

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

za rok 2011

časť- Aplikovaná informatika

riaditeľ ústavu:

prof. RNDr. Otokar Grošek, PhD.

e-mail: otokar.grosek@stuba.sk

Tel: ++421-2-602 91 226

Fax: ++421-2-654 20 415

I. PRACOVNÍCI

Profesor	prof. RNDr. Otokar Grošek, PhD.
Docenti	doc. RNDr. Jaroslav Fogel, PhD. doc. RNDr. Gabriel Juhás, PhD., (vedúci odd. SI) doc. RNDr. Karol Nemoga, PhD. doc. Dr. Ing. Miloš Oravec doc. Ing. Pavol Zajac, PhD., (vedúci odd.BIS)
Odborní asistenti	Ing. Štefan Balogh Ing. Alexander Hambalík, PhD. Ing. Matúš Jókay, PhD. RNDr. Igor Kossaczky, CSc. RNDr. Eva Kostrecová, PhD. Ing. Fedor Lehocki, PhD. Ing. Vladislav Novák Mgr. Marek Sýs, PhD. Mgr. Zuzana Ševčíková Ing. Michal Šrámka, PhD., PhD. Ing. Milan Vojvoda, PhD.
Výskumní pracovníci	Ing. Ondrej Gallo
Technickí pracovníci	Ing. Stanislav Marček Zuzana Šabíková (vedúca org.odd.) Brigita Timková
Doktorandi	Ing. Eugen Antal Ing. Michal Braško Ing. Lucia Cibulková Ing. Matej Féder Ing. Jaroslav Hamráček Ing. Viliam Hromada Ing. Igor Kazlov Ing. Ján Mazanec Mgr. Michal Mikuš Ing. Ľuboš Omelina Ing. Filip Pilka Ing. Marek Repka Ing. Martin Riesz Ing. Andrej Savka Ing. Juraj Varga Ing. Milan Zelina

II. ZARIADENIA

II. 1 Výukové a výskumné laboratóriá

- Laboratórium pre Bezpečnosť IT
- Laboratórium pre databázy - DIEDC (Database Information Education and Demonstration Center)
- Laboratórium medicínskej informatiky
- Laboratórium Komunikačných sietí
- Experimentálne laboratórium ÚIM

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. VÝUKA

III.1 Bakalárske štúdium (Bc.)

Algoritmizácia a programovanie	(1. sem. 3-2 h)	P. Zajac
Algoritmizácia a programovanie	(1. sem. 3-2 h)	M. Sýs
Algoritmizácia a programovanie	(1. sem. 3-2 h)	I. Kossaczký
Analýza a zložitosť algoritmov	(5. sem. 3-1 h)	M. Vojvoda
Klasické šifry	(4. sem. 2-2 h)	O. Grošek
Databázové systémy	(3. sem. 3-2 h)	M. Vojvoda
Operačné systémy	(3. sem. 3-2 h)	M. Jókay
Programovacie techniky	(2. sem. 3-2 h)	I. Kossaczký
Projektovanie databázových systémov	(4. sem. 3-1 h)	G. Juhás
Informačná bezpečnosť	(5. sem. 2-2 h)	E. Kostrecová
Počítačová kriminalita	(6. sem. 2-2 h)	E. Kostrecová
Modelovanie v softvérovom inžinierstve	(5. sem. 2-2 h)	J. Hanák
Základy kryptografie	(5. sem. 2-2 h)	O. Grošek
Rýchle algoritmy	(6. sem. 2-2 h)	K. Nemoga
Teoretické základy informatiky	(4. sem. 3-2h)	O. Grošek
Komunikačné siete 1	(4. sem. 3-1 h)	M. Oravec
Vývoj softvérových aplikácií 1	(3. sem. 2-2 h)	M. Šrámka
Architektúra softvérových systémov	(5. sem. 2-2 h)	G. Juhás
Manažment IT projektov	(6. sem. 2-2 h)	F. Lehocki
Workflow manažment systémy	(6. sem. 2-2 h)	F. Lehocki
Komunikačné siete 2	(6. sem. 4-1 h)	A. Hambalík/M. Oravec

III.2 Inžinierske štúdium (Ing.)

Počítačová grafika	(1. sem. 3-2 h)	M. Sýs
Objektovo orientované programovanie	(3. sem. 3-2 h)	V. Novák

Šifrovanie v komunikačných sieťach	(1. sem. 3-2 h)	K. Nemoga
Modelovanie a simulácia udalostných systémov	(1. sem. 3-2 h)	G. Juhás
Bezpečnosť informačných systémov s pohľadom praxe	(1.+ 3.sem. 3-2 h)	M. Zanechal
Formálne metódy	(1. sem. 3-2 h)	J. Fogel
Kryptoanalýza šifrátorov	(3. sem. 3-2 h)	M.Vojvoda, P.Zajac, M.Sýs
Analýza a syntéza udalostných systémov	(2. sem. 3-2 h)	G. Juhás
Biometria	(2 .sem. 3-2 h)	M.Oravec
Systémové programovanie	(2.,4. sem. 3-2h)	J. Fogel
Návrh šifrátorov	(3. sem. 3-2 h)	P. Zajac
Strojové učenie a neurónové siete	(1. sem. 3-2 h)	M. Oravec
Manažment podnikových procesov, workflow procesy a web servisy	(2.sem. 3-2 h)	F. Lehocki

III.3 Bakalárske a inžinierske štúdium pre zahraničných študentov (v anglickom jazyku)

Algoritmicizácia a programovanie	(1. sem. 12h konzul.)	J. Varga
Programovacie techniky	(2. sem. 12h konzul.)	M. Sýs
Log. systémy	(1. sem. 12 h konzul.)	Ľ. Omelina
Architektúra počítačov	(2. sem 12 h konzul.)	M. Jókay
Biznis manažment	(2. sem. 12 h konzul.)	F.Lehocki
Klasické šifry	(4. sem. 12 h konzul.)	O. Grošek

III.4 Dištančné štúdium

Algoritmicizácia a programovanie	(1. sem. 6x2 h konzul.)	A. Hambalík
----------------------------------	-------------------------	-------------

IV. VÝSKUMNÉ PROJEKTY

IV.1. Projekty VEGA, ESF riešené v roku 2011 na ÚIM

Projekt: grant VEGA 1/0214/10 - Návrh metód analýzy a klasifikácie pre biometrické rozpoznávanie obrazov ľudských tvárí a prevádzku komunikačných sietí

Zodpovedný riešiteľ: **doc. Dr. Ing. Miloš Oravec**

Riešitelia z ÚIM: Ing. Ján Mazanec, Ing. Filip Pilka, Ing. Ľuboš Omelina, Ing. Milan Zelina, Ing. Matej Féder

Projekt: grant VEGA 1/0244/09 – Riešenie aktuálnych kryptologických problémov

Vedúci projektu : **prof. RNDr.Otokar Grošek, PhD.**

Riešitelia z ÚIM: Ing. Vojvoda, PhD., Ing. Zajac, PhD., Ing. Jókay, Mgr. Mikuš, Mgr. Sýs, PhD., Ing. Novák, Ing. Adamko, doc. RNDr.Ladislav Satko, PhD.

ERASMUS Educational Project – Bilateral Agreement for the academic year 2006/08, SOCRATES programme“ HIGHER EDUCATION (ERASMUS) medzi University of La Laguna, Tenerife, Spain, Department of Statistics, Operations Research and Computation

Riešitelia: Pino Caballero-Gil, Candelania Hernández-Goya + 20 študentov a ÚIM FEI STU Bratislava

Riešitelia: **Otokar Grošek, Karol Nemoga, Milan Vojvoda + 20 študentov**

APVV 0513-10 Meracie, komunikačné a informačné systémy na monitorovanie kardiovaskulárneho rizika u pacientov s hypertenziou, obdobie realizácie 5/2011-4/2013. Zodpovedný riešiteľ: **Fedor Lehocki**.

Program na podporu mladých výskumníkov

Projekt: Kritické mriežky

Vedúci projektu : **Mgr. Marek Sýs, PhD.**

Riešitelia z ÚIM : Mgr. Mikuš

Program na podporu mladých výskumníkov

Projekt: GPU výpočty

Vedúci projektu : **Ing. Pavol Zajac, PhD.**

Riešitelia z ÚIM: Ing. Matúš Jókay.

IV.2. Výskumné úlohy

IV.3. Zahraničné projekty

Projekt SK-FR-0011-09

Názov projektu : Cryptographic Algorithms and Primitives with Increased Resistance Against Side Channel Attacks

Koordinátor: **prof. RNDr. Otokar Grošek, PhD.**

Spoluriešitelia: doc. Nemoga, Ing. Repka, Mgr. Sýs, Ing. Zajac

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

VEGA grant 1/0718/09

Názov úlohy: Algoritmy a metódy spracovania multimedialných signálov pre rozhranie človek-počítač

Zodpovedný riešiteľ: doc. Ing. Gregor Rozinaj, PhD.

Spoluriešitelia v roku 2011: doc. Dr. Ing. Miloš Oravec

Dátum oponentúry: 2011

VEGA grant VEGA 1/0961/11

Názov úlohy: Pokročilé algoritmy spracovania obrazov na efektívne vyhľadávanie a kódovanie ľudských tvárí

Zodpovedný riešiteľ: doc. Ing. Jarmila Pavlovičová, PhD.

