МИНИСТЕРСТВО НА ОТБРАНАТА
ИНСТИТУТ ПО ОТБРАНА „ПРОФЕСОР ЦВЕТАН ЛАЗАРОВ”
София 1592, бул. „Проф. Цветан Лазаров” № 2, факс: 02/92 21 808, http://di.mod.bg

СТАНОВИЩЕ

от проф. д.ик.н. Стоян Георгиев Денчев,
Директор на Института по Информация и Сигурност при Университета по библиотекознание и информационни технологии,
София-1784, бул. „Цариградско шосе“ 119, кабинет №213,
Телефон: +359878970440,
И-мейл: s.denchev@unibit.bg

за

дисертационен труд на тема:

„АНАЛИЗ НА УСТОЙЧИВОСТТА НА КРИПТОГРАФСКИ СИСТЕМИ С ПУБЛИЧЕН КЛЮЧ“

с автор:

инж. Андрей Георгиев Иванов

за получаване на образователната и научна степен

„Доктор“

по докторска програма:

„Автоматизирани системи за обработка на информация и управление“

в професионално направление:

5.2 „Електротехника, електроника и автоматика“

Научен ръководител: **полк. доц. д-р Николай Тодоров Стоянов**

София

22 януари 2023 г.

1. Общо описание на представените материали.

Представените за оценяване материали (Дисертационен труд и Автореферат) отговарят на изискванията на Закона за развитие на академичния състав, на Правилника към него и на Правилника на Института по отбрана „Професор Цветан Лазаров" за неговото прилагане, за получаване на научната и образователна степен „доктор".

Дисертационният труд е структуриран по следния традиционен и прегледен начин: Увод, три (3) Глави, Заключение, Използвана литература, Списък на публикациите, свързани с дисертационния труд, Списък на използваните термини, Математически означения и основни функции и Списък на фигурите, в общ обем от 144 страници.

В дисертацията са представени 10 фигури и 25 описани алгоритъма. Списъкът с използваната литература съдържа 114 източника.

2. Актуалност и значимост на изследването.

Представените за обсъждане от инж. Андрей Георгиев Иванов, Дисертационен труд и Автореферат на тема **„АНАЛИЗ НА УСТОЙЧИВОСТТА НА КРИПТОГРАФСКИ СИСТЕМИ С ПУБЛИЧЕН КЛЮЧ"** показват желанието на автора да представи пред научната общност в България и в частност в Института по отбрана „Професор Цветан Лазаров" резултатите от едно свое научно изследване, което е в завършен стадий на реализация.

Определено считам, че дисертационния труд е актуален и навременен.

Така както я е формулирал и автора, целта на това изследване е да докаже че публичната криптография продължава да се развива и прилага

всеобхватно, но за да е максимално полезна на текущата социална практика, е необходимо да се намалят до минимум възможностите за нейното компрометиране, чрез използване на способи за пълноценна атака спрямо процесите на генериране на публични ключове.

В тази връзка държа да подчертая, че инж. Андрей Иванов е реализирал успешно дефинираната от самия него цел, като е отговорил изчерпателно на следните въпроси:

- Възможно ли е да се изследват и да се приложат в практиката технологиите и механизмите за създаване на модели, които да послужат като основа, за реализирането и прилагането на алгоритмична база за работа в предстоящата пост-квантова ера.
- По какъв начин да се повиши процеса на устойчивостта и надеждността на генериране на ключове използвани в публичната криптография?
- Как да се реализира бърза и с високо качество оценка за наличие на внедрена клептография в системи, използващи публична криптографи?.

Авторът е решил успешно и някои други задачи, които в момента са намерили своето подобно решение в редица напреднали в научно отношение държави в света, но акцентът върху спецификата, му дава право с основание да претендира за някои научни и практически новости.

3. Основни научни и приложни приноси. Оценка на резултатите и приносите на кандидата.

Приемам не само по принцип, но и по същество научните и приложните приноси, получени в дисертационния труд, но не споделям начина по който ги е формулирал инж. Андрей Иванов.

Независимо от последната констатация, описаните приносни характеристики на изследването доказват, че дисертационният труд изпълнява своето предназначение и може да се счита за успешен опит да се отговори на една актуална и значима потребност.

4. Оценка на авторското участие.

Не установих плагиатстване и държа да подчертая, че авторството на докторантката е неоспоримо. Посочените резултати и приноси са получени след продължително натрупване на лични наблюдения, събиране на емпирични данни и упорита изследователска работа

5. Критични бележки и препоръки.

В процеса на оценката на представеното научно-приложно изследване бяха забелязани някои терминологични неточности. Забелязва се и несъразмерност в обосновката на различни авторови тези. Прекалено внимание е отделено на констативната част на дисертационния труд. Приносите биха могли визуално да се разделят на научни и приложни.

След разговори и задълбочени обсъждания с докторант Андрей Иванов и с неговия научен ръководител уважавания полк. доц. д-р Николай Тодоров Стоянов, част от забелязаните недостатъци бяха преодолени преди окончателната редакция на дисертационния труд.

Направените критични бележки и препоръки не намаляват значимостта на получените приносни резултати. Те по никакъв начин не ограничават тяхната научно-методологическа и приложна стойност.

6. Заключение.

Всичко изложено по-напред ми дава основание да гласувам

положително за присъждане на образователната и научна степен „доктор“ на **инж. Андрей Георгиев Иванов** по докторска програма: **„Автоматизирани системи за обработка на информация и управление“** в професионално направление: **5.2 „Електротехника, електроника и автоматика“.**

Подпис: /П/

проф. д.ик.н. Стоян Денчев

22 януари 2023 г.
гр. София