Универзитет „Гоце Делчев" - Штип

УНИВЕРЗИТЕТСКИ БИЛТЕН

Број 38, 15 април 2010 година

април 2010 година
Штип

С О Д Р Ж И Н А

Издавач:
Универзитет „Гоце Делчев“ - Штип

Главен и одговорен уредник: проф. д-р Саша Митрев
Уредници: проф. д-р Борис Крстев, м-р Ристо Костуранов
Лектор: Даница Гавриловска-Атанасовска
Техничко уредување: Славе Димитров, Благој Михов

Р Е Ф Е Р А Т

ЗА ИЗБОР НА ЕДЕН НАСТАВНИК ВО ЗВАЊЕ ДОЦЕНТ ЗА НАСТАВНО-НАУЧНАТА ОБЛАСТ ИНФОРМАТИКА НА ФАКУЛТЕТОТ ЗА ИНФОРМАТИКА ПРИ УНИВЕРЗИТЕТ „ГОЦЕ ДЕЛЧЕВ" ВО ШТИП

Наставно-научниот совет на Факултетот за информатика при Универзитетот „Гоце Делчев" во Штип, на седницата одржана на 27 јануари 2010 година, со Одлука бр. 2002-31/3 распиша Конкурс, објавен во весниците „Дневник" и „Лајм" на 4 февруари 2010 година, за избор на еден наставник во звање доцент за наставно-научната област ***информатика*** при Факултетот. На Конкурсот се пријави кандидатката **д-р Александра Никола Милева**. По разгледување на доставениот материјал, како и од лично познавање на кандидатката, до Наставно-научниот совет на Факултетот за информатика го доставуваме следниов

И З В Е Ш Т А Ј

Кандидатката **д-р Александра Никола Милева** е родена на 6 април 1975 година во Штип, каде завршува основно и средно образование со континуиран одличен успех. Дипломира во 1998 година, како најдобар дипломиран студент на Институтот за информатика при Природно-математичкиот факултет во Скопје, со просечен успех 9,06, со што се стекнува со звање **дипломиран инженер по информатика**. Дипломската работа со наслов *„Мрежно програмирање и JAVA"* ја изработува под менторство на проф. д-р Оливер Б. Попов. Во учебната 1998/99 година се запишува на постдипломски студии на Институтот за информатика при ПМФ во Скопје, на насоката Сметачко-комуникациски мрежи. Во 2004 година ја одбранува магистерската теза со наслов *„Автентикација кај мобилни ad hoc мрежи"* под менторство на проф. д-р Оливер Б. Попов и се стекнува со академски степен **магистер на информатички науки**. Во јануари 2010 година ја одбранува докторската дисертација со наслов *„Криптографски примитиви со квазигрупни трансформации"* на ПМФ во Скопје, под менторство на проф. д-р Смиле Марковски и се стекнува со академски степен доктор на информатички науки.

Во учебните 1999/2000 и 2000/2001 година е ангажирана како демонстратор на Институтот за информатика при ПМФ во Скопје. Во истиот временски период волонтира и на Рударско-геолошкиот факултет во Штип, каде ги одржува вежбите по предметите Информатика во рударството и Примена на сметачите во рударството. Во април 2001 година е избрана за соработник со звање помлад асистент на Рударско-геолошкиот факултет во Штип. Во октомври 2005 година е избрана во соработничко звање асистент на Рударско-геолошкиот факултет во Штип и ги изведува вежбите по предметите Информатика во рударството, Нумерички методи во рударството и Рудничка графика и дизајн. Од септември 2007 година работи како асистент на Факултетот за информатика при Универзитетот „Гоце Делчев" во Штип, каде ги изведува вежбите по предметите: Основи на програмирање, Објектно-ориентирано програмирање, Дигитална логика, Структури на податоци и алгоритми и Компјутерски мрежи. За истакнување е нејзиниот коректен однос кон студентите и исполнувањето на сите задолженија од наставниот процес, како и соработката со колегите во колективите во кои работела.

