SPRÁVA O VEDECKO-VÝSKUMNEJ ČINNOSTI
na Ústave informatiky a matematiky FEI STU v Bratislave

za rok 2017

riaditeľ ústavu:
prof. RNDr. Otokar Grošek, PhD. Tel: ++421-2-602 91 226
e-mail: otokar.grosek@stuba.sk Fax: ++421-2-654 20 415

I. PRACOVNÍCI

Profesori

prof. RNDr. Igor Bock, PhD.
prof. RNDr. Otokar Grošek, PhD.
prof. RNDr. Gabriel Juhás, PhD. (vedúci odd. SI)
prof. Dr. Ing. Miloš Oravec

Docenti

Dr. rer. nat. Martin Drozda
doc. RNDr. Ľubomír Marko, CSc. (vedúci odd. Matematiky)
doc. RNDr. Karol Nemoga, PhD.
doc. RNDr. Oľga Nánásiová, PhD.
doc. RNDr. Vladimír Olejček, PhD.
doc. Mgr. Marcel Polakovič, PhD.
doc. RNDr. Boris Rudolf, PhD.
doc. Ing. Michal Šrámka, PhD., PhD.
doc. Ing. Milan Vojvoda, PhD.
doc. RNDr. Michal Zajac, PhD.
doc. Ing. Pavol Zajac, PhD. (vedúci odd.BIS)

Odborní asistenti

Ing. Eugen Antal, PhD.
Ing. Štefan Balogh, PhD.
RNDr. Igor Brilla, PhD.
RNDr. Viera Čerňanová, PhD.
RNDr. Karla Čipková, PhD.
Mgr. Tomáš Fabšič, PhD.
Ing. Ondrej Gallo, PhD.
Ing. Alexander Hambalík, PhD.
Ing. Viliam Hromada, PhD.
Ing. Mgr. Matúš Jókay, PhD.
RNDr. Mária Kečkemétyová, PhD.
RNDr. Igor Kossaczký, CSc.
Ing. Stanislav Marček, PhD.
RNDr. Ivica Marinová, PhD.
Ing. Vladislav Novák
Mgr. Dávid Pancza, PhD.
RNDr. Elena Pastuchová, PhD.
Mgr. Marek Sýs, PhD.
Mgr. Michal Zákopčan, PhD.

Administratívni pracovníci	Zuzana Šabíková (tajomníčka ústavu) Emília Komžíková Mgr. Zuzana Šedová
Výskumní pracovníci	Ing. Dominik Sopiak Ing. Ľuboš Omelina, PhD.
Interní doktorandi	Ing. Eugen Antal (obhájil 26.4.2017) Ing. Zuzana Bukovčiková Ing. Maroš Čavojský Mgr. Tomáš Fabšič (obhájil 23.11.2017) Ing. Michala Gulášová Ing. Vojtěch Jirka (prerušené do 2.7.2018) Ing. Pavol Marák (prerušené do 2.9.2018) Ing. Juraj Mažári Ing. Milan Mladoniczky Ing. Dominik Sopiak (prerušené do 2.9.2019) Ing. Peter Špaček Ing. Juraj Varga (prerušené do 31.7.2018)
Externí doktorandi	Ing. Robert Bučko (zanechal 31.8.2017) Ing. Csaba Cserba (zanechal 3.4.2017) Ing. Igor Kazlov (prerušené do 30.8.2018) MUDr. Veronika Kurilová (prerušené do 2.9.2018) Ing. Peter Minarovský Ing. Štefan Počarovský (prerušené do 31.5.2018) Mgr. Tomáš Žilka (zanechal 31.8.2017) Mgr. Viktória Žilková (zanechala 31.8.2017)

II. ZARIADENIA

II.1. Výukové a výskumné laboratóriá

- Laboratórium Biometrie a spracovania signálov
- Laboratórium pre Bezpečnosť IT
- Antivírové laboratórium
- Experimentálne laboratórium ÚIM
- Laboratórium na meranie postranných kanálov
- Knižnica Oddelenia matematiky ÚIM
- Časopisecká knižnica Oddelenia matematiky ÚIM

LAB: Mobile Computing & Petri Net Lounge (ešte vo výstavbe)
Výkonné počítače:

- CPU 4-jadrový Intel Xeon E5-1620v3/RAM 256GB/SSD 256GB RAID0/HDD 2TB RAID5

- CPU 8-jadrový AMD FX-9590/RAM 32GB/SSD 256GB/ HDD 3TB/GPU 2x NVIDIA GTX970 v SLI
- CPU 4-jadrový Intel i7-4790/RAM16GB/SSD 256GB/ HDD 1TB Raid1

II.2. Špeciálne meracie zariadenia, počítače a vybavenie

- HP Proliant ML 150
  2x CPU INTEL XEON 2,8 GHz
  RAM 12 GB
  HDD 35 GB
- MSDN Academic Alliance (MSDN AA), MS Developers Network AA

III. VÝUČBA

III.1. Bakalárske štúdium (Bc.)

●Algebraické štruktúry (B-AS)	(6. sem 2-2 h)	O. Nánásiová/ D. Pancza
●Analýza a zložitosť algoritmov (B-AZA)	(5. sem. 3-1 h)	M. Vojvoda
●Databázové systémy (B-DBS)	(4. sem. 2-2 h)	M. Vojvoda/ Š. Balogh/ M. Čavojský/ M. Repka
●Diskrétna matematika (B-DM)	(4. sem .2-2 h)	M. Polakovič/ V. Čerňanová/ K. Čipková
●Diskrétne udalostné systémy (B-DUS)	(3. sem. 2-2 h)	G.Juhás/ V. Hromada/ S. Marček
●História informatiky (B-HI)	(4. sem. 2-1 h)	O. Grošek/ A. Hambalík
●Klasické šifry (B-KSIF)	(5. sem. 2-2 h)	O.Grošek/ E. Antal
●Lineárna algebra (B-LA)	(3. sem. 2-2 h)	M. Zajac/ I. Marinová/ O. Nánásiová
●Matematická štatistika (B-MATSTAT)	(4. sem. 3-2 h)	O.Nánásiová/ I. Marinová/ E.Pastuchová
●Matematika 1 (B-MAT1E)	(1. sem. 3-2 h)	M. Polakovič/ V.Čerňanová
●Matematika 1 (B-MAT1E)	(1. sem. 4-2 h)	Ľ. Marko/ M.Zákopčan
●Matematika 1 (B-MAT1I)	(1. sem. 3-2 h)	B. Rudolf/ E.Pastuchová/
●Matematika 1 op. (B-MAT1I)	(2. sem. 3-2 h)	I. Bock
●Matematika 1 op. (B-MAT1E)	(2. sem. 3-2 h)	M. Zajac
●Matematika 2 (B-MAT2E)	(2. sem. 3-2 h)	Ľ. Marko/ I.Brilla

●Matematika 2 (B-MAT2I)	(2. sem. 3-2 h)	B. Rudolf/ M. Zákopčan/ M. Kečkemétyová
●Matematika 2 op. (B-MAT2A)	(3. sem. 3-2 h)	M. Kečkemétyová
●Matematika 2 op. (B-MAT2K)	(3. sem. 3-2 h)	I.Brilla
●Matematika 3 (B-MAT3)	(3. sem. 3-2 h)	Ľ. Marko/ I.Brilla/ M. Kečkemétyová
●Matematika 4 (B-MAT4)	(4. sem. 3-2 h)	V. Olejček
●Objektovo orientované programovanie (B-OOP)	(3. sem. 2-2 h)	G. Juhás/ O. Gallo
●Operačné systémy (B-OS)	(5. sem. 2-2 h)	M. Šrámka/ M. Jókay/ M. Gulášová/ Š. Balogh
●Parciálne diferenciálne rovnice (B1-PDR) - SvF	(4. sem. 3-0 h)	I. Bock
●Počítačová kriminalita (B-PKRIM)	(6. sem. 2-2 h)	K. Nemoga/ Š. Balogh/ M. Gulášová
●Počítačové siete (B-PS)	(3. sem. 2-2 h)	M.Oravec/ D. Sopiak/ Z. Bukovčiková/ A. Hambalík/ V. Jirka
●Programovacie techniky (B-PT)	(3. sem. 3-2 h)	M. Drozda/ P. Marák/ S. Marček/ V. Novák
●Programovanie 1 (B-PROG1)	(1. sem. 2-2 h)	P. Zajac/ M. Sýs/ T. Fabšič/ V. Hromada/ M. Jókay/ I. Kossaczký
●Rýchle algoritmy (B-RAL)	(6. sem. 2-2 h)	K. Nemoga/ K. Čipková
●Seminár z B-MAT2I	(2. sem. 0-2 h)	B. Rudolf
●Seminár z B-MAT2E	(2. sem. 0-2 h)	Ľ. Marko
●Softvérové inžinierstvo (B-SWI)	(5. sem. 2-2 h)	M. Šrámka/ O. Gallo
●Vývoj softvérových aplikácií (B-VSA)	(6. sem. 2-2 h)	G. Juhás/ I. Kossaczký/ E. Antal

III.2. Inžinierske štúdium (Ing.)

