

РЕЦЕНЗИЯ

по процедура за защита на дисертационен труд на тема

„Методология за обработка, анализ и верификация на компютърни експертизи в цифровата криминалистика"

за придобиване на образователна и научна степен „доктор“

от

Кандидат: **маг. инж. Светлин Георгиев Стефанов**

Област на висше образование: **4. Природни науки, математика и информатика**

Професионално направление: **4.6. Информатика и компютърни науки**

Докторска програма: **„Информатика“**, катедра: **„Информатика“**

Факултет по приложна математика и информатика (ФПМИ)

Технически Университет – София

Рецензията по процедурата за защита на дисертационен труд за придобиване на образователна и научна степен „доктор“ на маг. инж. Светлин Георгиев Стефанов, е изготвена от **проф. д-р инж. Галина Тодорова Богданова**, Институт по математика и информатика при Българска академия на науките, в качеството на член на научното жури, съгласно Заповед №ОЖ-4.6-05/05.02.2025 г. и заповед №ОЖ-4.6-06/11.02.2025 г. на Ректора на ТУ-София.

1. Обща информация за представените документи и докторанта

Маг. инж. Светлин Георгиев Стефанов е завършил през 2018 г. магистратура по педагогика на обучението по математика в Пловдивския Университет "Паисий Хилендарски". Той работи от 2019 и досега в Национална Следствена Служба, София на длъжност програмист–криминалист и като вещо лице в съдебната система. Докторантът е зачислен в редовна докторантура от 01.07.2020 г. в катедра „Информатика“ на ФИМИ със заповед на Ректора на ТУ-София №1581/23.06.2020 г. Той е преминал от редовна в задочна форма на докторантура на 01.01.2023 г. и е отчислен с право на защита от 01.01.2025 г. със заповед на Ректора на ТУ-София №48/ 09.01.2025 г.

Предоставените документи по процедурата отговарят напълно, както на националните изисквания (Закон за развитие на академичния състав в Република България и Правилника за прилагането му), така и на изискванията на ТУ-София (Правилник за условията и реда за придобиване на научни степени в ТУ-София /актуализация към 19.10.2023 г./).

2. Актуалност на разработваните в дисертационния труд проблеми и анализ на съдържанието на дисертацията

Проблемите, разгледани в дисертацията са важни за обществото и имат висока степен на актуалност в областта на цифровата криминалистика. Направените изследвания и решените задачи са значими за сферата на експертно-криминалистична дейност в научно и научно-приложно отношение.

Дисертационният труд има обем от 136 стр. и следната структура: увод, пет глави, приноси, заключение, използвана литература, публикации по темата на дисертационния труд, списъци с фигури и таблици. Всяка от главите започва с въведение и завършва с обобщение, приноси и публикации на автора, свързани с изследванията в тази глава. В дисертацията са проучени и анализирани достатъчни по обем информация и литературни източници (117). Използвани са голям брой добре изработени фигури (53), които подобряват разбирането на текста, като списъкът на фигурите и на 4 таблици е приложен в дисертацията.

В увода на дисертационния труд е представена целта на изследването и са дефинирани четири задачи за постигането на целта. В първа глава са разгледани изследвания и анализи на съвременните модели, методи и техники за изготвяне на експертизи в цифровата криминалистика. Представени са основните понятия, библиометричен анализ на моделите на цифровото криминалистично разследване, анализ на текущото състояние и създаден концептуален модел. Във втора глава са описани методологията за разследване в цифровата криминалистика от практическа гледна точка и 12-те фази на методологията, както и подобрен модел за придобиване на цифрови доказателства.