Поширокиот научен интерес на кандидатката е од областа на безбедноста на информациите. Потесниот научен интерес на д-р Александра Милева е од областа на теоријата на квазигрупи, теоретската и практичната безбедност во комуникациските процеси и компјутерските мрежи, и криптографијата. Во последниве неколку години, таа активно се вклучи во истражувањата на својствата на квазигрупите, како и за примена на квазигрупите во дефинирањето и дизајнирањето на криптографски примитиви. Како резултат на своите истражувања, кандидатката објавува повеќе научни и стручни трудови, а добиените резултати ги има прикажано пред меѓународната и домашната јавност на неколку научни конференции и стручни собири одржани во земјава и во странство, што ги набројуваме во продолжение.

Презентации на домашни и странски конференции и работилници

1. Kalejska A., Popov O.B.: "*Management issues in wireless and mobile networks*", 4th International Conference on Informatics and Information Technology (CIIT), Bitola, December 2003.
2. Mileva A., Popov O.B.: "*Analysis of Authentication Protocols for Mobile Ad hoc Networks*", 2nd Balcan Conference in Informatics (BCI), ISBN 9989-668-49-3, Ohrid, November 2005.
3. Mileva A., Markovski S.: "*Correlation matrices and prop ratio tables for quasigroups of order 4*", 6th International Conference on Informatics and Information Technology (CIIT), Bitola, February 2008.
4. Smile Markovski, Danilo Gligoroski, Vesna Dimitrova, Aleksandra Mileva: "*Avalanche Effect in the Family of Block Ciphers "SD-(n,k)"*", Advanced Research Workshop: Scientific Support for the Decision Making in the Security Sector, NATO PROGRAMME SECURITY THROUGH SCIENCE, October 21-25, 2006, Velingrad, Bulgaria.
5. Markovski S., Mileva A.: *"Quasigroups generated by small permutations and exteded Feistel networks*", Mathematical conference: 85 years of Professor Blagoj Popov life, Ohrid, 05-07.2008.
6. Markovski S., Mileva A: "NaSHA - cryptographic hash functions", NIST The First SHA-3 Candidate Conference, Leuven, Belgium, 25-28 February 2009.
7. Mileva A., Markovski S.: "*Quasigroup string transformations and hash function design. A case study: the NaSHA hash function* ", ICT Innovations 2009.
8. Mileva A.:"*Analysis of some quasigroup transformations as Boolean functions*", MASSIE 2009.
9. Mileva A.:"*Cryptographic primitives with quasigroup transformations*", SEE Young Researchers Workshop во рамките на проектот TEMPUS JP SEE DOCTORAL STUDIES IN MATHEMATICAL SCIENCES, Охрид, 16-20.09.2009.

Вредноста на научните достигнувања на д-р Александра Милева се согледува од приложениов список на научни трудови, што се објавени во меѓународни и домашни научни списанија и зборници од конференции.

Објавени научни трудови

1. Милева А.: *„Автентикација кај мобилни ad hoc мрежи"*, магистерска теза,Скопје, 2004.
2. Kalejska A., Popov O.B.: "*Management issues in wireless and mobile networks*", Proceedings of the 4th International Conference on Informatics and Information Technology (CIIT), Bitola, December 2003: pp 280-291.
3. Mileva A., Popov O.B.: "*Analysis of Authentication Protocols for Mobile Ad hoc Networks*", Proceedings of the 2nd Balcan Conference in Informatics (BCI), ISBN 9989-668-49-3, Ohrid, November 2005: pp 462-469.
4. Markovski S., Dimitrova V., Mileva A.: "*A new method for computing the number of n-quasigroups*", Buletinul Academiei de Stiinte a Republicii Moldova. Matematica, ISBN 1024-7696, Number 3, 2006: pp 57-64.
5. B. Golomeov, A. Mileva, M. Golomeova: "*A software for metal balance of the selective flotation*", Proceedings of Balkanmine 2007, ISBN 978-86-87035-00-3, 10-13 September 2007, pp 287-291.
6. Mileva A., Markovski S.: "*Correlation matrices and prop ratio tables for quasigroups of order 4*", Proceedings of the 6th International Conference on Informatics and Information Technology (CIIT), Bitola, February 2008, pp. 17-22.
7. Markovski S., Mileva A: "*Generating huge quasigroups from small non-linear bijections via extended Feistel network*", Quasigroups and related systems, 17(1), 2009, pp.91-106.
8. Dimitrova V., Markovski S., Mileva A.: "*Periodic quasigroup string transformations*", Quasigroups and related systems, 17(2), 2009, pp.191-204.
9. Mileva A., Markovski S.: "*Quasigroup string transformations and hash function design. A case study: the NaSHA hash function*", ICT Innovations 2009 (Ed. D. Davcev, J. M. Gomez), Springer Berlin Heidelberg, pp. 367-376.
10. Милева А.: *„Криптографски примитиви со квазигрупни трансформации"*, докторска теза, Скопје, 2009.

