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

za rok 2018

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. (professor emeritus)
prof. RNDr. Otokar Grošek, PhD.
prof. RNDr. Gabriel Juhás, PhD. (vedúci odd. SI)
prof. Dr. Ing. Miloš Oravec
prof. Ing. Pavol Zajac, PhD. (vedúci odd.BIS)

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. 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.

Odborní asistenti

Ing. Eugen Antal, PhD.
Ing. Štefan Balogh, PhD.
RNDr. Igor Brilla, 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.
Mgr. Jozef Kollár, 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. Zuzana Bukovčiková Ing. Maroš Čavojský Ing. Martin Eliáš Ing. Vojtěch Jirka Ing. Pavol Marák Ing. Juraj Mažári Ing. Milan Mladoniczky Ing. Roderik Ploszek Ing. Michala Slugeňová, rod. Gulášová Ing. Dominik Sopiak Ing. Peter Špaček Ing. Juraj Varga
Externí doktorandi	Ing. Vojtěch Jirka Ing. Igor Kazlov MUDr. Veronika Kurilová Ing. Peter Minarovský Ing. Štefan Počarovský
Externí pracovníci	Bc. Tomáš Baka Ing. Matej Féder, PhD. Bc. Marián Krkoška Bc. Katarína Matalíková Bc. Ľubor Pernický Bc. Filip Podlucký Ing. Matej Smoleň Bc. Peter Švec Mgr. Tomáš Žilka

II. ZARIADENIA

II.1. Výukové a výskumné laboratóriá

- Laboratórium Biometrie a spracovania signálov
- Laboratórium pre Bezpečnosť IT
- Antivírusové 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. 2-2 h)	M. Vojvoda
●Databázové systémy (B-DBS)	(4. sem. 2-2 h)	M. Vojvoda/ Š. Balogh/ M. Čavojský/ V. Novák
●Diskrétna matematika (B-DM)	(4. sem .2-2 h)	M. Polakovič/ I. Marinová/ K. Čipková/ T. Žilka
●Diskrétne udalostné systémy (B-DUS)	(3. sem. 2-2 h)	G.Juhás/ S. Marček/ M. Mladoniczky/ J. Mažári
●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 1 (B-LA1)	(1. sem. 2-2 h)	M. Zajac/ I. Marinová/ D. Pancza/ T. Žilka
●Matematická štatistika (B-MATSTAT)	(3+4. sem. 3-2 h)	O.Nánásiová/ I. Marinová/ E.Pastuchová

●Matematika 1 (B-MAT1E)	(1. sem. 3-2 h)	M. Polakovič/ J. Kollár
●Matematika 1 (B-MAT1E)	(1. sem. 4-2 h)	M. Zajac/ M.Zákopčan
●Matematika 1 (B-MAT1I)	(1. sem. 3-2 h)	B. Rudolf/ E.Pastuchová/ K. Čipková
●Matematika 1 op. (B-MAT1I)	(2. sem. 3-2 h)	B. Rudolf
●Matematika 1 op. (B-MAT1E)	(2. sem. 3-2 h)	M. Zajac
●Matematika 2 (B-MAT2E)	(2. sem. 3-2 h)	Ľ. Marko/ M.Zákopčan
●Matematika 2 (B-MAT2)	(2. sem. 3-2 h)	Ľ. Marko/ M.Zákopčan
●Matematika 2 (B-MAT2I)	(2. sem. 3-2 h)	B. Rudolf/ M. Kečkemétyová
●Matematika 2 op. (B-MAT2A)	(3. sem. 3-2 h)	M. Kečkemétyová
●Matematika 2 op. (B-MAT2E)	(3. sem. 2-2 h)	I.Brilla
●Matematika 2 op. (B-MAT2)	(3. sem. 2-2 h)	I.Brilla
●Matematika 3 (B-MAT3E)	(3. sem. 3-2 h)	Ľ. Marko/ M. Kečkemétyová
●Matematika 3 (B-MAT3)	(3. sem. 2-2 h)	Ľ. Marko/ O. Nánásiová
●Matematika 3 op (B-MAT3)	(4. sem. 3-2 h)	I.Brilla
●Matematika 4 (B-MAT4)	(3. sem. 2-2 h)	Ľ. Marko/ O.Nánásiová
●Matematika 4 (B-MAT4)	(4. sem. 2-2 h)	D. Pancza
●Objektovo orientované programovanie (B-OOP)	(3. sem. 2-2 h)	G. Juhás/ O. Gallo/ J. Mažári/ M. Mladoniczky
●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. Smoleň/ R. Ploszek
●Počítačové siete (B-PS)	(3. sem. 2-2 h)	M. Smoleň/ R. Ploszek M.Oravec/ D. Sopiak/ Z. Bukovčiková/ A. Hambalík/ M. Féder
●Programovacie techniky (B-PT)	(3. sem. 3-2 h)	M. Drozda/ P. Marák/ V. Novák
●Programovanie 1 (B-PROG1)	(1. sem. 2-2 h)	P. Zajac/

		T. Fabšič/ V. Hromada/ M. Gulášová/ M. Krkoška/ Ľ. Pernický/ F. Podlucký/ P. Švec/ T. Baka/ K. Matalíková
●Programovanie 2 (B-PROG2)	(2. sem. 2-2 h)	P. Zajac
●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)	(4. sem. 2-2 h)	M. Vojvoda/ T. Fabšič
●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/ Z.Bukovčiková
●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)	B. Rudolf
●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
●Reprezentácia a získavanie znalostí (I-RZZ),	(2. sem. 2-2 h)	K. Nemoga / I. Kossaczký
●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/ Z. Bukovčiková
●Šifrovanie v komunikačných sieťach (I-SKS)	(1. sem. 3-2 h)	K. Nemoga/ M. Sýs/ T. Fabšič
●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)

●Bakalárky projekt	O. Gallo
●Databázové štruktúry	M. Čavojský
●Diskrétna matematika	M. Polakovič
●Klasické šifry	O. Grošek
●Mobilné výpočty	M. Drozda
●Modelovanie a simulácia udalostných systémov	G. Juhás
●Operačné systémy	M. Jókay
●Počítačové siete	A. Hambalík
●Modelovanie a simulácia udalostných systémov	G. Juhás

IV. VÝSKUMNÉ PROJEKTY

IV.1. Projekty VEGA, ESF, APVV a iné riešené v roku 2018 na ÚIM

Číslo projektu: VEGA 1/0159/17
Názov projektu: Bezpečná postkvantová kryptografia
Zodpovedný riešiteľ: prof. Ing. Pavol Zajac, PhD.
Zástupca vedúceho projektu: Ing. Viliam Hromada, PhD.

Spoluriešitelia z ÚIM v roku 2018: 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-Slugeňová, Ing. Peter Špaček, doc. RNDr. Oľga Nánásiová, PhD., RNDr. Karla Čipková, PhD., Mgr. Jozef Kollár, PhD.
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 2018: Ing. Dominik Sopiak, PhD., Ing. Zuzana Bukončiková, Ing. Vojtěch Jirka, Ing. Ľuboš Omelina, PhD., MUDr. Veronika Kurilová
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: Secure Communication in the Quantum Era
Číslo projektu: NATO SPS Project G5448
Zahraniční partneri: University of Malta, Malta,
Universidad Rey Juan Carlos, Španielsko
Florida Atlantic University, USA
Vedúci projektu za krajiny z NATO: prof. RNDr. Otokar Grošek, PhD.
Vedúci projektu za partnerskú krajinu: Dr. Christian Colombo (University of Malta)
Spoluvedúci projektu: Dr. Maria-Isabel Gonzales Vasco (University of Malta)
Prof. Rainer Steinwandt (Florida Atlantic University)
Riešitelia z ÚIM v roku 2018: doc. RNDr. Karol Nemoga, PhD., prof. Ing. Pavol Zajac, PhD., Ing. Viliam Hromada, PhD., Mgr. Tomáš Fabšič PhD., Ing. Ondrej Gallo PhD., Ing. Peter Špaček
Riešitelia z University of Malta: Gordon Pace
Riešitelia z Universidad Rey Juan Carlos: Manuel Arrayás, Angel L. Pérez del Pozo, Jose Luis Trueba
Riešitelia z Florida Atlantic University: Shi Bai, Shaun Miller, Edoardo Persichetti
Trvanie projektu: 2018-2021