●Algoritmy a dátové štruktúry (I-ADS)	(3. sem. 3-2 h)	M. Vojvoda
●Architektúra softvérových systémov (I-ASOS)	(3. sem. 2-2 h)	G. Juhás/ I. Kossaczký/ E. Antal
●Automaty a formálne jazyky (I-AFJ)	(2. sem. 2-2 h)	O. Grošek/

		V. Hromada
●Bezpečnosť informačných systémov s pohľadu praxe (I-BISPP)	(2. sem. 3-2 h)	M. Šrámka/ M. Gulášová
●Biometria (I-BIOM)	(3. sem. 2-2 h)	M. Oravec/ D. Sopiak
●Kódovanie (KOD_I) - FIIT	(1. sem. 2-2 h)	K. Čipková
●Logika (I-LOG)	(1.+3. sem. 2-2 h)	K. Nemoga/ K. Čipková
●Matematika (I-MAT)	(1. sem. 2-2 h)	I. Bock
●Mobilné výpočty (I-MOBV)	(3. sem. 2-2 h)	M. Drozda/ V. Novák
●Modelovanie a simulácia udalostných systémov (I-MSUS)	(1. sem. 2-2 h)	G. Juhás/ M. Mladoniczky/ J. Mažári
●Návrh a kryptoanalýza šifier (I-NKS)	(3. sem. 2-2 h)	P.Zajac
●Paralelné programovanie a distribuované systémy (I-PPDS)	(3. sem. 2-2 h)	M. Drozda/ M. Jókay
●Spoločenské, morálne a právne súvislosti vývoja informačných systémov (I-SMPSVIS)	(3. sem. 3-0 h)	M. Šrámka
●Strojové učenie a neurónové siete (I-SUNS)	(1. sem. 2-2 h)	M. Oravec/ D. Sopiak
●Šifrovanie v komunikačných sieťach (I-SKS)	(1. sem. 3-2 h)	K. Nemoga/ M. Sýs
●Úvod do počítačovej bezpečnosti (I-UPB)	(1. sem. 2-1 h)	P. Zajac/ Š. Balogh/ P. Špaček
●Základy kryptografie (I-ZKRY)	(1. sem. 2-2 h)	O. Grošek/ T. Fabšič

III.3. Doktorandské štúdium (PhD.)

●Dizertačná skúška D-DS-AI
●Dizertačný projekt I D-DP1-AI
●Dizertačný projekt II D-DP2-AI
●Dizertačný projekt III D-DP3-AI
●Dizertačný projekt IV D-DP4-AI
●Odborná angličtina D-AJ
●Predmet špecializácie Aplikovaná informatika I D-PS1-AI
●Predmet špecializácie Aplikovaná informatika II D-PS2-AI
●Teória odboru Aplikovaná informatika D-T-AI
●Vedecká práca I D-VP1-AI
●Vedecká práca II D-VP2-AI
●Vedecká práca III D-VP3-AI
●Vedecká práca IV D-VP4-AI

III.4. Bakalárske a inžinierske štúdium pre zahraničných študentov (v anglickom jazyku)

●Matematika 2	K. Čipková
●Objektovo-orientované programovanie	V. Novák
●Operačné systémy	M. Jókay
●Počítačová kriminalita	Š. Balogh
●Rýchle algoritmy	K. Nemoga
●Softvérové inžinierstvo	M. Šrámka
●Vývoj softvérových aplikácii	I. Kossaczký

III.5. Dištančné štúdium

IV. VÝSKUMNÉ PROJEKTY

IV.1. Projekty VEGA, ESF, APVV a iné riešené v roku 2017 na ÚIM

Číslo projektu: VEGA 1/0159/17
Názov projektu: Bezpečná postkvantová kryptografia
Zodpovedný riešiteľ: doc. Ing. Pavol Zajac, PhD.
Zástupca vedúceho projektu: Ing. Viliam Hromada, PhD.
Spoluriešitelia z ÚIM v roku 2017: prof. RNDr. Otokar Grošek, PhD., doc. Ing. Milan Vojvoda, PhD., Mgr. Ing. Matúš Jókay, PhD., Ing. Alexander Hambalík, PhD., Ing. Eugen Antal, PhD., Ing. Ondrej Gallo, PhD., Ing. Štefan Balogh, PhD., Mgr. Tomáš Fabšič, PhD., Ing. Michala Gulášová, Ing. Peter Špaček
Doba riešenia: 2017– 2020

Číslo projektu: VEGA 1/0867/17
Názov projektu: MLbiomedia- Pokročilé metódy strojového učenia na návrh biometrických a medicínskych systémov
Zodpovedný riešiteľ: prof. Dr. Ing. Miloš Oravec
Spoluriešitelia z ÚIM v roku 2017:
Doba riešenia: 2017 - 2020

IV.2. Výskumné úlohy

IV.2.1. Program na podporu mladých výskumníkov

IV.2.2 Pokračujúce projekty na podporu excelentných mladých výskumníkov

IV.3. Zahraničné projekty

IV.3.1. Bilaterálna spolupráca

Názov projektu: Kryptografia prináša bezpečnost a slobodu (Cryptography brings security and freedom
Číslo projektu: SK06-IV-01-001
Zahraničný partner: Selmenovo centrum, Institutt for Informatikk, Universotetet i Bergen, Nórsko

Vedúci projektu: prof. RNDr. Otokar Grošek, PhD.
Vedúci za nórsku stranu: Tor Helleseth
Riešitelia z ÚIM v roku 2017: doc. RNDr. Karol Nemoga, PhD., doc. Ing. Milan Vojvoda, PhD., doc. Ing. Pavol Zajac, PhD., Mgr. Ing. Matúš Jókay, PhD., Ing. Eugen Antal, Ing. Juraj Varga, Ing. Viliam Hromada, PhD., Ing. Pavol Marák, Mgr. Tomáš Fabšič
Riešitelia z Nórska: Igor Semaev, Lilya Budaghyan, Seyed M. M. H. Zadeh, Oleksandr Kholosha, Håvard Raddum
Trvanie projektu: 2014-2017

IV.4. Zapojenie členov ÚIM do výskumných projektov mimo ÚIM

Číslo projektu: APVV-15-0326
Názov projektu: Smart mestá a ich inteligentná energetická chrbtica
Vedúci projektu: prof. Ing. František Janíček, PhD., ÚEAE FEI STU
Spoluriešiteľ z ÚIM v roku 2016: RNDr. Igor Brilla, PhD.
Doba riešenia: 01.07.2016-30.09.2019

ke
Názov projektu: Inteligentné mechatronické systémy
Vedúci projektu: prof. Ing. Štefan Kozák, PhD., ÚAMt FEI STU
Spoluriešitelia z ÚIM v roku 2017: Prof. RNDr. Igor Bock, PhD., Doc. RNDr. Michal Zajac, PhD., RNDr. Mária Kečkemétyová, PhD.
Doba riešenia: 01.01.2017-31.12.2019

Číslo projektu: VEGA 1/0710/15
Názov projektu: Parametrizácia zrážkovo-odtokových procesov pre modelovanie extrémneho odtoku na malých povodiach
Vedúci projektu: prof. Ing. Silvia Kohnová, PhD., SvF STU
Spoluriešiteľ z ÚIM v roku 2015: doc. RNDr. Oľga Nánásiová, PhD.
Doba riešenia: 01.01.2015-31.12.2018

V. SPOLUPRÁCA

V.1. Domáca spolupráca

V.1.1. Pozvané prednášky

Meno: doc. Ing. Pavol Zajac, PhD.
Miesto: Fyzikálny ústav SAV
Prednáška: Post-kvantová kryptografia
Dátum: 24.11.2017

Meno: Dr.rer.nat. Martin Drozda
Miesto: Katedra informatiky, UKF v Nitre
Prednáška: JAYPAD - implementácia messenger aplikácie pre OS Android
Dátum: 7.12.2017

V.1.2. Spolupráca s domácimi inštitúciami

- Kriminalistický a expertízny ústav Policajného zboru MV SR, Bratislava
- Univerzita J. Selyeho v Komárne
- Metodicko-pedagogické centrum mesta Bratislavy
- Virtuálna akadémia bratislavského samosprávneho kraja
- Agentúra na podporu výskumu a vývoja, Bratislava
- Matematický ústav SAV, Bratislava
- Stredisko dištančného vzdelávania (SDV ICV CUP REK) záverečné práce
- Centire s. r. o., Záhradnícka 72, Bratislava – projekt e-Academy pre Daňové riaditeľstvo SR
- Ministerstvo financií SR, Národná koncepcia informatizácie verejnej správy
- Ústav merania SAV, Bratislava
- Slovenský ústav technickej normalizácie, Bratislava
- Ministerstvo zdravotníctva SR, Strategické ciele eHealth
- Národné centrum zdravotníckych informácií, Bratislava, eHealth
- Fakulta manažmentu, UK, Bratislava (doc. RNDr. Mária Bohdalová, PhD.)
- ÚIAa M FCHPT STU (prof. Kolesárová, doc. Šabo)
- Katedra matematiky a deskriptívnej geometrie SvF STU (prof. Mesiar, prof. Širáň, prof. Komorníková, prof. Mikula, doc. Kalina, doc. Jenča, RNDr. Ľubica Valášková, PhD.)
- Katedra matematickej analýzy FMFI UK (doc. Kubáček)
- Katedra matematiky AOS Liptovský Mikuláš (doc. Chovanec, doc. Jurečková, dr. Drobná)
- Katedra matematiky SjF STU (doc.Velichová, dr. Kováčová, doc. Dobrakovová)
- IBM Slovensko, s.r.o.
- Ministerstvo obrany SR

V1.3. Pozvané prednášky domácich odborníkov

Hosť (adresa):
Termíny:
Účel:
Prednáška:

V.2. Zahraničná spolupráca

V.2.1. Pozvané prednášky

Meno: doc. Ing. Pavol Zajac, PhD.
Miesto: Gaithersburg MD, USA
Prednáška: On the explicit reduction between MQ and decoding problems
Dátum: 2.8.2017

Meno: doc. Ing. Pavol Zajac, PhD.
Miesto: Brusel, Belgicko

Prednáška: Cyber Defence Cluster Workshop
Dátum: 10.-12.12.2017

V.2.2. Spolupráca so zahraničnými inštitúciami

- MINT, Emmy Noether Verein, Ulm, Germany (prof. Gudrun Kalmbachová).
- Institut für Algebra und Computermathematik TU, Vienna, Austria (prof. Dietmar Dorninger)
- University of Ljubljana, Ljubljana, Slovenia (doc. J.Bračič).
- Institut de Mathematiques, Université Louis Pasteur, France
- Eszterházy Károly Egyetem, Eger, Maďarsko (Dr. Kis Tóth Lajos, Tóthné dr. Parázsó Lenke)
- Matematický ústav AVČR (RNDr. Jiří Jarušek, DrSc., doc. RNDr. Vladimír Müller, DrSc., RNDr. Miroslav Šilhavý DrSc.)
- Ústav informatiky AVČR (prof. RNDr. Štefan Porubský, DrSc.).
- School of Computer Science, Tel Aviv Univerzity, Tel Aviv, Israel (Dr. Eran Tromer)
- Hubert Curien Laboratory, Jean Monnet University, Saint-Étienne, France (Prof. Viktor Fischer)
- Department of Mathematical Sciences, Florida Atlantic University, Boca Raton, FL, USA (Dr. Rainer Steinwandt)
- Prírodovedecká fakulta Univerzity Hradec Králové, Česká republika
- FernUniversität in Hagen (prof. Dr. Desel)
- University of Gdansk, Poland (Prof. Jaroslaw Pykacz)
- University of Houston, Department of Biomedical Engineering, USA (prof. Metin Akay)