Spoluriešitelia v roku 2011: doc. Dr. Ing. Miloš Oravec

Dátum oponentúry: 2014

KEGA grant 119-005TVU-4/2010

Názov úlohy: Rozvoj digitálnej gramotnosti v základnej a strednej škole

Zodpovedný riešiteľ: PaedDr. Mgr. Viola Gazdíková, PhD., Trnavská univerzita v Trnave

Spoluriešitelia v roku 2011: doc. Dr. Ing. Miloš Oravec

Dátum oponentúry: 2012

Projekt ITMS - 26110130083, 26140130013

Premena tradičnej školy na modernú (celé územie SR okrem BA)

Riešiteľ z ÚIM : Ing. Alexander Hambalík, PhD.

Trvanie : 2008-2013

Projekt ITMS - 26110130084, 26140130084

Premena tradičnej školy na modernú pre Bratislavský kraj

Riešiteľ z ÚIM : Ing. Alexander Hambalík, PhD.

Trvanie : 2008-2013

OPVaV-2008/4.1/01-SORO

Podpora budovania Centra excelentnosti pre Smart technológie, systémy a služby

ITMS : 262401 20005

Riešitelia: doc. RNDr. Gabriel Juhás, PhD., Ing. Fedor Lehocki

Trvanie : 05/2009-04/2011

OPVaV-2009/4.1/02-SORO

Podpora budovania Centra excelentnosti pre Smart technológie, systémy a služby II

ITMS : 262401 20029

Riešitelia: doc. RNDr. Gabriel Juhás, PhD., Ing. Fedor Lehocki, doc. Dr. Ing. Miloš Oravec

Trvanie : 02/2010-01/2013

Projekt 7. rámcového programu FP7-ICT-2011-7-287848

HBB-NEXT Next-Generation Hybrid Broadcast Broadband

Koordinátor: Rundfunk Berlin-Brandenburg, Germany

Koordinátor za STU: prof. Ing. Pavol Podhradský, PhD.

Riešiteľ: doc. Dr. Ing. Miloš Oravec

Trvanie: X/2011 – III/2013

Metódy spracovania policajne relevantných informácií,

Vedúca projektu: doc. RNDr. Ľudmila Gregušová, CSc.

Čiastková úloha projektu: Metódy ochrany policajne relevantných informácií.

Vedúca čiastkovej úlohy: RNDr. Eva Kostrecová, PhD.

Akadémia Policajného zboru v Bratislave, Katedra manažmentu a informatiky,

Trvanie: 01/2010 – 06/2012

V. SPOLUPRÁCA**V.1. Domáca spolupráca:****i) Pozvané prednášky**

ii) Spolupráca s domácimi inštitúciami

- Národný bezpečnostný úrad SR, Bratislava
- Ministerstvo obrany SR
- Kriminologicko expertízny ústav Policajného zboru MV SR, Bratislava
- Fakulta matematiky, fyziky a informatiky UK, Bratislava
- Asociácia projektu INFOVEK - projekt Informatizácia regionálneho školstva
- ÚIPŠ Bratislava, projekt Modernizácia vyučovacieho procesu – projekt ESF
- Elfa s.r.o. Košice, projekt Modernizácia vyučovacieho procesu – projekt ESF
- Datalan s.r.o. Bratislava, projekt Modernizácia vyučovacieho procesu – projekt ESF
- Metodicko-pedagogické centrum mesta Bratislavy
- Virtuálna akadémia bratislavského samosprávneho kraja
- Agentúra na podporu výskumu a vývoja, Bratislava
- Fakulta chemickej a potravinárskej technológie, STU Bratislava
- Technická univerzita, Zvolen
- Matematický ústav SAV, Bratislava
- Univerzita J. Selyeho, Komárno
- Univerzita Konštantína Filozofa UKF
- Katedra Inžinierskej pedagogiky a psychológie MfF STU Trnava
- 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
- Fakulta managementu, UK, Bratislava

V.2. Zahraničná spolupráca:

i) Pozvané prednášky

ii) Spolupráca so zahraničnými inštitúciami

- University of LA LAGUNA, Department of Statistics, Operations Research and Computing, Tenerife (prof. Pino Caballero-Gil)
- Ústav informatiky ČSAV, Praha, Česká republika (prof. Štefan Porubský)
- Department of Information Systems Security, Concordia University College of Alberta, Canada
- Fakulta informatiky MU Brno, Česká republika (doc. Václav Matyáš)
- Florida Atlantic University, Boca Raton, Florida, USA (prof. Spyros Magliveras, prof. Wandí Wei, prof. Rainer Steinwandt)
- Katedra matematiky FEL ČVUT Praha (doc. Marie Demlová, prof. Pavel Pták)
- Institut für Experimentelle Mathematik, Universität Duisburg-Essen, Germany, (prof. Tran van Trung, Pavol Švába)

- University of Washington, Tacoma USA (prof. Peter Horák)
- Lehrstuhl fuer Angewandte Informatik, Katholische Universitaet Eichstaett-Ingolstadt, Nemecko (prof. Joerg Desel a prof. Robert Lorenz)
- Fachgruppe Simulation und Modellierung, Institut fuer Systems Engineering, Universitaett Hannover, Nemecko (Dr. Martin Drozda)
- Department of Mathematics and Computer Science, Indiana State University, USA (prof. Robert Jajcay)
- Eszterházy Károly Főiskola, Eger, Maďarsko, (Dr. Kiss Tóth)
- AINTEK A.E, Grécko, (Mr. Panos Katsampanis)
- Virginia Tech, Blacksburg, Virginia, USA (prof, Sandeep K. Shukla)
- McMaster University, Hamilton, Kanada (prof. Ryzsard Janicki)
- University of Waterloo, Kanada (prof. Jo Atlee)
- University of Toronto, Kanada (prof. Eric Hehner)
- Universität Augsburg, Nemecko (prof. Robert Lorenz)
- Department of Computer Engineering and Mathematics, Universitat Rovira i Virgii, Spain (Dr. M.Šrámka)
- Laboratoire Hubert Curien, Université Jean Monnet, Saint –Etienne, France
- (prof. Viktor Fischer)
- Technische Universiteit Eindhoven, Eindhoven, Nederlands (Dr. Wei Chen, Mrs. Natalia Sidorova, Mr. Kees van Hee, Mr. Wil van der Aalst)
- University of Southampton, UK (prof. Robert Allen)
- Selmersenteret, Institut for Informatikk, Universitetet i Bergen, Norway, (prof. Tor Helleseth)
- Ecole Nationale de Police, Montbéliard, France (M. Michel Roggero)

iii) Zahraniční hostia

- **Ing. Ľuboš Gašpar** - pracovné stretnutie v rámci spolupráce s Laboratoire Hubert Curien, Université Jean Monnet, France - Projekt **SK-FR-0011-09** v termíne 23.4. – 7.5.2011

iv) Pobyty pracovníkov v zahraničí

Zahraničné cesty

Meno: Otokar Grošek

Miesto: St. Etienne, Francúzsko

Akcia: Na základe spoločného projektu **SK-FR-0011-09** boli vykonané merania kryptografických algoritmov so zvýšenou odolnosťou voči útokom postrannými kanálmi.

Účasť: spolupráca s Laboratoire Hubert Curien, Université Jean Monnet, France

Dátum: 13. – 16. 11.2011

Meno: Karol Nemoga

Miesto: St. Etienne, Francúzsko

Akcia: Na základe spoločného projektu **SK-FR-0011-09** boli vykonané merania kryptografických algoritmov so zvýšenou odolnosťou voči útokom postrannými kanálmi.

Účasť: spolupráca s Laboratoire Hubert Curien, Université Jean Monnet, France

Dátum: 13. – 16. 11.2011

Meno: Pavol Zajac

Miesto: St. Etienne, Francúzsko

Akcia: Projekt **SK-FR-0011-09**

Účasť: spolupráca s Laboratoire Hubert Curien, Université Jean Monnet, France

Dátum: 13. 11. 2011- 16. 11. 2011

Meno: Marek Sýs

Miesto: St. Etienne, Francúzsko

Akcia: Projekt **SK-FR-0011-09**

Účasť: spolupráca s Laboratoire Hubert Curien, Université Jean Monnet, France

Dátum: 13. 11. 2011- 16. 11. 2011

Meno: Marek Repka

Miesto: St. Etienne, Francúzsko

Akcia: Projekt **SK-FR-0011-09**

Účasť: spolupráca s Laboratoire Hubert Curien, Université Jean Monnet, France

Dátum: 27.03. 2011- . 09.04.2011

Meno: Marek Repka

Miesto: St. Etienne, Francúzsko

Akcia: štipendijný pobyt v rámci : „Národný štipendijný program na podporu mobility študentov, doktorandov, vysokoškolských učiteľov a výskumných pracovníkov“ – Sprostredkovala SAIA ,n.o. - hradené MŠ SR.

Účasť: spolupráca s Laboratoire Hubert Curien, Université Jean Monnet, France

Dátum: 01.09. 2011- 30.11.2011

V. 3. Členstvo v medzinárodných organizáciách a spoločnostiach

- doc. RNDr. Jaroslav Fogel, PhD. je členom IEEE Computer Society,
- prof. RNDr. Otokar Grošek, PhD. je členom AMS, SIAM,
- doc. RNDr. Karol Nemoga, PhD je členom IACR,
- doc. Dr. Ing. Miloš Oravec je členom IET,IEEE
- Ing. Fedor Lehocki je členom IEEE EBMS,
- RNDr. Eva Kostrecová, PhD je členom ETIS

VI. Obhájené dizertácie

JÓKAY, M : Steganografia v obraze a videu : dát. obhaj. 27.9.2011, čís. ved. odb. 9.2.9. - Bratislava : STU v Bratislave FEI, 2011.

