

## РЕЦЕНЗИЯ

от проф. д.н. Иван Ганчев Гарванов – УниБИТ  
член на Научно жури, назначено със Заповед на Ректора на Пловдивски  
университет „Паисий Хилендарски“ № Р33-5350/22.10.2021 г.

относно: Дисертационен труд на **Тони Пламенов Каравасилев**  
на тема “СОФТУЕРНА РАМКА ЗА КРИПТОГРАФСКИ УСЛУГИ”,  
представен за придобиване на образователна и научна степен “доктор”  
по докторска програма “Информатика”, професионално направление  
4.6 „Информатика и компютърни науки“, с научни ръководители проф.  
д-р Елена Петрова Сомова и доц. д-р Светослав Христосов Енков.

### 1. Общо описание

На първото заседание на Научното жури съм избран да напиша  
рецензия и съм получил пълен комплект с документи, включващ:

- дисертация
- автореферат на български и автореферат на английски език
- списък на отпечатани научни публикации по темата на дисертацията
- публикации по темата на дисертацията в пълен текст
- справка за изпълнението на минималните национални изисквания на справка за изпълнение на специфичните изисквания на Университета
- други документи, свързани със защитата на дисертационния труд.

## **2. Актуалност, цел и задачи**

През последните години сме свидетели на многобройни злоупотреби със сигурността на данните и информацията в информационните системи. Използването на криптографски услуги е едно от най-перспективните решения на този актуален научен проблем.

**Целта** на настоящата дисертация е разработване и изследване на обектно-ориентирана софтуерна рамка за криптографски услуги.

За постигане на целта на дисертационният труд са формулирани следните **научноизследователски задачи**:

1. Обзор и анализ на международните стандарти за криптографски системи, подходи за реализация на сигурна мрежова комуникация и добри практики за защита на информацията при пренос, съхранение и обработка на данни;

2. Проектиране на криптографски модел, базиран на криптографски услуги, протоколи, примитиви и йерархии от обекти. Разработване на методика за интеграция на криптографски услуги в реална работна среда;

3. Изграждане на обектно-ориентирана софтуерна рамка за криптографски услуги на базата на дефинирания криптографски модел;

4. Изследване на съвместимостта, производителността и качеството на изградената специализирана софтуерна рамка.

## **3. Обща характеристика на дисертационния труд**

Дисертационният труд се състои от 165 страници, структуриран в увод, четири глави, заключение, библиография, приложения, списък на публикациите по дисертацията, списък със забелязани цитирания по

дисертацията и декларация за оригиналност. Дисертационният труд съдържа 46 фигури, 10 таблици и 117 литературни източника.

В глава първа е направен обзор и анализ на криптографията както и приложенията и в различните видове криптографски системи. Анализирани са най-ефективните подходи за проектиране, реализиране и документиране за софтуерни рамки.

В глава втора са разгледани процесите по проектиране на криптографски модел и софтуерната рамка за криптографските услуги. Направен е функционален и сравнителен анализ на приложимостта на проектираната софтуерната рамка спрямо група от конкурентни софтуерни разработки за различни платформи.

В глава трета са проведени изследвания на предложеният криптографски модел с помощта на езика за програмиране PHP.

В глава четвърта е направен обзор и анализ на най-ефективните практики за постигане на цялостна защита на данните по време на техния пренос и съхранение, Разгледани са и редица алтернативни методи за постигане на сигурна комуникация между множество страни.

В заключение са систематизирани получените резултати и са дефинирани приносите на дисертационния труд. Очертани са бъдещите насоки за развитието на софтуерната рамка и нейния абстрактен криптографски модел.

Представените в дисертацията изследванията са подкрепени с програмен код, доказващ дълбокото разбиране на криптографските алгоритми.

#### **4. Приноси**

Приемам всички приноси на докторанта, а именно:

Създадени са методики (набор от препоръки, правила, инструменти и съвети) за осигуряване на защита на информационни системи в различен приложен контекст;

Проектирана е софтуерна рамка за криптографски услуги на базата на анализ на съществуващи решения от различни технологични среди;

Предложена е унифицирана архитектура за управление на криптографски услуги и примитиви чрез платформено независим подход за реализация.

Реализирана е софтуерна рамка за криптографски услуги като приложен инструмент за създаване, управление и конфигуриране на сигурни софтуерни услуги и среди;

Интегриран е криптографски модел в език за програмиране без наличието на вградена поддръжка на криптографски услуги и примитиви;

Тествана е създадената софтуерна рамка, автоматизирано и с реални потребители, и е направен анализ на получените резултати.

## **5. Автореферат**

Представените два варианта на автореферата на български и английски език отразяват достоверно съдържанието на дисертационния труд и съответстват на изискванията на ЗРАСРБ и ППЗРАСРБ. От приложена декларация за оригиналност на представените резултати, като и от представените публикации по дисертационния труд може да се съди, че описаните резултати са лично дело на докторанта.

## **6. Оценка за съответствие с минималните национални изисквания**

Докторантът **Тони Каравасилев** е апробирал части от дисертационния си труд в пет публикации – в трудове на конференции (3 международни и 2 национални). Една от публикациите е индексирана в световноизвестните бази от данни Scopus и Web of Science и има SJR=0,198. Четири от публикациите са в съавторство с научните ръководители и една е самостоятелна.

Съгласно минималните национални изисквания за получаване на ОНС „Доктор” по професионално направление 4.6. “Информатика и компютърни науки”, определени в ППЗРАСРБ се изискват наличие на поне 30 точки по Група показатели Г. Представените публикации по дисертационния труд формират тези 30 точки, което удовлетворява минималните национални изисквания.

Приложен е и списък с цитирания от който се вижда, че две от публикациите на кандидата са цитирани в четири научни публикации. С това се доказва необходимата публичност на постигнатите резултати.

## **7. Бележки и препоръки**

Част от представените резултати в дисертационния труд не са намерили отражение в публикациите по дисертацията и препоръката ми е те да бъдат публикувани.

## **8. Заключителна комплексна оценка**

Считам, че представеният дисертационен труд отговаря на всички изисквания и критерии на ЗРАСРБ, ППЗРАСРБ и специфичните критерии на правилника на Пловдивски университет „Паисий Хилендарски“ за прилагане на ЗРАСРБ. Постигнатите резултати ми

дават основание напълно убедено да дам положителна оценка и препоръчвам на почитаемото Научно жури да присъди образователната и научна степен „Доктор” на **Тони Пламенов Каравасилев** в професионално направление – 4.6. „Информатика и компютърни науки“, докторска програма – „Информатика“

29.11.2021 г.

гр. София

.....  
/Проф. д.н. И. Гарванов/