**СТАНОВИЩЕ**

от проф. д-р Маргарита Стефанова Теодосиева,

Русенски университет „Ангел Кънчев“

за дисертационния труд на доц. д-р Борислав Панайотов Стоянов,

факултет Математика и информатика при

Шуменския универитет „Еп. К. Преславски”,

катедра *Компютърна информатика*

на тема

КРИПТОГРАФСКИ АЛГОРИТМИ ЗА ЗАЩИТА НА ИНФОРМАЦИЯТА

за придобиване на научната степен „доктор на науките”

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

професионално направление 4.6. Информатика и компютърни науки,

научна специалност: Информатика

Представеният ми за становище дисертационен труд е посветен на разработването на модели на симетрични криптографски алгоритми за защита на информацията, чиито основи изграждащи елементи са преместващи регистри с обратна връзка, двоични функции и динамични системи с хаотично поведение. Проблемът е актуален със своята научна и научноприложна значимост.

**1. Кратки биографични данни**

Доц. д-р Борислав Стоянов е роден през 1976 г. в гр. Шумен. Завършва магистратура по информатика в Шуменския университет през 2000 г. Докторската си дисертация защитава през 2006 г. и придобива ОНС „доктор” по научна специалст *Информатика*. След

спечелен конкурс е назначен за доцент по Информатика през 2009 г. и веднага е избран за ръководител на катедра „Компютърна информатика" на факултет *Математика и информатика* на Шуменския университет.

Той има научни интереси в областта на защита на информацията, хемоинформатиката, невронните мрежи. Извън дисертационното изследване има публикувани статии в списанията Entropy, Journal of Cheminformatics, MATCH Commun. Math. Comput. Chem. и International Journal of Information Technology & Decision Making.

## 2. Общи сведения за дисертацията

Дисертационният труд е разгърнат върху 187 страници. Структуриран е в уводна част, четири глави, заключение и библиография от 188 заглавия. Налични са 29 фигури и 65 таблици.

## 3. Актуалност на дисертационното изследване

Уводната част обосновава актуалността на проблема, обекта, предмета и целта на изследването, поставените изследователските задачи, апробацията на резултатите и тяхната приложимост и полезност.

Актуалността на проблема за изследване на различни криптографски алгоритми за защита на информация произтича от необходимостта за запазване неприкосновеността на личната и служебна тайна. Критичността на криптографските модули поражда непрекъсната надпревара в синтезирането на нови техни конструкции.

## 4. Обект и предмет на дисертационното изследване

Обект на дисертационното изследване са филтърните 2-адични псевдослучайни генератори на редици, псевдослучайните генератори на редици на основата на нелинейни динамични системи,

криптографските алгоритмите за защита на изображения и за повишаване на комуникационната сигурност.

Предмет на изследване са аналитичните свойства и криптоустойчивостта на числовите генератори и криптографските алгоритмите за защита на графични файлове, което определя в максимална степен приложението им за защита на информация.

**5. Цел и изследователски задачи**

Правилно е определена целта на дисертационното изследване, а именно: 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. Поставянето на тази цел е свързано с възможността за разширяване на идеята за разработка на псевдослучайни генератори чрез използване на големия потенциал на съчетанията между класическите псевдослучайни числови генератори, преместващите регистри с обратна връзка и пренос и различни булеви функции.

За постигане на тази цел, авторът си е поставил 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 процеса на работа по дисертацията са решени успешно изследователските задачи и по този начин е постигната целта на изследването.

## 6. Научноизследователски приноси

Считам, че са основателни авторските претенции за постигнатите научноприложни приноси в следните направления:

1. В областта на разработването на псевдослучайни криптиращи алгоритми чрез преместващи регистри с обратна връзка са изследвани девет криптографски алгоритъма:
   - Сумиращ генератор изпълнен с N-преместващи регистри с обратна връзка и пренос с различна адичност;
   - Сумиращ-свиващ p-адичен псевдослучаен генератор;
   - Модифициран самосвиващ генератор изпълнен с преместващ
   - регистър с обратна връзка и пренос.
   - Нов модифициран самосвиващ генератор изпълнен с преместващ регистър с обратна връзка и пренос.
   - Самосвиващ генератор на основата на 2-адичен преместващ регистър с обратна връзка и пренос и свиващата функция на Джабри.
   - Самосвиващ псевдослучаен генератор на битове изпълнен с p-преместващ регистър с обратна връзка и пренос.
   - Вариант на MBSG изпълнен със същото свиващо правило, което е приложено върху преместващ регистър с обратна връзка и пренос.
   - Редактиращ битове-търсещ генератор базиран на преместващ регистър с обратна връзка и пренос, с експериментално паралелно криптиране.

