СТАНОВИЩЕ

от доц. д-р Златко Василев Захариев, ФПМИ, ТУ-София

относно дисертационния труд на **маг. инж. Светлин Георгиев Стефанов** за присъждане на образователната и научна степен **„доктор“** в професионално направление 4.6. „Информатика и компютърни науки“

Научна специалност: „Информатика“
Професионално направление: 4.6. „Информатика и компютърни науки“.
Автор: маг. инж. Светлин Георгиев Стефанов
Катедра: „Информатика“
Тема: „Методология за обработка, анализ и верификация на компютърни експертизи в цифровата криминалистика“
Научен ръководител: доц. д-р инж. Малинка Спасова Иванова, ФПМИ, ТУ-София

Настоящото становище се изготвя в съответствие със Заповед ОЖ-4.6-05/05.02.2025 и Заповед ОЖ-4.6-06/11.02.2025 на Ректора на ТУ-София за назначаване на научното жури.

1. Общи впечатления

Представеният дисертационен труд, разглежда изключително актуална тема в съвременния дигитален свят, където киберпрестъпността нараства и изисква ефективни инструменти за разследване. Дисертацията обхваща цялостен процес на разследване в цифровата криминалистика, като предлага методологичен подход за обработка, анализ и верификация на цифрови доказателства.

Трудът е структуриран в пет основни глави, всяка от които разглежда ключови аспекти на цифровата криминалистика:

1. Изследване и анализ на съвременни модели, методи и техники за изготвяне на експертизи – включва библиометричен анализ на използваните подходи в криминалистиката, както и представяне на разработен концептуален модел.
2. Методология за информационна обработка, анализ и верификация в цифровата криминалистика – дефинира стъпките на разследването, като обхваща придобиване, съхраняване, анализ и проверка на цифрови доказателства.
3. Проектиране на интелигентна информационна система с интегрирана методология – представя разработката на система, която автоматизира и подпомага разследващите експерти.
4. Машинно обучение и изкуствен интелект в цифровата криминалистика – изследва прилагането на алгоритми от изкуствения интелект за анализ на цифрови доказателства.
5. Разработване и оценка на софтуерна система за целите на цифровата криминалистика – описва разработен софтуерен прототип и неговата оценка чрез функционални тестове и обратна връзка от експерти.

Авторът демонстрира задълбочено познаване на областта и интегрира различни подходи – от теоретичен анализ на криминалистични методи до внедряване на алго-

ритми за машинно обучение. Използваната библиография е актуална и включва водещи изследвания в областта, като се прави систематизиране на съществуващите методи и тяхното надграждане. Особено впечатляващо е приложението на автоматизирани техники за анализ на цифрови доказателства, което показва опита на автора към практическите предизвикателства в областта.

Дисертацията е ясно и логично структурирана, като всяка глава надгражда предходната. Стойността на изследването е висока, тъй като не само предлага нова методология, но и представя реална имплементация, което я прави практически приложима. Наред с това, предложената методология може да бъде адаптирана към различни сценарии в областта на киберсигурността и криминалистичните разследвания. Трудът е значим принос в областта на цифровата криминалистика и отговаря на всички академични стандарти.

Разработената методология и представените резултати отговарят на съвременните научни изисквания в областта и имат значителен принос както за теорията, така и за практиката на цифровата криминалистика

2. Приноси

В дисертационния труд са представени следните основни приноси, които са докладвани от автора и са в съответствие с извършените научни изследвания и приложни разработки:

