.

Návaznost na další typy studijních programů

Studijní program přímo navazuje na bakalářský a magisterský studijní program "Informační bezpečnost" na FEKT, VUT v Brně.

B-IIb – Studijní plány a návrh témat prací (doktorské studijní programy)

Studijní povinnosti

Studium doktoranda probíhá podle individuálního studijního plánu, který zpracuje v úvodu studia školitel doktoranda ve spolupráci s doktorandem. V individuálním studijním plánu jsou specifikovány všechny povinnosti stanovené v souladu se Studijním a zkušebním řádem VUT, které musí doktorand k úspěšnému ukončení studia splnit. Tyto povinnosti jsou časově rozvrženy do celého období studia, jsou bodově ohodnoceny a v pevně daných termínech probíhá kontrola jejich plnění. Student si zapíše a vykoná zkoušky z povinných předmětů, povinně volitelných předmětů ohledem na zaměření jeho disertační práce, a dále volitelných předmětů (Angličtina pro doktorandy, Řešení inovačních zadání, Vědecké publikování od A do Z).
Ke státní doktorské zkoušce se může student přihlásit až po vykonání všech zkoušek předepsaných jeho individuálním studijním plánem. Před státní doktorskou zkouškou student vypracuje pojednání k disertační práci, v němž detailně popíše cíle práce, důkladné zhodnocení stavu poznání v oblasti řešené disertace, charakteristiku metod, které hodlá při řešení uplatňovat. Obhajoba pojednání, které je oponováno, je součástí státní doktorské zkoušky. V další části zkoušky musí student prokázat hluboké teoretické i praktické znalosti v oblasti kryptografie, systémové bezpečnosti, síťové bezpečnosti a elektrotechniky, elektroniky. Státní doktorská zkouška probíhá ústní formou a kromě diskuze nad pojednáním k disertační práci se také skládá z tematických okruhů týkajících se povinných a povinně volitelných předmětů.
K obhajobě disertační práce se student hlásí po vykonání státní doktorské zkoušky a po splnění podmínek pro ukončení, jakými jsou účast na výuce, vědecká a odborná činnost (tvůrčí činnost), a minimálně měsíční studijní nebo pracovní stáž na zahraniční instituci anebo účasti na mezinárodním tvůrčím projektu.

Požadavky na tvůrčí činnost

Součástí studijních povinností studentů programu "Informační bezpečnost" je pravidelné publikování výsledků své tvůrčí činnosti na mezinárodních konferencích a formou článků v časopisech, kdy důraz je kladen na prezentování v excelentních časopisech vedených v databázích WoS anebo SCOPUS. Alespoň u jednoho časopiseckého článku vedeného v databázi WoS musí student vykazovat majoritní podíl na výsledku, která má vazbu na téma jeho studia. Hodnocenou aktivitou v rámci tvůrčí činnosti je i podání návrhu projektu za účelem získání grantu a jeho následné řešení. Student má možnost se účastnit smluvního výzkumu a vědecko-výzkumných projektů, primárně řešených jeho školitelem. Podíl studenta na výsledcích aplikovaného výzkumu takových projektů je také hodnocen v oblasti tvůrčí činnosti studenta. Jednotlivé typy výstupů tvůrčí činnosti jsou kategorizovány a bodově hodnoceny, kdy Směrnicí děkana FEKT č. 8/2018 "Pravidla pro organizaci studia na FEKT" jsou pro termíny kontrol průběhu studia stanoveny minimální počty bodů.

Požadavky na absolvování stáží

Součástí studijních povinností v doktorském studijním programu "Informační bezpečnost" je absolvování části studia na zahraniční instituci nebo účast na mezinárodním tvůrčím projektu s výsledky publikovanými nebo prezentovanými v zahraničí nebo jiná forma přímé účasti studenta na mezinárodní spolupráci. Výjezdy jsou realizovány především ve spolupráci se zahraničními partnerskými institucemi v rámci programu ERASMUS+, Freemovers, CEEPUS, anebo Rozvojových projektů MŠMT. Možnosti absolvování pobytu na zahraniční instituci primárně nabízí školitel s ohledem na jeho vlastní zkušenosti a pobyty na partnerských institucích.