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 2018: RNDr. Igor Brilla, PhD.
Doba riešenia: 01.07.2016-30.09.2019

Názov projektu: Inteligentné mechatronické systémy
Vedúci projektu: prof. Ing. Alena Kozáková, PhD., ÚAMt FEI STU
Spoluriešitelia z ÚIM v roku 2018: 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 2018: doc. RNDr. Oľga Nánásiová, PhD.
Doba riešenia: 01.01.2015-31.12.2018

Číslo projektu: ITMS 312011F318 MŠVVaŠ SR
Názov projektu: Med&Com - osvojenie si nových spôsobov elektronickej komunikácie pacient-lekár a lekár-pacient
Vedúci projektu: MUDr. Marian Zelina, Sanitas Slovaca - agentúra pre rozvoj zdravia na Slovensku, o.z.
Spoluriešiteľ z ÚIM v roku 2018: Alexander Hambalík, Ing., PhD.
Doba riešenia: 01.11.2018-30.09.2020

Číslo projektu: VEGA grant 1/0039/17
Názov projektu: Real-world problem solving by means of complex networks
Vedúci projektu: prof. Beňušková FMFI UK
Spoluriešiteľ z ÚIM v roku 2018: doc. RNDr. Boris Rudolf, PhD.
Doba riešenia: 2017-2021

V. SPOLUPRÁCA

V.1. Domáca spolupráca

V.1.1. Pozvané prednášky

Meno: prof. RNDr. Otokar Grošek, PhD., doc. RNDr. Karol Nemoga, PhD., Mgr. Tomáš Fabšič, PhD.
Miesto: Fei STU, v rámci feistivalu, diskusiu viedol J. Porubský z časopisu FORBES
Prednáška: Je kvantový počítač reálna hrozba?
Dátum: 24.10.2018

Meno: prof. Ing. Pavol Zajac, PhD.
Miesto: Jasná pod Chopkom, 50. konferencia slovenských matematikov
Prednáška: Post-kvantová kryptografia
Dátum: 22.-25.11.2018

Meno: doc. RNDr. Oľga Nánásiová, PhD.

Miesto: Matematický ústav SAV
Prednáška: Probability Measures and logical connectives on Quantum Logics
Dátum: 4.12.2018

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 FCHPT STU (prof. RNDr. Anna Kolesárová, CSc.)
- Katedra matematiky a deskriptívnej geometrie SvF STU (prof. RNDr. Radko Mesiar, PhD., prof. RNDr. Jozef Širáň, DrSc., prof. RNDr. Magdaléna Komorníková, PhD., prof. RNDr. Karol Mikula, DrSc., prof. RNDr. Martin Kalina, PhD., doc. Mgr. Gejza Jenča, PhD., RNDr. Ľubica Valášková, PhD.)
- Katedra matematickej analýzy FMFI UK (doc., RNDr., Zbyněk Kubáček, CSc.)
- Katedra matematiky SjF STU (doc. RNDr. Daniela Velichová, CSc., Mgr. Monika Kováčová, PhD.)
- IBM Slovensko, s.r.o.
- Ministerstvo obrany SR
- Sanitas Slovaca - agentúra pre rozvoj zdravia na Slovensku, o.z.
- Katedra informatiky AOS Liptovský Mikuláš (doc. RNDr. Ferdinand Chovanec,CSc., RNDr. Eva Drobná, PhD.)

V1.3. Pozvané prednášky domácich odborníkov

Hosť (adresa):
Termíny:
Účel:
Prednáška:

V.2. Zahraničná spolupráca

V.2.1. Pozvané prednášky

Meno: prof. RNDr. Gabriel Juhás, PhD.
Miesto: RiSE Seminar, IST Austria, Am Campus 1, 3400 Klosterneuburg, Rakúsko
Prednáška: Synthesis Petri Nets from Prime Event Structures
Dátum: 21.02.2018

Meno: prof. RNDr. Otokar Grošek, PhD., Ing. Roderik Ploszek
Miesto: Mikulášská kryptobesídka, 29. – 30. 11. 2018, Praha, ČR
Prednáška: O histórii ruských šifier od Cyrila a Metoda až 2. sv. v.
Dátum: 30.11. 2018

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 (izr. prof. dr. Janko Bračič).
- Institut de Mathematiques, Université Louis Pasteur, France
- Eszterházy Károly Egyetem, Eger, Maďarsko (Dr. Kis Tóth Lajos, Tóthné dr. Parázsó Lenke)
- Matematický ústav AVČR (doc. RNDr. Vladimír Müller, 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)
- University of Malta, Malta (Dr. Christian Colombo)
- Universidad Rey Juan Carlos, Madrid, Spain (Dr. María Isabel González Vasco)

V.2.3. Zahraniční hostia

Hosť (adresa): prof. Maribel Gonzáles Vasco, Universidad Rey Juan Carlos, Španielsko
Termín: 6.-8.6.2018
Účel: účast na konferencii CECC 2018 v Smoleniciach

Hosť (adresa): prof. Léo Perrin, INRIA, Francúzsko

Termín: 6.-8.6.2018
Účel: účast na konferencii CECC 2018 v Smoleniciach

Hosť (adresa): prof. Christian Rechberger, TU Graz, Rakúsko
Termín: 6.-8.6.2018
Účel: účast na konferencii CECC 2018 v Smoleniciach

V.2.4. Pobyty pracovníkov ÚIM v zahraničí

Meno: Ing. Maroš Čavojský
Miesto: Praha, Česká republika
Účel: štúdijný pobyt v rámci programu Erasmus+
Dátum: 21.9.2017-8.2.2018

Meno: Ing. Peter Špaček
Miesto: Londýn, Veľká Británia
Účel: stáž na UCL, pedagogická a vedecká činnosť v spolupráci s Dr. N. T. Courtois
Dátum: 1.1 2018 – 31.3.2018

Meno: Ing. Zuzana Bukovčiková
Miesto: Peking a Shenzen, Čína
Účel: účast na tréningovom programe firmy Huawei
Dátum: 7.12.2018-23.12.2018

V.2.5. Zahraničné cesty

Meno: doc. RNDr. Karol Nemoga, PhD
Miesto: Bergen, Nórsko
Zámer cesty: účast na seminári s prof T. Hellesethom na Bergen University, Selmer Senter
Dátum: 10.-14.6.2018

Meno: prof. RNDr. Otokar Grošek, PhD.
Miesto: Valetta, Malta
Zámer cesty: pracovné stretnutie v rámci projektu NATO na spoluriešiteľskej univerzite
Dátum: 1.-4.10.2018

Meno: prof. Ing. Pavol Zajac, PhD.
Miesto: Valetta, Malta
Zámer cesty: pracovné stretnutie v rámci projektu NATO na spoluriešiteľskej univerzite
Dátum: 1.-4.10.2018

Meno: prof. RNDr. Otokar Grošek, PhD.
Miesto: Praha, Česká republika
Zámer cesty: pracovné stretnutie na Ústave informatiky AV ČR
Dátum: 14.9.2018

Meno: prof. RNDr. Otokar Grošek, PhD.
Miesto: Brusel, Belgicko
Zámer cesty: prebratie ocenenia v projekte NATO
Dátum: 28.-30.11.2018

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 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.
- **prof. Dr. Ing. Miloš Oravec** je členom IEEE IET.
- **RNDr. Elena Pastuchová, PhD.** je členkou ENS v Nemecku.