1. Научни и научно-приложни приноси:
    - Разработен е концептуален модел, представящ развитието на рамки и модели в цифрово криминалистично разследване, както и представящ значението на техники от изкуствен интелект, машинно и дълбоко обучение за подпомагане на експерт-криминалист.
    - Разработена е методология за цифрово разследване в цифровата криминалистика от практическа гледна точка DFIP, включваща 12 фази, за подпомагане дейности на експерт-криминалисти.
    - Предложен е подобрен модел за придобиване на цифрови доказателства за подпомагане изпълнението на фаза 2 от методологията.
    - Разработена е рамка за приложението на техники от изкуствен интелект в цифровата криминалистика, в цифрово криминалистично разследване и за подготовка на компютърни експертизи.
    - Създаден е класификационен модел за класификация на 17 вида файлови формати за подпомагане анализа на цифрови доказателства.
    - Създадени са два модела, съответно за изследване на текстовото съдържание и извличане на снимки от pdf файлове, за автоматизиране анализа на цифрови доказателства.
    - Създаден е модел за сентимент анализ на съдържанието на pdf файлове за подобряване на цифрово криминалистично разследване.
2. Приложни приноси
    - Създаден е функционален архитектурен модел на софтуерна система, който е теоретично обоснован и интегриращ методология за раз-

следване в цифровата криминалистика от практическа гледна точка DFIP.

- Разработен е софтуерен прототип на система за автоматизиране на дейности в цифровата криминалистика въз основа на създадената преди това методология за разследване в цифровата криминалистика от практическа гледна точка DFIP.

Тези приноси потвърждават, че дисертационният труд представлява значим принос в областта на цифровата криминалистика, като предлага иновативни решения за подобряване на ефективността на криминалистичните експертизи.

3. Познаване на проблема

Дисертационният труд демонстрира задълбочено разбиране на проблемите, свързани с обработката, анализа и верификацията на цифрови доказателства в криминалистичните разследвания. Сред основните предизвикателства, които изследването адресира, са увеличаващата се сложност на цифровите престъпления, необходимостта от надеждни методи за придобиване и анализ на цифрови доказателства и липсата на унифицирани стандарти за верификация.

В тази връзка, трудът предлага методология, която съчетава утвърдени криминалистични техники с иновативни алгоритми за анализ, подпомогнати от машинно обучение. Това позволява разработването на по-ефективни стратегии за разследване

4. Методология и научна обоснованост

Изследването е структурирано така, че да обхване всички ключови етапи от криминалистичното разследване – от придобиването и съхранението на доказателствата до тяхната проверка и представяне в експертни заключения. Предложената методология не само следва утвърдените криминалистични стандарти, но и ги надгражда чрез интегриране на автоматизирани алгоритми и изкуствен интелект, които оптимизират процеса и намаляват риска от грешки.

Авторът извършва сравнителен анализ на съществуващите методологии, като демонстрира предимствата на предложената рамка чрез криминалистични сценарии. Разработената методология е подложена на експериментална проверка и е оценена от експерти в областта, което потвърждава нейната практическа приложимост.

5. Оценка на структурата и оформлението

Дисертационният труд е добре структуриран и следва логическа последователност, която позволява ясно проследяване на научното изследване. Въведението въвежда читателя в контекста на цифровата криминалистика и очертава основните проблеми, които трудът се стреми да адресира. Всяка от последващите глави е изградена с ясно дефинирани цели и съдържа необходимата теоретична рамка, анализ на съществуващи подходи, методологични предложения и практически експерименти. Това осигурява плавен преход между различните етапи на изследването и поддържа консистентност в представянето на информацията.

Представянето на данните и резултатите е подкрепено с таблици, графики и илюстрации, които спомагат за визуализацията на ключовите концепции и анализи. Използваният език е академичен и прецизен.

Цитираната литература е актуална и добре подбрана, което подсилва научната стойност на изследването. Библиографските препратки са коректно оформени, което допринася за прозрачността на използваните източници.

Дисертационният труд отговаря на изискванията, като съчетава добре организирана структура, ясно изложение и стриктно спазване на академичните правила за оформяне на научни публикации.

6. Оценка на публикациите и личния принос на докторанта

В представения дисертационен труд са отчетени 8 (осем) научни публикации, които отразяват резултатите от изследването. Публикационната активност на докторанта е на високо ниво, като представените публикации са публикувани в рецензирани научни издания и представени на престижни научни конференции. Покриват се различните аспекти на изследването.