V.2.3. Zahraniční hostia

Hosť (adresa): Prof. Cristina Diogo (Universidade de Lisboa)
Termín: 17.-24.7.2017
Účel: výskumný pobyt

Hosť (adresa): Prof. Janko Bračič (University of Ljubljana)
Termín: 17.-24.7.2017
Účel: výskumný pobyt

V.2.4. Pobyty pracovníkov ÚIM v zahraničí

Meno: doc. Ing. Pavol Zajac, PhD.
Miesto: NIST, Gaithersburg MD, USA
Účel: výskumný pobyt v NIST a spolupráca na písaní článku *Joint multiplicative complexity of Boolean functions*
Dátum: 29.7.-6.8.2017

Meno: Ing. Maroš Čavojský
Miesto: Praha, Česká republika
Účel: štúdijný pobyt v rámci programu Erasmus+

Dátum: 21.9.2017-8.2.2018

V.2.5. Zahraničné cesty

Meno: prof. RNDr. Otokar Grošek, PhD.
Miesto: NATO HQ, Brusel, Belgicko
Zámer cesty: spolupráca s NATO
Dátum: 6.-8.6.2017

Meno: doc. RNDr. Karol Nemoga, PhD.
Miesto: NATO HQ, Brusel, Belgicko
Zámer cesty: spolupráca s NATO
Dátum: 6.-8.6.2017

V.2.6. Stáže zahraničných pracovníkov na ÚIM FEI STU

V.3. Členstvo v medzinárodných organizáciách a spoločnostiach[1]

- **prof. RNDr. Igor Bock, PhD.** je členom ISSMO a GAMM
- **RNDr. Igor Brilla, PhD.** je členom ISIMM a IACM
- **Dr.rer.nat. Martin Drozda** je členom ACM SIGMOBILE.
- **prof. RNDr. Otokar Grošek, PhD**. je zástupcom SR v European Cooperation in the field of Scientific and Technical Research (COST) Action IC1306: Cryptography for Secure Digital Interaction
- **RNDr. Ivica Marinová, PhD.** je členkou ENS v Nemecku
- **doc. RNDr. Ľubomír Marko, PhD.** je členom IACM a SIAM
- **doc. RNDr. Oľga Nánásiová, CSc.,** členka ENS v Nemecku, členka IQSA
- **doc. RNDr. Karol Nemoga, PhD.** je členom IACR a SIAM
- **doc. RNDr. Vladimír Olejček, PhD.** je členom IQSA, člen Bernoulli's Society, SIAM a AMS
- **prof. Dr. Ing. Miloš Oravec** je členom IEEE IET
- **RNDr. Elena Pastuchová, PhD.** je členkou ENS v Nemecku

[1] AMS - American Mathematical Society
ISSMO - International Society of Structural and Multidisciplinary Optimization
GAMM - Gesellschaft für Angewandte Mathematik und Mechanik
ISIMM - International Society for the Interaction of Mechanics and Mathematics
IACM - International Association for Computational Mechanics
SIAM - Society for Industrial and Applied Mathematics
IQSA - International Quantum Structures Assiociation
ENS - Emmy Noether Society
IEEE EMBS - The Institute of Electrical and Electronics Engineers, Engineering Medicine & Biology Society
IEEE IET - Institute of Electrical and Electronics Engineers, Institution of Engineering and Technology
IACR - International Association for Cryptologic Research

VI. OBHÁJENÉ DIZERTÁCIE

Ing. Eugen Antal – *Moderná kryptoanalýza klasických šifier,* školiteľ prof. RNDr. O. Grošek, PhD. , 26.4.2017

Mgr. Tomáš Fabšič - *Príspevok k analýze QC-LDPC McEliece kryptosystému,* školiteľ prof. RNDr. O. Grošek, PhD. , 23.11.2017

Ocenenia: - 1. Študentská osobnosť Slovenska ak.r. 2016/2017 - absolútny víťaz
2. Študentská osobnosť Slovenska ak.r. 2016/2017 - víťaz v kategórii "Informatika a matematicko-fyzikálne vedy"
3. Študent roka - od rektora STU za mimoriadny výsledok v oblasti výskumu a vývoja

VII. INÉ AKTIVITY

VII.1. Akademické a iné funkcie

- **prof. RNDr. Igor Bock, PhD.** je podpredsedom Odborovej komisie (OK) doktorandského štúdia v študijnom programe 3. stupňa 9.1.9 Aplikovaná matematika so sídlom na SvF STU.
- **prof. RNDr. Igor Bock, PhD.** je garantom externého doktorandského štúdia v odbore 9.1.9 Aplikovaná matematika na FEI STU.
- **prof. RNDr. Igor Bock, PhD.** je členom Odborovej komisie doktorandského štúdia v študijnom programe 3. stupňa 9.1.5 Numerická analýza a vedecko-technické výpočty so sídlom na FMFI UK.
- **prof. RNDr. Otokar Grošek, PhD.** je členom Vedeckej rady FEI STU
- **prof. RNDr. Otokar Grošek, PhD.** je predsedom Odborovej komisie (OK) doktorandského štúdia v odbore 9.2.9 Aplikovaná informatika na STU
- **prof. RNDr. Otokar Grošek, PhD.** je člen Odborovej komisie (OK) doktorandského štúdia v odbore 9-1-11 Pravdepodobnosť a matematická štatistika na UMB v Banskej Bystrici od r. 2009.
- **Ing. Alexander Hambalík, PhD.** je lektorom Virtuálnej akadémie Bratislavského samosprávneho kraja
- **Ing. Alexander Hambalík, PhD.** je členom odbornej komisie študentskej vedeckej konferencie FTDK v odbore informatika a prírodné vedy – Univerzita J. Selyeho v Komárne
- **Ing. Alexander Hambalík, PhD.** je akreditovaným skúšobným komisárom pre ECDL v Akreditovanom skúšobnom centre č. 062 FEI STU
- **Ing. Alexander Hambalík, PhD.** je členom komisie pre obhajoby záverečných projektov dvojročného špecializovaného kvalifikačného štúdia z informatiky, realizovaného v Metodicko pedagogickom centre Bratislava, Ševčenková ul.
- **Ing. Alexander Hambalík, PhD.** ELFA, s.r.o. Košice, Datalan, s.r.o. Bratislava, ÚIPŠ MŠ Bratislava, certifikovaný lektor v projekte MVP podporovaný ESF
- **Ing. Mgr. Matúš Jókay, PhD.** je členom AS FEI STU

- **prof. RNDr. Gabriel Juhás, PhD.** je členom OK študijného programu Aplikovaná informatika na STU
- **prof. RNDr. Gabriel Juhás, PhD.** je členom Rady Výskumného centra STU
- **prof. RNDr. Gabriel Juhás, PhD.** je členom riadiaceho výboru pre spoluprácu STU Bratislava a ENEL Slovenské elektrárne, a.s.
- **doc. RNDr. Ľubomír Marko, PhD.** je členom Odborovej komisie (OK) doktorandského štúdia v odbore 9.1.9 Aplikovaná matematika so sídlom na SvF STU.
- **doc. RNDr. Ľubomír Marko, PhD** je členom Vedeckej rady FEI STU
- **doc. RNDr. Oľga Nánásiová , PhD.** je členka Odborovej komisie (OK) doktorandského štúdia v odbore 9.1.9 Aplikovaná matematika so sídlom na SvF STU
- **doc. RNDr. Oľga Nánásiová , PhD.** je členka Odborovej komisie (OK) doktorandského štúdia v odbore 9-1-11 Pravdepodobnosť a matematická štatistika na UMB v Banskej Bystrici od r. 2009.
- **doc. RNDr. Oľga Nánásiová , PhD.** je členka komisie pre štátne skúšky doktorandského štúdia(dizertačná skúška, obhajoba dizertačnej práce) v študijných programoch 3.3.15. manažment a 3.3.22. podnikový manažment **na FM UK**
- **doc. RNDr. Karol Nemoga, PhD.** je členom Vedeckej rady Matematického ústavu SAV
- **doc. RNDr. Karol Nemoga, PhD.** je podpredseda Edičnej rady SAV
- **doc. RNDr. Karol Nemoga, PhD.** je člen Snemu SAV
- **doc. RNDr. Karol Nemoga, PhD.** je člen NATO ISEG, Brusel
- **doc. RNDr. Karol Nemoga, PhD.** je člen Vedeckej rady Prírodovedeckej fakulty Univerzity Hradec Králové
- **doc. RNDr. Vladimír Olejček, PhD.** je členom Odborovej komisie (OK) doktorandského štúdia v odbore 9.1.9 Aplikovaná matematika so sídlom na SvF STU.
- **prof. Dr. Ing. Miloš Oravec** je dekanom FEI STU
- **prof. Dr. Ing. Miloš Oravec** je predsedom Vedeckej rady FEI STU
- **prof. Dr. Ing. Miloš Oravec** je predsedom Kolégia dekana FEI STU
- **prof. Dr. Ing. Miloš Oravec** je členom Kolégia rektora STU v Bratislave a členom Vedeckej rady STU v Bratislave
- **prof. Dr. Ing. Miloš Oravec** je členom Vedeckých rád MFF UK, FEI TU v Košiciach, EF ŽU v Žiline, FIIT STU v Bratislave, MTF STU v Bratislave
- **prof. Dr. Ing. Miloš Oravec** je členom OK študijného programu Aplikovaná informatika a členom OK Kybernetika na STU
- **prof. Dr. Ing. Miloš Oravec** je garantom študijného programu bakalárskeho a inžinierskeho štúdia Aplikovaná informatika na FEI STU
- **prof. Dr. Ing. Miloš Oravec** je člen komisie KEGA (Kultúrna a edukačná grantová agentúra Ministerstva školstva, vedy, výskumu a športu SR)
- **doc. RNDr. Boris Rudolf, PhD.** je členom Odborovej komisie (OK) doktorandského štúdia v odbore 9.1.9 Aplikovaná matematika so sídlom na SvF STU
- **doc. Ing. Michal Šrámka, PhD.** je členom Odborovej komisie (OK) doktorandského štúdia v odbore 9.2.9 Aplikovaná informatika na STU
- **doc. RNDr. Michal Zajac, PhD.** je členom Odborovej komisie (OK) doktorandského štúdia v odbore 9.1.9 Aplikovaná matematika so sídlom na SvF STU
- **doc. RNDr. Michal Zajac, PhD.** je členom AS FEI STU