В трета глава е представено проектирането на интелигентна информационна система с интегрирана методология за подпомагане на разследвания в цифровата криминалистика и функционалната архитектура на системата. Четвъртата глава е посветена на използването на машинно обучение и изкуствен интелект (ИИ) в цифровото криминалистично разследване. Разработени са: рамка и анализи чрез техники от машинно обучение и ИИ, класификация на цифровите доказателства, анализ на текст и извличане на изображения от pdf файлове, големи езикови модели в резюме на pdf текст. В пета глава е представен разработен софтуерен прототип и е направена оценка на функционалността на софтуерната система за целите на цифровата криминалистика. Направено е микро обучение в курс по цифрова криминалистика и анализ на мнението на експерти в цифровата криминалистика.

Основен фокус на изследванията в дисертацията е създаването на методология, разработването на модели и интелигентна информационна система с помощта на използването на съвременни технологии като машинно обучение и ИИ.

3. Степен на познаване състоянието на проблема, съответствие на методиката на изследване с поставените цел и задачи и достоверност на приносите на дисертацията

От предоставените документи по процедурата се вижда, че маг. инж. Светлин Георгиев Стефанов работи в сферата на криминалистиката и има опит като вещо лице в съдебната система. Той притежава висока професионална степен на експертност и задълбочени знания в областта на цифровата криминалистика и дигиталните технологии. Компетентността му, научните и практически умения и знания освен в областта на цифровата криминалистика, но и в областта на информационните технологии са помогнали на автора при избора и процесите на разработка на създадените методи и модели. Съвкупността от всички тези фактори е допринесла за по-доброто разбиране и по-успешното решаване на проблемите и е причина избраната методика на изследване да съответства адекватно на поставените цел и задачи на дисертационния труд.

Проучванията, анализите и разработките в работата се основани на солидна база от научни и практически знания на автора и на изследваните от него източници на други автори. Това допринася за правилността на анализите, изводите и оценките и характеризира достоверността на материала, върху който се градят приносите на дисертационния труд.

4. Научни и научно приложни приноси на дисертационния труд

В дисертационния труд са представени достоверни резултати, които могат да бъдат квалифицирани като приноси от научен, научно-приложен и приложен характер.

Докторантът е формулирал и обосновал седем научни и научно-приложни приноси: 1) концептуален модел; 2) методология DFIP; 3) подобрен модел за придобиване на цифрови доказателства; 4) рамка за приложение на изкуствен интелект; 5) модел за класификация; 6) модел за изследване и извличане на PDF файлове и 7) сантимент анализ на PDF файлове. Той е представил и два приложни приноса (архитектурен модел на софтуерна система и софтуерен прототип, автоматизиращ дейностите в цифровата криминалистика). Подкрепям напълно направените от автора изводи относно постигнатите девет приноса.

Така определените приноси включват дефиниране, обосновка и доказване с нови средства и технологии на съществуващи научни проблеми, адаптиране и създаване на нови подходи и методи в цифровата криминалистика. Такива нови средства са разработените концептуален модел и практическата методология за цифровото разследване DFIP, включваща 12 фази, както и архитектурния модел на софтуерна система, интегриращ методологията DFIP. Оригинални подходи и решения на проблемите са и създадените подобрен модел за придобиване на цифрови доказателства, рамката за приложението на техники от ИИ, класификационния модел за анализ на цифрови доказателства и други модели и анализи, включващи изкуствен интелект, машинно и дълбоко обучение.

Предложените от автора методи и модели са напълно обосновани и могат да бъдат използвани в практиката. Някои от постигнатите резултати и приноси с научно и научно приложно значение в сферата на цифровата криминалистика, са подходящи да бъдат внедрени в институциите в тази област (например в пряката служебна работа на докторанта). Очевидно е тяхното голямо практическо значение, както за работата на криминалистите, така и за съдебната система при работата на вещите лица. Всяко от тези постижения на автора показва определен напредък в разглежданата сфера и демонстрира възможностите за приложение на технологиите в анализа и изследванията в областта на цифровата криминалистика.

Степента на личното участие на докторанта в изследванията и приносите е безспорна, без неговата висока експертност по темата и голям практически опит не биха били възможни получените резултати и направените публикации. Практическото значение на изследванията, методите и резултатите в това направление се вижда и от мненията на компетентни специалисти в областта на криминалистиката (дискутирани в трета глава и приложени в края на дисертацията).

