РЕЦЕНЗИЯ

за дисертационен труд за придобиване на образователна и научна степен „доктор“ в област на висше образование 4. Природни науки, математика и информатика, Професионално направление 4.6 Информатика и компютърни науки,
Специалност – Информатика

Автор на дисертационния труд: **Пламен Людмилов Спахиев**

Тема на дисертационния труд: **"Метод и проактивна система за анализ на големи данни за откриване на кибератаки с използване на изкуствен интелект"**

Рецензент: **проф. дн Пламенка Боровска**

1. Кратки биографични данни и данни за процедурата.

Пламен Людмилов Спахиев е роден на 25 октомври 1979 г. Завършва висшето си образование в Югозападния университет „Неофит Рилски“, където придобива степен „Магистър“ по Стопанско управление (2014–2016) и степен „Бакалавър“ в същата област (2011–2014). Средното си образование завършва в 9-та Френска езикова гимназия „А. дьо Ламартин“ в София. Професионалният му опит включва работа като асистент в Технически университет – София (от 2021 г. до сега) и като технически директор в iGaming.com Ltd. (от 2023 г. до сега). Работил е на различни технически и ръководни позиции в сферата на информационните технологии, включително в компании като КоректИТ България ООД, Линк Мобилити Девелопмент Хъб ООД и Проксиад България АД. Владее няколко чужди езика, сред които английски, френски, немски и руски.

Бил е задочен докторант във ФПМИ на ТУ-София в периода 2021-2025 година с научен ръководител доц. д-р. инж. Десислава Иванова.

След успешната вътрешна защита на дисертационния му труд в катедра Информатика на ФПМИ, ТУ-София (протокол 13/28.02.2025.) е стартирана процедура за защита със заповеди на Ректора на ТУ-София №ОЖ-4.6-11/10.03.2025г., заповед №ОЖ-4.6-13/ 18.03.2025г. и заповед № ОЖ-4.6-16/ 26.03.2025г.

2. Актуалност на разработвания в дисертационния труд проблем в научно и научно приложно отношение. Степен и нива на актуалността на проблема и конкретните задачи, разработени в дисертацията.

Фокусът на дисертационния труд е в областта на киберсигурността и използването на различни методи за Машинно обучение за анализ на големи масиви от данни, с цел откриване и превенция на кибератаки. В дисертационния труд е описан метод и базирана на него проактивна система за анализ на големи данни за ранно откриване на кибератаки с използване на изкуствен интелект. Основното предизвикателство е правилната подготовка на данните и внедряването на система, базирана на подобен метод, без тя да повлияе на правилното функциониране на останалите компоненти на информационно-технологичните системи.

Развитието на цифровите технологии и нарастващото използване на интернет и облачни услуги значително увеличават риска от кибератаки. В този контекст изкуственият интелект (ИИ) се очертава като ключов инструмент за разпознаване и предотвратяване на заплахи. Изследването е актуално и отговаря на реалните нужди на съвременната киберсигурност, като съчетава напреднали методи за машинно обучение със съвременни архитектурни принципи и алгоритми за анализ на данни.

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

Дисертационния труд обхваща 130 страници, състои се от три глави, заключение, кратко описание на приносите на дисертационния труд, списък с публикации, свързани с дисертационния труд, както и списък с използвана литература, съдържащ 108 източника.

Изчерпателният анализ на текущото състояние в областта киберсигурност, обзорът на различните видове атаки, векторите, по които те се изпълняват и методите за превенция от киберзаплахи направен в Първа глава, сравнителният анализ между различни видове алгоритми за Машинно обучение за обработка на големи масиви от табуларни данни, както и правилния подбор на технологии с цел практическо доказване на предложения метод, описан в Трета глава, показват задълбочените познания на дисертанта в изследваната област. Представени са основни тенденции за увеличение на използването на Изкуствен интелект при формирането на киберзаплахите, като е засегната и нуждата от реципрочни мерки. В резултат е обусловена необходимостта от изграждане на специализирана проактивна система, която да е в състояние да отговори адекватно на постоянно променящите се условия в защитата от кибератаки.

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

Основната цел на дисертационния труд е коректно формулирана, а именно създаването на метод, а в последствие и на реална проактивна система, базирана на него, за анализ на големи данни за откриване на кибератаки с използване на изкуствен интелект. За постигане на целите на дисертационния труд правилно са формулирани задачите, обхващащи (1) да се предложи оптимизиран метод за анализ на големи данни за откриване на кибератаки с използване на изкуствен интелект, (2) на негова база да бъде проектирана и създадена проактивна система за анализ на големи данни за откриване на кибератаки и (3) емпирично да бъдат доказани ползите от описания метод както и възможността за неговото практическо внедряване.

