ШУМЕНСКИ УНИВЕРСИТЕТ „ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“

С Т А Н О В И Щ Е

От проф. д-р Станимир Стоянов Станев,

от катедра „Компютърни системи и технологии“, ФМИ, Шуменски университет „Епископ Константин Преславски”

относно материалите, представени за защита на дисертационен труд за придобиване на научната степен **„доктор на науките“**

на тема **„Криптографски алгоритми за защита на информацията“**

с автор **доц. д-р Борислав Панайотов Стоянов**

от катедра „Компютърна инфоратика“Информационни технологии”, ФМИ, Шуменски Университет „Епископ Константин Преславски”

Област на висше образование: 4. Природни науки, математика и информатика

Професионално направление 4.6. Информатика и компютърни науки

Научна специалност „Информатика”

ШУМЕН
2015

Настоящото становището е изготвено и представено на основание на заповед РД-16-068/24.04.2015 г. на Ректора на Шуменски Университет „Епископ Константин Преславски“, както и на решение на научното жури, взето на неговото първо заседание. То е изготвено в съответствие с изискванията на Закона за развитие на академичния състав на Република България (ЗРАСРБ), Правилника за неговото прилагане, Правилника на Шуменския Университет „Епископ Константин Преславски”.

1.**Данни за дисертанта**

Доц. д-р Борислав Панайотов Стоянов е роден на 27 май 1976 г. в гр. Шумен. През 2000 г. завършва Шуменския Университет „Епископ Константин Преславски” с магистърска степен по специалност „Информатика“ . От 2002 г. е асистент в Катедрата „Информатика“ в Шуменския университет. В периода 2003 - 2006 г. е редовен докторант по Информатика в Катедра КСТ на ШУ с научен ръководител доц. Петър Милев и научен консултант проф. дтн Борислав Беджев. През 2006 г. успешно защитава дисетационен труд за ОНС „доктор” по научната специалност 01.01.12 Информатика, на тема „N-адични свиващи и комбиниращи псевдослучайни генератори на редици”. От 2007 г. е главен асистент в Катедра „Компютърни системи и технологии“. От 2009 г. е доцент по 01.01.12 Информатика в катедра „Компютърна информатика“. От 15 септември 2009 г. е ръководител на тази катедра. Научен ръководител е на двама докторанти. Участвал е в много национални научноизследователски проекти и такива към към Шуменския университет. Извън тематиката на дисертационното изследване доц. Стоянов има публикувани статии в следните списания с импакт фактор: MATCH Commun. Math. Comput. Chem., Journal of Cheminformatics, Bulgarian Chemical Communications, International Journal of Information Technology & Decision Making и Entropy.

2. **Данни за процедурата.**

Дисертационният труд на доц. д-р Стоянов е е обсъден и насочен за защита на разширено заседание на катедра „Компютърна информатика ” при ФМИ на на

25.06.2014г. Прегледът на представените ми документи показа, че при реализацията на дисертацията - в процеса на разработката и в провеждането на процедурата по предеварителна и окончателна защита на дисертационния труд няма допуснати нарушения.

Напълно са удовлетворенит специфичните наукометрични критерии за процедури в област на висше образование 4 Природни науки, математика и информатика от Правилника за развитие на академичния състав на Шуменския университет, чл. 34, ал. 3, и за процедури от професионално направление 4.6 Информатика и компютърни науки от протокол 3/15.11.2011 г. на Факултетския съвет на Факултета по математика и информатика на Шуменския университет.

3. Данни за дисертацията и автореферата

Дисертационния труд съдържа общо 187 страници. Съдържа увод, четири глави, заключение и библиография. Заключението обобщава и синтезира изводите по отделните глави. Налични са списък със съкращенията и декларация за оригиналност на получените резултати. Библиографията се състои от 188 заглавия. Включени са 29 фигури и 65 таблици. 197 страници и се състои от увод, три глави, заключение, списък на използваната литература и 3 приложения (31 страници). Докторантът е цитирал 229 източника, от които 21 са на кирилица, 163 - на латиница и 45 - от Интернет.

Резултатите от дисертационния труд са добре онагледени с 96 фигури и 20 таблици в основния текст, и 41 фигури и 1 таблица в трите приложения.

Актуалността на дисертационния труд произтича от необходимостта за разработване на нови методи за криптиране на данни и е несъмнена.

В увода е дефинирана основната цел на дисертационната работа и задачите за постигането й.

В първа глава е представен обектът за изследване. Изследвани са няколко криптографски алгоритъма.

Във втора глава е синтезиран модифициран самосвиващ генератор, предложен и изследван е нов модифициран самосвиващ генератор, изпълнен с преместващ регистър с обратна връзка и пренос, както и със свиващата функция

на Jabri. Извършено е експериментално паралелно криптиране, изследвано е филтриране на преместващ регистър с обратна връзка и пренос чрез бент булева функция.

