РЕЦЕНЗИЯ

На дисертационен труд за научната степен "доктор на науките" по професионално направление 4.6 Информатика и компютърни науки, научна специалност: Информатика
от доц. д-р **Борислав Панайотов Стоянов**
на тема "Криптографски алгоритми за защита на информацията".
Рецензент: акад. Иван П. Попчев

Със заповед No. РД-16-068/24.04.2015 г. на зам. ректор проф. д.и.н. Г. Колев, съм назначен за външен на ШУ член на научно жури за публична защита на докторска дисертация за придобиване на научната степен "доктор на науките" с тема "Криптографски алгоритми за защита на информацията" на доц. д-р Борислав Панайотов Стоянов в област на висше образование 4. Приложни науки, математика и информатика, професионално направление 4.6 Информатика и компютърни науки, научна специалност: Информатика.

Като член на научното жури съм получил:

1. Заповед No. РД-16-068/24.04.2015 г. на зам. ректор проф. д.и.н. Г. Колев.
2. Дисертационен труд "Криптографски алгоритми за защита на информацията".
3. Автореферат на дисертационен труд.
4. Копия на публикациите по темата на дисертационния труд.
5. Специфични критерии на ФМИ на ШУ "Епископ Константин Преславски".
6. CD с документи по процедурата по защитата на дисертационния труд.

В Закона за развитие на академичния състав в Република България (ЗРАСРБ) за "доктор на науките" са определени съответни изисквания в чл. 12, които трябва точно да се цитират:

Чл. 12 (1) "Научната степен "доктор на науките" се придобива от лице с образователна и научна степен "доктор".

Чл. 12 (3) Дисертационният труд по ал. 2 трябва да съдържа теоретични обобщения и решения на големи научни или научноприложни проблеми, които съответстват на съвременните постижения и представляват значителен и оригинален принос в науката.

Чл. 12 (4) Дисертационният труд по ал. 2 се подготвя самостоятелно и не може да повтаря буквално темата и значителна част от съдържанието на представения за придобиване на образователната и научна степен "доктор".

На тези изисквания в ЗРАСРБ съответстват точно на чл. 35 и чл. 37 (1) и (2) от Правилника за прилагане на ЗРАСРБ, приет от Министерския съвет.

Според протокол No. РД-05-08 на АС на ШУ "Епископ Константин Преславски" за научната степен "доктор на науките" **наукометричните критерии** са:

4.2.2.1.1. Минимум 25 научни статии по проблеми на дисертационния труд, от които 15 в реферирани издания.

4.2.2.1.2. Минимум 30 цитирания в реферирани издания по проблеми на дисертационния труд.

В специфичните критерии на ФМИ при ШУ "Епископ Константин Преславски" изискванията са:

- Поне 10 публикации в реферирани издания, като поне 5 от тях да са в периодични списания с импакт фактор/ранг;
- Поне 3 от представените публикации да са самостоятелни, от които поне една в списание с импакт фактор/ранг;
- Да има поне 20 цитирания, от които поне 5 да са в списания с импакт фактор/ранг или в монографии на реномирани издания.

На стр. 17 е формулирана **целта** на дисертационния труд "разработването и изследването на нови криптографски алгоритми за защита на информацията чрез използване на следните градивни елементи: линейни преместващи регистри с обратна връзка, преместващи регистри с обратна връзка и пренос, бент функции и хаотични функции."

За изпълнение на целта са поставени (стр. 17) **три** изследователски **задачи**:

1. Да се разработят и изследват криптографски алгоритми за генериране на псевдослучайни числа на основата на преместващи регистри с обратна връзка.
2. Да се разработят и изследват криптографски алгоритми за генериране на псевдослучайни числа чрез нелинейни динамични системи.
3. Да се разработят и изследват криптографски алгоритми за защита на изображения.

В дисертационния труд в обем от 187 страници, 29 фигури и 65 таблици са представени:

- Увод (16-19);
- Генериране на псевдослучайни двоични последователности чрез преместващи регистри с обратна връзка (**глава 1**, 23-65);
- Генериране на самосвиващи псевдослучайни генератори на битови последователности чрез преместващи регистри с обратна връзка (**глава 2**, 66-91);
- Генериране на псевдослучайни двоични последователности чрез нелинейни динамични системи (**глава 3**, 92-128);
- Защита на изображения чрез криптографски алгоритми (**глава 4**, 129-153);
- Заключение (155-157);
- Библиография (160-177);
- Публикации по дисертационния труд (178-181);
- Цитати по дисертационния труд (182-187).

По дисертационния труд има **27 публикации** в интервала 2004 – 2014 г., които могат да се систематизират така:

- 9 публикации в списания (NNo. P9, P13, P16, P19, P21, P22, P25, P23 и P27); На стр. 21 в дисертацията (таблица B) е

отбелязано, че 2 публикации (NNo. P13 и P16) са с IF/ранг без съответните числени показатели за 2014 г.;

- 18 публикации са в научно-тематични сборници (NNo. P1, P2, P3, P4, P5, P6, P7, P8, P10, P11, P12, P14, P15, P17, P18, P20, P24 и P26);
- 1 труд (NNo. 27) е в категорията accepted, но без съответен потвърждаващ документ;
- 9 публикации са **самостоятелни** (NNo. P2, P3, P11, P12, P13, P14, P15, P16 и P17);
- 8 публикации са на български език (NNo. P1, P2, P3, P4, P5, P6 и P8).