Další studijní povinnosti

Kromě vlastního studia povinných předmětů, povinně volitelných předmětů a volitelných předmětů a další odborných aktivit v rámci tvůrčí činnosti je součástí studia také povinná účast ve výuce. Studenti se účastní výukové činnosti v bakalářský a magisterských studijních programech v rámci numerických, počítačových anebo laboratorních cvičení některých např. z následujících předmětů: Základy kryptografie, Bezpečnost ICT 1/2, Komunikační technologie, Architektura sítí, Datová komunikace, Aplikovaná kryptografie, Objektově orientované programování, Multimediální služby, Teoretická informatika, Teorie sdělování, Telekomunikační a informační systémy, Seminář informační bezpečnosti, atd. Při zařazení studenta do výuky některého z výše uvedených předmětů se zohledňuje vlastní výběr studenta a také zaměření jeho disertační práce. K dalším studijním povinnostem z pohledu pedagogické praxe pak náleží i vedení studentů bakalářského a magisterského studia při jejich závěrečných pracích.

Návrh témat disertačních prací a témata obhájených prací

Kryptografická ochrana soukromí
Šifry pro zařízení s omezeným výpočetním výkonem
Návrh kryptografických algoritmů a jejich optimalizace pro hardwarové implementace
Hodnocení bezpečnosti komunikačních zařízení metodami postranních kanálů
Analýza datového provozu pomocí strojového učení

B-III – Charakteristika studijního předmětu

Název studijního předmětu	Bezpečnost systémů a zařízení			
Typ předmětu	specializace: bez specializace - Povinný			
Doporučený ročník / semestr	specializace: bez specializace - 1. / letní			
Rozsah studijního předmětu	39s		**Kreditů**	4
Prerekvizity, korekvizity, ekvivalence				
Způsob ověření studijních výsledků	zkouška	**Forma výuky**	Seminář	

Forma způsobu ověření studijních výsledků a další požadavky na studenta

Student vypracuje inviduální projekt na zadané téma. Následuje ústní zkouška, při které student prokáže znalosti nastudované a zpracované problematiky.

Garant předmětu	Malina Lukáš, Ing., Ph.D.
Zapojení garanta do výuky předmětu	Ing. Lukáš Malina, Ph.D. (přednášející) 80%

Vyučující

Ing. Lukáš Malina, Ph.D. (přednášející) 80%
doc. Ing. Jaroslav Koton, Ph.D. (přednášející) 20%

Stručná anotace předmětu

1. Úvod do bezpečnosti vestavěných systémů a odolných zařízení
2. Lehká kryptografie pro výpočetně a paměťově omezená zařízení
3. Autentizační systémy, technologie a protokoly
4. Autentizační předměty a zabezpečené hardwarové moduly
5. Programovatelné čipové karty
6. Bezpečnost na chytrých zařízeních
7. Bezpečnost jednočipových zařízení, embedded systemů a optimalizace algoritmů
8. Reverzní inženýrství a softwarová bezpečnost
9. Kryptoanalýza postranními kanály – úvod
10. Kryptoanalýza postranními kanály – proudová analýza
11. Kryptoanalýza postranními kanály – protiopatření
12. Metodiky hodnocení bezpečnosti zařízení a systémů
13. Vybraná témata z bezpečnosti systémů a zařízení

Studijní literatura a studijní pomůcky

BURDA, Karel. Aplikovaná kryptografie. Brno: VUTIUM, 2013. 255 s. ISBN 978-80-214-4612-0. (základní literatura)
MAYES, Keith E.; MARKANTONAKIS, Konstantinos (ed.). Smart cards, tokens, security and applications. Second Edition. Springer International Publishing AG, 2017. 531 s. ISBN: 3319504983 (základní literatura)
MANGARD, Stefan a OSWALD, Elisabeth a POPP, Thomas: Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security). Secaucus, NJ, USA:Springer-Verlag New York, Inc., 2007, ISBN 0387308571. (doporučená literatura)
PETERS, Eric: Advanced DPA Theory and Practice: Towards the Security Limits of Secure Embedded Circuits. Springer Publishing Company, 2013, ISBN 1461467829. (doporučená literatura)
AMBROSE, Jude, Alexandar INGJATOVIC a Sri PARAMESWARAN. Power analysis side channel attacks: the processor design-level context. Saarbrücken: VDM Verlag, 2010, xvi, 277 s. : il. ISBN 978-3-8364-8508-1. (doporučená literatura)
RANKL, Wolfgang, Wolfgang EFFING a Kenneth COX. Smart card handbook. 4th ed. Chichester: John Wiley, 2010, xliv, 1043 s. : il. ISBN 978-0-470-74367-6. (doporučená literatura)
KLEIDERMACHER, David, KLEIDERMACHER, Mike. Embedded systems security: practical methods for safe and secure software and systems development. Elsevier, 2012. (doporučená literatura)

Informace ke kombinované nebo distanční formě

Rozsah konzultací (soustředění)	39 hod./semestr	**hodin**

Informace o způsobu kontaktu s vyučujícím

Konzultace probíhají vždy po předchozí domluvě s vyučujícím. Se studenty kombinovaného studia probíhá komunikace písemně formou emailu, případně ústně nebo s využitím komunikační techniky (videohovoru, telefonátu). S ohledem na charakter výuky předmětu pro studenty denního studia jsou opory pro studenty kombinované formy studia shodné.