VII.2. Členstvo v domácich spoločnostiach a organizáciách[2]

[2] JSFM - Jednota slovenských matematikov a fyzikov

- **prof. RNDr. Igor Bock, PhD.** je členom JSMF, SSM
- **RNDr. Igor Brilla, PhD.** je členom SSM
- **prof. RNDr. Otokar Grošek, PhD.** je členom JSMF
- **RNDr. Mária Kečkemétyová, PhD.** je členkou JSMF
- **RNDr. Ivica Marinová, PhD.** je členkou JSMF
- **doc. RNDr. Ľubomír Marko, PhD.** je členom SSM
- **doc. RNDr. Oľga Nánásiová, CSc.** je členkou celoštátneho výboru SSM, členkou JSMF a Slovenskej štatistickej a demografickej spoločnosti
- **doc. RNDr. Karol Nemoga, PhD.** je členom JSMF a Slovenského plynárenského a naftového zväzu
- **doc. RNDr. Vladimír Olejček, PhD.** je členom JSMF
- **prof. Dr. Ing. Miloš Oravec** je členom SKSI
- **RNDr. Elena Pastuchová, PhD.** je členkou JSMF a Slovenskej štatistickej a demografickej spoločnosti
- **doc. Mgr. Marcel Polakovič, PhD.** je členom JSMF
- **doc. RNDr. Boris Rudolf, PhD.** je členom JSMF
- **doc. RNDr. Michal Zajac PhD.** je členom JSMF

VII.3. Vedenie prác študentov v súťažiach

Súťaž Keymaker (súčasť konferencie Mikulášska kryptobesídka):

1. miesto v kategórii diplomových prác - Ing. Peter Špaček, vedúci P. Zajac
2. miesto v kategórii diplomových prác – Ing. Martin Eliáš, vedúci E. Antal

VIII. PUBLIKÁCIE

ADC Vedecké práce v zahraničných karentovaných časopisoch

ADC01 BRENKUŠ, Juraj - STOPJAKOVÁ, Viera - ČERŇANOVÁ, Viera - ARBET, Daniel - NAGY, Lukáš - SEDLÁK, Vladimír. A novel method towards time-efficient fault analysis of analog and mixed-signal circuits. In *Journal of Circuits Systems and Computers*. Vol. 26, No. 8 (2017), Art. no. 1740005 [20] s. ISSN 0218-1266. V databáze: CC: 000399226200006 ; SCOPUS: 2-s2.0-85017368725.

ADC02 ZAJAC, Pavol. Upper bounds on the complexity of algebraic cryptanalysis of ciphers with a low multiplicative complexity. In *Designs, Codes and Cryptography*. Vol. 82, Iss. 1 (2017), s. 43-56. ISSN 0925-1022. V databáze: CC: 000392310500004.

SSM - Slovenskej spoločnosti pre mechaniku
SSKI - Slovenská spoločnosť pre kybernetiku a informatiku
SBIMI - Spoločnosť biomedicínskeho inžinierstva a medicínskej informatiky

ADM Vedecké práce v zahraničných časopisoch registrovaných v databázach Web of Science alebo SCOPUS

ADM01 ANTAL, Eugen - GROŠEK, Otokar - HORÁK, Peter. On a mnemonic construction of permutations. In *Journal of Mathematical Cryptology*. Vol. 11, Iss. 1 (2017), s. 45-53. ISSN 1862-2976. V databáze: SCOPUS: 2-s2.0-85014641684&.

ADM02 ROKICKI, Markus - DROZDA, Martin. Evaluating trade-offs in energy-efficient error detection. In *International Journal of Communication Systems : Energy Efficient Networking*. Vol. 30, Iss. 7 (2017), Art. no. e3028 [18] s. ISSN 1074-5351. V databáze: WOS: 000405964000007 ; SCOPUS: 2-s2.0-84939181523.

ADN Vedecké práce v domácich časopisoch registrovaných v databázach Web of Science alebo SCOPUS

ADN01 ANTAL, Eugen - ELIÁŠ, Martin. Evolutionary Computation in cryptanalysis of classical ciphers. In *Tatra Mountains Mathematical Publications*. Vol. 70, (2017), s. 179-197. ISSN 1210-3195.

ADN02 VARGA, Juraj - ŠVANDA, Dominik - VARCHOLA, Marek - ZAJAC, Pavol. Authentication based on gestures with smartphone in hand. In *Journal of Electrical Engineering*. Vol. 68, No. 4 (2017), s. 256-266. ISSN 1335-3632. V databáze: WOS: 000410953500002.

ADN03 ZAJAC, Pavol. Connecting the complexity of MQ- and code-based cryptosystems. In *Tatra Mountains Mathematical Publications*. Vol. 70, (2017), s. 163-177. ISSN 1210-3195.

AFB Publikované pozvané príspevky na domácich vedeckých konferenciách

AFB01 JUHÁS, Gabriel - MOLNÁR, Ľudovít - ONDRISOVÁ, Miriam - JUHÁSOVÁ, Ana. Data, information and technology services for research and management of science. In *ICETA 2017 : 15th IEEE International conference on emerging elearning technologies and applications : Information and communication technologies in learning. Starý Smokovec, Slovakia. October 26-27, 2017*. Danvers : IEEE, 2017, S. 189-194. ISBN 978-1-5386-3296-3. V databáze: IEEE ; SCOPUS: 2-s2.0-85040774660.

AFC Publikované príspevky na zahraničných vedeckých konferenciách

AFC01 ANDONOVA, Monika - PAVLOVIČOVÁ, Jarmila - KAJAN, Slavomír - ORAVEC, Miloš - KURILOVÁ, Veronika. Diabetic retinopathy screening based on CNN. In *Proceedings ELMAR-2017 : 59th International symposium. Zadar, Croatia. 18-20 September, 2017*. Zagreb : University of Zagreb, 2017, S. 51-54. ISSN 1334-2630. ISBN 978-953-184-230-3. V databáze: IEEE ; SCOPUS: 2-s2.0-85041553056.

AFC02 BOCK, Igor. Regularized optimal design problem for a viscoelastic plate vibrating against a rigid obstacle. In *CSMO 2015 : 27th IFIP TC conference on system modeling and optimization. Sophia Antipolis, France. June 29-July 3, 2015*. Cham : Springer, 2017, S. 127-136. ISBN 978-3-319-55794-6. V databáze: SCOPUS: 2-s2.0-85018681863.

AFC03 BRILLA, Igor. Numerical determination of voltage potential inside three dimensional orthotropic media using variational methods. In *CAIP´2017 : 13° Congreso interamericano de computación aplicado a la industria de procesos. Ciudad de México, México. 25 al 28 de Septiembre de 2017*. Ciudad de México : ITAM, 2017, S. 136-143. ISBN 978-607-8242-11-5.

AFC04 BUKOVČIKOVÁ, Zuzana - SOPIAK, Dominik - ORAVEC, Miloš - PAVLOVIČOVÁ, Jarmila. Face verification using convolutional neural networks with Siamese architecture. In *Proceedings ELMAR-2017 : 59th International symposium. Zadar, Croatia. 18-20 September, 2017*. Zagreb : University of Zagreb, 2017, S. 205-208. ISSN 1334-2630. ISBN 978-953-184-230-3. V databáze: IEEE ; SCOPUS: 2-s2.0-85041514847.

AFC05 FABŠIČ, Tomáš - HROMADA, Viliam - STANKOVSKI, Paul - ZAJAC, Pavol - GUO, Qian - JOHANSSON, Thomas. A reaction attack on the QC-LDPC McEliece cryptosystem. In *Post-quantum cryptography : 8th International conference. Utrecht, The Netherlands. June 26-28, 2017*. Cham : Springer, 2017, S. 51-68. ISBN 978-3-319-59878-9. V databáze: SCOPUS: 2-s2.0-85021776403.

AFC06 GERÁT, Jozef - SOPIAK, Dominik - ORAVEC, Miloš - PAVLOVIČOVÁ, Jarmila. Vehicle speed detection from camera stream using image processing methods. In *Proceedings ELMAR-2017 : 59th International symposium. Zadar, Croatia. 18-20 September, 2017*. Zagreb : University of Zagreb, 2017, S. 201-204. ISSN 1334-2630. ISBN 978-953-184-230-3. V databáze: IEEE ; SCOPUS: 2-s2.0-85041521346.

AFC07 MAŽÁRI, Juraj - JUHÁS, Gabriel - MLADONICZKY, Milan - GAŽO, Tomáš - MAKÁŇ, Martin. Netgrif workflow management system based on Petriflow language. In *Algorithms and Tools for Petri nets : Workshop AWPN 2017. Kgs. Lyngby, Denmark. October 19-20, 2017*. Kgs. Lyngby : DTU Compute, 2017, S. 39-44. ISSN 1601-2321.

AFC08 MLADONICZKY, Milan - JUHÁS, Gabriel - MAŽÁRI, Juraj - GAŽO, Tomáš - MAKÁŇ, Martin. Petriflow: Rapid language for modelling Petri nets with roles and data fields. In *Algorithms and Tools for Petri nets : Workshop AWPN 2017. Kgs. Lyngby, Denmark. October 19-20, 2017*. Kgs. Lyngby : DTU Compute, 2017, S. 45-50. ISSN 1601-2321.