Избраната методика на изследване напълно отговаря на поставената цел и задачи на дисертационния труд и обхваща широк спектър от технологии и алгоритми за Машинно обучение като Дърво на решенията, Случайна гора и Логистична регресия. Допълнително са използвани похвати за балансиране на набора от данни, както и Генетични алгоритми с цел откриване на най-подходящите за конкретната цел хиперпараметри, използвани за конфигуриране на алгоритмите за машинно обучение.

5. Кратка аналитична характеристика на естеството и оценка на достоверността на материала, върху който се градят приносите на дисертационния труд.

Дисертационният труд е структуриран в логическа последователност в посока анализ на текущото състояние на изследваната област, методологии и технологии, техните предимства и недостатъци и по-нататъшното им развитие и надграждане за постигане на приносите на дисертационния труд. В първа глава е направен задълбочен анализ на текущото състояние на изследваната област, а именно скорошния пик в развитието на Изкуствения интелект, като е акцентирано върху нарастващата сложност на кибератаките и влиянието на Изкуствения интелект върху защитните механизми. Във втора глава е предложен метод за анализ на големи данни за откриване на кибератаки, основан на Машинно обучение. Методът се основава на идеята за двуслойна архитектура, която подобрява точността на детекция чрез поетапно обработване на входящите данни. В трета глава е представена архитектура на проактивна система за анализ на големи данни аз откриване на кибератаки, базирана на метода описан във втора глава. Архитектурата и се състои от двукомпонентна, трислойна структура, където първия компонент тренира моделите за МО, а втория ги прилага върху реални данни.

6. Научни и научноприложни приноси на дисертационния труд.

Оценявам като ***научно-приложен принос*** предложения метод за анализ на големи данни за откриване на кибератаки с използване на изкуствен интелект.

Предложената архитектура, както и практическото изпълнение на проактивна система за анализ на големи данни за откриване на кибератаки, базирана на предложения метод като **приложен принос**.

Приносите на дисертационния труд определям като доказване с нови средства на съществени нови страни в съществуващи научни проблеми и теории, методи на изследване, и получаване и доказване на нови факти. Характерът на приносите за внедряване определям като иновативни подходи и технологии.

Значимост на приносите за науката и практиката.

Резултатите от дисертационния труд са внедрени както следва:

На основа на предложения модел е изградена система за анализ на големи данни за откриване на кибератаки с използване на изкуствен интелект, послужила за практическо доказателство на ползите от модела.

7. Оценка на степента на личното участие на дисертанта в приносите.

Представеният дисертационен труд, научните публикации свързани с него и цялостната научно-изследователска и преподавателска дейност на дисертанта убедително показват, че получените резултати са изключително дело на Пламен Людмилов Спахиев.

8. Преценка на публикациите по дисертационния труд: брой, характер на изданията, в които са отпечатани.

Представени са данни за 3 публикации, свързани с изследванията в дисертационния труд, представени на 48, 49 и 50та Международна научна конференция „Приложения на математиката в инженерството и икономиката“ съответно в годините 2022, 2023 и 2024, първата публикувана в сборника към конференцията, останалите две в процес на публикация. Следователно, са изпълнени минималните изисквания за научната степен „доктор“ на Закона за развитието на академичния състав в Република България и Правилника за условията и реда за придобиване на научни степени в Технически университет – София в област на висше образование 4. Природни науки, математика и информатика, професионално направление 4.6 Информатика и компютърни науки.

9. Мнения, препоръки и бележки.

Дисертационният труд е изготвен прецизно в стройна логическа последователност. Изследваният проблем е социално значим, постигнати са значими приноси при научните изследвания. Резултатите практически внедрими.

10. Заключение с ясна положителна или отрицателна оценка на дисертационния труд.

В заключение, считам че дисертационният труд на тема ”Метод и проактивна система за анализ на големи данни за откриване на кибератаки с използване на изкуствен интелект“ с автор Пламен Людмилов Спахиев е изготвен прецизно и на високо професионално ниво, получените приноси от научно-приложен и приложен характер са значими, напълно са удовлетворени изискванията на Закона за развитието на академичния състав в Република България, както и на Правилника за условията и реда за придобиване на научни степени в Технически университет – София. Предлагам убедено на научното жури да присъди на Пламен Людмилов Спахиев образователната и научна степен „доктор” в област на висше образование 4. Природни науки, математика и информатика, професионално направление 4.6 Информатика и компютърни науки, специалност – Информатика.

