Р Е Ц Е Н З И Я

на дисертационен труд за придобиване на образователна и научна степен "доктор"

Тема:	**„Изследване на методи за машинно обучение за криптиране на информация**"
Автор:	**инж. Димитър Георгиев Тодоров**
Научен ръководител:	**доц. д-р инж. Милена Николова Карова**
Научна специалност:	**„Компютърни системи, комплекси и мрежи"**
Професионално направление:	**35.3 Комуникационна и компютърна техника**
Обучаващо звено:	**Технически университет–Варна** **Факултет по Изчислителна Техника и Автоматизация** **Катедра „Компютърни науки и технологии"**
Рецензент:	**доц. д-р инж. Антония Тодорова Ташева** катедра „Компютърни системи", Факултет „Компютърни системи и технологии", Технически университет–София

Настоящата рецензия е изготвена в качеството ми на член на научно жури и рецензент по процедура за защита на дисертационен труд съгласно Заповед на Ректора на Технически университет–Варна №326/20.05.2022 г. и протокол №Д.18.2/13.05.2022 от първо заседание на Научното жури.

1. Актуалност и значимост на разработвания в дисертационния труд проблем.

Темата на дисертационния труд "**Изследване на методи за машинно обучение за криптиране на информация**" е безспорно актуална, съчетавайки две от най-популярните тематики за научни изследвания в последното десетилетие, а именно алгоритмите за машинно обучение и криптографията като основа на сигурността на информацията. Докторантът се е съсредоточил върху анализа и предсказването на вида на алгоритъма, към който принадлежи

даден секретен ключ и за постигане на тази цел е формулирал и изпълнил 4 задачи.

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

Литературния обзор обхваща общо 121 източника, от които 11 са на кирилица и 110 – на латиница. Докторантът е подбрал източниците си като се е придържал към класически литературни източници основополагащи съответно за теорията на криптографията и на алгоритмите за машинно обучение. Видимо тази база е разширена чрез богат набор от съвременни статии и публикации в предметната област на изследването, а именно 59 източника са от последните 5 години (2017-2022).

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

Избраната от докторанта методика на изследване е класическа, като включва първоначален анализ на предметна област, формулиране на цели, задачи и работни хипотези, теоретични изследвания и накрая провеждане на експериментални изследвания. Изпълнението на етапите от методологията в пълнота водят до успешното постигане на поставената цел и за решаване задачите на дисертационния труд.

4. Кратка аналитична характеристика на дисертационния труд.

Представеният дисертационен труд е в обем от 137 страници и се състои от увод, четири глави, заключение, списъци с приносите по дисертационния труд, публикациите и участията на докторанта в научно-изследователски проекти, списъци с фигури и графики, таблиците и използваните съкращения и използваната литература.

В **първа глава** се прави преглед на теорията на криптографските алгоритми и машинното обучение, като се търси тяхното сечение. Разгледани са начини за разпознаване и възстановяване на симетрични секретни ключове чрез електромагнитен анализ и подход с машинно обучение и идентифициране на симетрични алгоритми чрез прилагане на CNN към следи, извлечени от IPT. **Втора глава** предлага обобщен подход за решаване на решаване на проблема с повишаване на устойчивостта на симетричната криптография срещу атаки по метода на грубата сила чрез машинно обучение. Избрани са и са описани два алгоритъма на машинно обучение и 4 симетрични криптографски алгоритми. Въз основа на тях е създаден унифициран формат за представяне на обучаващите данни. В **трета глава** се предлага пример за практическо прилагане на избраните алгоритми в програмен продукт, реализиран от докторанта. **Четвърта глава** представя проведените експериментални изследвания и получените от тях резултати, както и направеният сравнителен анализ от докторанта. Към всяка глава са направени изводи, а в заключението те са обобщени и са посочени насоки за бъдещи научни изследвания.

5. Научни и научно-приложни приноси на дисертационния труд. Значимост на приносите за науката и практиката.