LEHOCKI, F : Modely diagnostických systémov : čís. ved. odb. 9.2.9, obhaj. 2.6.2011. - Bratislava : STU v Bratislave FEI, 2011.

VII. INÉ AKTIVITY

VII.1. Akademické a iné funkcie

- prof. RNDr. Otokar Grošek, PhD. je členom Vedeckej rady FEI STU

- prof. RNDr. Otokar Grošek, PhD. je podpredsedom 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.
- prof. RNDr. Otokar Grošek, PhD. je členom hlavného výboru Slovenskej spoločnosti pre kybernetiku a informatiku pri SAV
- prof. RNDr. Otokar Grošek, PhD. je garantom inžinierskeho a doktorandského študijného programu štúdia Aplikovaná informatika na FEI STU
- doc. RNDr. Gabriel Juhás, PhD. je predsedom Vedeckej rady FEI STU
- doc. RNDr. Gabriel Juhás, PhD. je členom OK študijného programu Aplikovaná informatika na STU
- doc. RNDr. Gabriel Juhás, PhD. je členom Rady Výskumného centra STU
- doc. RNDr. Gabriel Juhás, PhD. je dekanom FEI STU
- doc. RNDr. Gabriel Juhás, PhD. je členom riadiaceho výboru pre spoluprácu STU Bratislava a ENEL Slovenské elektrarne, a.s.
- doc. RNDr. Gabriel Juhás, PhD. je spolu-garantom študijného programu inžinierskeho a doktorandského štúdia Aplikovaná informatika na FEI STU
- doc. RNDr. Gabriel Juhás, PhD. je garantom bakalárskeho študijného programu štúdia Aplikovaná informatika na FEI STU
- 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, Ševčenkova 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 (Modernizácia vyučovacieho procesu na ZŠ a SŠ. ITMS: 26110130083, 26140130013 a ITMS: 26110130084, 26140130084. Opatrenie 1.1 Premena tradičnej školy na modernú – celé územie SR (okrem BA) a Opatrenie 4.1 Premena tradičnej školy na modernú pre Bratislavský kraj; projekt podporovaný ESF.
- doc. RNDr. Karol Nemoga, PhD je členom, predsedom Vedeckej rady Matematického ústavu SAV
- doc. RNDr. Karol Nemoga, PhD. Podpredseda Edičnej rady SAV, predseda Knižničnej rady SAV, člen Národného komitétu pre IASA
- doc. RNDr. Jaroslav Fogel, PhD. je spolugarantom študijného programu doktorandského štúdia Aplikovaná informatika na FEI STU
- doc. RNDr. Jaroslav Fogel, PhD. je členom OK študijného programu Aplikovaná informatika na STU
- doc. RNDr. Jaroslav Fogel, je členom Vedeckej rady FI PEVŠ
- doc. Dr. Ing. Miloš Oravec je prodekanom FEI STU
- doc. Dr. Ing. Miloš Oravec je členom Vedeckej rady FEI STU
- doc. Dr. Ing. Miloš Oravec je členom OK študijného programu Aplikovaná informatika na STU

- doc. Dr.Ing. Miloš Oravec je spolugarantom študijného programu doktorandského štúdia Aplikovaná informatika na FEI STU

VII.2. Členstvo v domácich spoločnostiach a organizáciách

- doc. RNDr. Jaroslav Fogel, PhD. je členom SSKI, JSMF
- prof. RNDr. Otokar Grošek, PhD. je členom JSMF.
- doc. RNDr. Karol Nemoga, PhD je členom JSMF
- Ing. Fedor Lehocki je členom SBIMI (Spoločnosť biomedicínskeho inžinierstva a medicínskej informatiky)
- Ing. Fedor Lehocki je členom technickej komisie Informačné technológie (TK 37), Slovenského ústavu technickej normalizácie

VII.3. Vedenie súťaží študentov

Prof. RNDr. Otokar Grošek, PhD. : Bc. Martin Košdy,
Útoky postrannými kanálmi na systémy založené na EC , súťaž KEYMAKER, ČR - absolútny víťaz

Ing. Milan Vojvoda Bc. : Viliam Hromada
Chybová analýza prúdových šifrier - práca dostala Cenu dekana a bola navrhnutá na Cenu Rektora

Doc. Ing. Pavol Zajac, PhD. : Bc. Radoslav Čagala, súťaž KEYMAKER, ČR – víťaz
kategórie diplomových prác

VIII. Publikácie

Zoznam publikácií za rok 2011

AAB Vedecké monografie vydané v domácich vydavateľstvách

Počet záznamov: 2

AAB1 **JUHÁS, G.:** Algebraically Generalised Petri Nets. - Bratislava : RT Systems, 2011. - 185 s. - ISBN 978-80-970519-3-8

AAB2 **JUHÁS, G.:** Are These Events Independent? It Depends!. - Bratislava : RT Systems, 2011. - 145 s. - ISBN 978-80-970519-2-1

ABC Kapitoly vo vedeckých monografiách vydané v zahraničných vydavateľstvách

Počet záznamov: 1

ABC1 **ORAVEC, M. - PAVLOVIČOVÁ, J. - MAZANEC, J. - OMELINA, E. - FÉDER, M. - BAN, J.:** Efficiency of Recognition Methods for Single Sample per Person Based Face Recognition.
In: Reviews, Refinements and New Ideas in Face Recognition. - Rijeka : InTech, 2011.

- ISBN 978-953-307-368-2. - S. 181-206

ACB Vysokoškolské učebnice vydané v domácich vydavateľstvách

Počet záznamov: 1

ACB1 **JUHÁS, G.**: Modelovacie formalizmy udalostných systémov. - Bratislava : RT Systems, 2011. - 112 s. - ISBN 978-80970519-1-4

ADE Vedecké práce v zahraničných nekarentovaných časopisoch

Počet záznamov: 4

ADE1 **BAN, J. - FÉDER, M. - ORAVEC, M. - PAVLOVIČOVÁ, J.**: Non-Conventional Approaches to Feature Extraction for Face Recognition.
In: Acta Polytechnica Hungarica. - ISSN 1785-8860. - Vol. 8, No. 4 (2011), s. 75-90

ADE2 **BENIAK, M. - PAVLOVIČOVÁ, J. - ORAVEC, M.**: 3D Chrominance Histogram Based Face Localisation.

In: International Journal of Signal and Imaging Systems Engineering. - ISSN 1748-0701 (ON-LINE). - ISSN 1748-0698 (PRINT). - Vol. 4, Iss. 1 (2011), s. 3-12

ADE3 **PILKA, F. - ORAVEC, M.**: A NARX Neural Network Algorithm for Video Traffic Prediction.

In: Journal of Electrical and Electronics Engineering (JEEE). - ISSN 1844-6035. - Vol. 4, No. 1 (2011), s. 179-184

ADE4 **ZELINA, M. - ORAVEC, M.**: Feature Selection for Application Recognition in Communication Networks.

In: AD ALTA : Journal of Interdisciplinary Research. - ISSN 1804-7890. - Vol. 1, Iss. 1 (2011), s. 115-117

ADF Vedecké práce v domácich nekarentovaných časopisoch

Počet záznamov: 3

ADF1 **KOSTRECOVÁ, E.**: Iniciatívy v rámci medzinárodnej spolupráce štátov a svetových inštitúcií pri ochrane elektronického priestoru.

In: Policajná teória a prax. - ISSN 1335-1370. - Roč. 19, č. 2 (2011), s. 134-138

ADF2 **PILKA, F. - ORAVEC, M.**: Prediction Methods for MPEG-4 and H.264 Video Transmission.

In: Journal of Electrical Engineering. - ISSN 1335-3632. - Vol. 62, No. 2 (2011), s. 57-64

ADF3 **RACKO, J. - MIKOLÁŠEK, M. - BENKO, P. - HARMATHA, L. - GALLO, O. - GRANZNER, R. - SCHWIERZ, F.**: Coupled Defect Level Recombination in the P-N Junction.

In: Journal of Electrical Engineering. - ISSN 1335-3632. - Vol. 62, No. 6 (2011), s. 355-358

AFC Publikované príspevky na zahraničných vedeckých konferenciách

Počet záznamov: 11

AFC1 **BALOGH, Š. - PONDELÍK, M.**: Capturing Encryption Keys for Digital Analysis.