VI. OBHÁJENÉ DIZERTÁCIE

VII. INÉ AKTIVITY

VII.1. Akademické a iné funkcie

- **prof. RNDr. Igor Bock, PhD.** je členom 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 členom Odborovej komisie doktorandského štúdia v študijnom programe 3. stupňa 9.1.5 Numerická analýza a vedecko-technické výpočty so sídlom na FMFI UK.
- **Dr.rer.nat. Martin Drozda** je členom Odborovej komisie (OK) doktorandského štúdia v odbore 9.2.9 Aplikovaná informatika na STU
- **prof. RNDr. Otokar Grošek, PhD.** je členom Vedeckej rady FEI STU

---

[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

- **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
- **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)
- **prof. Dr. Ing. Miloš Oravec** je členom Odborovej komisie (OK) doktorandského štúdia v odbore 9.2.9 Aplikovaná informatika na STU
- **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. Milan Vojvoda, 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]

- **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
- **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

[2] JSFM - Jednota slovenských matematikov a fyzikov
SSM - Slovenskej spoločnosti pre mechaniku
SSKI - Slovenská spoločnosť pre kybernetiku a informatiku
SBIMI - Spoločnosť biomedicínskeho inžinierstva a medicínskej informatiky

VIII. PUBLIKÁCIE

ADC Vedecké práce v zahraničných karentovaných časopisoch

ADC01 BOCK, Igor. Dynamic contact of a thermoelastic Mindlin-Timoshenko beam with a rigid obstacle. In *Mathematics and Mechanics of Solids*. Vol. 23, Iss. 3 (2018), s. 411-419. ISSN 1081-2865. V databáze: CC: 000429895300010.

ADC02 BRAČIČ, Janko - DIOGO, Cristina - ZAJAC, Michal. Reflexive sets of operators. In *Banach Journal of Mathematical Analysis*. Vol. 12, No. 3 (2018), s. 751-771. ISSN 1735-8787. V databáze: CC: 000437870200012.

ADC03 FABŠIČ, Tomáš - GROŠEK, Otokar - NEMOGA, Karol - ZAJAC, Pavol. On generating invertible circulant binary matrices with a prescribed number of ones. In *Cryptography and Communications*. Vol. 10, Iss. 1 (2018), s. 159-175. ISSN 1936-2447. V databáze: SCOPUS: 2-s2.0-85041074817 ; CC: 000428746900011.

ADC04 QI, Feng - ČERŇANOVÁ, Viera - SHI, Xiao-Ting - GUO, Bai-Ni. Some properties of central Delannoy numbers. In *Journal of Computational and Applied Mathematics*. Vol. 328, (2018), s. 101-115. ISSN 0377-0427. V databáze: CC: 000412619100007 ; SCOPUS: 2-s2.0-85028836678.

ADC05 ZAJAC, Pavol. Using local reduction for the experimental evaluation of the cipher security. In *Computing and Informatics*. Vol. 37, No. 2 (2018), s. 349-366. ISSN 1335-9150. V databáze: CC: 000437824300005 ; SCOPUS: 2-s2.0-85049180794.

ADE Vedecké práce v ostatných zahraničných časopisoch

ADE01 MAŽÁRI, Juraj - MLADONICZKY, Milan - JUHÁS, Gabriel - GAŽO, Tomáš - MAKÁŇ, Martin. Petriflow + Netgrif = Petri net driven application development. In *Petri Net Newsletter*. Vol. 86, (2018), s. 3-16. ISSN 0391-1804.

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

ADM01 HROMADA, Viliam - PETHŐ, Tibor. Phase-shift fault analysis of Grain v1. In *International Journal of Electronics and Telecommunications*. Vol. 64, No. 2 (2018), s. 131-136. ISSN 0867-6747. V databáze: WOS: 000435922400004 ; SCOPUS: 2-s2.0-85048792769.

ADM02 LODERER, Marek - PAVLOVIČOVÁ, Jarmila - ORAVEC, Miloš. Comparative study of local binary pattern derivatives for low size feature vector representation in face recognition. In *Acta Polytechnica Hungarica*. Vol. 15, no. 4 (2018), s. 199-216. ISSN 1785-8860. V databáze: WOS: 000442389300011 ; SCOPUS: 2-s2.0-85052659546.

ADM03 RADDUM, Havard - ZAJAC, Pavol. MRHS solver based on linear algebra and exhaustive search. In *Journal of Mathematical Cryptology*. Vol. 12, No. 3 (2018), s. 143-157. ISSN 1862-2976. V databáze: WOS: 000443309500003 ; SCOPUS: 2-s2.0-85050078561.

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

ADN01 BOCK, Igor - KEČKEMÉTYOVÁ, Mária. An optimal control problem for a viscoelastic plate in a dynamic contact with an obstacle. In *Tatra Mountains Mathematical Publications*. Vol. 71, (2018), s. 27-37. ISSN 1210-3195. V databáze: SCOPUS: 2-s2.0-85061426826.

ADN02 GROŠEK, Otokar - FABŠIČ, Tomáš. Computing multiplicative inverses in finite fields by long division. In *Journal of Electrical Engineering*. Vol. 69, No. 5 (2018), s. 400-402. ISSN 1335-3632. V databáze: WOS: 000453413200012 ; SCOPUS: 2-s2.0-85059569379.

AFB Publikované pozvané príspevky na domácich vedeckých konferenciách

AFB01 JUHÁS, Gabriel - MOLNÁR, Ladislav - JUHÁSOVÁ, Ana - ONDRIŠOVÁ, Miriam - MLADONICZKY, Milan - MAŽÁRI, Juraj. Continual improvement process in scientific publishing. In *ICETA 2018 : 16th International Conference on Emerging eLearning Technologies and Applications. Starý Smokovec, Slovensko. November 15-16, 2018*. Danvers : IEEE, 2018, S. 245-250. ISBN 978-1-5386-7912-8. V databáze: IEEE: 8572053 ; SCOPUS: 2-s2.0-85060296024.

AFB02 MOLNÁR, Ladislav - JUHÁS, Gabriel - ONDRIŠOVÁ, Miriam - JUHÁSOVÁ, Ana - MAŽÁRI, Juraj - MLADONICZKY, Milan. Scaling and structuring of digital literacy. In *ICETA 2018 : 16th International Conference on Emerging eLearning Technologies and Applications. Starý Smokovec, Slovensko. November 15-16, 2018*. Danvers : IEEE, 2018, S. 389-394. ISBN 978-1-5386-7912-8. V databáze: IEEE: 8572088 ; SCOPUS: 2-s2.0-85060284857.

AFC Publikované príspevky na zahraničných vedeckých konferenciách

AFC01 ANTAL, Eugen - ZAJAC, Pavol. ManuLab system demonstration. In *HistoCrypt 2018 : 1st International conference on historical cryptology. Uppsala, Sweden. June 18-20, 2018*. Linköping : University Electronic Press, 2018, S. 125-128. ISBN 978-91-7685-252-1.

AFC02 BREZOVSKÝ, Matúš - SOPIAK, Dominik - ORAVEC, Miloš. Action recognition by 3D convolutional network. In *Proceedings ELMAR-2018 : 60th International symposium. Zadar, Croatia. September 16-19, 2018*. 1. ed. Zagreb : University of Zagreb, 2018, S. 71-74. ISSN 1334-2630. ISBN 978-953-184-244-0. V databáze: IEEE: 8534657 ; WOS: 000454262700017.

AFC03 BRILLA, Igor - JANÍČEK, František. Numerical determination of voltage potential inside 3D anisotropic media using variational methods. In *Compendio de ciencia aplicada 2018 : IV Congreso Multidisciplinario de Ciencias Aplicadas en Latinoamérica. Yucatán, Mexico. Noviembre 20-23 de 2018*. Coyoacán : Ciudad Universitaria, 2018, S. 34-41. ISBN 978-607-30-1322-2.

AFC04 ČAVOJSKÝ, Maroš - UHLÁR, Marek - IVANIŠ, Marián - MOLNÁR, Martin - DROZDA, Martin. User trajectory extraction based on WiFi scanning. In *W-FiCloud 2018 : 6th International conference on future internet of things and cloud workshops. Barcelona, Spain. August 6-8, 2018*. Piscataway : IEEE, 2018, S. 115-120. ISBN 978-1-5386-7810-7. V databáze: IEEE: 8488184 ; SCOPUS: 2-s2.0-85056535248.

AFC05 HAMBALÍK, Alexander - MARÁK, Pavol. 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 : Líceum Kiadó, 2018, S. 200-206. ISBN 978-615-5621-86-4.