Демонстрирана е активност в академичната общност. Отразените цитирания потвърждават интереса към изследването и неговото значение. Личният принос на докторанта в колективните публикации е ясно дефиниран.

ЗАКЛЮЧЕНИЕ

Дисертационният труд на маг. инж. Светлин Стефанов е значим принос в областта на цифровата криминалистика. Разработената методология и софтуерното решение имат потенциал за реално приложение в експертната практика. Авторът демонстрира задълбочени познания в областта, прилагайки модерни технологии и аналитични подходи.

С оглед на изложените научни приноси и качеството на проведеното изследване, считам, че дисертационният труд напълно отговаря на изискванията за присъждане на образователната и научна степен „доктор“. Убедено давам своята **положителна оценка** и предлагам допускането му до защита.

29.04.2025
гр. София

Изготвил становището:
доц. д-р Златко Захариев
Катедра „Информатика“
ФПМИ
Технически Университет - София

EVALUATION REPORT

by Assoc. Prof. Dr. Zlatko Vasilev Zahariev, FAMI, TU-Sofia

on the dissertation of **M. Eng. Svetlin Georgiev Stefanov** for the awarding of the educational and scientific degree **"Doctor"** in professional field 4.6. "Informatics and Computer Science

Scientific Specialty: „Informatics“
Professional Field: 4.6. "Informatics and Computer Science"
Author: M. Eng. Svetlin Georgiev Stefanov
Department: „Informatics“
Title: „Methodology for Processing, Analysis, and Verification of Computer Expert Reports in Digital Forensics“
Scientific Advisor: Assoc. Prof. Dr. Eng. Malinka Spasova Ivanova, FAMI, TU-Sofia

This evaluation report is prepared in accordance with Order ОЖ-4.6-05/05.02.2025 and ОЖ-4.6-06/11.02.2025 of the Rector of TU-Sofia for the appointment of the scientific jury.

1. General Impressions

The presented dissertation addresses an extremely relevant topic in the modern digital world, where cybercrime is on the rise, requiring effective investigative tools. The dissertation covers the entire digital forensic investigation process by proposing a methodological approach for processing, analyzing, and verifying digital evidence.

The work is structured into five main chapters, each examining key aspects of digital forensics:

6. Study and analysis of modern models, methods, and techniques for expert report preparation – includes a bibliometric analysis of forensic approaches and presents a developed conceptual model.
7. Methodology for information processing, analysis, and verification in digital forensics – defines the investigation steps, covering the acquisition, storage, analysis, and verification of digital evidence.
8. Design of an intelligent information system with an integrated methodology – presents the development of a system that automates and supports forensic experts.
9. Machine learning and artificial intelligence in digital forensics – explores the application of artificial intelligence algorithms for digital evidence analysis.
10. Development and evaluation of a software system for digital forensics – describes the developed software prototype and its evaluation through functional tests and expert feedback.

The author demonstrates deep knowledge of the field and integrates various approaches – from theoretical analysis of forensic methods to the implementation of machine learning algorithms. The bibliography used is up-to-date and includes leading studies in the field, systematically categorizing and enhancing existing methods. Particularly impressive is the application of automated techniques for digital evidence analysis, reflecting the author's practical experience in the field.

The dissertation is clearly and logically structured, with each chapter building upon the previous one. The research has high value, as it not only proposes a new methodology but also presents a real implementation, making it practically applicable. Furthermore, the pro-

posed methodology can be adapted to different scenarios in cybersecurity and forensic investigations. The study is a significant contribution to the field of digital forensics and meets all academic standards.

The developed methodology and presented results comply with modern scientific requirements in the field and have a significant contribution to both the theory and practice of digital forensics.