- In: IDAACS 2011 : 6th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. Prague, Czech Republic, 15 - 17 September 2011. - Piscataway : IEEE, 2011. - ISBN 978-1-4577-1425-2. - S. 759-763
- AFC2 **BAN, J. - FÉDER, M. - ORAVEC, M. - PAVLOVIČOVÁ, J.:** Enhancement of One Sample per Person Face Recognition Accuracy by Training Sets Extension.
In: Proceedings ELMAR-2011 : 53rd International Symposium ELMAR-2011,14-16 September 2011, Zadar, Croatia. - Zadar : Croatian Society Electronics in Marine, 2011. - ISBN 978-953-7044-12-1. - S. 25-28
- AFC3 **HROMADA, V. - VOJVODA, M.:** Fault Analysis of Stream Ciphers.
In: Mikulášská kryptobesídka 2011 : Sborník příspěvků: Praha, 1. - 2. decembra 2011. - Praha : Trusted Network Solutions, 2011. - S. 69-70
- AFC4 **JÓKAY, M.:** The Design of a Steganographic system Based on the GOP Structure in the Video Standard MPEG-4.
In: Recent Researches in Computers and Computing : International Conference on Computers and Computing (ICCC'11). Lanzarote, Spain, 27.-29.5.2011. - : WSEAS Press, 2011. - ISBN 978-1-61804-000-8. - S. 95-99
- AFC5 **OMELINA, L. - ORAVEC, M.:** Efficient Face Expression Generation for Face Recognition.
In: Proceedings ELMAR-2011 : 53rd International Symposium ELMAR-2011,14-16 September 2011, Zadar, Croatia. - Zadar : Croatian Society Electronics in Marine, 2011. - ISBN 978-953-7044-12-1. - S. 29-32
- AFC6 **OMELINA, L. - ORAVEC, M.:** Universal Biometric Evaluation System.
In: IWSSIP 2011 : 18th International Conference on Systems, Signals & Image Processing. - : IEEE eXpress, 2011. - ISBN 978-9958-9966-3-4. - S. 307-310
- AFC7 **PILKA, F. - ORAVEC, M.:** Multi-Step Ahead Prediction Using Neural Networks.
In: Proceedings ELMAR-2011 : 53rd International Symposium ELMAR-2011,14-16 September 2011, Zadar, Croatia. - Zadar : Croatian Society Electronics in Marine, 2011. - ISBN 978-953-7044-12-1. - S. 269-272
- AFC8 **RACKO, J. - MIKOLÁŠEK, M. - GRMANOVÁ, A. - BREZA, J. - BENKO, P. - GALLO, O. - HARMATHA, L.:** A New Model of Multiphon Excitation Trap-Assisted Band-to-Band Tunneling.
In: EDS'11. Electronic Devices and Systems IMAPS CS International Conference 2011 : Brno, Czech Republic, June 22-23, 2011. - Brno : VUT v Brně, 2011. - ISBN 978-80-214-4303-7. - S. 168-174
- AFC9 **VÁLKY, G. - LEHOCKI, F. - KOVÁČ, M.:** Wireless System for Online Acquisition of ECG Waveforms of Human Heart.
In: AMA-IEEE Medical Technology Conference: Healthcare IT : 2nd AMA-IEEE Medical Technology Conference on Delivering on the Promise of Cost Effective Quality Healthcare. Boston, Massachusetts, 16-18 October 2011. - Piscataway : IEEE,

2011. - CD-ROM

- AFC10 **ZELINA, M. - ORAVEC, M.:** Early Detection of Internet Applications.
In: Proceedings of 9th International Conference VSACKÝ CĀB 2011. - : Brno
University of Technology, 2011. - ISBN 978-80-214-4319-8. - S. 157-160
- AFC11 **ZELINA, M. - ORAVEC, M.:** Early Detection of Network Applications Using
Neural Networks.
In: Proceedings ELMAR-2011 : 53rd International Symposium ELMAR-2011,14-16
September 2011, Zadar, Croatia. - Zadar : Croatian Society Electronics in Marine,
2011. - ISBN 978-953-7044-12-1. - S. 161-164
- AFD Publikované príspevky na domácich vedeckých konferenciách
Počet záznamov: 17
- AFD1 **BALOGH, Š. - CHOVANČĀK, D.:** Použitie dataminig metód pri odhaľovaní
nových typov malware a pri sieťových útokoch.
In: Znalosti 2011 : 10. ročník konferencie, Stará Lesná, Vysoké Tatry, 31. ledna -
2.února 2011. Sborník príspevků. - Ostrava : Fakulta elektrotechniky a informatiky,
VŠB - Technical University of Ostrava, 2011. - ISBN 978-80-248-2369-0. - S. 255-
258
- AFD2 **BLAŠKO, R. - ORAVEC, M. - PAVLOVIČOVĀ, J. - HANÚSKOVĀ, V. -
LEHOCKI, F.:** Image Preprocessing for Diagnostics Support in Ophthalmology.
In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Roč. 17,
mimoriadne č. : ELOSYS, Trenčín, 11.-14.10.2011 (2011), s. 5-8
- AFD3 **BRAŠKO, M.:** On Comparison of Stream Ciphers Proposals in Estream Project.
In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Roč. 17,
mimoriadne č. : ELOSYS, Trenčín, 11.-14.10.2011 (2011), s. 189-193
- AFD4 **CIBULKOVĀ, L. - LEHOCKI, F. - HANÚSKOVĀ, V. - ORAVEC, M. -
PAVLOVIČOVĀ, J.:** Modelovanie klinických procesov v zdravotníctve.
In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Roč. 17,
mimoriadne č. : ELOSYS, Trenčín, 11.-14.10.2011 (2011), s. 194-198
- AFD5 **CIBULKOVĀ, L. - LEHOCKI, F.:** Modelovanie Workflow procesov.
In: ŠVOČ 2011 : Študentská vedecká a odborná činnosť. Zborník vybraných prác.
Bratislava, Slovak Republic, 4.5.2011. - Bratislava : STU v Bratislave FEI, 2011. -
ISBN 978-80-227-3508-7. - S. 30-33
- AFD6 **HROMADA, V. - VOJVODA, M.:** Chybová analýza prúdových šifier.
In: ŠVOČ 2011 : Študentská vedecká a odborná činnosť. Zborník vybraných prác.
Bratislava, Slovak Republic, 4.5.2011. - Bratislava : STU v Bratislave FEI, 2011. -
ISBN 978-80-227-3508-7. - S. 25-29
- AFD7 **JÓKAY, M. - PLANČÍK, M. - ZAJAC, P.:** Remarks on GPU Usage in
Cryptanalysis.
In: GCCP 2011 Proceedings : 7th International Workshop on Grid Computing for
Complex Problems. Bratislava, Slovakia, October 24 - 26, 2011. - Bratislava : Slovak

Academy of Sciences, 2011. - ISBN 978-80-970145-5-1. - S. 78-85

- AFD8 **JUHÁS, G.** - FOLTIN, M. - **ŠEVČÍKOVÁ, Z.** - JUHÁSOVÁ, A.: Zmráka sa.
In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Roč. 17,
mimoriadne č. : ELOSYS, Trenčín, 11.-14.10.2011 (2011), s. 204-207
- AFD9 KOVÁČ, M. - **LEHOCKI, F.**: Mobilné riešenia pre manažment chronických ochorení.
In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Roč. 17,
mimoriadne č. : ELOSYS, Trenčín, 11.-14.10.2011 (2011), s. 208-210
- AFD10 LODERER, M. - **REPKA, M.**: Časový útok využívajúci cache kolízie na posledné kolo šifry AES.
In: ŠVOČ 2011 : Študentská vedecká a odborná činnosť. Zborník vybraných prác.
Bratislava, Slovak Republic, 4.5.2011. - Bratislava : STU v Bratislave FEI, 2011. -
ISBN 978-80-227-3508-7. - S. 20-24
- AFD11 MARKO, T. - **ADAMKO, L.**: Extrakcia delta bodov z odtlačkov dlaní.
In: ŠVOČ 2011 : Študentská vedecká a odborná činnosť. Zborník vybraných prác.
Bratislava, Slovak Republic, 4.5.2011. - Bratislava : STU v Bratislave FEI, 2011. -
ISBN 978-80-227-3508-7. - S. 15-19
- AFD12 **MAZANEC, J.**: Designing a Complex Face Recognition System.
In: ELITECH'11 : 13th Conference of Doctoral Students Faculty of Electrical
Engineering and Information Technology. Bratislava, Slovak Republic, 17 May,
2011. - Bratislava : Nakladateľstvo STU, 2011. - ISBN 978-80-227-3500-1. - S. 1-5
- AFD13 **MAZANEC, J.** - **ORAVEC, M.**: Systém rozpoznávania tvárí založený na metóde LBP.
In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Roč. 17,
mimoriadne č. : ELOSYS, Trenčín, 11.-14.10.2011 (2011), s. 217-221
- AFD14 **REPKA, M.**: DPA of an Aes Implementation.
In: ELITECH'11 : 13th Conference of Doctoral Students Faculty of Electrical
Engineering and Information Technology. Bratislava, Slovak Republic, 17 May,
2011. - Bratislava : Nakladateľstvo STU, 2011. - ISBN 978-80-227-3500-1. - S. 1-6
- AFD15 STRAČÁR, P. - SLAMKA, M. - **ORAVEC, M.** - PAVLOVIČOVÁ, J.: Kernel and Linear Methods for Biometric Face Recognition.
In: IN-TECH 2011 : Proceedings of International Conference on Innovative Technologies. Bratislava, Slovak Republic, 1.9.-3.9.2011. - Jaroměř : Jan Kudláček, 2011. - ISBN 978-80-904502-6-4. - S. 524-527
- AFD16 **ŠEVČÍKOVÁ, Z.** - **KAZLOV, I.** - JUHÁSOVÁ, A.: Možnosti využitia analýzy a syntézy udalostných systémov v praxi.
In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Roč. 17,
mimoriadne č. : ELOSYS, Trenčín, 11.-14.10.2011 (2011), s. 227-229
- AFD17 **ZELINA, M.** - **ORAVEC, M.**: Decision Trees for Recognition of Internet

Applications.

In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Roč. 17, mimoriadne č. : ELOSYS, Trenčín, 11.-14.10.2011 (2011), s. 234-237

AFG Abstrakty príspevkov zo zahraničných konferencií

Počet záznamov: 2

AFG1 **JÓKAY, M. - ZAJAC, P.:** Analysis of Data Structures in MP4 Files Usable for Steganography.

In: ISCAMI 2011 : Book of abstracts.Malenovice,Czech Republic, 6.-8.5.2011. - Ostrava : University of Ostrava, 2011. - S. 34

AFG2 **ZAJAC, P. - ČAGALA, R.:** Algebraic Cryptanalysis of the Block Cipher Gost.

In: 11th Central European Conference on Cryptology : Debrecen, Hungary, 30 June - 2 July, 2011. - Debrecen : University of Debrecen, 2011. - S. 1

AFK Postery zo zahraničných konferencií

Počet záznamov: 1

AFK1 **OMELINA, E.:** Face Recognition from Single Sample.