B-III – Charakteristika studijního předmětu

Název studijního předmětu	Diskrétní procesy v elektrotechnice			
Typ předmětu	specializace: bez specializace - Povinně volitelný			
Doporučený ročník / semestr	specializace: bez specializace - 1. / letní			
Rozsah studijního předmětu	39s		**Kreditů**	4
Prerekvizity, korekvizity, ekvivalence				
Způsob ověření studijních výsledků	zkouška	**Forma výuky**	Seminář	

Forma způsobu ověření studijních výsledků a další požadavky na studenta

písemná

Garant předmětu	Diblík Josef, prof. RNDr., DrSc.
Zapojení garanta do výuky předmětu	prof. RNDr. Josef Diblík, DrSc. (přednášející) 80%

Vyučující

prof. RNDr. Josef Diblík, DrSc. (přednášející) 80%
Mgr. Irena Hlavičková, Ph.D. (přednášející) 20%

Stručná anotace předmětu

1. Základní aparát a základní metody vyšetřování diskrétních procesů (5 týdnů).
2. Diskrétní počet (vybrané diferenční vztahy na základě spojitých analogií). Diferenční rovnice a systémy.
3. Základní pojmy, užívané v diskrétních rovnicích (rovnovážné body, periodické body, body potenciálně rovnovážné a potenciálně periodické, stabilita řešení, přitahující a odpuzující body) a jejich ilustrace na příkladech (modelování obvodů diskrétními rovnicemi, přenos informace).
4. Rekurzivní algoritmy řešení systémů diskrétních rovnic a rovnic vyšších řádů (případ konstantních koeficientů, metoda variace parametrů, metoda neurčitých koeficientů).
5. Konstrukce obecného řešení. Transformace některých nelineárních rovnic na lineární. Diferenční rovnice sestavované na bázi vzorkování, impulsové podněty, výpočet charakteristik z odezvy signálu (odezva Diracovy distribuce), přechodné děje.
6. Aplikace diferenčních rovnic – stabilita procesů. Stabilita rovnovážných bodů. Typy stability a nestability.
7. Stabilita lineárních systémů s proměnnou maticí. Stabilita nelineárních systémů podle lineární aproximace.
8. Ljapunovova přímá metoda pro zjištění stability.
9. Fázová analýza dvourozměrného diskrétního systému s konstantními koeficienty, klasifikace rovnovážných bodů.
10. Aplikace diferenčních rovnic - řízení procesů. Diskrétní ekvivalenty spojitých systémů.
11. Diskrétní teorie řízení, řiditelnost, úplná řiditelnost, matice řiditelnosti, kanonické tvary řiditelnosti, řiditelná kanonická forma, konstrukce algoritmu řízení.
12. Pozorovatelnost úplná pozorovatelnost, nepozorovatelnost, princip duality, matice pozorovatelnosti.
13. Kanonické tvary pozorovatelnosti, vztah řiditelnosti a pozorovatelnosti. Stabilizace řízení dle zpětné vazby.

Studijní literatura a studijní pomůcky

Diblík, J., Diskrétní metody v elektroinženýrství, elektronický text, Brno, 2014 (základní literatura)
Mickens, Ronald E., Difference Equations: Theory, Applications and Advanced Topics, Third Edition, Chapman & Hall/CRC, 2016 (základní literatura)
Oppenheim, Alan, V., Schaffer, Ronald, W., Discrete-Time Signal Processing, 3rd Edition, Pearson, 2014 (základní literatura)
Miček, J., Jurečka, M., Moderné prostriedky implementácie metód číslicového spracovania signálov I.. EDIS, Žilina, 2013 (doporučená literatura)
Sami Fadali, M., Visioli, A., Digital Control Engineering, Analysis and Design, 2nd Edition, Elsewier, AP, 2013 (doporučená literatura)
Farlow, S. J., Solution Manual: Introduction to Differential Equations and Their Applications , Dover Publications, 2016. (rozšiřující literatura)
Banerjee, D., From Continuous to Discrete: Integer Equations, Difference Equations, and Digital Electronics, Dog Ear Publishing, LLC, 2014 (rozšiřující literatura)

Informace ke kombinované nebo distanční formě

Rozsah konzultací (soustředění)	39 hod./semestr	**hodin**

Informace o způsobu kontaktu s vyučujícím

Konzultace probíhají v konzultačních hodinách po předchozí domluvě s vyučujícím. Se studenty kombinovaného studia probíhá komunikace písemně formou emailu, případně ústně nebo s využitím komunikační techniky (videohovoru, telefonátu). S ohledem na charakter výuky předmětu pro studenty denního studia jsou opory pro studenty kombinované formy studia shodné.