2. Contributions

The dissertation presents the following major contributions, reported by the author, which align with the conducted scientific research and applied developments:

3. Scientific and Applied Contributions:
    - A conceptual model has been developed, illustrating the evolution of frameworks and models in digital forensic investigation, emphasizing the role of artificial intelligence, machine learning, and deep learning techniques in supporting forensic experts.
    - A methodology for digital investigation in digital forensics has been developed from a practical perspective (DFIP), consisting of 12 phases to assist forensic experts.
    - An improved model for digital evidence acquisition has been proposed to support phase 2 of the methodology.
    - A framework has been developed for applying artificial intelligence techniques in digital forensics, forensic investigation, and the preparation of computer expert reports.
    - A classification model has been created to categorize 17 types of file formats to aid digital evidence analysis.
    - Two models have been developed: one for textual content analysis and another for image extraction from PDF files, automating digital evidence analysis.
    - A sentiment analysis model has been created for analyzing the content of PDF files to enhance digital forensic investigations.
4. Applied Contributions:
    - A functional architectural model of a software system has been created, theoretically justified and integrating the digital forensics investigation methodology from a practical perspective (DFIP).
    - A software prototype for automating activities in digital forensics has been developed based on the previously established DFIP methodology.

These contributions confirm that the dissertation represents a significant advancement in digital forensics, offering innovative solutions to improve the effectiveness of forensic expert investigations.

3. Understanding of the Problem

The dissertation demonstrates a deep understanding of the issues related to processing, analyzing, and verifying digital evidence in forensic investigations. Among the key challenges addressed in the study are the increasing complexity of digital crimes, the need

for reliable methods for acquiring and analyzing digital evidence, and the lack of unified standards for verification.

In this regard, the dissertation proposes a methodology that combines established forensic techniques with innovative analysis algorithms supported by machine learning. This enables the development of more effective investigative strategies.

4. Methodology and Scientific Justification

The study is structured to encompass all key stages of forensic investigation – from acquiring and storing evidence to verifying and presenting it in expert conclusions. The proposed methodology not only adheres to established forensic standards but also enhances them by integrating automated algorithms and artificial intelligence, optimizing the process and reducing error risks.

The author conducts a comparative analysis of existing methodologies, demonstrating the advantages of the proposed framework through forensic scenarios. The developed methodology undergoes experimental validation and expert evaluation, confirming its practical applicability.

5. Evaluation of Structure and Formatting

The dissertation is well-structured and follows a logical sequence that allows for a clear understanding of the scientific study. The introduction provides context in digital forensics and outlines the main issues the research aims to address. Each subsequent chapter is constructed with clearly defined objectives and contains the necessary theoretical framework, analysis of existing approaches, methodological proposals, and practical experiments. This ensures a smooth transition between different research stages and maintains consistency in the presentation of information.

The presentation of data and results is supported by tables, graphs, and illustrations, aiding the visualization of key concepts and analyses. The language used is academic and precise.

The cited literature is current and well-selected, strengthening the scientific value of the study. Bibliographic references are correctly formatted, ensuring transparency of the sources used.

The dissertation meets the required standards by combining a well-organized structure, clear exposition, and strict adherence to academic rules for scientific publication formatting.

11. Evaluation of Publications and Personal Contribution

The dissertation reports eight (8) scientific publications, reflecting the research findings. The doctoral candidate's publication activity is at a high level, with articles published in peer-reviewed scientific journals and presented at prestigious scientific conferences. Various aspects of the study are covered.

Active engagement in the academic community is demonstrated. The recorded citations confirm interest in the research and its significance. The doctoral candidate's personal contribution in co-authored publications is clearly defined.

CONCLUSION

The dissertation of M.Eng. Svetlin Stefanov is a significant contribution to the field of digital forensics. The developed methodology and software solution have potential real-world applications in forensic practice. The author demonstrates in-depth knowledge in the field, applying modern technologies and analytical approaches.

Given the presented scientific contributions and the quality of the conducted research, I conclude that the dissertation fully meets the requirements for awarding the educational and scientific degree "Doctor." I confidently give my ***positive assessment*** and propose that the dissertation be admitted for defense.

29.04.2025
Sofia

Prepared by:
Assoc. Prof. Dr. Zlatko Zahariev
Department of Informatics
FAMI
Technical University of Sofia