In: ICVSS 2011. Registration, Recognition and Reconstruction in Image and Video : International Computer Vision Summer School 2011. Sicily, 11-16 July, 2011. - : University of Catania, 2011. - S. 56

BCI Skriptá a učebné texty

Počet záznamov: 1

BCI1 **KOSTRECOVÁ, E. - JÓKAY, M. - KOSTREC, M.:** Počítačová kriminalita. - 1. vyd. - Bratislava : STU v Bratislave, 2011. - 109 s. - ISBN 978-80-227-3410-3

BDE Odborné práce v zahraničných nekarentovaných časopisoch

Počet záznamov: 5

BDE1 **ANTAL, E. - JÓKAY, M.:** Rotorový šifrátor Fialka M-125. Diel 1. Popis šifrátoru.

In: Crypto-World. - ISSN 1801-2140. - Roč. 13, č. 4 (2011), s. 18-27

BDE2 **ANTAL, E. - JÓKAY, M.:** Rotorový šifrátor Fialka M-125. Diel 2. Porovnanie s viacerými rotorovými šifrátormi.

In: Crypto-World. - ISSN 1801-2140. - Roč. 13, č. 5 (2011), s. 15-23

BDE3 **ANTAL, E. - JÓKAY, M.:** Rotorový šifrátor Fialka M-125. Diel 3. Vybrané vlastnosti šifry.

In: Crypto-World. - ISSN 1801-2140. - Roč. 13, č. 6 (2011), s. 23-32

BDE4 **ANTAL, E. - JÓKAY, M.:** Rotorový šifrátor Fialka M-125. Diel 4: Implementácia a možnosti využitia.

In: Crypto-World. - ISSN 1801-2140. - Roč. 13, č. 9 (2011), s. 9-15

BDE5 **ANTAL, E. - JÓKAY, M.:** Rotorový šifrátor Fialka M-125. Úvod k seriálu.

In: Crypto-World. - ISSN 1801-2140. - Roč. 13, č. 4 (2011), s. 17

BEC Odborné práce v zahraničných recenzovaných zborníkoch (konferenčných aj

nekonferenčných)

Počet záznamov: 1

BEC1 HAMBALÍK, A.: Komunikačné siete a komunikačné protokoly.

In: Trendy ve vzdělávání 2011. Informační technologie a technické vzdělávání : 9. ročník mezinárodní vědecko-odborné konference, Olomouc, 23.-24. června 2011. - Olomouc : agentura Gevak s.r.o., 2011. - ISBN 978-80-86768-34-2. - S. 280-283

BEF Odborné práce v domácich nerecenzovaných zborníkoch (konferenčných aj nekonferenčných)

Počet záznamov: 6

BEF1 BALOGH, Š. - LEHOCKI, F. - JUHÁS, G.: Ehealth na Slovensku a jeho implementácia.

In: SMART S2AI : Workshop SMART systémov a služieb v oblasti aplikovanej informatiky. Bratislava, 18. apríla 2011. - Bratislava : STU v Bratislave FEI, 2011. - ISBN 978-80-227-3513-1. - S. 11-13

BEF2 GALLO, O. - NEČAS, T. - JUHÁS, G.: Syntéza asynchronných číslicových obvodov pomocou Petriho sietí.

In: SMART S2AI : Workshop SMART systémov a služieb v oblasti aplikovanej informatiky. Bratislava, 18. apríla 2011. - Bratislava : STU v Bratislave FEI, 2011. - ISBN 978-80-227-3513-1. - S. 6-8

BEF3 KAZLOV, I. - JUHÁS, G.: Úvod do problematiky Workflow sietí so zdieľanými zdrojmi.

In: SMART S2AI : Workshop SMART systémov a služieb v oblasti aplikovanej informatiky. Bratislava, 18. apríla 2011. - Bratislava : STU v Bratislave FEI, 2011. - ISBN 978-80-227-3513-1. - S. 14-16

BEF4 LEHOCKI, F. - ORAVEC, M. - BALOGH, Š. - JUHÁSOVÁ, A.: Vybrané modely diagnostických systémov.

In: SMART S2AI : Workshop SMART systémov a služieb v oblasti aplikovanej informatiky. Bratislava, 18. apríla 2011. - Bratislava : STU v Bratislave FEI, 2011. - ISBN 978-80-227-3513-1. - S. 1-5

BEF5 MARČEK, S. - DROZDA, M. - JUHÁS, G.: Introduction to Intrusion Detection System for High Dimensional Space for WSN.

In: SMART S2AI : Workshop SMART systémov a služieb v oblasti aplikovanej informatiky. Bratislava, 18. apríla 2011. - Bratislava : STU v Bratislave FEI, 2011. - ISBN 978-80-227-3513-1. - S. 17-18

BEF6 ŠEVČÍKOVÁ, Z. - JUHÁS, G.: Využitie Petriho sietí v Smart systémoch.

In: SMART S2AI : Workshop SMART systémov a služieb v oblasti aplikovanej informatiky. Bratislava, 18. apríla 2011. - Bratislava : STU v Bratislave FEI, 2011. - ISBN 978-80-227-3513-1. - S. 9-10

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

Počet záznamov: 1

BFA1 HAMBALÍK, A.: Digitalis képek erdetiségének vizsgálata.

In: Agria Media 2011 : International Conference on Information. October 11 - 12, 2011. - Eger : Eszterházy Károly Főiskola, 2011. - S. 32

DAI Dizertačné a habilitačné práce

Počet záznamov: 2

DAI1 **JÓKAY, M.**: Steganografia v obraze a videu : dát. obhaj. 27.9.2011, čís. ved. odb. 9.2.9. - Bratislava : STU v Bratislave FEI, 2011. - 140 s. + Autoref. 2011, 21 s. (http://is.stuba.sk/zp/portal_zp.pl?podrobnosti=55011)

DAI2 **LEHOCKI, F.**: Modely diagnostických systémov : čís. ved. odb. 9.2.9, obhaj. 2.6.2011. - Bratislava : STU v Bratislave FEI, 2011. - 111 s. + autoref. 2011, 23 s.

IX. VÝCHOVA VEDECKÝCH PRACOVNÍKOV

IX. 1. Interní doktorandi

Školiteľ: prof. RNDr. Otokar Grošek, PhD.

Doktorand: Mgr. Michal Mikuš

Forma vzdelávania: doktorandské štúdium – interná forma

Odbor: Aplikovaná informatika

Pracovisko: ÚIM FEI STU

Dizertačná skúška: 30.03.2009

Predpokladaný termín ukončenia: 30.09.2012

Téma práce: Kryptografia na konečných grupách

Školiteľ: prof. RNDr. Otokar Grošek, PhD.

Doktorand: Ing. Matúš Jókay

Forma vzdelávania: doktorandské štúdium – interná forma

Odbor: Aplikovaná informatika

Pracovisko: ÚIM FEI STU

Dizertačná skúška: 30.03.2009

Predpokladaný termín ukončenia: 30.09.2011(**obhajoba 27.9.11, ukončené**)

Téma práce: Steganografia v obraze a videu

Školiteľ: doc. RNDr. Gabriel Juhás, PhD.

Doktorand: Ing. Martin Riesz

Forma vzdelávania: doktorandské štúdium – interná forma

Odbor: Aplikovaná informatika

Pracovisko: ÚIM, FEI STU

Dizertačná skúška: 28.02.2011

Predpokladaný termín ukončenia: 30.08.2012

Téma práce: Modelovanie a simulácia udalostných systémov, Petriho siete, konkurentné systémy.

Školiteľ: doc. RNDr. Frank Schindler, PhD.

Doktorand: Ing. Michal Braško

Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 28.02.2011
Predpokladaný termín ukončenia: 30.08.2012
Téma práce: Tvorba, testovanie a použitie náhodných postupností v informatike.

Školiteľ: doc. RNDr. Gabriel Juhás, PhD.
Doktorand: Ing. Stanislav Marček
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 28.02.2011
Predpokladaný termín ukončenia: 30.09.2012
Téma práce: Modelovanie a simulácia udalostných systémov

Školiteľ: doc. RNDr. Gabriel Juhás, PhD.
Doktorand: Ing. Ondrej Gallo
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 28.02.2011
Predpokladaný termín ukončenia: 30.09.2012
Téma práce: Analýza a syntéza Petriho sietí

Školiteľ: doc. Dr. Ing. Miloš Oravec
Doktorand: Ing. Ján Mazanec
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 12.11.2009
Predpokladaný termín ukončenia: 06/2012
Téma práce: Rozpoznávanie tvári a tvárových črt

Školiteľ: doc. Dr. Ing. Miloš Oravec
Doktorand: Ing. Filip Pilka
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 12.11.2009
Predpokladaný termín ukončenia: 04/2012
Téma práce: Neurónové siete a predikcia dát

Školiteľ: doc. Dr. Ing. Miloš Oravec
Doktorand: Ing. Ľuboš Omelina
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 28.02.2011

Predpokladaný termín ukončenia: 30.08.2012
Téma práce : Návrh metód rozpoznávania vzorov v biometrii

Školiteľ: doc. Dr. Ing. Miloš Oravec
Doktorand: Ing. Milan Zelina
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 28.02.2011
Predpokladaný termín ukončenia: 30.08.2012
Téma práce: Analýza a klasifikácia prevádzky komunikačných sietí

Školiteľ: doc. RNDr. Gabriel Juhás, PhD.
Doktorand: Ing. Igor Kazlov
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 28.02.2012
Predpokladaný termín ukončenia: 30.08.2013
Téma práce: Analýza udalostných systémov s viacerými inštanciami

Školiteľ: doc. Dr. Ing. Miloš Oravec
Doktorand: Ing. Matej Féder
Forma vzdelávania: doktorandské – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 28.02.2012
Predpokladaný termín ukončenia: 30.08.2013
Téma práce: Návrh metód extrakcie príznakov a klasifikácie dát v biometrii

Školiteľ: prof. RNDr. Otokar Grošek, PhD.
Doktorand: Ing. Marek Repka
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 28.02.2012
Predpokladaný termín ukončenia: 30.08.2013
Téma práce: Postranné kanály

Školiteľ: doc. RNDr. Gabriel Juhás, PhD.
Doktorand: Ing. Jaroslav Hamráček
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 2011
Predpokladaný termín ukončenia: ukončil **1.10.2011**
Téma práce: Virtualizácia elektronických služieb

Školiteľ: prof. RNDr. Otokar Grošek, PhD.