B-III – Charakteristika studijního předmětu

Název studijního předmětu	Moderní digitální bezdrátová komunikace			
Typ předmětu	specializace: bez specializace - Povinně volitelný			
Doporučený ročník / semestr	specializace: bez specializace - 1. / letní			
Rozsah studijního předmětu	39s		**Kreditů**	4
Prerekvizity, korekvizity, ekvivalence				
Způsob ověření studijních výsledků	zkouška	**Forma výuky**	Seminář	

Forma způsobu ověření studijních výsledků a další požadavky na studenta

písemná

Garant předmětu	Sigmund Milan, prof. Ing., CSc.
Zapojení garanta do výuky předmětu	prof. Ing. Milan Sigmund, CSc. (přednášející) 100%

Vyučující

prof. Ing. Milan Sigmund, CSc. (přednášející) 100%

Stručná anotace předmětu

1. Řečový signál a hlasové technologie
2. Teorie radiokomunikačních signálů
3. Množiny signálů s diskrétním časem a se spojitým časem
4. Nadějné metody v rádiové komunikaci
5.-6. Systémy s rozprostřeným spektrem
7. Systémy pracující v kódovém multiplexu
8.-9. Zpracování radiokomunikačních signálů
10. Dominantní interference v multiuživatelském prosředí
11. Koexistence mobilních systémů a její modelování v programu MATLAB
12. Metody a nástroje družicové komunikace
13. Atmosférické optické spoje

Studijní literatura a studijní pomůcky

K.D. Rao, M.N. Swamy, Digital Signal Processing: Theory and Practice, Springer, Singapore, 2018. (základní literatura)
L. Fa-Long, Ch. Zhang, Signal Processing for 5G: Algorithms and Implementations, John Wiley & Sons, Chichester, 2016. (základní literatura)
B. Boashash, Time-Frequency Signal Analysis and Processing: A Comprehensive Reference, Academic Press, London, 2016. (doporučená literatura)

Informace ke kombinované nebo distanční formě

Rozsah konzultací (soustředění)	39 hod./semestr	**hodin**

Informace o způsobu kontaktu s vyučujícím

Konzultace probíhají vždy po předchozí domluvě s vyučujícím. Se studenty kombinovaného studia probíhá komunikace písemně formou emailu, případně ústně nebo s využitím komunikační techniky (videohovoru, telefonátu). S ohledem na charakter výuky předmětu pro studenty denního studia jsou opory pro studenty kombinované formy studia shodné.

B-III – Charakteristika studijního předmětu

Název studijního předmětu	Numerické úlohy s parciálními diferenciálními rovnicemi				
Typ předmětu	specializace: bez specializace - Povinně volitelný				
Doporučený ročník / semestr	specializace: bez specializace - 1. / letní				
Rozsah studijního předmětu	39s			**Kreditů**	4
Prerekvizity, korekvizity, ekvivalence					
Způsob ověření studijních výsledků	zkouška	**Forma výuky**	Seminář		

Forma způsobu ověření studijních výsledků a další požadavky na studenta

Student vypracuje literární rešerši na zadané téma v rozsahu 10-20 normostran. Následuje ústní zkouška, při které student prokáže znalosti nastudované a zpracované problematiky.