AFC06 MOJŽIŠ, Ján - BALOGH, Štefan - ÁSVÁNYI, Michal - BUDINSKÁ, Ivana. Collaborative learning supported with MediaWiki platform in technical university environment. In *Teaching and Learning in a Digital World : 20th International Conference on Interactive Collaborative Learning (ICL2017), Vol. 1. Budapest, Hungary. September 27-29, 2017*. Cham : Springer, 2018, S. 660-665. ISBN 978-3-319-73209-1.

AFC07 PAVLOVIČOVÁ, Jarmila - KAJAN, Slavomír - MARKO, Martin - ORAVEC, Miloš - KURILOVÁ, Veronika. Bright lesions detection on retinal images by convolutional neural network. In *Proceedings ELMAR-2018 : 60th International symposium. Zadar, Croatia. September 16-19, 2018*. 1. ed. Zagreb : University of Zagreb, 2018, S. 79-82. ISSN 1334-2630. ISBN 978-953-184-244-0. V databáze: IEEE: 8534658 ; WOS: 000454262700019.

AFC08 SOPIAK, Dominik - BUKOVČIKOVÁ, Zuzana - ORAVEC, Miloš - PAVLOVIČOVÁ, Jarmila. The analysis of quality indicators on face recognition in video frames. In *Proceedings ELMAR-2018 : 60th International symposium. Zadar, Croatia. September 16-19, 2018*. 1. ed. Zagreb : University of Zagreb, 2018, S. 155-158. ISSN 1334-2630. ISBN 978-953-184-244-0. V databáze: IEEE: 8534652 ; WOS: 000454262700036.

AFD Publikované príspevky na domácich vedeckých konferenciách

AFD01 ANTAL, Eugen - JAVORKA, Peter - HLIBOKÝ, Tomáš. Cryptanalysis of the columnar transposition using meta-heuristics. In *CECC 2018 : Central European conference on cryptology. Smolenice, Slovakia. June 6-8, 2018*. Bratislava : Slovak Academy of Sciences, 2018, S. 24-26. ISBN 978-80-968374-5-8.

AFD02 BRILLA, Igor - JANÍČEK, František. Numerical determination of voltage potential inside two dimensional nonhomogeneous media using variational methods. In *Power engineering 2018. Energy-Ecology-Economy 2018 : 14th International scientific conference. Tatranske Matliare, Slovakia. June 5-7, 2018*. 1. vyd. Bratislava : Slovak University of Technology, 2018, S. 166-170. ISBN 978-80-89402-98-4.

AFD03 FABŠIČ, Tomáš - HROMADA, Viliam - ZAJAC, Pavol. Reaction attacks on cryptosystems using QC-LDPC codes. In *CECC 2018 : Central European conference on cryptology. Smolenice, Slovakia. June 6-8, 2018*. Bratislava : Slovak Academy of Sciences, 2018, S. 62-63. ISBN 978-80-968374-5-8.

AFD04 GULÁŠOVÁ, Michala - JÓKAY, Matúš. Tailored-made attack for JPEG algorithm. In *ELITECH´18 [elektronický zdroj] : 20th Conference of doctoral students. Bratislava, Slovakia. May 23, 2018*. 1. ed. Bratislava : Vydavateľstvo Spektrum STU, 2018, CD-ROM, [5] s. ISBN 978-80-227-4794-3.

AFD05 GULÁŠOVÁ, Michala - JÓKAY, Matúš. JPEG compatibility steganalysis. In *CECC 2018 : Central European conference on cryptology. Smolenice, Slovakia. June 6-8, 2018*. Bratislava : Slovak Academy of Sciences, 2018, S. 53-55. ISBN 978-80-968374-5-8.

AFD06 KUCHÁRIK, Michal - BALOGH, Zoltán - DROZDA, Martin. Petri net model of student choices in a LMS moodle e-course. In *DIVAI 2018 : 12th International scientific conference on distance learning in applied informatics. Štúrovo, Slovakia. May 2-4, 2018*. Praha : Wolters Kluwer ČR, 2018, S. 303-311. ISSN 2464-7470. ISBN 978-80-7598-059-5. V databáze: WOS: 000459255700027.

AFD07 MAŽÁRI, Juraj - JUHÁS, Gabriel - MLADONICZKY, Milan. Process mining: From event sourcing to event structures. In *ELITECH´18 [elektronický zdroj] : 20th Conference of doctoral students. Bratislava, Slovakia. May 23, 2018*. 1. ed. Bratislava : Vydavateľstvo Spektrum STU, 2018, CD-ROM, [5] p. ISBN 978-80-227-4794-3.

AFD08 MLADONICZKY, Milan - JUHÁS, Gabriel - MAŽÁRI, Juraj. Inter-process synchronization of instances in Petriflow language. In *ELITECH´18 [elektronický zdroj] : 20th Conference of doctoral students. Bratislava, Slovakia. May 23, 2018*. 1. ed. Bratislava : Vydavateľstvo Spektrum STU, 2018, CD-ROM, [5] p. ISBN 978-80-227-4794-3.

AFD09 PLOSZEK, Roderik. Linux security modules overview. In *ELITECH´18 [elektronický zdroj] : 20th Conference of doctoral students. Bratislava, Slovakia. May 23, 2018*. 1. ed. Bratislava : Vydavateľstvo Spektrum STU, 2018, CD-ROM, [7] s. ISBN 978-80-227-4794-3.

AFD10 ŠPAČEK, Peter - ZAJAC, Pavol. MQ schemes in NIST PostQuantum competition. In *ELITECH´18 [elektronický zdroj] : 20th Conference of doctoral students. Bratislava, Slovakia. May 23, 2018*. 1. ed. Bratislava : Vydavateľstvo Spektrum STU, 2018, CD-ROM, [4] p. ISBN 978-80-227-4794-3.

AFD11 ZAJAC, Pavol. Potential for backdoors in BIKE key generation. In *CECC 2018 : Central European conference on cryptology. Smolenice, Slovakia. June 6-8, 2018*. Bratislava : Slovak Academy of Sciences, 2018, S. 58-59. ISBN 978-80-968374-5-8.

AFG Abstrakty príspevkov zo zahraničných konferencií

AFG01 HAMBALÍK, Alexander - MARÁK, Pavol. Skúsenosti z tvorby výkonného softvérového systému na využitie v daktyloskopii a biometrii v školských podmienkach. In *Trendy ve vzdělávání : Technika, informatika a inovace ve vzdělávání napříč obory. 16. Mezinárodní vědecko-odborní konference. Slatinice u Olomouce, Česká Republika. 16.-18. 5.2018*. 1. vyd. Olomouc : Univerzita Palackého v Olomouci, 2018, S. 66. ISBN 978-80-244-5318-7.

AFG02 NÁNÁSIOVÁ, Oľga - VALÁŠKOVÁ, Ľubica - ČERŇANOVÁ, Viera. Probability measures and projections on quantum logics. In *Contemporary Computational Science [elektronický zdroj] : proceedings of the International Multi-Conference on Computational Science (CS 2018). Kraków, Poland. 2-5 July 2018.*

Kraków : AGH University of Science and Technology Press, 2018, online, s. 78. ISBN 978-83-66016-22-4.

AFH Abstrakty príspevkov z domácich konferencií

AFH01 ZAJAC, Pavol. Post-kvantová kryptografia. In *50. konferencia slovenských matematikov : zborník abstraktov. Jasná pod Chopkom, SR, 22. - 25. 11. 2018*. 1. vyd. Žilina : EDIS, 2018, S. 51. ISBN 978-80-554-1500-0.

BEE Odborné práce v zahraničných zborníkoch (konferenčných aj nekonferenčných)

BEE01 GROŠEK, Otokar. O histórii ruských šifier od Cyrila a Metoda po 2. sv. v. In *Mikulášská kryptobesídka 2018 : sborník příspěvků. Praha, Česká republika. 29.-30.11.2018*. 1. vyd. Bílovice nad Svitavou : Trusted Network Solutions, 2018, S. 27-28.

BEE02 HLIBOKÝ, Tomáš - ANTAL, Eugen. Meta-heuristiky a ohodnocovanie textu pri lúštení transpozičných šifier. In *Mikulášská kryptobesídka 2018 : sborník příspěvků. Praha, Česká republika. 29.-30.11.2018*. 1. vyd. Bílovice nad Svitavou : Trusted Network Solutions, 2018, S. 29-30.