AFD Publikované príspevky na domácich vedeckých konferenciách

AFD01 GULÁŠOVÁ, Michala - JÓKAY, Matúš. Steganalysis. In *ELITECH´17 [elektronický zdroj] : 19th Conference of doctoral students. Bratislava, Slovakia. May 24, 2017*. 1. ed. Bratislava : Spektrum STU, 2017, CD-ROM, [4] p. ISBN 978-80-227-4686-1.

AFD02 MARKOŠOVÁ, Mária - RUDOLF, Boris - ČAJÁGI, Martin - NÁTHER, Peter. Analytically solvable models of the scale free growing network with hierarchy. In *Aplimat 2017 [elektronický zdroj] : proceedings of the 16th conference on Applied Mathematics. Bratislava, 31.1. -2.2. 2017*. 1. vyd. Bratislava : Vydavateľstvo Spektrum STU, 2017, CD-ROM, S. 1014-1023. ISBN 978-80-227-4650-2.

AFH Abstrakty príspevkov z domácich konferencií

AFH01 BOHDALOVÁ, Mária - KALINA, Martin - NÁNÁSIOVÁ, Oľga. Modelovanie kauzality II. In *PRASTAN 2017 : zborník abstraktov. Oščadnica, SR, 5. - 8. októbra 2017*. 1. vyd. Bratislava : Jednota slovenských matematikov a fyzikov, 2017, S. 7. ISBN 978-80-89829-04-0.

AFH02 NÁNÁSIOVÁ, Oľga - ČERŇANOVÁ, Viera - VALÁŠKOVÁ, Ľubica. Modelovanie logických spojok. In *PRASTAN 2017 : zborník abstraktov. Oščadnica, SR, 5. - 8. októbra 2017*. 1. vyd. Bratislava : Jednota slovenských matematikov a fyzikov, 2017, S. 18. ISBN 978-80-89829-04-0.

BEE Odborné práce v zahraničných zborníkoch (konferenčných aj nekonferenčných)

BEE01 ELIÁŠ, Martin - ANTAL, Eugen. Lúštenie historických šifier na GRIDe pomocou GA a PGA. In *Mikulášská kryptobesídka 2017 : sborník příspěvků. Praha, ČR, 31. 11. - 1. 12. 2017*. 1. vyd. Bílovice nad Svitavou : Trusted Network Solutions, 2017, S. 65-66.

BFA Abstrakty odborných prác zo zahraničných podujatí (konferencie...)

BFA01 HAMBALÍK, Alexander. Virtuális laboratórium biometria témájú oktatáshoz és kutatáshoz. In *Agria Média 2017, ICI 15 : 12. Információtechnikai és oktatástechnológiai konferencia és kiállitás. Eger, Hungary. Október 11-13, 2017*. Eger : Eszterházy Károly Egyetem, 2017, S. 44-45.

BFA02 HROMADA, Viliam - PETHŐ, Tibor. Desynchronization fault analysis of Grain v1. In *CECC 2017 : Book of abstracts : 17th Central European conference on cryptology. Warsaw, Poland. June 28-30, 2017*. Warsaw : University of Technology, 2017, S. 39-40.

BFA03 ZAJAC, Pavol. Hybrid encryption from McEliece cryptosystem. In *CECC 2017 : Book of abstracts : 17th Central European conference on cryptology. Warsaw, Poland. June 28-30, 2017*. Warsaw : University of Technology, 2017, S. 16-17.

DAI Dizertačné a habilitačné práce

DAI01 ANTAL, Eugen. *Moderná kryptoanalýza klasických šifier : dát. obhaj. 26.4.2017, č. ved. odb. 9-2-9*. Bratislava :. STU v Bratislave FEI,. 2017. 133 s. Dostupné na internete: <http://is.stuba.sk/zp/portal_zp.pl?podrobnosti=130771>.

DAI02 FABŠIČ, Tomáš. *Contributions to the Analysis of the QC-LDPC McEliece Cryptosystem : dát. obhaj. 23.11.2017, č. ved. odboru 9-2-9*. Bratislava :. STU v Bratislave FEI,. 2017. 119 s. Dostupné na internete: <http://is.stuba.sk/zp/portal_zp.pl?podrobnosti=130770>.

FAI Redakčné a zostavovateľské práce knižného charakteru (bibliografie, encyklopédie, katalógy, slovníky, zborníky...)

FAI01 KALINA, Martin (ed.) - MINÁROVÁ , Mária (ed.) - NÁNÁSIOVÁ, Oľga (ed.). *PRASTAN 2017 : zborník abstraktov. Oščadnica, SR, 5. - 8. októbra 2017*. 1. vyd. Bratislava : Jednota slovenských matematikov a fyzikov, 2017. 25 s. ISBN 978-80-89829-04-0.

GHG Práce zverejnené na internete

GHG01 FABŠIČ, Tomáš - GALLO, Ondrej - HROMADA, Viliam. Demonstration of acoustic cryptanalysis. In *CryptArchi 2017 [elektronický zdroj] : 15th International workshop on cryptographic architectures embedded in logic devices. Smolenice, Slovakia. June 18-21, 2017*. Saint-Étienne : Laboratoire Hubert Curien, 2017, online, S. 11.

Štatistika: kategória publikačnej činnosti

ADC	Vedecké práce v zahraničných karentovaných časopisoch	2
ADM	Vedecké práce v zahraničných časopisoch registrovaných v databázach Web of Science alebo SCOPUS	2
ADN	Vedecké práce v domácich časopisoch registrovaných v databázach Web of Science alebo SCOPUS	3
AFB	Publikované pozvané príspevky na domácich vedeckých konferenciách	1
AFC	Publikované príspevky na zahraničných vedeckých konferenciách	8
AFD	Publikované príspevky na domácich vedeckých konferenciách	2
AFH	Abstrakty príspevkov z domácich konferencií	2
BEE	Odborné práce v zahraničných zborníkoch (konferenčných aj nekonferenčných)	1
BFA	Abstrakty odborných prác zo zahraničných podujatí (konferencie...)	3
DAI	Dizertačné a habilitačné práce	2
FAI	Redakčné a zostavovateľské práce knižného charakteru (bibliografie, encyklopédie, katalógy, slovníky, zborníky...)	1
GHG	Práce zverejnené na internete	1
Súčet		**28**

IX. VÝCHOVA VEDECKÝCH PRACOVNÍKOV

IX.1. Interní doktorandi

Doktorand: Ing. Eugen Antal
Školiteľ: prof. RNDr. Otokar Grošek, PhD.
Školiteľ špecialista: Mgr. Marek Sýs, PhD.
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 5.6.2013
Téma práce: Moderná kryptoanalýza klasických šifier
Obhájil: 26.4.2017

Doktorand: Ing. Zuzana Bukovčiková
Školiteľ: prof. Dr. Ing. Miloš Oravec
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika

Pracovisko: ÚIM, FEI STU
Dizertačná skúška:
Predpokladaný termín ukončenia:
Téma práce: Obsahovo orientované prehľadávanie obrazov pre biometriu

Doktorand: Ing. Maroš Čavojský
Školiteľ: Dr.rer.nat. Martin Drozda
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 18.2.2016
Predpokladaný termín ukončenia: 2018
Téma práce: Metodológia a systém na efektívne testovanie mobilných aplikácií

Doktorand: Mgr. Tomáš Fabšič
Školiteľ: prof. RNDr. Otokar Grošek, PhD.
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 30.9.2015
Prerušenie: 1.2.-2.9.2014
Téma práce: Postranné kanály
Obhájil: 23.11.2017

Doktorand: Ing. Michala Gulášová
Školiteľ: doc. Ing. Milan Vojvoda, PhD.
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška:
Predpokladaný termín ukončenia: 31.8.2019
Téma práce: Steganografia a stegoanalýza

Doktorand: Ing. Vojtěch Jirka
Školiteľ: prof. Dr. Ing. Miloš Oravec
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 22.5.2014
Predpokladaný termín ukončenia: 2018
Téma práce: Nové metódy biometrického rozpoznávania tvárí v neriadených podmienkach využitím metód strojového učenia
Prerušenie: 1.7.2015-2.7.2018

Doktorand: Ing. Pavol Marák
Školiteľ: prof. RNDr. Otokar Grošek, PhD.
Školiteľ špecialista: Ing. Alexander Hambalík, PhD.
Forma vzdelávania: doktorandské štúdium – interná forma

Odbor: Aplikovaná informatika
Pracovisko: ÚIM**,** FEI STU
Dizertačná skúška: 25.4.2015
Predpokladaný termín ukončenia:
Téma práce: Charakteristické vlastnosti odtlačkov prstov a dlaní a ich automatické rozpoznávanie
Prerušené: 01. 09. 2017 - 02. 09. 2018

Doktorand: Ing. Juraj Mažári

Školiteľ: prof. Ing. Gabriel Juhás, PhD.
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška:
Téma práce: Syntéza workflow procesov z pozorovaného správania

Doktorand: Ing. Milan Mladoniczky

Školiteľ: prof. Ing. Gabriel Juhás, PhD.
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška:
Téma práce: Analýza a korekcia workflow procesov so zdieľanými zdrojmi

Doktorand: Ing. Dominik Sopiak

Školiteľ: prof. Dr. Ing. Miloš Oravec
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 16.5.2016
Predpokladaný termín ukončenia: 2019
Téma práce: Návrh multimodálneho biometrického systému
Prerušenie: 1.9.2017 -2.9.2019

Doktorand: Ing. Peter Špaček

Školiteľ: doc. Ing. Pavol Zajac, PhD.
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Predpokladaný termín ukončenia:
Téma práce: Bezpečná postkvantová kryptografia

Doktorand: Ing. Juraj Varga

Školiteľ: doc. Ing. Pavol Zajac, PhD.
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 14.6.2013
Predpokladaný termín ukončenia:

Téma práce: Bezpečnosť mobilných zariadení
Prerušenie: 01.8.2016 - 31.7.2018

IX.2. Externí doktorandi

Doktorand: Ing. Robert Bučko
Školiteľ: doc. RNDr. Jaroslav Fogel, PhD.
Forma vzdelávania: doktorandské štúdium – externá forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM FEI STU
Dizertačná skúška: 28.3.2015
Predpokladaný termín ukončenia: 31.8.2015
Téma práce: Verifikačné metódy v multiagentových systémoch
Zanechal: 31.8.2017