Garant předmětu	Fiala Pavel, prof. Ing., Ph.D.
Zapojení garanta do výuky předmětu	prof. Ing. Pavel Fiala, Ph.D. (přednášející) 100%

Vyučující

prof. Ing. Pavel Fiala, Ph.D. (přednášející) 100%

Stručná anotace předmětu

1. Úvod do funkcionální analýzy, diferenciální operátory, přehled parciálních diferenciálních rovnic, probíraných v kurzu, okrajové a počáteční podmínky.
2. Metoda konečných diferencí (MKD). Metoda konečných prvků (MKP) – úvod. Diskretizace oblasti na konečné prvky. Aproximace polí z uzlových nebo hranových hodnot.
3. Dopředná úloha: Sestavení rovnic pro uzlové a hranové hodnoty Galerkinovou metodou.
4. Aplikace Galerkinovy metody na statická a kvazistatická pole (Poissonova a Helmholtzova rovnice).
5. Kombinace MKP a MKD pro časově proměnná pole (difuzní a vlnová rovnice). Spojení rovnice pole s obvodem se soustředěnými parametry, nestacionární úlohy časová a frekvenční doména.
6.-7. Sdružené úlohy, modely s respektováním teorie relativity, stochastické modely.
8. Optimalizační úlohy polí. Přehled deterministických metod. Lokální a globální optimum.
9. Nepodmíněné úlohy – metoda gradientní, největšího spádu, Newtonovy metody, stochastické modely, magnetohydrodynamika a relativistický přístup k popisu modelu.
10. Stochastické modelování ve spojení s MKP, mikroskopický přístup k aplikaci MKP, Nanometrické geometrie, modely, efekty, jevy.
11. Inverzní úlohy pro eliptické rovnice. Metoda nejmenších čtverců. Deterministické regularizační metody, Přehled metod hladinových množin pro inverzní úlohy a optimální návrh.
12. Použití inverzních úloh v tomografii.
13. Metody a modely modelování atomových a subatomových úrovní, nanoelektronika, periodické struktury, strukturální modelování, fotonika, biofotonika.

Pozn. Všechny body osnovy budou doplněny praktickou ukázkou nebo sestavením vlastního programu v prostředí programů MATLAB nebo ANSYS.

Studijní literatura a studijní pomůcky

J.A.Stratton, Electromagnetic Theory, McGraw-Hill Book Company, New York and London, 1941, https://archive.org/details/electromagnetict031016mbp/page/n637 (základní literatura)
Sadiku, M.: Electromagnetics (second edition), CRC Press, 2001 (základní literatura)
SIAM Journal on Control and Optimization, ročník 2013 a výše (doporučená literatura)
IEEE Transactions on Magnetics, ročník 2012 a výše (doporučená literatura)
Chari, M, V. K., Salon S. J.: Numerical Methods in Electromagnetism. Academic Press, 2000 (rozšiřující literatura)
Bossavit Alain.: Computational Electromagnetism – Variational formulations, complementarity, edge elements. Academic Press, 1998 (rozšiřující literatura)
Inverse Problems. IoP Electronic Journals, http://www.iop.org/EJ/journal/IP http://www.inverse-problems.com/ (elektronická literatura)
Level set methods http://www.math.ucla.edu/applied/cam/index.html (elektronická literatura)

Informace ke kombinované nebo distanční formě

Rozsah konzultací (soustředění)	39 hod./semestr	**hodin**

Informace o způsobu kontaktu s vyučujícím

Konzultace probíhají vždy po předchozí domluvě s vyučujícím. Se studenty kombinovaného studia probíhá komunikace písemně formou emailu, případně ústně nebo s využitím komunikační techniky (videohovoru, telefonátu). S ohledem na charakter výuky předmětu pro studenty denního studia jsou opory pro studenty kombinované formy studia shodné.

B-III – Charakteristika studijního předmětu

Název studijního předmětu	Optimalizační metody a teorie hromadné obsluhy			
Typ předmětu	specializace: bez specializace - Povinně volitelný			
Doporučený ročník / semestr	specializace: bez specializace - 1. / zimní			
Rozsah studijního předmětu	39s		**Kreditů**	4
Prerekvizity, korekvizity, ekvivalence				
Způsob ověření studijních výsledků	zkouška	**Forma výuky**	Seminář	

Forma způsobu ověření studijních výsledků a další požadavky na studenta

ústní

Garant předmětu	Sklenář Jaroslav, doc. Ing., CSc.
Zapojení garanta do výuky předmětu	doc. Ing. Jaroslav Sklenář, CSc. (přednášející) 80%

Vyučující

doc. Ing. Jaroslav Sklenář, CSc. (přednášející) 80%
doc. Mgr. Pavel Rajmic, Ph.D. (přednášející) 20%