Дата: 29.05.2025г., София

РЕЦЕНЗЕНТ:

(проф. дн Пламенка Боровска)

REVIEW

for PhD thesis for the acquisition of the educational and scientific degree "PhD" in the field of higher education 4. Natural Sciences, Mathematics and Informatics, Professional field 4.6 Informatics and Computer Sciences,
Specialty - Informatics

Author of the dissertation work: **Plamen Lyudmilov Spahiev**

Topic of the dissertation work: **"Method and Proactive System for Analyzing Big Data to Detect Cyberattacks Using Artificial Intelligence"**

Reviewer: **Prof. DSc Plamenka Borovska**

1. Brief biographical and procedural data.

Plamen Lyudmilov Spahiev was born on October 25, 1979. He graduated from the South-West University "Neofit Rilski", where he obtained a Master's degree in Business Administration (2014–2016) and a Bachelor's degree in the same field (2011–2014). He completed his secondary education at the 9th French Language High School "A. de Lamartine" in Sofia. His professional experience includes work as an assistant at the Technical University - Sofia (from 2021 to present) and as a technical director at iGaming.com Ltd. (from 2023 to present). He has been in various technical and management positions in the field of information technology, including companies such as CorrectIT Bulgaria OOD, Link Mobility Development Hub OOD and Proxyad Bulgaria AD. He is fluent in several foreign languages, including English, French, German and Russian.

He was a part-time doctoral student at the FPMI of TU-Sofia in the period 2021-2025 with scientific supervisor Prof. PhD Desislava Ivanova.

After the successful internal defense of his PhD thesis at the Department of Informatics of the FPMI, TU-Sofia (protocol 13/28.02.2025.), a defense procedure was launched with orders of the Rector of TU-Sofia No. ОЖ-4.6-11/10.03.2025, order No. ОЖ-4.6-13/ 18.03.2025 and order No. ОЖ-4.6-16/ 26.03.2025. I have been appointed as a member of the scientific jury by orders of the Rector of TU-Sofia as follows: №ОЖ-4.6-11/10.03.2025, №ОЖ-4.6-13/ 18.03.2025 and №ОЖ-4.6-16/ 26.03.2025.

2. Relevance of the problem developed in the PhD thesis in scientific and scientifically applied terms. Degree and levels of relevance of the problem and specific tasks developed in the dissertation.

The focus of the dissertation is in the field of cybersecurity and the use of various Machine Learning methods for analyzing large data sets, in order to detect and prevent cyberattacks. The dissertation describes a method and a proactive system for analyzing Big data based on it for early detection of cyberattacks using artificial intelligence. The main challenge is the correct

preprocessing of the data and the implementation of a system based on such a method, without it affecting the proper functioning of the other components of the information technology systems.

The development of digital technologies and the increasing use of the Internet and cloud services significantly increase the risk of cyberattacks. In this context, artificial intelligence (AI) has emerged as a key tool for recognizing and preventing threats. The research is relevant and meets the real needs of modern cybersecurity, combining advanced machine learning methods with modern architectural principles and data analysis algorithms.

3. Degree of knowledge of the state of the problem and creative interpretation of the literary material.

The dissertation covers 130 pages, consists of three chapters, a conclusion, a brief description of the contributions of the thesis, a list of publications related to the dissertation, as well as a list of used literature, containing 108 sources.

The comprehensive analysis of the current state in the field of cybersecurity, the overview of different types of attacks, the vectors by which they are implemented and the methods for preventing cyber threats made in the First Chapter, the comparative analysis between different types of Machine Learning algorithms for processing large arrays of tabular data, as well as the correct selection of technologies for the purpose of practical demonstration of the proposed method, described in the Third Chapter, show the in-depth knowledge of the PhD candidate in the researched area. The main trends for increasing the use of Artificial Intelligence in the formation of cyber threats are presented, and the need for reciprocal measures is also touched upon. As a result, the need to build a specialized proactive system that is able to adequately respond to the constantly changing conditions in cyberattack protection has arisen.