5. Преценка на публикациите по дисертационния труд

Представени са осем публикации по темата на дисертационния труд, които покриват напълно, дори надхвърлят минималните национални изисквания и необходимите критерии. Пет от публикациите са публикувани в престижни световни издания, а три публикации в сборници от международни конференции са под печат. Не е установено плагиатство в представените за конкурса научни трудове.

Повечето от изданията, в които публикациите са отпечатани (или са под печат) са индексирани в Scopus и Web of Science, като една от тях има SJR (Q4). Всичките публикации са в съавторство и на английски език.

От представените известни на автора цитирания от други автори и от приложените към документите мнения на професионални експерти-криминалисти, е видно, че публикациите, методите и моделите на докторанта имат отзвук и значимост в изследваната област на цифровата криминалистика.

6. Използване на резултатите от дисертационния труд в научната и социалната практика

Постигнатите резултати имат научно и практическо значение, както в сферата на цифровата криминалистика, така и за работата на вещите лица в съдебната система и за други приложения.

Наличието на постигнат пряк ефект и използването на разработените методи от докторанта и негови колеги в преките им служебни задачи се доказва и от приложените документи в края на дисертацията с мнения на компетентни специалисти.

7. Оценка на съответствието на автореферата с изискванията за изготвянето му, както и на адекватността на отразяване на основните положения и приносите на дисертационния труд

Общи данни и съдържание на автореферата: предоставеният автореферат е с общ обем от 32 страници (на български език). Съдържанието на автореферата се състои от увод, разделите на дисертацията, заключение, приноси, публикации по темата на дисертационния труд и summary (на английски език). Представен е списък с 8 публикации на автора по темата на дисертацията, публикувани в престижни издания и покриващи (дори надхвърлящи) минималните национални изисквания.

Авторефератът описва синтезирано, разбираемо и логично дисертационния труд. Той представя актуалните проблеми в областта на цифровата криминалистика, целта на изследването, задачите, представително описание на петте основни глави на дисертацията, намерените решения и постигнати резултати в дисертационния труд. Акцентирано е на разработената методология, проектирането на интелигентната информационна система, използването на машинно обучение и ИИ, както и на справката с научните приноси.

Направено е сравнение на съдържанието на автореферата и на дисертационния труд и изводи относно съответствието на автореферата с дисертационния труд:

- Авторефератът има достатъчен обем страници и е написан е грамотно. Той оформен в съответствие с изискванията на Закона за развитие на академичния състав в Република България и на изискванията на ТУ-София.
- Структурата и съдържанието на автореферата следват стриктно структурата и съдържанието на дисертационния труд и са коректно представени. Авторефератът адекватно отразява основните елементи на дисертацията и приносите и дава точна представа за постигнатото от докторанта.
- Дадени са конкретни решения на поставените задачи с научно и практическо значение в областта на цифровата криминалистика. Представени са ясно и добре формулирани научните, научно-приложни и приложни приноси на кандидата.

В заключение авторефератът има пълно съответствие с изискванията за изготвянето му и точно отразява дисертационния труд.

8. Мнения, препоръки и бележки

Нямам съществени забележки към структурата и съдържанието на предоставения дисертационен труд и автореферат.

Препоръки: Авторът може да систематизира и публикува направените оригинални изследвания и получените решения в обобщен монографичен труд, както

и да продължи и в бъдеще своите научни изследвания в това актуално научно направление.

Въпроси: Има ли в чужбина подобни модели в цифровата криминалистика и приложими ли са получените решения в дисертацията в други страни?