Ќе дадеме кус приказ само на некои позначајни трудови.

Во трудовите 4, 7 и 8 се дадени некои од резултатите во кои се третираат проблеми од теоријата на квазигрупите. Во 4 е даден еден нов метод за генерирање на n-арни квазигрупи, користејќи ги класите од изотопија на (n-1) – арните квазигрупи. Пресметани се бројот на вакви бинарни, тернарни, 4-арни и 5-арни квазигрупи од помали редови (2, 3, 4, 5), кои е можно да се пресметаат со користење само на персонални компјутери. Трудот 7 содржи еден двојно логаритамски ефикасен метод за генерирање на квазигрупи од огромни редови (2^{16}, 2^{64}, 2^{512}, 2^{1024}...), при што основната идеја е да се користат Фејстелови мрежи и пермутација од мал ред (8, 16, 32, 256...). Прикажани се и својствата што ги имаат вака конструираните квазигрупи. Трудот 8 дефинира едно трансформациско својство на квазигрупите, периодичноста, и се дадени условите една квазигрупа да биде периодична од даден облик.

Во трудовите 6, 9 и 10 се прикажани резултатите поврзани со примената на квазигрупите во криптографијата. Трудот 6 дава анализа на корелациските матрици и на пропагирачките табели на квазигрупите од ред 4. Трудот 9 содржи анализа на методите искористени во дизајнот на хаш-функцијата NaSHA, предложена како нов дизајн на хаш-функција на конкурсот за избор на нов светски SHA-3 стандард за криптографска хаш-функција, организиран од страна на NIST (National Institute for Standards and Technologies of USA):

1. Markovski S., Mileva A: "*NaSHA*", Submission to NIST SHA-3 competition, First Round Candidate (51 of 64), 2008, достапно на http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/documents/NaSHA.zip

Трудот 10 е докторската дисертација на кандидатката и во него се содржат речиси сите научни достигнувања на д-р Милева.

Кандидатката ги објавува следниве книги, скрипти, научни и стручни трудови и технички извештаи.

Книги

1. Голомеов Б., Милева А.: „*Нумерички методи во рударството*”, УГД – Штип, 2008.

Скрипта за предавања

1. Голомеов Б., Милева А.: „*Прирачник за Microsoft Word и Microsoft Excel*”, УГД – Штип, 2002.

Објавени стручни трудови

1. Милева А., Димитрова В.: „Кратка историја на криптографијата I”, СИГМА 76 (2006/2007), ISBN1409-6803, Вол. 27, Бр. 4, 18-21.
2. Димитрова В., Милева А.: „Кратка историја на криптографијата II”, СИГМА 77 (2007/2008), ISBN1409-6803, Вол. 28, Бр. 1, 18-21.
3. Димитрова В., Милева А.: „Кратка историја на криптографијата III”, СИГМА 78 (2007/2008), ISBN1409-6803, Вол. 28, Бр. 2, 1-6.
4. Милева А., Димитрова В.: „Кратка историја на криптографијата IV”, СИГМА 79 (2006/2007), ISBN1409-6803, Вол. 28, Бр. 3, 20-25.

Технички извештаи

1. Markovski S., Mileva A., Dimitrova V., Gligoroski D.: “*On a Conditional Collision attack on NaSHA-512*”, eprint archive 2009/034, http://eprint.iacr.org/2009/034.pdf

Од ова може да заклучиме дека д-р Милева активно делува и во унапредувањето на наставата, како и во ширењето на науката меѓу подмладокот од нашата земја.