BEE03 MAŽÁRI, Juraj - JUHÁS, Gabriel - MLADONICZKY, Milan. Petriflow in actions: Events call actions call events. In *Algorithms and Tools for Petri nets : Workshop AWPN 2018. Augsburg, Germany. October 11-12, 2018*. Augsburg : Universität Augsburg, 2018, S. 21-26.

BEE04 MLADONICZKY, Milan - JUHÁS, Gabriel - MAŽÁRI, Juraj. Process communication in petriflow: A case study. In *Algorithms and Tools for Petri nets : Workshop AWPN 2018. Augsburg, Germany. October 11-12, 2018*. Augsburg : Universität Augsburg, 2018, S. 27-32.

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

BFA01 FABŠIČ, Tomáš. A reaction attack on LEDApkc. In *CBC 2018 : The Sixth Code-Based Cryptography Workshop. Abstracts. Davie, Florida, USA. April 5-6, 2018*. Florida : Atlantic University, 2018, [1] s.

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

FAI01 NEMOGA, Karol (ed.) - ZAJAC, Pavol (ed.) - ŠPAČEK, Peter (ed.). *CECC 2018 : Central European conference on cryptology. Smolenice, Slovakia. June 6-8, 2018*. Bratislava : Slovak Academy of Sciences, 2018. ISBN 978-80-968374-5-8.

GHG Práce zverejnené na internete

GHG01 ANTAL, Eugen - MÍRKA, Jakub. Selected encrypted messages found in Slovak and Czech archives. In *HistoCrypt 2018 : 1st International conference on historical cryptology. Uppsala, Sweden. June 18-20, 2018*. Linköping : University Electronic Press, 2018, online. ISBN 978-91-7685-252-1. Dostupné na internete: <https://www2.lingfil.uu.se/histocrypt2018/Antal_HCC18.pdf>.

Štatistika: kategória publikačnej činnosti

ADC	Vedecké práce v zahraničných karentovaných časopisoch	5
ADE	Vedecké práce v ostatných zahraničných časopisoch	1
ADM	Vedecké práce v zahraničných časopisoch registrovaných v databázach Web of Science alebo SCOPUS	3
ADN	Vedecké práce v domácich časopisoch registrovaných v databázach Web of Science alebo SCOPUS	2
AFB	Publikované pozvané príspevky na domácich vedeckých konferenciách	2
AFC	Publikované príspevky na zahraničných vedeckých konferenciách	8
AFD	Publikované príspevky na domácich vedeckých konferenciách	11
AFG	Abstrakty príspevkov zo zahraničných konferencií	2
AFH	Abstrakty príspevkov z domácich konferencií	1
BEE	Odborné práce v zahraničných zborníkoch (konferenčných aj nekonferenčných)	4
BFA	Abstrakty odborných prác zo zahraničných podujatí (konferencie...)	1
FAI	Redakčné a zostavovateľské práce knižného charakteru (bibliografie, encyklopédie, katalógy, slovníky, zborníky...)	1
GHG	Práce zverejnené na internete	1
Súčet		**42**

IX. VÝCHOVA VEDECKÝCH PRACOVNÍKOV

IX.1. Interní doktorandi

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: Ing. Martin Eliáš
Školiteľ: prof. RNDr. Otokar Grošek, PhD.
Forma vzdelávania: doktorandské štúdium – interná forma

Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška:
Predpokladaný termín ukončenia:
Téma práce: Spracovanie šifrovanej korešpondencie z českých a slovenských archívov
Zanechal: 1.11.2018

Doktorand: Ing. Michala Slugeňová, rod. Gulášová

Školiteľ: doc. Ing. Milan Vojvoda, PhD.
Školiteľ špecialista: Ing. Matúš Jókay, 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
Zanechal: 1.9.2018, prestúpil na Externé štúdium

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: 9/2019
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. Roderik Ploszek
Školiteľ: doc. Ing. Milan Vojvoda, PhD.
Školiteľ špecialista: Ing. Matúš Jókay, PhD.
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška:
Téma práce: Bezpečnosť operačných systémov

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: prof. 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: prof. 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. Vojtěch Jirka

Školiteľ: prof. Dr. Ing. Miloš Oravec
Forma vzdelávania: doktorandské štúdium – externá forma, do 1.9.2018 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. 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

IX.3. Doktorandi vedení pracovníkmi ÚIM na iných pracoviskách

X. ÚČASŤ PRACOVNÍKOV ÚSTAVU NA KONFERENCIÁCH

X.1. Zahraničné konferencie

NÁZOV KONFERENCIE : CODE-BASED CRYPTOLOGRAPHY WORKSHOP 2018
Miesto: Davie, Florida, USA
Dátum: 4.-8.4.2018
Meno: Mgr. Tomáš Fabšič, PhD.
Príspevok: A reaction Attack on LEDApkc

NÁZOV KONFERENCIE : Trendy ve vzdělávaní 2018
Miesto: Slatinice u Olomouca, Česká republika
Dátum: 16.-18.5.2018
Meno: Ing. Alexander Hambalík, PhD.
Príspevok: Experience from creating a powerful software system for use in dactyloscopy and biometrics in school conditions

NÁZOV KONFERENCIE : Workshop Quantum Contextuality in Quantum Mechanics and Beyond
Miesto: Praha, Česká republika
Dátum: 18.-20.5.2018
Meno: doc. RNDr. Oľga Nánásiová, PhD.
Príspevok: Quantum probability and a Boolean function

NÁZOV KONFERENCIE : 3rd Conference on Information Technology, Systems Research and Computational Physics
Miesto: Krakow, Poľsko
Dátum: 1.-6.7.2018
Meno: doc. RNDr. Oľga Nánásiová, PhD.
Príspevok: Probability measures and projections on quantum logics

NÁZOV KONFERENCIE : Emerging Trends in Mathematics and Mechanics
Miesto: Krakow, Poľsko
Dátum: 17.-22.6.2018
Meno: prof. RNDr. Igor Bock, PhD.
Príspevok: An optimal design with respect to thickness of a viscoelastic plate in a dynamic contact with an obstacle

NÁZOV KONFERENCIE : International Conference on Historical Cryptology (HistoCrypt 2018)
Miesto: Uppsala, Švédsko
Dátum: 18.-20.6.2018
Meno: Ing. Eugen Antal, PhD.
Príspevok: Selected encrypted messages found in Slovak and Czech archives

NÁZOV KONFERENCIE : International Conference on Historical Cryptology (HistoCrypt 2018)
Miesto: Uppsala, Švédsko
Dátum: 18.-20.6.2018
Meno: Ing. Eugen Antal, PhD., prof. Ing. Pavol Zajac, PhD.
Príspevok: ManuLab System Demonstration

NÁZOV KONFERENCIE : 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)
Miesto: Barcelona, Španielsko
Dátum: 5.-9.8.2018
Meno: Ing. Maroš Čavojský
Príspevok: User Trajectory Extraction Based on WiFi Scanning

NÁZOV KONFERENCIE : ELMAR 2018
Miesto: Zadar, Chorvátsko
Dátum: 15.-20.9.2018
Meno: Ing. Zuzana Bukovčíková
Príspevok: The analysis of quality indicators on face recognition in video frames

NÁZOV KONFERENCIE : Algorithms and Tools for Petri Nets
Miesto: Augsburg, Nemecko
Dátum: 11.-12.10.2018
Meno: Ing. Juraj Mažári
Príspevok: Petriflow in Actions: Events Call Actions Call Events

NÁZOV KONFERENCIE : Algorithms and Tools for Petri Nets
Miesto: Augsburg, Nemecko
Dátum: 11.-12.10.2018
Meno: Ing. Milan Mladoniczky
Príspevok: Process Communication in PetriFlow: A Case Study

NÁZOV KONFERENCIE : Algorithms and Tools for Petri Nets
Miesto: Augsburg, Nemecko
Dátum: 11.-12.10.2018
Meno: prof. RNDr. Gabriel Juhás, PhD.