Stručná anotace předmětu

1. Teorie optimalizace. Základní pojmy, různé typy a existence řešení (Weierstrassův theorem). Metody založené na kalkulu.
2. Lineární programování. Teorie a Simplexová metoda.
3. Celočíselné programování. Metody řešení a využití indikátorových proměnných při vytváření modelů které jsou mimo rozsah Lineárního programování (modely s logickými podmínkami, disjunktní omezení, apod.)
4. Teorie Nelineárního programování. Konvexní množiny a funkce, podmínky optimality.
5. Optimalizační algoritmy Nelineárního programování a jejich aplikace.
6. Dynamické programování s konečným horizontem. Úvod do rekurze, řešení různých typů praktických úloh metodami Dynamického programování.
7. Úvod do Stochastického programování. Terminologie, základní tvary deterministických ekvivalentů a jejich řešení.
8. Úvod do Dynamického programování s nekonečným horizontem. Terminologie, Markovský rozhodovací proces, Bellmanovy rovnice a jejich řešení.
9. Heuristické optimalizační algoritmy jako metoda řešení problému lokálních extrémů (genetické a podobné algoritmy založené na populacích řešení).
10. Základy Teorie hromadné obsluhy, úvod do náhodných procesů, Poissonův proces detailně.
11. Modely jednoduchých systémů s jednou frontou (model M/M/1 a podobné).
12. Složitější modely s jednou frontou (M/G/1,G/M/1,apod.). Síťové modely, Jacksonův theorem.
13. Simulační metody a jejich použití při analýze systémů hromadné obsluhy.

Studijní literatura a studijní pomůcky

Popela, P., Sklenář, J.: Optimization. Teaching notes, University of Malta, 2003. (základní literatura)
Sklenář, J.: Queuing Theory. Teaching notes, University of Malta, 2016. (základní literatura)
Sklenář, J.: Dynamic Programming Theory and Applications. Teaching notes, University of Malta, 2017. (doporučená literatura)
Popela, P.: Nonlinear Programming. Teaching notes, University of Malta, 2003. (doporučená literatura)
Attard, N., Sklenář, J.: Linear Programming. Teaching notes, University of Malta, 2007. (doporučená literatura)
Sklenář, J.: Introduction to Integer Linear Programming. Teaching notes, University of Malta, 2017. (doporučená literatura)
Sklenář, J.: Infinite Horizon Dynamic Programming Models. Teaching notes, University of Malta, 2017. (doporučená literatura)
Popela, P.: Stochastic Programming. Teaching notes, University of Malta, 2008. (doporučená literatura)
Sklenář, J.: Queuing Theory - Worksheets. Teaching notes, University of Malta, 2016. (doporučená literatura)
Sklenář, J.: Network Flow Models. Teaching notes, University of Malta, 2017. (doporučená literatura)

Informace ke kombinované nebo distanční formě

Rozsah konzultací (soustředění)	39 hod./semestr	**hodin**

Informace o způsobu kontaktu s vyučujícím

Konzultace probíhají vždy po předchozí domluvě s vyučujícím. Se studenty kombinovaného studia probíhá komunikace písemně formou emailu, případně ústně nebo s využitím komunikační techniky (videohovoru, telefonátu). S ohledem na charakter výuky předmětu pro studenty denního studia jsou opory pro studenty kombinované formy studia shodné.

B-III – Charakteristika studijního předmětu

Název studijního předmětu	Pokročilá kryptografie			
Typ předmětu	specializace: bez specializace - Povinný			
Doporučený ročník / semestr	specializace: bez specializace - 1. / zimní			
Rozsah studijního předmětu	39s		**Kreditů**	4
Prerekvizity, korekvizity, ekvivalence				
Způsob ověření studijních výsledků	zkouška	**Forma výuky**	Seminář	

Forma způsobu ověření studijních výsledků a další požadavky na studenta

písemná

Garant předmětu	Hajný Jan, doc. Ing., Ph.D.
Zapojení garanta do výuky předmětu	doc. Ing. Jan Hajný, Ph.D. (přednášející) 100%

Vyučující

doc. Ing. Jan Hajný, Ph.D. (přednášející) 100%

Stručná anotace předmětu

1. Úvod do základů kryptografických algoritmů
2. Kryptografie eliptických křivek
3. Závazková schémata
4. Sigma protokoly
5. Zaslepený digitální podpis
6. Skupinové podpisy
7. Pověřovací schémata
8. Elektronické hlasování
9. Kryptoměny
10. Sdílené tajemství
11. Postkvantová kryptografie I
12. Postkvantová kryptografie II
13. Vybrané partie z moderní kryptografie

Studijní literatura a studijní pomůcky

BURDA, K. Aplikovaná kryptografie. monografie. monografie. Brno: VUTIUM, 2013. 255 s. ISBN: 978-80-214-4612- 0. (základní literatura)

