

СТАНОВИЩЕ

върху дисертационен труд за придобиване на ОНС доктор

Автор на дисертационния труд: инж. Димитър Георгиев Тодоров

Тема на дисертационния труд: **Изследване на методи за машинното обучение за криптиране на информация**

Член на научното жури: доц. д-р инж. Венцислав Николов

1. Актуалност на разработения в дисертационния труд проблем в научно и науно-приложно отношение. Степен и нива на актуалност на проблема и конкретните задачи, разработени в дисертацията.

Проучването, анализа и изследването на методите и алгоритмите за машинно обучение с цел разпознаване на алгоритъма, към който принадлежи даден секретен ключ в криптографията е актуална тема. При машинното обучение от съществена важност е подходящата обработка на входните и изходните данни и в тази връзка обикновено е необходимо данните да бъдат представени в подходящ вид, за да могат да бъдат практически изпълнени изследваните алгоритми.

Като обект на научните изследвания докторантът е формулирал устойчивостта на симетричните криптографски алгоритми, а като предмет на изследванията повишаването на устойчивостта на симетричните криптографски алгоритми.

2. Степен на познаване на състоянието на проблема и творческа интерпретация на литературния материал.

В процеса на изследванията докторантът се е запознал в достатъчна степен със състоянието на проблема. Обърнато е особено внимание на публикации свързани с тематика като разпознаване и възстановяване на криптографски симетрични секретни ключове. Наличните в литературата резултати и изводи са взети предвид при избора на алгоритми за реализация и изследване и спомага за значително повишаване на качеството на анализа на получените експериментални резултати.

3. Съответствие на избраната методика на изследване и поставената цел и задачи на дисертационния труд с постигнатите приноси.

За поставената цел и задачи е разработено приложение на програмния език C# с използване на средата за разработка Visual Studio, версии 2012 и 2019, като освен това са използвани библиотеки от Accord .NET Framework 3.8. Приложението е реализирано с множество нишки. Чрез софтуерната реализация са проведени експерименти свързани с: оценяване на ефектите от размера на еднородната среда, броя на примерите, начина на прилагане на предложените алгоритми и прилагането им върху различни хардуерни конфигурации.

Получените резултати са представени в подходящ графичен вид, като са анализирани и обобщени. Показана е точността на резултатите и са направени съответни изводи.

4. Научни и/или научно-приложни приноси на дисертационния труд.

В представения научен труд е предложен алгоритъм за обработка и представяне на входни данни за алгоритми на машинното обучение и използването им като обучаващо множество. Направена е реализация на разгледаните алгоритми за машинно обучение, като по-съществено внимание е обърнато на k-nearest neighbors (kNN) и Support vector machine (SVM), изследвани са различни конфигурационни параметри на алгоритмите и резултатите при различни размери на криптографския ключ. Формулирани са възможности за практическа приложимост на реализираните алгоритми. Считаю, че приносите са предимно от приложен характер с отделни елементи, които могат да се оценят с научно-приложен характер.

5. Преценка на публикациите по дисертационния труд.

Към дисертационния труд има шест публикации, от които две са в научни издания реферирани и индексирани в световноизвестни бази от данни с научна информация. Всички публикации са на английски език, една е самостоятелна, а в пет от публикациите докторантът е водещ автор. Публикациите са достатъчни за образователната и научна степен доктор.

6. Мнения, препоръки и бележки.

Авторът трябва да обърне по-голямо внимание на наличието на правописни, стилистични, пунктуационни и друг тип грешки в научния труд.

7. Заключение с ясна положителна или отрицателна оценка на дисертационния труд.

Считаю, че минималните изисквания за образователната и научна степен доктор са покрити и предлагам положителна оценка на разработения дисертационен труд.

21.06.2022 г.

Гр. Варна

.....
/ доц. д-р инж. В. Николов/