Кандидатката е учесник во следниве **проекти**:

1. TEMPUS JEP-13574-98: Реформи на студиите на поле на геологијата и рударството, 1998-2000 (координатор: проф. д-р Борис Крстев).
2. „Алатки и техники за прибирање информации за напади на компјутерски мрежи и заштита од нив“ - предавач на семинар во рамките на проектот MathIND - The Balcan and Eastern European Network of Excellence for the Diffusion of Mathematics for Industry Expertise, 27-28.09.2003 (координатор: проф. д-р Смиле Марковски).
3. “Algebraic Structures and their Applications in Coding Theory and Cryptography” - предавач на интензивен курс во рамките на DAAD проектот Center of Excellence for Applications of Mathematics, Охрид, 10-17.09.2009 (координатор: академик, проф. д-р Дончо Димовски).
4. “SEE Young Researchers Workshop” – учесник во работилница во рамките на проектот TEMPUS JP SEE DOCTORAL STUDIES IN MATHEMATICAL SCIENCES, Охрид, 16-20.09.2009.

Кандидатката изработува и софтвер за пресметување на биланс на метали на селективна флотација, специјално правен за рудникот за олово и цинк „САСА“ - Македонска Каменица (дел од апликативен проект на проф. д-р Благој Голомеов). Со мали промени може да се примени и за други руднициа и за други метали или неметали.

Д-р Милева е член на Здружението на информатичарите на Македонија. Од странските јазици зборува и пишува на англиски јазик.

ЗАКЛУЧОК И ПРЕДЛОГ

Врз основа на претходно наведените факти, Рецензентската комисија заклучува дека кандидатката д-р Александра Милева ги исполнува сите суштински и законски критериуми, како и критериумите за избор на наставници и соработници на Универзитетот „Гоце Делчев“ во Штип, да биде избрана за наставник на Факултетот за информатика на УГД во Штип. Таа има богато наставно искуство како асистент, има добиено светски признати научни резултати кои се објавени во меѓународни и домашни научни списанија, презентирани пред домашната и светската научна јавност, а исто така преку софтверски пакети, учебници и стручни трудови се афирмира како истакнат стручњак во својата информатичка професија.

Рецензентската комисија има посебно задоволство и чест да му предложи на Наставно-научниот совет на Факултетот за информатика **да ја избере д-р Александра Милева за доцент по наставно-научната област информатика** на Факултетот за информатика на УГД во Штип..

РЕЦЕНЗЕНТСКА КОМИСИЈА

Д-р Смиле Марковски - редовен професор на ПМФ во Скопје, с.р.
Д-р Лидија Горачинова-Илиева - доцент на ФИ во Штип, с.р.
Д-р Сашо Коцески - доцент на ФИ во Штип, с.р.

ПРИЛОГ

Табела за вреднување на активностите на д-р Александра Милева, доктор на информатички науки, според критериумите за избор на наставници и соработници на Универзитетот „Гоце Делчев“ во Штип

Ред. број	Наставно-образовна дејност	Поени	
		во земјава	во странство
1.	Позитивно рецензиран универзитетски учебник	15	
2.	Интерна скрипта од предавања	4	
3.	Вежби (неделен просечен фонд на часови во двата семестра во изборниот период)	25,4	
4.	Статија во наставно-образовно списание	4*4=16	
	Вкупно:	**60,4**	

Ред. број	Научноистражувачка дејност	Поени	
		во земјава	во странство
1.	Труд со оригинални научни резултати, објавени во научно списание опфатено во (останати)	3*3=9	
2.	Труд со оригинални научни резултати, објавени во зборник од трудови во научен собир	3*1=3	2*2=4
3.	Учество на научен собир со реферат (усно)...	1,5*7=10,5	2*2=4
4.	Одбранета докторска теза	8	
5.	Одбранета магистерска работа	4	
6.	Учесник во научен проект (максимум во три проекта)		2*3=6
	Вкупно:	**48,5**	

Ред. број	Стручно-апликативна дејност и организациско-развојна дејност	Поени	
		во земјава	во странство
1.	Учесник во научен проект (максимум во три проекта)		2*8=16
2.	Елаборати и експертизи		4
3.	Изработен и рецензиран програмски пакет	3	
4.	Стручни награди и признанија	4	
5.	Член на факултетски орган, комисија	2	
	Вкупно:	**29**	

Вкупно:	**137,9**