Školiteľ špecialista: Ing. Milan Vojvoda, PhD.
Doktorand: Ing. Viliam Hromada
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: jún 2012
Predpokladaný termín ukončenia: 30.09.2014
Téma práce: Kryptoanalýza prúdových šifrier

Školiteľ: doc. RNDr. Jaroslav Fogel, PhD.
Doktorand: Ing. Lucia Cibulková
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: jún 2012
Predpokladaný termín ukončenia: 30.9.2014
Téma práce: Vybrané modely diagnostických systémov

Školiteľ: prof. RNDr. Otokar Grošek, PhD.
Doktorand: Ing. Eugen Antal
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 01/02 2013
Predpokladaný termín ukončenia: 05.09.2014
Téma práce: Moderná kryptoanalýza klasických šifrier

Školiteľ: prof. RNDr. Otokar Grošek, PhD.
Doktorand: Ing. Juraj Varga
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 01/02 2013
Predpokladaný termín ukončenia: 05.09.2014
Téma práce: Štatistické metódy v kryptoanalýze podporované počítačovou analýzou.

Školiteľ: doc. RNDr. Gabriel Juhás, PhD.
Doktorand: Ing. Andrej Savka
Forma vzdelávania: doktorandské štúdium – interná forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 28.02.2013
Predpokladaný termín ukončenia: 05.09.2014
Téma práce: Workflow manažment systémy a manažment zmien udalostných systémov

IX.2. Externí doktorandi

Školiteľ: doc. Dr. Ing. Miloš Oravec
Doktorand: Mgr. Miloslav Valčo
Forma vzdelávania: doktorandské štúdium – externá forma

Odbor: Aplikovaná informatika

Pracovisko: ÚIM FEI STU

Dizertačná skúška: 09.2013

Predpokladaný termín ukončenia: 31.08.2016

Téma práce: Návrh metód rozpoznávania tvárí v neriadených podmienkach využitím metód strojového učenia

Školiteľ: doc. RNDr. Gabriel Juhás, PhD.

Doktorand: Mgr. Zuzana Ševčíková

Forma vzdelávania: doktorandské štúdium – externá forma

Odbor: Aplikovaná informatika

Pracovisko: ÚIM FEI STU

Dizertačná skúška: 30.03.2010

Predpokladaný termín ukončenia: 30.09.2012

Téma práce: Sémantika Petriho sietí a ich rozšírenie

Školiteľ: doc. RNDr. Frank Schindler, PhD.

Doktorand: Mgr. Tibor Szabó

Forma vzdelávania: doktorandské štúdium – externá forma

Odbor: Aplikovaná informatika

Pracovisko: ÚIM FEI STU

Dizertačná skúška: 30.09.2011

Predpokladaný termín ukončenia: 30.9.2013

Téma práce: Počítačová podpora vzdelávania

Školiteľ: doc. RNDr. Gabriel Juhás, PhD.

Doktorand: Ing. Fedor Lehocki

Forma vzdelávania: doktorandské štúdium – externá forma

Odbor: Aplikovaná informatika

Pracovisko: ÚIM FEI STU

Dizertačná skúška: 14.09.2009

Predpokladaný termín ukončenia: 31.09.2012 (obhajoba - 2.6.2011- ukončené)

Téma práce: Vybrané modely diagnostických systémov

Školiteľ: doc. RNDr. Jaroslav Fogel, PhD.

Doktorand: Ing. Štefan Balogh

Forma vzdelávania: doktorandské štúdium – externá forma

Odbor: Aplikovaná informatika

Pracovisko: ÚIM FEI STU

Dizertačná skúška: jún 2011

Predpokladaný termín ukončenia: 30.9.2013

Téma práce: Analýza operačnej pamäte s cieľom odhalenia neznámeho kódu (vírusu).

Školiteľ: prof. RNDr. Otokar Grošek, PhD.

Doktorand: Jozef M. Kollár

Forma vzdelávania: doktorandské štúdium – externá forma

Odbor: Aplikovaná informatika

Pracovisko: ÚIM FEI STU

Dizertačná skúška: 09.2012
Predpokladaný termín ukončenia: 30.08.2014
Téma práce: Automatizované dešifrovanie textov M. Kukučina

Školiteľ: doc. Dr. Ing. Miloš Oravec
Doktorand: Pavol Stračár
Forma vzdelávania: doktorandské štúdium –externá forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM FEI STU
Dizertačná skúška: jún 2011
Predpokladaný termín ukončenia: 30.08.2014
Téma práce: Rozpoznávanie tvári v biometrii využitím metód strojového učenia

Školiteľ: doc. RNDr. Gabriel Juhás, PhD.
Doktorand: Ing. Štefan Počarovský
Forma vzdelávania: doktorandské štúdium – externá forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM FEI STU
Dizertačná skúška: 28.02.2011
Predpokladaný termín ukončenia: 30.08.2012
Téma práce: Útoky postrannými kanálmi

Školiteľ: doc. RNDr. Jaroslav Fogel, PhD
Doktorand: Veronika Hanúsková
Forma vzdelávania: doktorandské štúdium – externá forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM FEI STU
Dizertačná skúška: 09.2012
Predpokladaný termín ukončenia: 31.08.2015
Téma práce: Nové metódy diagnostiky v oftalmológii

Školiteľ: doc. RNDr. Jaroslav Fogel, PhD
Doktorand: Robert Bučko
Forma vzdelávania: doktorandské štúdium – externá forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM FEI STU
Dizertačná skúška: 09.2012
Predpokladaný termín ukončenia: 31.08.2015
Téma práce: Verifikačné metódy v multiagentových systémoch

Školiteľ: prof. RNDr. Otokar Grošek, PhD.
Doktorand: Ing. Vladislav Novák
Forma vzdelávania: doktorandské – externá forma
Odbor: Aplikovaná informatika
Pracovisko: ÚIM, FEI STU
Dizertačná skúška: 30.09.2011
Predpokladaný termín ukončenia: 28.02.2013
Téma práce: Spracovanie prirodzeného jazyka

X. ÚČASŤ PRACOVNÍKOV KATEDRY NA KONFERENCIÁCH

X.1. Zahraničné konferencie

NÁZOV KONFERENCIE: 11th Central European Conference on Cryptography.

Meno: prof. RNDr. Otokar Grošek, PhD.,

Miesto: Debrecén, H

Dátum: 29.06. – 02.07. 2011

Meno: prof. RNDr. Otokar Grošek, PhD.,

Príspevok: člen programového výboru

NÁZOV KONFERENCIE: : Mikulášská kryptobesídka

Meno: prof. RNDr. Otokar Grošek, PhD.,

Miesto: Praha, ČR

Dátum: 1. – 2. 12.2011

Meno: prof. RNDr. Otokar Grošek, PhD.,

Príspevok: „Osudy dobrého vojáka Švejka za světové války“

NÁZOV KONFERENCIE: Mikulášská kryptobedíska

Miesto: Praha, Česká republika

Dátum: 1.-2.12.2011

Meno: Viliam Hromada, Milan Vojvoda

Príspevok: Fault Analysis of Stream Ciphers

NÁZOV KONFERENCIE: ISCAMI 2011

Miesto: Malenovice, Česká republika

Dátum: 6.5.2011 – 8.5.2011

Meno: Matúš Jókay

Príspevok: Analysis of data structures in MPEG4 usable for steganography

NÁZOV KONFERENCIE: ICC 2011

Miesto: Lanzarote, Španielsko

Dátum: 27.5.2011 – 29.5.2011

Meno: Matúš Jókay

Príspevok: The design of a steganographic systém based on the GOP structure in the video standard MPEG-4

NÁZOV KONFERENCIE: ICC 2011

Miesto: Lanzarote, Španielsko

Dátum: 27.5.2011 – 29.5.2011

Meno: Michal Mikuš

Príspevok: On implementation of the Gentry-Halevi somewhat homomorphic scheme

NÁZOV KONFERENCIE: 11th Central European Conference on Cryptology

Miesto: Debrecen, Hungary

Dátum: 30. 6. - 2.7. 2011

Meno: Pavol Zajac

Príspevok: Algebraic cryptanalysis of the block cipher GOST

NÁZOV KONFERENCIE: Mikulášská kryptobesídka 2011

Miesto: Praha

Dátum: 1. -2. 12. 2011

Meno: Pavol Zajac

Príspevok: R. Čagala: Algebraic cryptanalysis GOST

NÁZOV KONFERENCIE: 53rd International Symposium ELMAR-2011

Miesto: Zadar, Chorvátsko

Dátum: 14-16 September 2011

Meno: Milan Zelina, Miloš Oravec

Príspevok: Early Detection of Network Applications Using Neural Networks

NÁZOV KONFERENCIE: 53rd International Symposium ELMAR-2011

Miesto: Zadar, Chorvátsko

Dátum: 14-16 September 2011

Meno: Féder, M., Oravec, M.