SCHNEIER, Bruce. Applied cryptography: protocols, algorithms, and source code in C. 20th anniversary edition. Indianapolis: Wiley, 2015, xxv, 758 stran : ilustrace. ISBN 978-1-119-09672-6. (základní literatura)

MENEZES, A. J, Paul C VAN OORSCHOT a Scott A VANSTONE. Handbook of applied cryptography. Boca Raton: CRC Press, c1997. ISBN 0849385237. (doporučená literatura)

Washington, Lawrence C. Elliptic curves: number theory and cryptography. Chapman and Hall/CRC, 2003. (rozšiřující literatura)

Schoenmakers, Berry. Lecture notes cryptographic protocols. 2018. (rozšiřující literatura)

Hoffstein, J., Pipher, J. C., Silverman, J. H., Silverman, J. H.: An introduction to mathematical cryptography. New York: springer (2008). (rozšiřující literatura)

Bernstein, D.J., Buchmann, J., Dahmen, E.: Post-Quantum Cryptography Springer (2008) (rozšiřující literatura)

Ochodková, Eliška. Matematické základy kryptografických algoritmů [online]. [cit. 2013-06-11]. Dostupné z: http://mi21.vsb.cz/sites/mi21.vsb.cz/files/unit/mat_zaklady_kryptografickych_algoritmu.pdf (CS) (elektronická literatura)

Informace ke kombinované nebo distanční formě

Rozsah konzultací (soustředění)	39 hod./semestr	**hodin**

Informace o způsobu kontaktu s vyučujícím

Konzultace probíhají vždy po předchozí domluvě s vyučujícím. Se studenty kombinovaného studia probíhá komunikace písemně formou emailu, případně ústně nebo s využitím komunikační techniky (videohovoru, telefonátu). S ohledem na charakter výuky předmětu pro studenty denního studia jsou opory pro studenty kombinované formy studia shodné.

B-III – Charakteristika studijního předmětu

Název studijního předmětu	Statistika. stochastické procesy, operační výzkum			
Typ předmětu	specializace: bez specializace - Povinně volitelný			
Doporučený ročník / semestr	specializace: bez specializace - 1. / zimní			
Rozsah studijního předmětu	39s		**Kreditů**	4
Prerekvizity, korekvizity, ekvivalence				
Způsob ověření studijních výsledků	zkouška	**Forma výuky**	Seminář	

Forma způsobu ověření studijních výsledků a další požadavky na studenta

písemná

Garant předmětu	Baštinec Jaromír, doc. RNDr., CSc.
Zapojení garanta do výuky předmětu	doc. RNDr. Jaromír Baštinec, CSc. (přednášející) 80%

Vyučující

doc. RNDr. Jaromír Baštinec, CSc. (přednášející) 80%
Ing. Michal Fusek, Ph.D. (přednášející) 20%

Stručná anotace předmětu

1. Klasická a axiomatická definice pravděpodobnosti. Podmíněná pravděpodobnost, úplná pravděpodobnost., náhodná veličina, číselné charakteristiky.
2. Diskrétní a spojitá rozdělení náhodných veličin. Vlastnosti normálního rozdělení. Limitní věty.
3. Statistika. Výběr. Zpracování statistického materiálu. Základná parametry základního souboru a charakteristiky výběru.
4. Základní bodové a intervalové odhady. Testy dobré shody. Analýza rozptylu.
5. Operační výzkum. Lineární programování. Grafické řešení. Simplexová metoda.
6. Duální úloha. Analýza citlivosti. Ekonomická interpretace lineárního programování.
7. Nelineární programování.
8. Řešení úloh nelineárního programování.
9. Náhodné procesy, základní pojmy, charakteristiky náhodných procesů.
10. Diskrétní Markovovy řetězce. Homogenní Markovovy řetězce, klasifikace stavů. Regulární Markovovy řetězce, limitní vektor, fundamentální matice, střední doba prvého přechodu.
11. Absorpční řetězce, střední doba průchodu, přechodu a setrvání. Analýza Markovových řetězců pomocí Z-transformace. Výpočet mocniny matice přechodu.
12. Spojité Markovovy řetězce. Klasifikace pomocí Laplaceovy transformace. Poissonův proces. Lineární proces růstu, lineární proces zániku , lineární proces růstu a zániku.
13. Markovské rozhodovací procesy. Ocenění přechodů. Asymptotické vlastnosti. Rozhodovací procesy s alternativami. Skryté Markovské procesy.