NÁZOV KONFERENCIE : IV CONGRESO MULTIDISCIPLINARIO DE CIENCIAS APLICADAS EN LATINOAMÉRICA, COMCAPLA 2018
Miesto: Mérida, Yucatán, México
Dátum: 20.-23.11.2018
Meno: RNDr. Igor Brilla, PhD.
Príspevok: Numerical determination of voltage potential inside 3D anisotropic media using variational methods

NÁZOV KONFERENCIE : Mikulášska kryptobesídka 2018
Miesto: Praha, Česká republika
Dátum: 29.-30.11.2018
Meno: Ing. Eugen Antal, PhD.

Príspevok: Meta Heuristics and Text Evaluation in Cryptanalysis of the Columnar Transposition

NÁZOV KONFERENCIE : Mikulášska kryptobesídka 2018
Miesto: Praha, Česká republika
Dátum: 29.-30.11.2018
Meno: Ing. Roderik Ploszek
Príspevok: O histórii ruských šifier od Cyrila a Medota po 2 sv. v. (predniesol namiesto prof. Grošeka)

X.2. Domáce konferencie

NÁZOV KONFERENCIE : EEE 2018 – ENERGETIKA, EKOLÓGIA, EKONOMIKA
Miesto: Tatranské Matliare
Dátum: 5.-7.6.2018
Meno: RNDr. Igor Brilla, PhD.
Príspevok: Numerical determination of voltage potential inside two dimensional nonhomogeneous media using variational methods

NÁZOV KONFERENCIE : CECC 2018
Miesto: Smolenice
Dátum: 5.-8.6.2018
Meno: prof. Ing. Pavol Zajac, PhD.
Príspevok: Potential for backdoors in BIKE key generation

NÁZOV KONFERENCIE : CECC 2018
Miesto: Smolenice
Dátum: 5.-8.6.2018
Meno: Ing. Eugen Antal, PhD.
Príspevok: Cryptoanalysis of the columnar transposition using meta-heuristics

NÁZOV KONFERENCIE : CECC 2018
Miesto: Smolenice
Dátum: 5.-8.6.2018
Meno: Ing. Michala Gulášová-Slugeňová
Príspevok: JPEG compatibility steganalysis

NÁZOV KONFERENCIE : CECC 2018
Miesto: Smolenice
Dátum: 5.-8.6.2018
Meno: Mgr. Tomáš Fabšič, PhD.
Príspevok: Reaction attacks on cryptosystems using QC-LDPC codes

NÁZOV KONFERENCIE : CECC 2018
Miesto: Smolenice
Dátum: 5.-8.6.2018
Meno: Ing. Peter Spaček

NÁZOV KONFERENCIE : IEEE ICETA 2018
Miesto: Starý Smokovec
Dátum: 14.-16.11.2018
Meno: prof. RNDr. Gabriel Juhás, PhD.
Príspevok: Scaling and structuring of digital literacy

NÁZOV KONFERENCIE : IEEE ICETA 2018
Miesto: Starý Smokovec
Dátum: 14.-16.11.2018
Meno: Ing. Juraj Mažári
Príspevok: Continual Improvement Process in Scientic Publishing

NÁZOV KONFERENCIE : 50. konferencia slovenských matematikov
Miesto: Jasná pod Chopkom
Dátum: 22.-25.11.2018
Meno: prof. Ing. Pavol Zajac, PhD.
Príspevok: Post-kvantová kryptografia

XI. HABILITAČNÉ A INAUGURAČNÉ KONANIA

XI.1. Inauguračné konania

prof. Ing. Pavol Zajac: *Aplikácia rovníc s viacerými pravými stranami na ťažké problémy v kryptografii*, prednáška sa uskutočnila 22.5.2018 v B-klube na FEI, menovaný za profesora bol 19.9.2018

XI.2. Habilitačné konania

doc. RNDr. Michal Zajac, PhD. – oponent habilitačnej práce **Mgr. Branislava Ftoreka, PhD.** (Strojnícka fakulta Žilinskej univerzity) na SvF STU 26.9.2018

XI.3. Členstvá v komisiách

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

prof. RNDr. Otokar Grošek, PhD. - predseda komisie pri dizertačnej skúške Ing. Michaly Gulášovej-Slugeňovej, 2.3.2018

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

prof. RNDr. Igor Bock, PhD.- člen komisie na obhajobu dizertačnej práce Ing. Mateja Medľu s názvom *Solving partial differential equations using finite volumemethod on non-uniform grids.* (obhájená 28.8.2018 na Katedre matematiky a deskriptívnej geometrie, SvF STU)

XII.4. Oponentské posudky k dizertačnej práci

prof. RNDr. Igor Bock, PhD.- práca Ing. Michala Kollára s názvom *Solving partial differential equations on surfaces with applications to geodetic data analysis* (obhájená 28.8.2018 na Katedre matematiky a deskriptívnej geometrie, SvF STU)

prof. RNDr. Igor Bock, PhD.- práca RNDr. Ing. Matúša Tibenského s názvom *Usage of gradient schemes for numerical solution of non-linear parabolic Equations* (obhájená 28.8.2018 na Katedre matematiky a deskriptívnej geometrie, SvF STU)

XII.5. Skúšky doktorandov z doktorandských predmetov

Meno Doktoranda	Odbor štúdia	Meno skúšajúceho	Predmet	Dátum

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

XIII.1. ŠVOČ

Meno: prof. RNDr. Igor Bock, PhD.
Člen komisie pre posúdenie prác Študentskej vedeckej konferencie na Staveb. Fak. STU v sekcii Matematické a počítačové modelovanie, 19.4.2018

Meno študenta	Roč.	Názov práce	Vedúci	Udelené ocenenia a návrhy
Matej Ohradzanský	3. BŠ	Lúštenie substitučných šifier pomocou N-gramov	prof. Ing. Pavol Zajac, PhD.	Cena dekana, Cena Zväzu slovenských vedeckotechnických spoločností
Bc. Tomáš Sovič	2. IŠ	Analýza vybraných vlastností bigramovej substitúcie	Ing. Eugen Antal, PhD.	Diplom dekana

Bc. Tomáš Hliboký	2. IŠ	Ohodnotenie textu pri kryptoanalýze transpozičných šifier	Ing. Eugen Antal, PhD.	Diplom dekana
Jakub Machovec	3. BŠ	Lúštenie šifrovanej korešpondencie Marie Antoinette	Ing. Eugen Antal, PhD.	
Lukáš Gnip	3. BŠ	Analýza šifrovanej korešpondencie Karla Rabenhaupta s Amáliou Alžbetou	Ing. Eugen Antal, PhD.	
Bc. Matúš Ješko	2. IŠ	Permutačné polynómy nad poľom GF(5^2) a ich využitie pri kryptoanalýze vybraných klasických šifier	prof. RNDr. Otokar Grošek, PhD.	