Doktorand: Ing. Csaba Cserba
Školiteľ: prof. RNDr. Gabriel Juhás, PhD.
Forma vzdelávania: doktorandské štúdium – externá forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška:
Predpokladaný termín ukončenia:
Téma práce: Analýza Petriho sietí
Zanechal: 3.4.2017

Doktorand: Ing. Igor Kazlov
Školiteľ: prof. RNDr. Gabriel Juhás, PhD.
Forma vzdelávania: doktorandské štúdium –externá forma od 1.6.2014, interná forma do 31.5.2014
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 14.11.2012
Predpokladaný termín ukončenia: 30.8.2013
Téma práce: Analýza udalostných systémov s viacerými inštanciami
Prerušenie: 31.8.2017 - 30.8.2018

Doktorand: MUDr.Veronika Kurilová (rod. Hanúsková)
Školiteľ: prof. Dr. Ing. Miloš Oravec
Forma vzdelávania: doktorandské štúdium – externá forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM FEI STU
Dizertačná skúška: 29.4.2014
Predpokladaný termín ukončenia:
Téma práce: Nové metódy diagnostiky v oftalmológii
Prerušenie: 1.9.2016-2.9.2018

Doktorand: Ing. Peter Minarovský
Školiteľ: doc. Ing. Michal Šrámka, PhD.
Forma vzdelávania: doktorandské štúdium – externá forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška:
Predpokladaný termín ukončenia: máj 2020
Téma práce: Unikátnosť kódu

Doktorand: Ing. Štefan Počarovský
Školiteľ: prof. RNDr. Gabriel Juhás, PhD.
Forma vzdelávania: doktorandské štúdium – externá forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 19.3.2014
Predpokladaný termín ukončenia:
Téma práce: Virtualizácia elektronických služieb
Prerušenie: 01.6.2016 - 31.5.2018

Doktorand: Mgr. Tomáš Žilka
Školiteľ: prof. RNDr. Igor Bock, PhD.
Prijatý dňa: 8.7.2010
Forma vzdelávania: doktorandské štúdium – externá forma od 2.9.2015
Odbor: 9.1.9 Aplikovaná matematika
Pracovisko: OM ÚIM FEI STU v Bratislave
Dátum dizertačnej skúšky: 28.2.2012
Predpokladaný termín ukončenia: 31.8.2016
Prerušenie: 1.9.2014-1.9.2015
Téma práce: Dynamický kontakt dosky s prekážkou
Zanechal: 31.8.2017

Doktorand: Mgr. Viktória Žilková (rod. Rozborová)
Školiteľ: doc. RNDr. Michal Zajac, PhD.
Prijatá dňa: 8.7.2010
Forma vzdelávania: doktorandské štúdium – externá forma od 2.9.2015
Odbor: 9.1.9 Aplikovaná matematika
Pracovisko: OM ÚIM FEI STU v Bratislave
Dátum dizertačnej skúšky: 28.2.2012
Predpokladaný termín ukončenia: 31.8.2016
Prerušenie: 1.9.2014-1.9.2015
Téma práce: Hyperreflexívnosť priestorov lineárnych operátorov
Zanechala: 31.8.2017

IX.3. Doktorandi vedení pracovníkmi ÚIM na iných pracoviskách

Doktorand: Ing. Dušan Janál
Školiteľ: doc. RNDr. Oľga Nánásiová, PhD.
Forma vzdelávania: doktorandské štúdium – denná forma

Odbor: 9.1.9 Aplikovaná matematika
Pracovisko: Katedra matematiky a deskriptívnej geometrie
Dátum dizertačnej skúšky: 27.3. 2013
Ukončil štúdium: 31.8.2017
Téma práce: Viacrozmerné štatistické metódy a ich aplikácie

X. ÚČASŤ PRACOVNÍKOV ÚSTAVU NA KONFERENCIÁCH

X.1. Zahraničné konferencie

NÁZOV KONFERENCIE : *Olomoucké dny aplikované matematiky*
Miesto: Olomouc, Česká republika
Dátum: 30.5.-2.6.2017
Meno: prof. RNDr. Igor Bock, PhD.
Príspevok: On hyperbolic variational inequalities

NÁZOV KONFERENCIE : *Petri Nets 2017 a ACSD 2017*
Miesto: Zaragoza, Španielsko
Dátum: 27.-30.6.2017
Meno: prof. Ing. Gabriel Juhás, PhD.

NÁZOV KONFERENCIE : PQCrypto 2017
Miesto: Utrecht, Holandsko
Dátum: 26-28.6.2017
Meno: Mgr. Tomáš Fabšič, PhD.
Príspevok: A Reaction Attack on the QC-LDPC McEliece Cryptosystem

NÁZOV KONFERENCIE : *17th Central European Conference on Cryptology CECC´17*
Miesto: Varšava, Poľsko
Dátum: 27.6.-1.7.2017
Meno: Ing. Viliam Hromada, PhD.
Príspevok: Desynchronisation Fault Analysis of Grain v1

NÁZOV KONFERENCIE : *17th Central European Conference on Cryptology CECC´17*
Miesto: Varšava, Poľsko
Dátum: 27.6.-1.7.2017
Meno: doc. Ing. Pavol Zajac, PhD.
Príspevok: Hybrid encryption from McEliece cryptosystem

NÁZOV KONFERENCIE : *59th International Symposium Elmar 2017*
Miesto: Zadar, Chorvátsko
Dátum: 17.-20.9.2017
Meno: Ing. Dominik Sopiak
Príspevok: Vehicle Speed Detection from Camera Stream using Image Processing Methods
Príspevok: Face Verification Using Convolutional Neutral Networks with Siame Arcitecture

NÁZOV KONFERENCIE : *Agria Media 2017*
Miesto: Eger, Maďarsko
Dátum: 11.-13.10.2017

Meno: Ing. Alexander Hambalík, PhD.
Príspevok: Virtuális laboratórium biometria témájú oktatáshoz és kutatáshoz

NÁZOV KONFERENCIE : Algorithms and Tools for Petri Nets – Proceeding of the Workshop AWPN 2017
Miesto: Lyngby, Dánsko
Dátum: 19.-20.10.2017
Meno: prof. RNDr. Gabriel Juhás, PhD., Ing. Juraj Mažári, Ing. Milan Mladoniczky
Príspevok: Petriflow: Rapid language for modellins Petri nets witj roles and data fields
Príspevok: Netgrif Workflow Management Systém based on Petriflow language

NÁZOV KONFERENCIE : *Web Summit*
Miesto: Lisabon, Portugalsko
Dátum: 5.-10.11.2017
Meno: Dr.rer.nat. Martin Drozda

NÁZOV KONFERENCIE : *Web Summit*
Miesto: Lisabon, Portugalsko
Dátum: 5.-10.11.2017
Meno: Ing. Maroš Čavojský

NÁZOV KONFERENCIE : *Mikulášska kryptobesídka 2017*
Miesto: Praha, Česká republika
Dátum: 29.11.-1.12.2017
Meno: Ing. Eugen Antal, PhD.
Príspevok: Lúštenie historických šifier na GRIDe pomocou GA a PGA

NÁZOV KONFERENCIE : *Mikulášska kryptobesídka 2017*
Miesto: Praha, Česká republika
Dátum: 29.11.-1.12.2017
Meno: Ing. Peter Špaček
Príspevok: Mc Eliece Engine for TLS

NÁZOV KONFERENCIE : Mikulášska kryptobesídka 2017
Miesto: Praha, Česká republika
Dátum: 29.11.-1.12.2017
Meno: doc. Ing. Pavol Zajac PhD.

X.2. Domáce konferencie

NÁZOV KONFERENCIE :
Miesto:
Dátum:
Meno:
Príspevok:

NÁZOV KONFERENCIE : *Štipendijný program EHP Slovensko* Záverečná konferencia
Miesto: Bratislava, Austria Trend Hotel

Dátum: 25.1.2017
Meno: prof. RNDr. Otokar Grošek, PhD.
Príspevok: O vysledkoch projektu SK06-IV-01-001

NÁZOV KONFERENCIE : Kryptorealita a budúcnosť IT bezpečnosti
Miesto: Kongresové centrum hotela Holiday Inn v Bratislave
Dátum: 16.5.2017
Meno: prof. RNDr. Otokar Grošek, PhD.

NÁZOV KONFERENCIE : *European Historical Ciphers Colloquium 2017*
Miesto: Smolenice
Dátum: 17.-19.5.2017
Meno: Ing. Eugen Antal, PhD.

NÁZOV KONFERENCIE : *European Historical Ciphers Colloquium 2017*
Miesto: Smolenice
Dátum: 17.-19.5.2017
Meno: doc. Ing. Pavol Zajac, PhD.