Studijní literatura a studijní pomůcky

Baštinec, J.: Statistika, stochastické procesy, operační výzkum. Brno 2017 (základní literatura)
Montgomery, D.C., Runger, G.C.: Applied Statistics and Probability for engineers. 6th Edition. John Wiley \& Sons, Inc., New York 2015.ISBN-13: 978-1118539712. (základní literatura)
Baštinec, J.: Statistika, stochastické procesy, operační výzkum. Sbírka příkladů. Brno 2017 (doporučená literatura)
Miller, I., Miller, M.: John E. Freund's Mathematical Statistics. 8th Edition. Prentice Hall, Inc., New Jersey 2012. (doporučená literatura)
Taha, H.A.: Operations research. An Introduction. 9th Edition, Macmillan Publishing Company, New York 2013.ISBN-13: 978-0132555937 (doporučená literatura)
Anděl, J.: Statistické úlohy, historky a paradoxy. Matfyzpress, MFF UK Praha, 2018. (doporučená literatura)
Zapletal, J.: Základy počtu pravděpodobnosti a matematrické statistiky. PC-DIR,VUT, Brno, 1995 (doporučená literatura)
Papoulis, A., Pillai, S. U.: Probability, Random Variables and Stochastic Processes, 4th Edition, 2012. ISBN-13: 978-0071226615 (doporučená literatura)
Nagy, I.: Základy bayesovského odhadování a řízení, ČVUT, Praha, 2003 (doporučená literatura)
Sarma, R. D.:Basic Applied Mathematics for the Physical Sciences 3rd New edition Edition, 2017, ISBN-13: 978-8131787823 (doporučená literatura)

Informace ke kombinované nebo distanční formě

Rozsah konzultací (soustředění)	39 hod./semestr	**hodin**

Informace o způsobu kontaktu s vyučujícím

Konzultace se studenty probíhají vždy po předchozí domluvě s vyučujícím. Se studenty kombinovaného studia probíhá komunikace písemně formou emailu, případně telefonicky. S ohledem na charakter výuky předmětu pro studenty denního studia jsou studijní opory pro studenty kombinované formy studia shodné.

B-III – Charakteristika studijního předmětu

Název studijního předmětu	Zkouška z angličtiny před státní doktorskou zkoušku			
Typ předmětu	specializace: bez specializace - Povinný			
Doporučený ročník / semestr	specializace: bez specializace - 1. / celoroční			
Rozsah studijního předmětu			**Kreditů**	4
Prerekvizity, korekvizity, ekvivalence				
Způsob ověření studijních výsledků	zkouška	**Forma výuky**	Zkouška ústní	
Forma způsobu ověření studijních výsledků a další požadavky na studenta				
ústní				
Garant předmětu	Zmrzlá Petra, Mgr., Ph.D.			
Zapojení garanta do výuky předmětu	Mgr. Petra Zmrzlá, Ph.D. (přednášející) 100%			
Vyučující				
Mgr. Petra Zmrzlá, Ph.D. (přednášející) 100%				
Stručná anotace předmětu				

1.Analýza odborného textu
2. Poslech a metody porozumění
3. Reprodukce textu
4. Funkce jazyka, gramatické struktury
5. Obtížná slova, srovnání s češtinou
6. Akademická angličtina
7.Psaní ve vědě a technice
8. Prezentace - subskills
9. Prezentace
10. Žánry angličtiny ve vědě a technice
11. Poslech univerzitních přednášek
12. Psaný diskurz
13. Opakování

Studijní literatura a studijní pomůcky

Krhutová M.: Parameters of Professional Discourse, Tribun-EU, 2009 (základní literatura)
Vince M.: Advanced Language Practice, Heinemann, 1994 (doporučená literatura)
Leki, I.: Academic writing, CUP, 2006 (rozšiřující literatura)
Studijní materiály UJAZ pro doktorandy (elektronická literatura)

Informace ke kombinované nebo distanční formě

Rozsah konzultací (soustředění)	3 hod./semestr	**hodin**

Informace o způsobu kontaktu s vyučujícím

Konzultace probíhají vždy po předchozí domluvě s vyučujícím. Se studenty kombinovaného studia probíhá komunikace písemně formou emailu, případně ústně v dohodnutém termínu. S ohledem na charakter výuky předmětu pro studenty denního studia jsou opory pro studenty kombinované formy studia shodné.

B-IV – Údaje o odborné praxi

Charakteristika povinné odborné praxe

Rozsah	0	**týdnů**	0	**hodin**	

Přehled pracovišť, na kterých má být praxe uskutečňována	**Smluvně zajištěno**

Zajištění odborné praxe v cizím jazyce (u studijních programů uskutečňovaných v cizím jazyce)