XIII.2. VEDENIE UKONČENÝCH DIPLOMOVÝCH PRÁC

Bečárová Andrea, Bc.	Riešenie dekódovacieho problému	P. Zajac
Bednár Dávid, Bc.	Tvorba užívateľského rozhrania k rozvrhovému systému pre FEI	M. Jókay
Bernát Ondrej, Bc.	Elektronický systém prezenčky	M. Jókay
Bezák Radovan, Bc.	Post-kvantová kryptografia	P. Zajac
Brezovský Matúš, Bc.	Lokalizácia športových aktivít z video sekvencie pomocou CNN	D. Sopiak
Červenka Martin, Bc.	Inovatívne metódy prezentácie produktov v ecommerce prostredí	O. Haffner
Demeterová Anna, Bc.	Návrh a implementácia informačného systému na podporu zákazníkom	G. Juhás
Dický Martin, Bc.	Zaslepené podpisy	P. Zajac
Drahovský Michal, Bc.	Škálovateľný klient-server systém pre rozšírenú realitu	M. Drozda
Duda Kristián, Bc.	Analýza klient-server systému pre rozšírenú realitu	M. Drozda
Dutko Jozef, Bc.	Optimalizácia obsahu pre VR headsety	R. Vargic
Dzvoník Ján, Bc.	Využitie hlasových asistentov v praktických aplikáciach	O. Haffner
Führich Richard, Bc.	Internetom podporovaná tvorba blokových schém	K. Žáková
Gálik Ondrej, Bc.	Systém na kontrolu prístupu do objektov pomocou smartfónu	E. Antal
Gažová Michaela, Bc.	Kryptosystém založený na teórii formálnych jazykov	V. Hromada
Greguš Ján, Bc.	Ochrana logických obvodov	M. Vojvoda
Grupač Richard, Bc.	Monitorovanie a manažment súborového systému	Š. Balogh
Hliboký Tomáš, Bc.	Využitie meta-heuristík pri lúštení transpozičných šifier	E. Antal
Hók Marián, Bc.	Podporný informačný systém pre vybrané procesy v malom pivovare	E. Kučera
Horecký Lukáš, Bc.	Využitie algoritmov rozpoznávania pre praktické aplikácie	O. Haffner
Hornák Michal, Bc.	Návrh zariadenia pre inteligentnú domácnosť	M. Jagelka
Hosťanský Andrej, Bc.	Spracovanie údajov inerciálnej navigačnej sústavy v interiéri	S. Marček
Hrdlík Martin, Bc.	Pokročilé metódy rozpoznávania prekážok a navigácie autonómnych bezpilotných systémov	P. Ťapák
Hrebík Marek, Bc.	Detekcia športových aktivít z video sekvencie	D. Sopiak
Huňady Jakub, Bc.	Detekcia tvárí pomocou hlbokých konvolučných sietí na zariadení Nvidia TX1	D. Sopiak

Iványek Tomáš, Bc.	Ochrana zdravotných údajov	K. Nemoga
Ivaniš Marián, Bc.	Distribuovaný firewall na báze OS Linux	M. Huba
Jahič Jakub, Bc.	Interaktívna vzdelávacia aplikácia v 3D engine pre objektovo orientované programovanie	E. Kučera
Jamrichová Romana, Bc.	MQ-podpisy s menším verejným kľúčom	V. Hromada
Javorka Peter, Bc.	Lúštenie transpozičných šifier pomocou meta-heuristík	E. Antal
Jenikovský Michal, Bc.	Tvorba 3E vizualizácie založenej na vlastnom grafickom frameworku	E. Kučera
Ješko Matúš, Bc.	Permutačné polynómy nad poľom GF(5^2) a ich využitie pri kryptoanalýze vybraných klasických šifier	O. Grošek
Jurina Marek, Bc.	Spracovanie dynamického obrazu pre monitorovanie a riadenie hydraulického systému	P. Bisták
Kačinetz Kristián, Bc.	Spracovanie údajov inerciálnej navigačnej sústavy v exteriéri	S. Marček
Kádek László, Bc.	Daktyloskopický sieťový systém DBOX-server	A. Hambalík
Kerekeš Gabriel, Bc.	Využtie EJBCA v systéme mobilnej peňaženky a vylepšenie prepoužiteľnosti celého riešenia	M. Repka
Kertýs Jakub, Bc.	Virtuálne laboratórium založené na platforme Java a Android	P. Bisták
Kimlička Kamil, Bc.	Akustický útok na RSA	T.Fabšič
Kirka Juraj, Bc.	Autorizačný server mYstable pre projekt Medusa	M. Jókay
Kolárik Kamil, Bc.	Aplikácia multikriteriálneho a multivariantného rozhodovania	O. Haffner
Kolibaš Maroš, Bc.	Získavanie poznatkov z procesných logov cez process mining a použitím data mining technológií.	D. Pancza
Kosár Andrej, Bc.	Ukážková implementácia výukového OS Nachos	M. Jókay
Košút Matej, Bc.	Palubný počítač formou mobilnej aplikácie	P. Bisták
Kováčik Jakub, Bc.	Webová aplikácia pre ovládanie žalúzií ako súčasti inteligentného domu	P. Bisták
Kováčik Martin, Bc.	Návrh a implementácia logovacieho informačného systému	G. Juhás
Kramár Matúš, Bc.	Bezpečnosť identifikátorov a autentifikácie používateľov	O. Grošek
Kubica Daniel, Bc.	Jednoúčelové heslá	M. Jókay
Kvačkaj Michal, Bc.	Vývoj administrátorského rozhrania pre systém dynamického vytvárania edukačných hier	Ľ. Stuchlíková
Kytka Miroslav, Bc.	Systém na otváranie dverí pomocou čipových kariet	E. Antal
Leskovský Roman, Bc.	Príspevok v oblasti vyhodnocovania ergonómie pracoviska	E. Kučera
Lipták Timotej, Bc.	Autonómny štart, vznášanie sa a pristávanie UAV	P. Ťapák
Martiš Pavol, Bc.	Spracovanie workflow procesov na účely ich kontroly a optimalizácie	G. Juhás
Maták Timotej, Bc.	Využitie EHR v klinickej praxi	A. Hambalík
Matišák Jakub, Bc.	Správa virtuálnych experimentov	K. Žáková
Mihálik Viliam, Bc.	Implementácia kontroly IPC do systému Medusa	M. Jókay
Mikuš František, Bc.	Analýza techník sociálneho inžinierstva	Š. Balogh
Molnár Martin, Bc.	Ovládanie UAV gestami ruky	P. Ťapák
Mucha Vladimír, Bc.	Spracovanie a vizualizácia medicínskych snímok s využitím strojového učenia a virtuálnej reality	J. Cigánek
Odziomková Kristína, Bc.	Návrh a implementácia tiketovacieho informačného systému	G. Juhás
Ondovčík Peter, Bc.	Evolúcia umelého života	I. Sekaj
Orlický Peter, Bc.	Strojové učenie pri klasifikácii obrazu a videa	R. Vargic
Pavličko Kamil, Bc.	Web front-end pre mobilnú aplikáciu s využitím technológie chatbot	M. Drozda

Pätoprstý Michal, Bc.	Systém prístupových bodov pre interaktívne web a mobilné aplikácie	K. Žáková
Ploszek Roderik, Bc.	Concurenncy in LSM Medusa	M. Jókay
Polaček Ján, Bc.	Klasifikácia tvárí pomocou konvolučných sietí pre Android OS	D. Sopiak
Prieboj Tomáš, Bc.	Analýza wifi dát a ich herné využitie	M. Drozda
Priganc Martin, Bc.	Automatizácia testovacieho systému programového vybavenia bánk	P. Bisták
Pšenák Martin, Bc.	Útoky na šifru GMR-2	M. Vojvoda
Rehák Pavol, Bc.	Bezpečné dvoj a viacúčastnícke výpočty.	K. Nemoga
Rybecký Viktor, Bc.	Využitie mobilných zariadení v medicínskej praxi	A. Hambalík
Seidl Matúš, Bc.	Nástroje pre mapovanie a generovanie ontológií z rôznych dátových zdrojov.	I. Kossaczký
Slaninka Tomáš, Bc.	Prúdové šifry v homomorfných kryptosystémoch	V. Hromada
Slezák Dávid, Bc.	Detekcia a sledovanie objektov v obraze	D. Sopiak
Smiešny Róbert, Bc.	Aplikácia pre zobrazoanie údajov z malého mechatronickéhovozidla na platforme Android	P. Fuchs
Smolár Martin, Bc.	Optimalizácia hlasovej biometrie ladením parametrov verifikácie hlasových vzoriek	Š. Balogh
Smoleň Matej, Bc.	Symetrické šifrovanie s umožnením vyhľadávania	M. Vojvoda
Soják Peter, Bc.	Evolučné programovanie a jeho využitie pri lúštení klasických šifier	E. Antal
Sokolík Jakub, Bc.	Zber a vyhodnocovanie dát s optimalizáciou jazdy na mechatronickom vozidle	P. Fuchs
Sovič Tomáš, Bc.	Lúštenie bigramovej substitúcie	E. Antal
Stroka Kristián, Bc.	Online riadenie termo-opticko-mechanickej sústavy	K. Žáková
Sýkorová Lenka, Bc.	Bezpečnosť databázových systémov	O. Grošek
Sýs Peter, Bc.	Aktualizácia steganografickej knižnice StegoDisk	M. Jókay
Šebeň Andrej, Bc.	Aplikácia na platforme Android pre zobrazovanie parametrov mechatronického vozidla prenášaných pomocou rozhrania mikro USB	P. Fuchs
Šidová Viera, Bc.	Dešifrovanie s nepravým kľúčom vedúce ku korektne vyzerajúcej správe	M. Vojvoda
Šranko Kristián, Bc.	Systém na detekciu škodlivého kódu s využitím analýzy pamäte	Š. Balogh
Štěpánek Martin, Bc.	Multiplatformová aplikácia pre získavanie dát o lokalitách s bezbariérovým prístupom	E. Kučera
Štrba Tomáš, Bc.	Analýza nasadenia ITIL manažmentového nástroja pre IT servisné pracovisko a návrh integrácie	I. Kossaczký
Taraj Miroslav, Bc.	Daktyloskopický sieťový systém DBOX-klint	A. Hambalík
Toman Marek, Bc.	Daktyloskopický systém s podporou GPU akcelerácie	A. Hambalík
Trebichavský Martin, Bc.	Použitie konečných automatov v konštrukcii šifrátorov	K. Nemoga
Uhlár Marek, Bc.	Genereovanie portrétu správania systému s dopravným oneskorením	M. Huba
Úroda Jozef, Bc.	Optimalizácia hlasovej biometrie ladením parametrov verifikácie hlasových vzoriek	A. Hambalík
Uzsák Richard, Bc.	Aplikácia pre zobrazovanie údajov z malého mechatronického vozidla na platforme Android	P. Fuchs
Vismek Marián, Bc.	Rozšírenie knižnice StegoDisk o podporu FUSE	M. Jókay
Vraniak Juraj, Bc.	Univerzálne, platformovo nezávislé konzolové rozhranie	I. Kossaczký
Vyskoč Jakub, Bc.	Mobilná webová aplikácia pre efektívnu výmenu údajov pri hľadaní pracovných pozícií	P. Bisták
Weinzettl Adam, Bc.	oauth 2 pre mobilnú peňaženku	M. Repka