NÁZOV KONFERENCIE : *ELITECH'17*
Miesto: Bratislava, FEI STU
Dátum: 24. 5. 2017
Meno: Ing. Michala Gulášová
Príspevok: Steganalysis

NÁZOV KONFERENCIE : *Cryptographic Architectures Embedded in Logic Devices*
Miesto: Smolenice
Dátum: 20.6.2017
Meno: Ing. Viliam Hromada, PhD., Ing. Ondrej Gallo, PhD.
Príspevok: Demonstration of the Acoustic Cryptanalysis

NÁZOV KONFERENCIE : *Conference on Differential and Difference Equations and Applications CDDEA 2017*
Miesto: Jasná
Dátum: 26.-30.6.2017
Meno: RNDr. Mária Kečmétyová, PhD.
Príspevok: An optimal control problem for a viscoelastic plate in a dynamic contact with an obstacle

NÁZOV KONFERENCIE : PRASTAN 2017, Slovensko - česká konferencia
Miesto: Oščadnica
Dátum: 5. – 8. októbra 2017
Meno: doc. RNDr. Oľga Nánásiová, PhD., RNDr.Viera Čerňanová, PhD.
Príspevok: Modelovanie logických spojok

NÁZOV KONFERENCIE : PRASTAN 2017, Slovensko - česká konferencia
Miesto: Oščadnica
Dátum: 5. – 8. októbra 2017
Meno: doc. RNDr. Oľga Nánásiová, PhD.
Príspevok: Modelovanie kauzality II

XI. HABILITAČNÉ A INAUGURAČNÉ KONANIA

XI.1. Inauguračné konania

XI.2. Habilitačné konania

prof. RNDr. Otokar Grošek, PhD. - Člen habilitačnej komisie RNDr. Tatiany Jajcayovej, PhD. na MFF UK, 18.9.2017

XI.3. Členstvá v komisiách

prof. RNDr.Igor Bock, PhD. – predseda habilitačnej komisie Ing. Márie Kúdelčíkovej, PhD. Stavebná fak. STU v Bratislave, 25.05.2017

XII. ČINNOSŤ V OBLASTI DOKTORSKÝCH DIZERTAČNÝCH PRÁC (DrSc.) A DOKTORANDSKÝCH DIZERTAČNÝCH PRÁC

XII.1. Obhajoby dizertačnej práce na ÚIM

XII.2. Dizertačné skúšky na ÚIM

XII.3. Dizertačné skúšky a obhajoby dizertačných prác na iných pracoviskách

prof. RNDr. Otokar Grošek, PhD. – predseda komisie na obhajobu dizertačnej práce RNDr. Petra Kostolányiho na FMFI UK dňa 20.6.2017

doc. RNDr. Michal Zajac, PhD. – člen komisie a oponent dizertačnej práce Mgr. Anny Miškovej na Prírodovedeckej fakulte UPJŠ Košice, 29.5.2017

doc. RNDr. Michal Zajac, PhD. – člen komisie a oponent dizertačnej práce Mgr. Antona Belana na FMFI UK v Bratislave 30.8.2017

XII.4. Oponentské posudky k dizertačnej práci

prof. RNDr. Igor Bock, PhD.- práca Ing. Mgr. Lukáša Tomeka s náyvom *Finite volume methods for mean curvature flow of surfaces* (obhájená 28.8.2017 na Katedre matematiky a deskriptívnej geometrie, SvF STU)

doc. RNDr. Michal Zajac, PhD. – práca RNDr. Anny Miškovej s názvom *Time-Frequency Analysis of Toeplitz Operators* (obhájená 29.5.2017 na ÚMV PF UPJŠ v Košiciach)

doc. RNDr. Michal Zajac, PhD. – práca Mgr.. Antona Belana s názvom *Potreba dôkazov vo vyučovaní matematiky* (obhájená 30.8.2017 na FMFI UK v Bratislave)

XII.5. Skúšky doktorandov z doktorandských predmetov

Meno Doktoranda	Odbor štúdia	Meno skúšajúceho	Predmet	Dátum
Michala Gulášová	API/BIS	Karol Nemoga	Kódovanie	12.4.2017
Michala Gulášová	API/BIS	Otokar Grošek	Viacrozmerné štatistické metódy	30.6.2017
Peter Minarovský	API	Michal Šrámka	Ochrana súkromia	2.2.2017
Peter Minarovský	API	Michal Šrámka	Komunikačné siete	19.7.2017

XIII. ŠVOČ, VEDENIE DIPLOMOVÝCH PRÁC, ČLENSTVO V ŠTÁTNICOVÝCH KOMISIÁCH

XIII.1. ŠVOČ

Meno: prof. RNDr. Igor Bock, PhD.
Predseda komisie pre posúdenie prác Študentskej vedeckej konferencie na Staveb. Fak. STU v sekcii Matematické a počítačové modelovanie, 21.4.2017

Sekcia: Aplikovaná informatika

Študent:

Sekcia :
Meno:

XIII.2. VEDENIE UKONČENÝCH DIPLOMOVÝCH PRÁC

Adamec Miroslav, Bc.: Export emailov z databáz MS Exchange a Outlook plugin pracujúci s týmito emailami (K. Čipková)
Balla Martin, Bc.: Generovanie binárnych vektorov s definovanou váhou (P. Zajac)
Balušík Igor, Bc.: Paralelné bio-inšpirované algoritmy (I. Sekaj)
Bekeč Kamil, Bc.: Detekcia prienikov pomocou pascí (P. Zajac)
Benčík Adam, Bc.: Nástroje pre generovanie ontológii a import faktov (I. Kossaczky)
Benkő Henrich, Bc.: Interaktívna aplikácia Biometria 2 (M. Oravec)
Biľanská Alexandra, Bc.: Zachytávanie dúhovky vo viditeľnom spektre pre použitie v biometrii (M. Oravec)
Blaškovič Peter, Bc.: Pass-phrase generátor (M. Jókay)
Blšták Norbert, Bc.: Využitie mobilných zariadení pre potreby manažmentu chronických ochorení (F. Lehocki)

Bujňák Emil, Bc.: Návrh nového modulu systému EBF2017 - Change Request a Test Management (A. Hambalík)
Bukovčiková Zuzana, Bc.: Klasifikácia tvárí pomocou hlbokých konvolučných sietí (M. Oravec)
Buzák Pavol, Bc.: Využitie Raspberry Pi pre online riadenie termooptickej sústavy (K. Žáková)
Čech Michal, Bc.: Implementácia webovej služby pre prístup k simulačnému prostrediu OpenModelica (K. Žáková)
Dragan Filip, Bc.: Návrh základnej infraštruktúry a zabezpečenia systému EBF2017 (A. Hambalík)
Ďuriš Vladimír, Bc.: Online modelovanie nábytkových zostáv - pre CAD, CAM systémy (S. Marček)
Eliáš Martin, Bc.: Lúštenie historických šifier na GRIDe (E. Antal)
Fačkovec Matej, Bc.: Tvorba biometrického systému na zariadení Raspberry Pi podľa biometriky ucha (M. Oravec)
Gačko Michal, Bc.: Tvorba API pre online prístup k Python orientovaným výpočtovým prostrediam (K. Žáková)
Gažo Tomáš, Bc.: Server pre správu rolí a používateľov (G. Juhás)
Gerát Jozef, Bc.: Detekcia rýchlosti vozidla z video záznamu (M. Oravec)
Glagoličová Simona, Bc.: Využitie komunikačných botov v praktických aplikáciách (E. Kučera)
Goliaš Pavol, Bc.: Komplexné crowd-sourcing riešenie pre projekt Mapa zločinu (I. Kossaczky)
Gontkovič Jozef, Bc.: Spracovanie vstupu geo-vyhľadávania (M. Jókay)
Gregová Barbora, Bc.: Návrh nového modulu systému EBF2017 - Release a Incident Management (A. Hambalík)
Grűnvaldský Dávid, Bc.: Šifrovací systém založený na kvázigrupách (M. Vojvoda)
Halušková Martina, Bc.: ZHFE kryptosystém (V. Hromada)
Hladík Jaroslav, Bc.: Silná autentifikácia a autorizácia (M. Šrámka)
Hoblík Jakub, Bc.: Virtuálne laboratórium založené na technológii Node.js implementované do Moodle (P. Bisták)
Hoferica Ondrej, Bc.: Možnosti využitia konvolučných neurónových sietí pri extrakcii komplexných markantov v odtlačkoch prstov (A. Hambalík)
Hölgye Tamás, Bc.: Interaktívna aplikácia Biometria 1 (M. Oravec)
Hranický Andrej, Bc.: Zber údajov (S. Marček)
Chudík Andrej, Bc.: Elektronická časomiera (R. Balogh)
Janikovský Filip, Bc.: Útok na ochranu návrhu logických obvodov (M.Vojvoda)
Jergel František, Bc.: Extension Field Cancellation (V. Hromada)
Jež Lukáš, Bc.: Flexibilné plánovanie distribúcie zásielok (D. Pancza)
Kačur Jakub, Bc.: Internet of Things v inteligentných budovách (Š. Kozák)
Kelemen Tomáš, Bc.: Zber a poskytovanie informácii zo senzorov (S. Marček)
Képešiová Zuzana, Bc.: Tvorba webových aplikácií so zameraním na vývoj v oblasti front-end-u (P. Bisták)
Kiesel Martin, Bc.: Yap 3.0 (M. Jókay)
Kollár Ondrej, Bc.: Modul pre virtuálne a vzdialené laboratória v systéme Moodle (P. Bisták)
Košarník Jakub, Bc.: Internet veci v digitálnych výrobách (Priemysel 4.0) (Š. Kozák)
Králik Martin, Bc.: Softvérový balík pre optimálny robustný návrh riadenia metódou portrétu správania (M. Huba)
Kúkel Matúš, Bc.: Nespojiteľná komunikácia v sieti (M. Šrámka)
Lehota Ľuboš, Bc.: Rozpoznávanie emócií (E. Kučera)
Lenčéš Lukáš, Bc.: Systém pre analýzu dát z bezpečnostných senzorov (Š. Balogh)
Lepko Martin, Bc.: Návrh, analýza a testovanie systému pre rozšírenú realitu (M. Drozda)
Makáň Martin, Bc. Portál pre správu organizácií a procesov (G. Juhás)
Malý Patrik, Bc.: Návrh a implementácia CWA-instance retrievera (I. Kossaczky)
Maťo Jozef, Bc. Nový generuj-a-testuj útok na A5/1 (M. Vojvoda)
Mažári Juraj, Bc.: Server pre správu procesov a aktivit (G. Juhás)
Medvec Miroslav, Bc.: Analýza programov s využitím dynamickej analýzy a analýzy pamäte (Š. Balogh)
Mičuda Jakub, Bc.: Post-kvantové kryptosystémy v praxi (P. Zajac)
Mihalik Matej, Bc.: Ovládanie UAV gestami ruky (P. Ťapák)
Michlo Patrik, Bc.: Návrh, analýza a testovanie hry pre rozšírenú realitu (M. Drozda)
Mladoniczky Milan, Bc.: Server pre správu formulárov a dátového modelu (G. Juhás)
Moravčík Roman, Bc.: Mobilný distribuovaný AFIS systém (M. Oravec)
Novotná Mária, Bc.: Využitie virtuálnej reality v praktických aplikáciách v priemysle a vo vzdelávaní (E. Kučera)
Novotný Patrik, Bc.: 3D LED kocka a jej využitie pri online experimentovaní (K. Žáková)
Pagáč Vladimír, Bc.: Návrh a implementácia Kalmanovho filtra (O. Gallo)
Polák Maroš, Bc.: Generátor MRHS rovníc pre MQ-kryptosystémy (V. Hromada)