В трета глава са синтезирани и изследвани псевдослучайни генератори на битове. Проведено е експериментално тестване, показващо пълно преминаване на приложените статистически тестове.

В четвърта глава е разработена и изследвана схема за защита на изображения чрез преместващ регистър с обратна връзка и пренос филтриран чрез функцията на Jabri и схема за защита на изображения чрез атрактора на Lorenz. Синтезирана е схема за защита на изображения чрез изображението на Duffing и изображението на Чебишев.

От съдържанието на главите на дисертацията ясно проличава отличното познаване на изследвания проблем от дисертанта. Коректно е избрана методиката на изследването в съответствие с предмета на дисертацията.

Дисертационният труд като цяло съответства на изискванията на ЗРАСРБ . Езикът и стилът на дисертацията са ясни и професионални. Потвърждавам, че представения дисертационен труд за присъждане на НС „доктор на науките" не повтаря темата и съдържанието на дисертацията за ОНС „доктор".

Представеният автореферат по дисертационния труд се състои от 56 стр. По обем и съдържание вярно, точно и ясно отразява съдържанието на дисертационния труд и формулираните приноси.

4. Научни и научно-приложни приноси

Резултатите от дисертацията дават нови научните знания в областта на информационната защита.

Приемам претенциите на доц. Стоянов за теоретичен подход за синтез на криптографски алгоритми за защита на информацията, който обхваща следните направления:

1. В областта на разработването на псевдослучайни криптиращи алгоритми чрез преместващи регистри с обратна връзка са изследвани десет криптографски алгоритъма.

2. В областта на повишаване скритостта на комуникационните системи са изследвани два криптографски алгоритъма.

3. В областта на синтезирането на криптографски алгоритми за генериране на псевдослучайни двоични редици чрез нелинейни динамични системи са изследвани осем криптографски алгоритъм

4. В областта на моделиране на криптографски алгоритми за защита на изображения са изследвани три криптографски алгоритъма.

Смятам, че доц. Стоянов е успял да доразвие, модифицира и продложи редица нови криптографски алгоритми чрез синтезираните производни схеми между класическите псевдослучайни генератори, булеви функции и нелинейни динамични системи. Това ми дава основание да отбележа, че поставения и решен научноприложен проблем в дисертационния труд съответства на съвременните постижения и представлява значителен и оригинален принос в науката.

5. Публикации и цитирания.

По темата на дисертационния труд, озаглавен „Криптографски алгоритми за защита на информацията" доц. Стоянов има публикувани 27 научни труда, от които 16 бр. са в реферирани издания,с общ импакт фактор 2.301 и общ импакт ранг 4.495. В сборници от научни форуми са публикувани 16 бр. статии. Б. Стоянов е публикувал 8 бр. самостоятелни статии. Той е и първи автор в 13 бр. от представените съавторски научни статии. Запознах се със съдържанието на публикациите по дисертационния труд и убедено мога да заявя, че доц. Стоянов кратко и много точно оформя своите научни изследвания.

В публикациите равномерно са отразени получените резултати, представени в отделните части на дисертацията. Приносите в дисертационния труд и публикациите по него са лично дело на докторанта.

Цитиранията на статиите на доц. Стоянов са 37 бр., от които 32 бр. са в реферирани издания, а 20 бр. са в списания с импакт фактор/ранг. Това несъмнено потвърждава високите научни постижения на дисертанта.

Могат да се посочат и някои пропуски в работата. Не обсъждам тези от редакционен характер, от типа на твърде общата тема на дисертацията,

анотацинния характер на изводите към отделните глави и твърде раздробените формулировки на приносите. Недостатъчно е приложен системния подход при анализа на проблемите, разглеждани в дисертацията.

Посочените пропуски не поставят под съмнение общата положителна оценка на дисертацията и могат да се приемат като препоръки за бъдещата научна дейност на доц. Стоянов.

1. Заключение

Като цяло дисертационният труд отговаря на изискванията на ЗРАСРБ, Правилника за неговото прилагане и Правилника на Шуменски университет „Епископ Константин Преславски" за условията и реда за придобиване на научни степени и заемане на академични длъжности.

Давам положителна оценка на дисертационния труд на тема: „Криптографски алгоритми за защита на информацията ". Убедено предлагам на уважаемото Научно жури да присъди на **доц. д-р Борислав Панайотов Стоянов** научната степен **„доктор на науките" в професионално направление 4.6 „Информатика и компютърни науки",** и ще гласувам за това.

19.05.2015 г.

Член на научното жури: .....

гр. Шумен (проф. д-р Станимир Станев)