9. Заключение

Изследваните проблеми в дисертацията са актуални и значими за областта на цифровата криминалистика. Дисертационният труд се базира на достатъчно по обем информация и е написан грамотно. Работата е оформена според изискванията на Закона за развитие на академичния състав в Република България, Правилника за приложението му и на Правилника за условията и реда за придобиване на научни степени в ТУ-София (актуализация към 19.10.2023 г.). Докторантът е доказал своята компетентност и практически знания в изследваната област, като е намерил ясни, точни и конкретни решения на поставените задачи. Представил е разбираемо и логично разработената методология и постигнатите резултати. Направените публикации в престижни издания покриват напълно и надхвърлят минималните национални изисквания в професионалното направление.

В заключение давам **положителна оценка на дисертационния труд и препоръчвам на научното жури да се присъди** на маг. инж. Светлин Георгиев Стефанов образователната и научна степен „доктор“ по професионално направление 4.6. „Информатика и компютърни науки“ в докторска програма „Информатика“.

Дата:

25.04.2025 г.

РЕЦЕНЗЕНТ:

/проф. д-р инж. Галина Богданова/

REVIEW

under the procedure for defending a dissertation on the topic

"Methodology for processing, analysis and verification of computer expertise in digital forensics"

for the acquisition of the educational and scientific degree of "Doctor"

from

Candidate: **M.Sc. Ing. Svetlin Georgiev Stefanov**

Field of Higher Education: **4. Natural Sciences, Mathematics and Informatics**

Professional field: **4.6. Informatics and Computer Science**

Doctoral program: **"Informatics", Department: "Informatics"**

Faculty of Applied Mathematics and Informatics (FAMI)

Technical University of Sofia

The review of the procedure for defending a dissertation for the acquisition of the educational and scientific degree of "Doctor" of Master. Ing. Svetlin Georgiev Stefanov, was prepared by **prof. dr. eng. Galina Todorova Bogdanova**, Institute of Mathematics and Informatics at the Bulgarian Academy of Sciences, as a member of the scientific jury, according to Order No. №ОЖ--6-05/05.02.2025 and Order No. №ОЖ-4.6-06/11.02.2025 of the Rector of the Technical University of Sofia.

1. General information about the submitted documents and the PhD student

Mag. Ing. Svetlin Georgiev Stefanov graduated in 2018 with a Master's degree in Pedagogy of Mathematics Education at the University of Plovdiv "Paisii Hilendarski". He has been working since 2019 at the National Investigation Service, Sofia as a programmer-forensic scientist and as an expert in the judicial system. The PhD student has been enrolled in full-time doctoral studies since 01.07.2020 at the Department of Informatics of FAMI by order of the Rector of the Technical University of Sofia No. 1581/23.06.2020. He passed from full-time to part-time doctoral studies on 01.01.2023 and was expelled with the right to defense from 01.01.2025. by order of the Rector of the Technical University of Sofia No. 48/ 09.01.2025.

The documents provided under the procedure fully comply with both the national requirements (the Law on the Development of the Academic Staff in the Republic of Bulgaria and the Regulations for its Implementation) and the requirements of the Technical University of Sofia (Regulations on the Terms and Conditions for Acquiring Scientific Degrees at the Technical University of Sofia (updated as of 19.10.2023).

2. Relevance of the problems developed in the dissertation and analysis of the content of the dissertation

The problems addressed in the dissertation are important for society and have a high degree of relevance in the field of digital forensics. The research done and the tasks solved are significant for the field of forensic science in scientific and applied terms.

The dissertation has a volume of 136 pages, and the following structure: introduction, five chapters, contributions, conclusion, literature used, publications on the topic of the dissertation, lists of figures and tables. Each of the chapters begins with an introduction and ends with a summary, contributions, and publications of the author related to the research in that chapter. In the dissertation, sufficient information and literature sources are studied and analysed (117). Many well-made figures (53) were used, which improved the understanding of the text, and the list of figures and 4 tables was applied in the dissertation.

In the introduction of the dissertation, the purpose of the research is presented, and four tasks are defined to achieve the goal. The first chapter discusses research and analysis of modern models, methods and techniques for the preparation of expertise in digital criminalistics. The basic concepts, bibliometric analysis of the models of digital forensic investigation, analysis of the current state and created conceptual model are presented. Chapter two describes the methodology for investigation in digital forensics from a practical point of view and the 12 phases of the methodology, as well as an improved model for acquiring digital evidence.