Приемам формулираните от докторанта общо 6 приноса и считам, че те могат да се отнесат към категорията обогатяване на съществуващото научно знание, както следва:

Научни приноси:

1. Предложен е алгоритъм за поставяне на данни в еднородна среда, осигуряващ подходящ вид на входните данни за обучение на алгоритми за машинно обучение;
2. Предложен е подход за формиране на обучаващо множество за класифициране на криптографски данни с помощта на предложения алгоритъм за поставяне на данни в еднородна среда;

Научно-приложни приноси:

3. Предложен е подход за проектиране, конфигуриране и имплементиране на модел за подготовка на криптографски данни за работа с алгоритми от машинно обучение.

Приложни приноси:

4. С използване на предложените подходи е реализирана система за разпознаване на криптографски данни чрез използване на имплементации на алгоритми за машинно обучение и предложения алгоритъм за поставяне на данни в еднородна среда;
5. На базата на експериментални изследвания са определени подходяща конфигурация и параметри на модел за класификация на криптографски данни с цел увеличаване на устойчивостта на симетричните криптографски алгоритми;
6. С използване на разработената система за разпознаване на криптографски данни е предоставена възможност за реализиране на модел на многопрофилно криптиране или криптиране с различни алгоритми в единна среда.

6. Оценка за степента на личното участие на дисертанта в приносите

Рецензентът не може да даде категорична оценка за личното участие на докторанта в приносите, тъй като единствената самостоятелна статия на докторанта е в областта на Стеганографията, не представя резултати пряко свързани с дисертацията.

7. Преценка на публикациите по дисертационния труд.

Представен е списък с 6 публикации на докторанта, от които 1 самостоятелна, а докторантът е първи автор в 4 от 5-те публикации в съавторство. Самостоятелната статия на докторанта е на български език. Докторантът има 3 статии представяни на конференции и 3 в списания,

издавани от ТУ-Варна. Две от публикациите, представени на международни конференции проведени в България, са индексирани в Scopus. Няма данни за открити цитирания към този момент.

8. Използване на резултатите от дисертационния труд.

Докторантът е предоставил списък с три участия в научно-изследователски проекти при ФИТА на ТУ-Варна. Заглавията на проектите корелират с темата на научните изследвания на докторанта и можем да предположим, че те са в пряка връзка. Конкретни доказателства за приложението и ефекта от резултатите на изследванията на докторанта могат да се оценят при едно по-подробно представяне на неговите задачи в тези проекти.

9. Препоръки за бъдещо използване на научните и научно-приложните приноси на дисертационния труд.

Препоръчвам на докторанта да продължи своите научни и научно-приложни изследвания в областта, като ориентира публикационната си дейност към международни форуми и издания, както и участието си във трансгранични проекти с научни звена и бизнеса.

Резултатите от работата на докторанта биха могли да се адаптират към курсове по „Криптография“ или „Информационна сигурност“ от магистърски курс на обучение.

10. Оценка на автореферата с дисертационния труд

Авторефератът към дисертационния труд е в общ обем 40 страници и е структуриран правилно, като включва всички задължителни елементи. Съдържанието му ясно и точно представят систематизирано работата на докторанта по неговия дисертационен труд.

11. Критични бележки по дисертацията.

Дисертационният труд като цяло е добре оформен и структуриран, авторът е показал добро познаване на предметната област и прилагане на научния апарат. Забележките от предварителното мнение са коригирани в по-голямата си част.

В увода и в изложението на дисертационния труд, докторанта неправилно използва думата „*синхронна*“ като еквивалентен термин на общоприетия термин „*симетрична*“ криптография. Синхронността при поточните криптографски алгоритми има различно значение и употребата води до неясноти и объркване у читателя.

12. Заключение.

Въпреки направените критични бележки, считам, че инж. Димитър Георгиев Тодоров е изпълнил поставените в дисертацията му цели и задачи и представените от него материали отговарят на минималните изисквания на ЗРАСРБ за придобиване на образователна и научна степен „доктор“ по професионално направление 5.3 Комуникационна и компютърна техника, докторска програма „Компютърни системи, комплекси и мрежи”. Предвид изложеното давам своето положително мнение за представения дисертационен труд и предлагам на членовете на Научното жури да бъде присъдена образователната и научна степен „доктор” на инж. Димитър Георгиев Тодоров по научна специалност „Компютърни системи, комплекси и мрежи” в професионално направление 5.3 Комуникационна и компютърна техника.

Дата 20.06.2022 г. Подпис: .....

гр. София *(доц. д-р инж. А. Ташева)*