

СТАНОВИЩЕ

от проф. д-р Юлиан Андреев Василев, Икономически университет – Варна,
професор в ПН 4.6 „Информатика и компютърни науки“

Автор на дисертационния труд: Михаела Димитрова Годорова

Тема на дисертационния труд: Изследване на хешираща функция за
информационна защита

Научен ръководител: проф. д.н. Борислав Панайотов Стоянов

Първично звено, открило процедурата за защита на дисертацията:

Катедра „Компютърна информатика“ при Шуменски университет „Епископ
Константин Преславски“

Основание за написване на становището: Заповед N: РД-16-066/28.06.2019
г. на ректора на ШУ за откриване на процедура за защита и утвърждаване на
научно жури; проведено първо заседание на научното жури на 03.07.2019а г.

I. Общо представяне на дисертационния труд

Дисертационният труд е в общ обем 108 страници. Структуриран е във:
въведение, три глави, заключение, приложения и използвана литература.

В **увода** е обоснована актуалността на проблематиката. Основна цел на
автора е „разработване и изследване на хешираща функция за информационна
защита чрез използване на математически функции от теория на хаоса и Бент
булеви функции, които се подлагат на различни филтри“. След прочитане на целия
труд считам, че целта е постигната. Изследователска теза е дадена като част от
целта на разработката. В увода са формулирани 3 задачи. Формулирани са предмет
и обект на изследването. Изведени са 4 новости. Обоснована е приложимостта и
полезността на изследването.

Първа глава (в обем 22 страници) е озаглавена „Криптография и
криптографски системи“. Проучени са някои симетрични и асиметрични
криптографски алгоритми. Проучени са някои хеш функции. Първа глава завършва
с изводи.

Втора глава (в обем 27 страници) е озаглавена „Псевдослучайни генератори,
базирани на хаотични системи“. Проучени са разновидности на псевдо случайни
генератори. Проведени са няколко статистически теста в средата на софтуерни
продукти – NIST, DIEHARD, ENT. Втора глава завършва с изводи.

Трета глава (в обем 21 страници) е озаглавена „Разработване и изследване
на хешираща функция за информационна защита“.

В **заключението** на труда са синтезирани основните изводи, акцентирано е
на резултатите от теоретичната и практическата част. Формулирани са някои
препоръки за бъдеща работа.

II. Преценка за формата и съдържанието на дисертационния труд

Дисертационният труд е структуриран коректно. Стилът на изложението е научен. Изложението по отделни глави е балансирано. Авторефератът отразява в синтезиран вид съдържанието на дисертационния труд. По темата на дисертационния труд са публикувани 2 статии и 1 доклад.

III. Положителни моменти

Докторантът има отлични теоретични познания в изследваната проблематика. Докторантът има една публикация в Scopus. Докторантът отговаря на МНИ и минималните изисквания на ШУ за придобиване на ОНС „доктор“ в ПН 4.6.

IV. Бележки и препоръки

Добре в бъдещи изследвания (съответно и в научни публикации) да се засили полемичността и проблематиката при описание на съществуващото положение. Да се избягва представянето на научен труд като учебник.

Статистическите тестове следва да се интерпретират един по един, а не с общо заключение „...псевдослучайният генератор има задоволителни статистически свойства...“ (с. 52, 61).

Сравнително големи таблици (като на пример таблици 2.6 и 2.7) могат да се дадат като приложения.

Атаката „човек по средата“ на английски език се превежда като “man in the middle”. На с. 81 е написан друг текст на английски език.

Някои фигури (от 3.1 до 3.11) са дадени в след изводите на трета глава без интерпретация.

Някои литературни източници нямат издателство. Следва да бъде дадено.

V. Научни и научно-приложни приноси на дисертационния труд

Изведените приноси моменти са формулирани коректно и са достижения на автора на дисертацията.

VI. Въпроси по дисертационния труд

Моля да бъде дадена подробна интерпретация на резултатите на всеки един статистически тест (от с. 52 и 61).


VII. Обобщена оценка на дисертационния труд

Считам, че докторант Михаела Тодорова е показала умение за разработване на самостоятелно научно изследване от мащаба на дисертационен труд. Докторантът умее да борави със специализирана литература и да изразява лично мнение.

Направените критични бележки и препоръки не омаловажават изведените от автора приноси моменти. Формулираните бележки и препоръки целят подобряване бъдещата работа на докторант Михаела Тодорова.

Като член на научното жури за присъждане на образователна и научна степен „доктор“ давам положителната си оценка за готовността на кандидата Михаела Тодорова да придобие образователната и научна степен „доктор“ в ПН 4.6 „Информатика и компютърни науки“

30.07.2019 г.
Гр. Варна

Изготвил становището: 
(проф. д-р Юлиан Василев)