Príspevok: Enhancement of One Sample per Person Face Recognition Accuracy by Training Sets Extension

NÁZOV KONFERENCIE: 53rd International Symposium ELMAR-2011

Miesto: Zadar, Chorvátsko

Dátum: 14-16 September 2011

Meno: Pilka, F., Oravec, M.

Príspevok: Multi-step Ahead Prediction Using Neural Networks

NÁZOV KONFERENCIE: 53rd International Symposium ELMAR-2011

Miesto: Zadar, Chorvátsko

Dátum: 14-16 September 2011

Meno: Omelina, L., Oravec, M.

Príspevok: Efficient Face Expression Generation for Face Recognition

NÁZOV KONFERENCIE: Trendy ve vzdělávání 2011

Miesto: Olomouc, ČR

Dátum: 23-24. 6. 2011

Meno: Hambalík, A.

Príspevok: Komunikačné siete a komunikačné protokoly (Communication networks and communication protocols)

NÁZOV KONFERENCIE: Agria Media 2011

Miesto: Eger, Maďarsko

Dátum: 11-12. 10. 2011

Meno: Hambalík, A.

Príspevok: Digitális képek eredetiségének vizsgálata (The examination of the authenticity of digital pictures)

NÁZOV KONFERENCIE: Mikulášská kryptobesídka 2011

Miesto: Praha, Česká republika

Dátum: 1.12.2011 – 2.12.2011

Meno: Varga, J.

Príspevok: bez príspevku

NÁZOV KONFERENCIE: Mikulášská kryptobesídka 2011

Miesto: Praha, Česká republika

Dátum: 1.12.2011 – 2.12.2011

Meno: Antal, E.

Príspevok: bez príspevku

NÁZOV KONFERENCIE: IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems

Miesto: Praha, ČR

Dátum: 14.09.2011 – 18.09.2011

Meno: Balogh, Š.

Príspevok: Capturing Encryption Keys for Digital Analysis

NÁZOV KONFERENCIE: AMA-IEEE EMBE Medical Technology Conference 2011

Miesto: Boston, USA

Dátum: 16.-18.10.2011

Meno: Cibulková, L.

Príspevok: Modelling of Clinical Processes

X. 2. Domáce konferencie

NÁZOV KONFERENCIE : ELEKTROTECHNIKA, INFORMATIKA A TELEKOMUNIKÁCIE 2011

Miesto: Trenčín

Dátum: 11. – 14.10.2011

Meno: Grošek, O.

Príspevok: člen programového výboru

XI. HABILITAČNÉ A INAUGURAČNÉ KONANIA

XI.1. Inauguračné konania

XI.2. Habilitačné konania

Habilitačná prednáška + habilitácia: **Ing. Pavol Zajac, PhD.**, 28.11.2011

XI.3. Členstvá v komisiách

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

XII.1. Členstvá v komisiách

doc. Dr. Ing. Miloš Oravec – člen komisie pre obhajobu dizertačnej práce Ing. Fedora Lehockého v študijnom odbore 09-02-9 Aplikovaná informatika s názvom "Modely diagnostických systémov", FEI STU Bratislava, 2.6.2011

doc. Dr. Ing. Miloš Oravec – člen komisie pre obhajobu dizertačnej práce Ing. Matúša Jókaya v študijnom odbore 09-02-9 Aplikovaná informatika s názvom " Steganografia v obraze a videu ", FEI STU Bratislava, 27.9.2011

doc. Dr. Ing. Miloš Oravec – člen skúšobnej komisie pre dizertačnú skúšku Ing. Ľuboša Omelinu, FEI STU Bratislava, 18.2.2011

doc. Dr. Ing. Miloš Oravec – člen skúšobnej komisie pre dizertačnú skúšku Ing. Milana Zelinu, FEI STU Bratislava, 28.2.2011

prof. RNDr. Otokar Grošek, PhD. – predseda skúšobnej komisie pre dizertačnú skúšku Ing. Ľuboša Omelinu, FEI STU Bratislava, 18.2.2011

prof. RNDr. Otokar Grošek, PhD. - člen skúšobnej komisie pre dizertačnú skúšku Ing. Milana Zelinu, FEI STU Bratislava, 28.2.2011

prof. RNDr. Otokar Grošek, PhD. - člen komisie pre obhajobu dizertačnej práce Ing. Abdullaha Sultana, FEI STU, 3.5.2011

prof. RNDr. Otokar Grošek, PhD. – predseda skúšobnej komisie pre dizertačnú skúšku Ing. Michala Braška, FEI STU Bratislava, 9.6.2011

Ing. Milan Vojvoda, PhD. - člen skúšobnej komisie pre dizertačnú skúšku Ing. Milana Zelinu, FEI STU Bratislava, 28.2.2011

Ing. Milan Vojvoda, PhD. – člen skúšobnej komisie pre dizertačnú skúšku Ing. Michala Braška, FEI STU Bratislava, 9.6.2011

XII.2. Konania na iných pracoviskách

RNDr. Eva Kostrecová, PhD.

- oponent dizertačnej práce - Doktorand: Dipl. Ing. Heinz Hille, MBA: Technology Management for fast Process Adjustment in the context of Application Modeling and Knowledge Management (Technologické tiadenie na rýchle úpravy procesov v súvislosti s modelovaním aplikácií a znalostným manažmentom) (Dizertačná práca), Fakulta managementu, Univerzita Komenského - v Bratislave, september 2011

prof. RNDr. Otokar Grošek, PhD.

- predseda komisie na vykonanie dizertačnej skúšky Ing. Jozefa Tomečka, MÚ SAV 17.10.

prof. RNDr. Otokar Grošek, PhD.

- oponent dizertačnej práce Cándido Caballero Gil, Soluciones para la Autenticación y Gestión de Subredes en MANETs y VANETs, Universidad de La Laguna, Tenerife, Spain (31.10. 2011)

prof. RNDr. Otokar Grošek, PhD.

- oponent dizertačnej práce Jezabel Molina Gil, Nuevas Herramientas De Seguridad Cooperativa Para Redes Ad-Hoc Vehiculares, Universidad de La Laguna, Tenerife, Spain (31.10. 2011)

Mgr. Marek Sýs, PhD.

- examinátor komisie na vykonanie dizertačnej skúšky Ing. Jozefa Tomečka vo vednom odbore 9-1-9 Aplikovaná matematika konanej na matematickom ústave SAV.

XII.3. Oponentské posudky k písomnej práci k dizertačnej skúške

RNDr. Eva Kostrecová, PhD.

- oponent seminárnej práce

Doktorand: Ing. Mária Molnárová: Bezpečnostnoprávna ochrana citlivých informácií (Seminárna práca k dizertačnej skúške), Katedra manažmentu a informatiky, Akadémia Policajného zboru v Bratislave, júl 2010

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

XIII.1. ŠVOČ

Meno : doc. Dr.Ing. Miloš Oravec

Funkcia: člen komisie 13th Conference of Doctoral Students Elitech 2011, 17.5.2011

Sekcia: Aplikovaná informatika

Meno: Ing. Milan Vojvoda, PhD.

Funkcia : vedúci - Bc. Viliam Hromada - Chybová analýza prúdových šifrier- práca dostala Cenu dekana a bola navrhnutá na Cenu rektora

Sekcia: Aplikovaná informatika

Meno: prof. RNDr. Otokar Grošek, PhD.

Funkcia: predseda odbornej komisie

Sekcia: Aplikovaná informatika

Meno: doc. RNDr. Ľubomír Marko, CSc.,

Funkcia: člen odbornej komisie

Sekcia: Aplikovaná informatika

Meno: Ing. Fedor Lehocki, PhD.

Funkcia: člen odbornej komisie

Sekcia: Aplikovaná informatika

Meno : Ing. Vladislav Novák

Funkcia: organizácia na katedre, tajomník

Sekcia: Aplikovaná informatika

Meno : Mgr. Marek Sýs, PhD.