Zlacký Radoslav, Bc.	Entropia náhodných generátorov používaných v praxi	M. Sýs
Zlatohlávek Ľuboš, Bc.	Tvorba hardvérového a softvérového vybavenia pre inteligentné zrkadlo	P. Bisták
Židovský Peter, Bc.	Distribuovaný firewall na báze OS Linux	S. Klúčik

XIII.3. ČLENSTVO V ŠTÁTNICOVÝCH KOMISIÁCH

Meno	**Bc. 12.6.**	**Bc. 3.-4.7.**	**Ing. BIS 13.-14.-15.6.**	**Ing. MSUS 13.-14.-15.6.**	**Iné**
E. Antal			X		
Š. Balogh			X		
Z. Bukovčíková		X X		X	
I. Brilla				X	
K. Čipková		X X			
M. Drozda		X X		X X	
T. Fabšič		X X	X X		
O. Gallo	X	X X		X X X	
O. Grošek		X X	X X		FIIT STU
M. Gulášová-Slugeňová	X		X		
A. Hambalík		X X	X	X X	
V. Hromada	X	X X	X	X	
M. Jókay		X X	X X X		
G. Juhás	X	X X		X X X	
M. Kečkemétyová		X		X X X	
I. Kossaczký		X X		X X	
P. Marák		X X	X		
S. Marček		X X		X X X	
I. Marinová		X	X		
Ľ. Marko		X X		X	
J. Mažári				X X	
M. Mladoniczky		X X		X X	
K. Nemoga		X	X		
V. Novák		X X	X		
D. Pancza				X	
E. Pastuchová		X		X	
M. Polakovič		X		X	
B. Rudolf		X	X		
D. Sopiak		X X			
M. Sýs		X	X		
P. Špaček		X X	X X		
M. Šrámka			X	X	

M. Vojvoda	**X**	**X X**	**X X**	**X**	FIIT STU
M. Zajac		**X X**	**X**		
P. Zajac		**X X**	**X X**		
M. Zákopčan		**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

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 **č**lenka 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. Mathematical Methods in Applied Sciences– 1 recenzia
2. Journal of Applied Mathematics, Statistics and Informatics – 1 recenzia
3. Mathematical Reviews – 11 prehľadov
4. Zentralblatt für Mathematik – 14 prehľadov

prof. Otokar Grošek, PhD. : 1 Recenzia pre J. of Combinatorial Design
1 recenzia pre J. of Mathematical Cryptology

1 recenzia pre Tatra Mountains Math. Pub.

doc. RNDr. Michal Zajac, PhD.: Mathematica Slovaca – 1 recenzia
Positivity – 1 recenzia
Mathematical Reviews – 3 prehľady
Zentralblatt für Mathematik – 5 prehľadov

XIV.4. Recenzie príspevkov na vedecké konferencie

RNDr. Igor Brilla, PhD.: 3 príspevky na konferenciu COMCAPLA 2018

1. Programación lineal aplicada al control de la concentración máxima de un contaminante.
2. Algunos criterios clásicos para verificar la estabilidad tipo Hurwitz de polinomios.
3. Aplicación de los criterios clásicos de estabilidad en sistemas con bifurcaciones.

XIV.5. Recenzie vedeckých projektov

prof. RNDr. Igor Bock, PhD. – Projekt VEGA – 1 recenzia

XV. ORGANIZÁCIA KONFERENCIÍ, ČLENSTVÁ VO VÝBOROCH

NÁZOV KONFERENCIE : 50. konferencia slovenských matematikov
Miesto: Jasná pod Chopkom
Dátum: 22.-25.11.2018
Meno: doc. RNDr. Oľga Nánásiová, PhD.
Funkcia: členka programového výboru, vedecká sekcia

NÁZOV KONFERENCIE : HistoCrypt 2018 1st International Conference on Historical Cryptology
Miesto: Uppsala University, Sweden
Dátum: 18.-20.6.2018
Meno: prof. RNDr Otokar Grošek, PhD.
Funkcia: člen programového výboru a chairman of the morning session June 19, 2018

NÁZOV KONFERENCIE : 39th International Conference on Applications and Theory of Petri Nets and Concurrency
Miesto: Bratislava
Dátum: 24.-29.06.2018
Meno: prof. RNDr. Gabriel Juhás, PhD.
Funkcia: Organizing Commitee Chair

NÁZOV KONFERENCIE : 39th International Conference on Applications and Theory of Petri Nets and Concurrency

Miesto: Bratislava
Dátum: 24.-29.06.2018
Meno: Ing. Juraj Mažári
Funkcia: Web Chair

NÁZOV KONFERENCIE : 39th International Conference on Applications and Theory of Petri Nets and Concurrency
Miesto: Bratislava
Dátum: 24.-29.06.2018
Meno: Ing. Milan Mladoniczky
Funkcia: Tools Exhibition Chair

NÁZOV KONFERENCIE : 18th International Conference on Application of Concurrency to System Design
Miesto: Bratislava
Dátum: 24.-29.06.2018
Meno: prof. RNDr. Gabriel Juhás, PhD.
Funkcia: General Chair

NÁZOV KONFERENCIE : 18th International Conference on Application of Concurrency to System Design
Miesto: Bratislava
Dátum: 24.-29.06.2018
Meno: Ing. Juraj Mažári
Funkcia: Web Chair

NÁZOV KONFERENCIE : 18th International Conference on Application of Concurrency to System Design
Miesto: Bratislava
Dátum: 24.-29.06.2018
Meno: Ing. Milan Mladoniczky
Funkcia: Tools Exhibition Chair

NÁZOV KONFERENCIE : IV CONGRESO MULTIDISCIPLINARIO DE CIENCIAS APLICADAS EN LATINOAMÉRICA, COMCAPLA 2018
Miesto: Mérida, Yucatán, México
Dátum: 20.-23.11.2018
Meno: RNDr. Igor Brilla, PhD.
Funkcia: člen vedeckýho výboru konferencie

XVI. SEMINÁRE

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

Seminár: CRYPTO
Vedúci: prof. Ing. Pavol Zajac, PhD.

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

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