Забелязани са общо 37 **цитирания** на 15 труда в това число са и 4 цитирания в Applied Mathematical Sciences /accepted/. Не са отбелязани поне 5 цитирания в списания с импакт фактор/ранг или в монографии в реномирани издания. Показаните в Таблица В в дисертацията на стр. 21 20 цитирания в списания с IF/ранг и в монографии в реномирани издания не могат да се приемат без съответните числени показатели, а монографията не е посочена.

Забелязаните цитирания, въпреки че авторите, които цитират са ограничени и в т.ч. са съавтори и в други публикации показват, че резултатите от дисертационния труд са станали достояние до определен кръг от специалисти.

В автореферата на стр. 5 е даден списък на 11 научни форуми, на които са докладвани резултати от дисертационните изследвания. Във връзка с приложимостта и полезността в автореферата на стр. 6 са дадени изпълнени 4 проекти от фонд Научни изследвания на Шуменския университет и проект по Оперативна програма "Развитие на човешките ресурси".

Приносите в дисертационния труд могат накратко да се систематизират така:

1. Предложени са псевдослучайни криптиращи алгоритми чрез преместващи регистри с обратна връзка. Показани са съответни статистически резултати.
2. Даден е метод (в т. 1.5 е алгоритъм) за синтез на клас сигнали, наречени перфектни двумерни масиви (ПДМ), чиято двумерна периодична автокорелационна функция има нулево ниво на страничните листи. Накратко е изследвано приложението на ПДМ в комуникационните и роботизираните системи за разпознаване на образи.
3. Систематизирани са криптографски алгоритми за генериране на псевдослучайни двоични редици чрез нелинейни динамични системи.
4. Изследвани са криптографски алгоритми за защита на изображения: чрез функцията на Jabri, атрактори на Lorenz, изображението на Duffing и на Chebyshev.

Според чл. 12 (4) от ЗРАСРБ "дисертационният труд не може да повтаря буквално темата и значителна част от съдържанието на

представения за придобиване на образователната и научна степен "доктор". Може да **се констатира, че това условие е спазено**, тъй като:

- Темата на дисертацията за "доктор" е "Изследване на N-адични свиващи и комбиниращи псевдослучайни генератори на редици" (2006 г.)
- Публикациите по дисертацията за "доктор" са 6 в интервала 2004 – 2005 г. и те не са включени в публикациите за "доктор на науките".

Критични бележки:

1. В списъка на публикациите по дисертационния труд липсват такива с отбелязан импакт фактор/ранг.
2. В библиографията, публикациите по дисертационния труд и цитиранията има съществени библиографски непълноти, а към нито една публикация не е написан ISSN или ISBN, което ги превръща в неразпознаваеми.
3. В заключението липсват съгласно чл. 12(3) съдържателно представяне на "теоретични обобщения" и "решения на големи научни или научноприложни проблеми". Това, което липсва е може би резултат от факта, че се представят 19 алгоритъма, които са самоопределени като: един нов (алгоритъм 2.2), два модифицирани (алгоритъм 2.1 и алгоритъм 3.6), а останалите?

Въпроси по дисертационния труд:

1. Според чл. 12 (3) от ЗРАСРБ "дисертационният труд трябва да съдържа теоретични обобщения". Въпросите са: кои са тези обобщения, как са доказани и на кои точно страници в дисертацията се намират, в кои публикации са описани, как те се цитират?
2. На няколко места в текста (например глава 4) има твърдения, че "на база теоретичните и експериментални изследвания следва, че предложеният алгоритъм е подходящ за практическа защита на изображения", от тук може да се постави въпросът има ли доказателства (експериментални) за практическа защита.
3. Като продължение на горния въпрос е подходящо да се поясни казаното от доц. д-р Б. Стоянов на предварителното обсъждане (защита) на 16.04.2015 г., че приложенията са при информационния обмен между компютърните системи и в повишаване на сигурността на облачните технологии.
4. Липсват насоки за бъдещи изследвания и приложения като резултат от получените приноси в дисертацията.

Заключение

Представеният от д-р Борислав Панайотов Стоянов дисертационен труд за научната степен "доктор на науките" в професионално направление 4.6 Информатика и компютърни науки, научна специалност:

Информатика отговаря на изискванията на ЗРАСРБ, на Правилника за прилагане на ЗРАСРБ, на наукометричните критерии на ШУ "Епископ Константин Преславски" и на специфичните критерии на ФМИ към същия университет и давам **положително заключение**.

Предлагам Научното жури единодушно да гласува на доц. д-р Борислав Панайотов Стоянов да се присъди научната степен "доктор на науките" по професионално направление 4.6 Информатика и компютърни науки, научна специалност: Информатика.

21.05.2015 г.

Рецензент: .....

Акад. Иван П. Попчев