The third chapter presents the design of an intelligent information system with an integrated methodology to support investigations in digital forensics and the functional architecture of the system. The fourth chapter is dedicated to the use of machine learning and artificial intelligence (AI) in digital forensic investigation. Developed: framework and analysis through machine learning and AI techniques, classification of digital evidence, text analysis and image extraction from pdf files, large language models in pdf text summary. In the fifth chapter, a developed software prototype is presented and an assessment of the functionality of the software system for the purposes of digital forensics is made. Micro training has been done in a course on digital forensics and analysis of the opinion of experts in digital forensics.

The focus of research in the dissertation is the creation of methodology, the development of models and an intelligent information system using modern technologies such as machine learning and AI.

3. Degree of knowledge of the state of the problem, compliance of the research methodology with the set goals and objectives and credibility of the contributions of the dissertation

Based on the provided documents, it is evident that works in the field of forensics and has experience as an expert in the judicial system. He possesses a high professional degree of expertise and in-depth knowledge in the field of digital forensics and digital technologies. His competence, scientific and practical skills, and knowledge not only in the field of digital forensics but also in information technology have significantly aided the author in the selection

and development processes of the created methods and models. The combination of all these factors has contributed to better understanding and more successful problem-solving, ensuring that the chosen research methodology adequately aligns with the goals and objectives of the dissertation.

The studies, analyses, and developments within the work are based on a solid foundation of the author's scientific and practical knowledge, as well as the sources he has researched from other authors. This contributes to the accuracy of the analyses, conclusions, and evaluations, reflecting the credibility of the material on which the dissertation's contributions are built.

4. Scientific and Applied Contributions of the Dissertation

The dissertation presents credible results that can be categorized as scientific, scientifically-applied, and applied contributions.

The doctoral candidate has formulated and substantiated seven scientific and scientifically-applied contributions: 1. Conceptual model; 2. DFIP methodology; 3. Improved model for acquiring digital evidence; 4. Framework for applying artificial intelligence; 5. Classification model; 6. Model for exploring and extracting PDF files; 7. Sentiment analysis of PDF files. Additionally, the candidate has introduced two applied contributions: (1) an architectural model of a software system, and (2) a software prototype that automates activities in digital forensics. I fully support the conclusions made by the author regarding the achieved nine contributions.

These contributions include defining, substantiating, and proving existing scientific problems with new tools and technologies, as well as adapting and creating new approaches and methods in digital forensics. Such tools include the developed conceptual model and practical methodology for digital investigations—DFIP, comprising 12 phases—as well as the architectural model of a software system that integrates the DFIP methodology. Original approaches and solutions to problems include the improved model for acquiring digital evidence, the framework for applying AI techniques, the classification model for analyzing digital evidence, and other models and analyses involving artificial intelligence, machine learning, and deep learning.

The methods and models proposed by the author are fully justified and can be used in practice. Some of the results and contributions with scientific and applied significance in the field of digital forensics are suitable for implementation in institutions operating within this area (e.g., in the direct professional work of the candidate). Their significant practical relevance is evident, both for the work of forensic experts and for the judicial system when collaborating with expert witnesses. Each of these achievements demonstrates notable progress in the investigated field and showcases the potential for technology application in analyses and investigations in digital forensics.

The degree of the doctoral candidate's personal involvement in the research and contributions is undeniable. Without his high level of expertise on the topic and extensive practical experience, the achieved results and published works would not have been possible. The practical significance of the research, methods, and results in this direction is also evident from the opinions of competent specialists in the field of forensics (discussed in Chapter Three and attached at the end of the dissertation).