Funkcia: člen odbornej komisie

Sekcia: Aplikovaná informatika

XIII.2. VEDENIE UKONČENÝCH DIPLOMOVÝCH PRÁC

E. Antal : Niektoré problémy kryptoanalýzy šifry Fialka M-125 (O. Grošek)

T. Zaťko: ZEP v Slovenskej republike a Európskej únii (O. Grošek)

M. Dubovský : Ochrana laserových show (M.Sýs)

B. Šulej: Metódy pre priamy prístup do pamäte PC (Š. Balogh)

T. Marko: Extrakcia významových znakov z odtlačkov dlaní (L. Adamko)

T. Straka : Kryptograficky silné generátory náhodných znakov (L. Adamko)

M. Bella: Útok na hašovaciú funkciu MD4 (M. Vojvoda)

J. Hribik: Verifikované schémy zdieľania tajomstva (K. Nemoga)

J. Varga: Lineárne rekurentné postupnosti nad Z_m (K. Nemoga)

J. Štefanička: Nástroje zneužívané pri crackingu (E. Kostrecová)

L. Pír: Sofistikované kamerové systémy v ochrane objektov (M. Kempný)

M. Paulínyi: Ochrana pred spammingom (E. Kostrecová)

V. Hromada - Chybová analýza prúdových šifíer (M. Vojvoda)

R. Blaško: Využitie umelej inteligencie v diagnostike zdravotného stavu pacienta (M. Oravec)

J. Režnák, J.: Rozpoznávanie tváří v biometrii kernelovými metódami KPCA a GDA (M. Oravec)

J. Baroš : Miera poškodenia videa po vložení na verejné úložisko anonymného zdieľania multimediálneho obsahu (M. Jókay)

R. Čagala.: Algebraická kryptoanalýza šifry GOST (P. Zajac)

M. Plančík: Algebraická kryptoanalýza šifry Serpent (P. Zajac)

M. Páleníková : Cube attack (P. Zajac)

M. Hrušovský: Nástroje ochrany klientov v internet bankingu (Z. Ševčíková)

M. Kováč: Analýza deadlockových stavov v Petriho sieti (Z. Ševčíková)

M. Mádel: Transformácia workflow procesov do Petriho sietí (Z. Ševčíková)

R. Jadrončík: Identifikácia programov z nesequenčného správania (G. Juhás)

S. Lucký: Analýza dynamickej korektnosti Petriho sietí (G. Juhás)

S. Madaras: Možnosti prekladov workflow modelov do Petriho sietí (G. Juhás)

L. Oles: Syntéza Petriho sietí (G. Juhás)

M. Rástocký: Analýza procesov s dynamickou zmenou alokácie zdrojov (G. Juhás)

M. Marko: Webový portál pre výučbu CMS Joomla (M. Foltin)

M. Súlovec: Tvorba framework-u pre komunikačný model typu klient-server (Ľ. Stuchlíková)

T. Búgel: Automatizovaný systém rozpoznávania originality obrázkov (A. Hambalík)

M. Meszáros: Verifikácia konkurentných programov napísaných v jazyku C (J. Fogel)

J. Plevko: Konštrukcia Buchiho automatov z formúl logiky LTL (J. Fogel)

M. Veselý: Univerzálny softvérový tester aktívnych prvkov sietí LAN (A. Hambalík)

R. Lipovský: Virtualizácia v boji proti malware (Š. Balogh)

M. Hochel: Návrh server – klientskej aplikácie a komunikačného rozhrania pre riadenie automatického skladu (J. Dorner)

M. Gašparík: Snímanie objektov kamerou a ich rozpoznanie (J. Dorner)

F. Drugda: Informačné systémy na elektronickú preskripciu liekov z pohľadu lekára (Š. Balogh)

M. Dzúrik: Implementácia NZP (Š. Balogh)

B. Botto: Systém na tvorbu interaktívnych kurzov pre potreby slovenského zdravotníctva (F. Lehocki)

E. Buček: Tvorba balíka knižníc na vývoj 3D grafických aplikácií (Ľ. Stuchlíková)

A. Cvečko: Architektúra EHR (F. Lehocki)

M. Kováč: Telemedicínske aplikácie v zdravotníctve (F. Lehocki)

L. Kuba: Modely diagnostických systémov (F. Lehocki)

D. Tekeljak: Vzdialený prístup správcu na spracovaný server zabezpečený pomocou biometrických znakov (A. Hambalík)

M. Hatala: Využitie moderných ICT v rehabilitácii pacientov (F. Lehocki)

M. Hurňák: Transformácia modelu z VHDL do Petriho sieti (O. Gallo)

M. Kaša: Transformácia časového správania logického obvodu do Petriho sieti (O. Gallo)

L. Cibulková: Modelovanie workflow procesov (O. Gallo)

Ľ. Belicová: Modelovanie a analýza workflow procesov (O. Gallo)

J. Vlk : Akademický informačný systém založený na platforme J2EE (V. Novák)

XIII.3. ČLENSTVO V ŠTÁTNICOVÝCH KOMISIÁCH

- Ing. Matúš Jókay - člen štátnicovej komisie pre ŠP AI
- prof. RNDr. Otokar Grošek, PhD. – predseda a člen štátnicovej komisie pre ŠP AI
- doc. RNDr. Jaroslav Fogel, PhD. – predseda a člen štátnicovej komisie pre ŠP AI
- doc. RNDr. Karol Nemoga, PhD. – predseda a člen štátnicovej komisie pre ŠP AI
- Ing. Milan Vojvoda, PhD. – člen štátnicovej komisie pre ŠP AI
- doc. RNDr. Gabriel Juhás, PhD. – predseda a člen štátnicovej komisie pre ŠP AI
- doc. Dr. Ing. Miloš Oravec - člen štátnicovej komisie pre ŠP AI
- Ing. Fedor Lehocki – člen štátnicovej komisie pre ŠP AI
- Ing. Alexander Hambalík, PhD. – člen štátnicovej komisie pre ŠP AI
- Ing. Pavol Zajac, PhD. – člen štátnicovej komisie pre ŠP AI
- Mgr. Zuzana Ševčíková – člen štátnicovej komisie pre ŠP AI
- doc. Dr. Ing. Miloš Oravec – člen ŠS ING štúdia KAIVT FEI STU
- doc. Dr. Ing. Miloš Oravec - člen ŠS Bc štúdia KAIVT FEI STU
- doc. Dr. Ing. Miloš Oravec – člen komisie ŠS ING štúdia FEI TU Košice, 24.5.2011
- doc. Dr. Ing. Miloš Oravec - člen komisie štátnych skúšok ING štúdia, ŠP Počítačov a komunikačné systémy a siete, FIIT STU, 6.6.2011
- doc. Dr. Ing. Miloš Oravec – predseda komisie štátnych skúšok ING štúdia, ŠP Aplikovaná informatika, FEI STU, 22.6.2011
- doc. Dr. Ing. Miloš Oravec – predseda komisie štátnych skúšok Bc štúdia, ŠP Aplikovaná informatika, FEI STU, 29.6.2011
- Mgr. Michal Mikuš – člen štátnicovej komisie pre ŠP AI
- Ing. Ondrej Gallo – tajomník štátnicovej komisie pre ŠP AI
- RNDr. Eva Kostrecová. PhD. – člen štátnicovej komisie pre ŠP AI

XIV. EDIČNÉ AKTIVITY

XIV.1. Vydávanie časopisov

XIV.2. Členstvá v redakčných radách časopisov

- **prof. RNDr. Otokar Grošek, PhD.** je členom redakčnej rady Tatra Mountains Mathematical Publications.
- **prof. RNDr. Otokar Grošek, PhD.** je členom redakčnej rady Journal of Mathematical Cryptology (vydavateľstvo Walter de Gruyter)
- **doc. RNDr. Gabriel Juhás, PhD.** je členom redakčnej rady Transactions on Petri Nets and Other Models of Concurrency (vydavateľstvo Springer-Verlag)
- **doc. RNDr. Karol Nemoga, PhD.** je výkonný redaktor časopisu Tatra Mountains Mathematical Publications

- **doc. RNDr. Karol Nemoga, PhD.** je výkonným redaktorom slovenskej jednotky časopisu Zentralblatt Math.
- **doc. Dr. Ing. Miloš Oravec** je editorom časopisu Central European Journal of Computer Science (CEJCS), publisher: Versita, co-published with Springer Verlag

XIV.3. Recenzie pre vedecké časopisy a knihy

- **prof. RNDr. Otokar Grošek, PhD.** - Mathematical reviews – 1
- **prof. RNDr. Otokar Grošek, PhD.** - JEEE – 1
- **prof. RNDr. Otokar Grošek, PhD.** - Design Codes and Cryptography – 1
- **prof. RNDr. Otokar Grošek, PhD.** - Kybernetika – 1
- **prof. RNDr. Otokar Grošek, PhD.** - Journal of Computers (JCP) – 1

- **Ing. Milan Vojvoda, PhD.** - Journal of Electrical Engineering - 1

- **Ing. Pavol Zajac, PhD.** - Journal of Mathematical Cryptology - 1
- **Ing. Pavol Zajac, PhD.** - Mathematical Reviews - 1
- **Ing. Pavol Zajac, PhD.** - ZentralBlatt MATH - 1

- **Mgr. Marek Sýs PhD.** - Journal of Mathematical Cryptology- 1

XIV.3. Recenzie príspevkov na vedecké konferencie

prof. RNDr. Otokar Grošek, PhD. - CECC 2011 - posudky 4 článkov

doc. Dr. Ing. Miloš Oravec - posudky 6 článkov pre konferenciu ICNC'11-FSKD'11 (The 7th International Conference on Natural Computation and The 8th International Conference on Fuzzy Systems and Knowledge Discovery), 26-28 July 2011, Shanghai, China

doc. Dr. Ing. Miloš Oravec – posudok 1 článku do časopisu Journal of Electrical Engineering (EČ), jún 2011

XIV.4. Recenzie vedeckých projektov

doc. Dr. Ing. Miloš Oravec - posudok vedeckého projektu pre Vedeckú grantovú agentúru Ministerstva školstva SR a Slovenskej akadémie vied (VEGA), október 2011

XV. ORGANIZÁCIA KONFERENCIÍ

NÁZOV KONFERENCIE : Isabel 2011, 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies

Miesto: Barcelona, Španielsko

Dátum: 26.-29.10.2011

Meno: doc. Dr. Ing. Miloš Oravec

Funkcia: člen programového výboru

NÁZOV KONFERENCIE : The 7th International Conference on Natural Computation, The 8th International Conference on Fuzzy Systems and Knowledge Discovery, ICNC'11-FSKD'11

Miesto: Shanghai, China

Dátum: 26.-28.7.2011

Meno: doc. Dr. Ing. Miloš Oravec

Funkcia: člen programového výboru

XVI. SEMINÁRE

Seminár CRYPTO

vedúci: prof. RNDr. Otokar Grošek, PhD.

Seminár STROJOVÉ UČENIE

vedúci : doc. Dr. Ing. Miloš Oravec