Račák Martin, Bc.: Rozvrhový systém pre FEI (M. Jókay)
Rosa Daniel, Bc.: Komunikačný bot pre e-shop (O. Haffner)
Sabol Peter, Bc.: Riadenie „towercoptera“ v prostredí Internetu (K. Žáková)
Saal Marek, Bc.: Komunikačný bot pre vyhľadávanie receptov v slovenskom jazyku (E. Kučera)
Schwartz Ján, Bc.: Implementácia webovej služby pre prístup k výpočtovému prostrediu Octave (K. Žáková)
Siegl Róbert, Bc.: SOS systém cez sociálne siete (M. Šrámka)
Slaninka Marek, Bc.: Automatizácia domácnosti (J. Jakubec)
Špaček Peter, Bc.: Implementácia McEliece šifrovania do TLS (P. Zajac)
Takáč Ondrej, Bc.: Kryptografia pri ochrane medicínskych informácií (K. Nemoga)
Tarasovič Tomáš, Bc.: Využitie moderných 3D enginov v priemysle a inteligentnej domácnosti (E. Kučera)
Tomík Martin, Bc.: Predspracovanie obrazu ucha na jednodoskovom počítači (M. Oravec)
Uhrin Radoslav, Bc.: Post procesing RNG (K. Nemoga)
Vavrica Marek, Bc.: Návrh a realizácia inteligentného vrátnika na báze operačného systému Android (P. Bisták)
Vaš Peter, Bc.: Detekcia správania programov (Š. Balogh)
Veres Ádám, Bc.: Firemný sieťový administrátor služobných ciest pre malé a stredné firmy (A. Hambalík)
Vida Matúš, Bc.: Metódy snímania únavy vodiča automobilu, jeho monitorovanie a stimulácia pozornosti (P. Fuchs)
Vodička Marek, Bc.: Tvorba multimodálneho biometrického systému na jednodoskovom počítači (M. Oravec)
Vrták Maroš, Bc.: Biometrické rozpoznávanie odtlačkov prstov pomocou nových metód strojového učenia (M. Féder)
Zachar Michal, Bc.: Tvorba biometrického systému na zariadení Raspberry Pi podľa biometriky tváre (M. Oravec)
Zimka Erik, Bc.: Detekcia objektov v obraze pri zhoršených svetelných podmienkach (O. Gallo)

XIII.3. ČLENSTVO V ŠTÁTNICOVÝCH KOMISIÁCH

Meno	**Bc. 15.6.**	**Bc. 6.-7.7.**	**Ing. BIS 13.-14.6.**	**Ing. MSUS 13.-14.6.**	**Iné**
E. Antal		X X			
Š. Balogh		X X	X X		
I. Bock		X	X		
I. Brilla		X		X	
M. Čavojský	X	X X		X X	
V. Čerňanová		X		X	
K. Čipková				X X	
M. Drozda		X X		X X	
T. Fabšič		X	X X		**Ang.- 7.7.**
O. Gallo	X	X X		X X	
O. Grošek	X	X	X X		**Ang.- 7.7.**
M. Gulášová		X	X	X	
A. Hambalík		X X	X	X	
V. Hromada	X	X X	X	X	
M. Jókay		X X	X	X	
G. Juhás		X X		X X	
M. Kečkemétyová				X	
I. Kossaczký		X X		X X	
P. Marák		X X	X	X	
S. Marček				X X	

I. Marinová				X	
Ľ. Marko		X X		X X	
O. Nánásiová		X X	X		
K. Nemoga		X	X		
V. Novák		X		X X	
V. Olejček					
D. Pancza				X X	
E. Pastuchová		X		X	
M. Polakovič		X X	X		
B. Rudolf		X X			
D. Sopiak		X X			
M. Sýs			X X		
M. Šrámka		X	X		
J. Varga					
M. Vojvoda	X	X X	X	X	
M. Zajac		X	X X		
P. Zajac		X X	X	X	
M. Zákopčan		X X		X X	

XIV. EDIČNÉ AKTIVITY

XIV.1. Vydávanie časopisov

Oddelenie matematiky FEI STU v Bratislave je spolueditorom periodika Tatra Mountains Mathematical Publications. Hlavným editorom je MÚ SAV v Bratislave.

XVI.1.1 Editované čísla v roku 2017

Tatra Mountains: Number Theory and Cryptology ´17 (editori: O. Goršek, S. Jakubec, K. Nemoga, P. Zajac)

XIV.2. Členstvá v redakčných radách časopisov

- **prof. RNDr. Otokar Grošek, PhD**. je členom redakčnej rady Tatra Mountains Mathematical Publications. (vydavateľstvo Walter de Gruyter).
- **prof. RNDr. Otokar Grošek, PhD.** je členom redakčnej rady Journal of Mathematical Cryptology (vydavateľstvo Walter de Gruyter)
- **prof. RNDr. Gabriel Juhás, PhD.** je členom redakčnej rady Transactions on Petri Nets and Other Models of Concurrency (vydavateľstvo Springer-Verlag)
- **doc. RNDr. Oľga Nánásiová, CSc.** je členka redakčnej rady Forum Statisticum Slovacum

- **doc. RNDr. Karol Nemoga, PhD.** je výkonný redaktor časopisu Tatra Mountains Mathematical Publications (vydavateľstvo Walter de Gruyter).
- **doc. RNDr. Karol Nemoga, PhD.** je výkonným redaktorom slovenskej jednotky časopisu Zentralblatt für Mathematik, Springer-Verlag, Berlin.
- **prof. Dr. Ing. Miloš Oravec** je editorom časopisu Central European Journal of Computer Science (CEJCS), publisher: Versita, co-published with Springer Verlag
- **doc. RNDr. Michal Zajac, PhD.** je výkonným redaktorom časopisu Mathematica Slovaca pre oblasť funkcionálna analýza (vydavateľ MÚ SAV a Springer-Verlag)

XIV.3. Recenzie pre vedecké časopisy, knihy, zborníky a učebnice

prof. RNDr. Igor Bock, PhD. – 1. Mathematics and Mechanics of Solids – 1 recenzia
2. Acta Polytechnica Hungarica – 1 recenzia
3. AMUC– 1 recenzia
4. Applications of mathematics – 1 recenzia
5. Mathematical Reviews – 11 prehľadov
6. Zentralblatt für Mathematik – 14 prehľadov

prof. RNDr. Otokar Grošek, PhD. – 1. J. of Mathematical Cryptology: 1 recenzia
2. Recenzia knihy "Random Numbers and Computers" by Ronald T. Kneusel. Pre Springer USA
3. Tatra Mountains Mathematical Publications: 3

doc. RNDr. Oľga Nánásiová, CSc. – Internetional Journal of Theoretical Physics 2 recenzie
- Foundation of Physics 1 recenzia

doc. Ing. Michal Šrámka, PhD. – J. of Mathematical Cryptology: 2 recenzie

doc. RNDr. Michal Zajac, PhD. - 1. AMUC– 1 recenzia,
2. Mathematica Slovaca – 2 recenzie
3. Mathematical Reviews – 4 prehľady
4. Zentralblatt für Mathematik – 4 prehľady

XIV.4. Recenzie príspevkov na vedecké konferencie

prof. RNDr. Otokar Grošek, PhD. – HistoCrypt 2017: 6 recenzií príspevkov

doc. Ing. Michal Šrámka, PhD. – International Joint Conference on Neural Networks (IJCNN 2017): 8 recenzií príspevkov

XIV.5. Recenzie vedeckých projektov

prof. RNDr. Igor Bock, PhD. – Projekt VEGA – 1 recenzia
prof. RNDr. Otokar Grošek, PhD. – Recenzia projektu VEGA: 1
doc. RNDr. Oľga Nánásiová, CSc. – Projekt VEGA – 1 recenzia

XV. ORGANIZÁCIA KONFERENCIÍ, ČLENSTVÁ VO VÝBOROCH

NÁZOV KONFERENCIE : *European Historical Ciphers Colloquium 2017*
Miesto: Smolenice
Dátum: 17.-19.5.2017
Meno: prof. RNDr. Otokar Grošek, PhD.
Funkcia: člen organizačného výboru

NÁZOV KONFERENCIE : ELITECH 17
Miesto: Bratislava
Dátum: 24.05.17
Meno: prof. RNDr. Otokar Grošek, PhD.
Funkcia: predseda komisie

NÁZOV KONFERENCIE : Cryptographic architectures embedded in logic devices, 15th CryptArchi Workshop
Miesto: Smolenice
Dátum: 18.-21.6.17
Meno: prof. RNDr. Otokar Grošek, PhD.
Funkcia: člen Steering committee

NÁZOV KONFERENCIE : CECC 2017
Miesto: Waršava
Dátum: 28.-30.6.2017
Meno: prof. RNDr. Otokar Grošek, PhD.
Funkcia: člen org. výboru

NÁZOV KONFERENCIE : PRASTAN 2017, Slovensko - česká konferencia
Miesto: Oščadnica
Dátum: 5. – 8. októbra 2017
Meno: doc. RNDr. Oľga Nánásiová, CSc.
Funkcia: členka programového a organizačného výboru

NÁZOV KONFERENCIE : PRASTAN 2017, Slovensko - česká konferencia
Miesto: Oščadnica
Dátum: 5. – 8. októbra 2017
Meno: RNDr. Elena Pastuchová, PhD.
Funkcia: členka programového výboru

XVI. SEMINÁRE

Seminár: VARIAČNÉ NEROVNICE A OPTIMÁLNE RIADENIE V MECHANIKE
Vedúci: prof. RNDr. Igor Bock, PhD.

Seminár: CRYPTO

Vedúci: doc. Ing. Pavol Zajac, PhD.

Seminár: MACHINE LEARNING
Vedúci: prof. Dr. Ing. Miloš Oravec

Seminár: APLIKÁCIE MATEMATIKY
vedúci: doc. RNDr. Oľga Nánásiová, PhD.