5. Assessment of Publications on the Dissertation

Eight publications related to the dissertation topic have been presented, fully meeting and even exceeding the minimum national requirements and necessary criteria. Five of the publications have been published in prestigious global journals, while three publications in proceedings from international conferences are in press. No plagiarism has been detected in the scientific works submitted for the competition.

Most of the journals where the publications have been published (or are in press) are indexed in Scopus and Web of Science, with one publication having an SJR ranking (Q4). All publications are co-authored and written in English.

Based on citations known to the author by other researchers and the opinions of professional forensic experts attached to the documents, it is evident that the candidate's publications, methods, and models have impact and significance in the field of digital forensics.

6. Utilization of the Dissertation Results in Scientific and Social Practice

The achieved results have scientific and practical significance, both in the field of digital forensics and for the work of expert witnesses in the judicial system, as well as for other applications.

The presence of a direct impact and the use of the developed methods by the doctoral candidate and his colleagues in their professional duties are demonstrated by the documents attached at the end of the dissertation, including opinions from competent specialists.

7. Evaluation of the Compliance of the Dissertation Summary with Requirements, and the Adequacy of Reflecting the Core Elements and Contributions of the Dissertation

General Information and Content of the Dissertation Summary: The provided summary spans a total of 32 pages (in Bulgarian). It includes an introduction, the chapters of the dissertation, a conclusion, the contributions, publications on the dissertation topic, and a summary (in English). A list of eight publications by the author on the dissertation topic has been presented, published in prestigious journals, fully meeting (and even exceeding) the minimum national requirements.

The summary synthesizes the dissertation clearly, logically, and comprehensibly. It addresses current issues in the field of digital forensics, the research objective, the tasks, a representative description of the dissertation's five main chapters, the solutions found, and the results achieved. Special attention is given to the developed methodology, the design of the intelligent information system, the use of machine learning and AI, and the report on scientific contributions.

Comparison and Conclusions:

- **Volume and Structure:** The summary is sufficiently detailed, well-written, and formatted in accordance with the requirements of the Law for the Development of the Academic Staff in the Republic of Bulgaria and the standards of TU-Sofia.
- **Compliance:** The structure and content of the summary strictly follow those of the dissertation, accurately reflecting its core elements and contributions. It provides a precise overview of the achievements of the doctoral candidate.
- **Scientific and Practical Relevance:** Clear and well-formulated solutions to the defined tasks with scientific and practical significance in digital forensics are presented. The candidate's scientific, applied, and practical contributions are explicitly highlighted.

In conclusion, the dissertation summary fully complies with the requirements and accurately reflects the dissertation's essence.

8. Opinions, Recommendations, and Notes

I have no significant remarks regarding the structure and content of the provided dissertation and dissertation summary.

Recommendations: The author could systematize and publish the conducted original research and obtained solutions in a consolidated monograph. Furthermore, the author is encouraged to continue pursuing scientific research in this relevant and timely academic field in the future.

Questions: Are there similar models in digital forensics abroad, and can the solutions presented in the dissertation be applied in other countries?

9. Conclusion

The problems examined in the dissertation are current and significant for the field of digital forensics. The dissertation is based on sufficient and well-sourced information and is written competently. The work is structured in compliance with the requirements of the Law for the Development of the Academic Staff in the Republic of Bulgaria, its associated regulations, and the rules for obtaining academic degrees at TU-Sofia (updated as of October 19, 2023).

The doctoral candidate has demonstrated their expertise and practical knowledge in the researched field by providing clear, precise, and concrete solutions to the defined tasks. The methodology developed and the achieved results have been presented in an understandable and logical manner. The publications in prestigious journals fully meet and even exceed the minimum national requirements for the professional field.

In conclusion, **I give a positive assessment of the dissertation and recommend that the scientific jury confer upon** M. Eng. Svetlin Georgiev Stefanov the educational and scientific degree of "Doctor" in the professional field 4.6 "Informatics and Computer Science" within the doctoral program "Informatics."

Date:

25.04.2025

REVIEWER:

/ Prof. Dr. Eng. Galina Bogdanova /