- Филтриране на преместващ регистър с обратна връзка и пренос чрез бент булева функция.

2. В областта на повишаване скритостта на комуникационните системи са изследвани два криптографски алгоритъма:
   - Метод за синтезиране на перфектни двумерни масиви.
   - Алгоритъм за обработка на сигнали без загуба на информация.
3. В областта на синтезирането на криптографски алгоритми за генериране на псевдослучайни двоични редици чрез нелинейни динамични системи са изследвани осем криптографски алгоритъма:
   - Псевдослучаен генератор на битове базиран на стандартното кръгово изображение.
   - Псевдослучаен генератор на битове базиран на стандартното изображение на Чириков филтрирано чрез свиващото правило на Джаби.
   - Псевдослучаен генератор базиран на изображението на Камбанка (Tinkerbell).
   - Псевдослучаен генератор базиран на изображението на Заславски.
   - Псевдослучаен генератор базиран на изображението на Чебишев.
   - Модифициран псевдослучаен генератор базиран на изображението на Чебишев.
   - Псевдослучаен генератор базиран на изображението на Дюфинг
   - Псевдослучаен генератор базиран на атрактора на Лоренц, филтриран чрез бент булева функция.
4. В областта на моделиране на криптографски алгоритми за защита на изображения са изследвани три криптографски алгоритъма:

- Схема за защита на изображения чрез преместващ регистър с обратна връзка и пренос филтриран чрез функцията на Джабри.
- Схема за защита на изображения чрез атрактора на Лоренц.
- Схема за защита на изображения чрез изображението на Дюфинг и изображението на Чебишев.

Бих допълнила, че в първа глава е направена своеобразна класификация на поточните криптографски алгоритми изградени чрез линейни преместващи регистри с обратна връзка и преместващи регистри с обратна връзка и пренос.

**7. Анализ на публикациите по дисертационния труд**

Част от резултатите са докладвани на редица международни конференции, което говори, че с тях е запознат голям кръг от интересуващата се научна общност. Всеки доклад е издаден в съответния конферентен сборник. Следва да се отбележи, че до 2006 г. сборник Lecture Notes in Computer Science притежаваше импакт фактор и по своя род е много реномирано научно издание. Останалите публикации са в международни списания, от които отличавам следните: Mathematical Problems in Engineering, The Scientific World Journal, Journal of Automation and Information Sciences, Applied Mathematical Sciences, Advanced Studies in Theoretical Physics и European Journal of Scientific Research.

Със своята публикационна дейност доц. Стоянов напълно е удовлетворил всички наукометрични изисквания за придобиване на научната степен „доктор на науките" на Шуменския университет.

Постигането на високата цел на дисертационното изследване ми дава основание да направя следния извод: получените научноприложни резултати съответстват на съвременните

постижения и представляват значителен и оригинален принос в науката.

**8. Анализ на автореферата**

Авторефератът на дисертационния труд точно отразява получените резултати и приноси от доц. Стоянов.

**9. Заключение**

В заключение считам, че представеният дисертационен труд напълно удовлетворява изискванията на Закона за развитие на академичния състав в Република България., Правилника за прилагането му, Правилника за развитие на академичния състав на Шуменския университет и Специфичните критерии на факултета по *Математика и информатика* на Шуменския университет. Ето защо, давам положителна оценка на дисертационния труд и препоръчвам на уважаемото Научно жури да присъди научната степен „доктор на науките" на доц. д-р Борислав Панайотов Стоянов в област на висшето образование 4. Природни науки, математика и информатика, професионално направление 4.6. Информатика и компютърни науки, научна специалност *Информатика*.

май, 2015 г.

Изготвил становището:

/проф. д-р Маргарита Теодосиева/