4. Compliance of the selected research methodology with the set goal and tasks of the thesis.

The main goal of the dissertation is correctly formulated, namely the creation of a method, and subsequently a real proactive system based on it, for analyzing big data for detecting cyberattacks using artificial intelligence. To achieve the goals of the dissertation, the tasks have been correctly formulated, covering (1) to propose an optimized method for analyzing Big data for detecting cyberattacks using artificial intelligence, (2) on its basis to design and create a proactive system for analyzing Big data for detecting cyberattacks and (3) to empirically prove the benefits of the described method as well as the possibility of its practical implementation.

The selected research methodology fully meets the set of goal and tasks of the thesis and covers a wide range of technologies and algorithms for Machine Learning such as Decision Tree, Random Forest and Logistic Regression. Additionally, techniques for balancing the dataset were used, as well as Genetic Algorithms to discover the most suitable hyperparameters for the specific purpose, used to configure the machine learning algorithms.

5. Brief analytical characterization of the nature and assessment of the credibility of the material on which the contributions of the dissertation are built.

The thesis is structured in a logical sequence towards an analysis of the current state of the research area, methodologies and technologies, their advantages and disadvantages and their further development and upgrading to achieve the contributions of the thesis. In the first chapter, an in-depth analysis of the current state of the research area is made, namely the recent peak in the development of Artificial Intelligence, with an emphasis on the increasing complexity of cyberattacks and the influence of Artificial Intelligence on protective mechanisms. In the second chapter, a method for analyzing Big data for detecting cyberattacks, based on Machine Learning, is proposed. The method is based on the idea of a two-layer architecture that improves the accuracy of detection through step-by-step processing of input data. In the third chapter, an architecture of a proactive system for analyzing Big data for detecting cyberattacks, based on the method described in the second chapter, is presented. Its architecture consists of a two-component, three-layer structure, where the first component trains the MO models and the second applies them to real data.

6. Scientific and applied scientific contributions of the dissertation work.

I evaluate as a ***scientific-applied contribution*** the proposed method for analyzing Big data for detecting cyberattacks using artificial intelligence.

The proposed architecture, as well as the practical implementation of a proactive system for analyzing big data for detecting cyberattacks, based on the proposed method, as an ***applied contribution***.

I define the contributions of the dissertation work as proving with new means significant new aspects in existing scientific problems and theories, research methods, and obtaining and proving new facts. I define the nature of the contributions for implementation as innovative approaches and technologies.

Significance of contributions to science and practice.

The results of the thesis are implemented as follows:

Based on the proposed model, a system for analyzing Big data to detect cyberattacks using artificial intelligence was built, which served as practical proof of the benefits of the model.

7. Assessment of the degree of the dissertation candidate's personal participation in the contributions.

The presented dissertation work, the scientific publications related to it and the overall scientific research and teaching activities of the dissertation candidate convincingly show that the results obtained are exclusively the work of Plamen Lyudmilov Spahiev.

8. Assessment of publications on the dissertation: number, nature of the editions in which they were printed.

Data are presented for 3 publications related to the research in the thesis, presented at the 48th, 49th and 50th International Scientific Conference "Applications of Mathematics in Engineering

and Economics" in the years 2022, 2023 and 2024 respectively, the first one published in the conference proceedings, the other two in the process of publication. Therefore, the minimum requirements for the scientific degree "PhD" of the Act on the Development of the Academic Staff in the Republic of Bulgaria and the Regulations on the Terms and Procedure for Acquiring Scientific Degrees at the Technical University - Sofia in the field of higher education 4. Natural Sciences, Mathematics and Informatics, professional field 4.6 Informatics and Computer Science are met.

9. Opinions, recommendations and notes.

The thesis is prepared precisely in a coherent logical sequence. The problem under study is socially significant, significant contributions to scientific research have been achieved. The results are practically implementable.

10. Conclusion with a clear positive or negative assessment of the dissertation.

In conclusion, I believe that the thesis on the topic "Method and proactive system for analyzing big data for detecting cyberattacks using artificial intelligence" with author Plamen Lyudmilov Spahiev has been prepared precisely and at a high professional level, the contributions received of a scientific-applied and applied nature are significant, the requirements of the Act on the Development of Academic Staff in the Republic of Bulgaria, as well as the Regulations on the Terms and Procedure for Acquiring Scientific Degrees at the Technical University - Sofia, have been fully met. I strongly suggest to the scientific jury to award Plamen Lyudmilov Spahiev the educational and scientific degree of "PhD" in the field of higher education 4. Natural Sciences, Mathematics and Informatics, professional field 4.6 Informatics and Computer Sciences, specialty - Informatics.

Date: May 29th, 2025

Sofia

REVIEWER:

(Prof. Plamenka Borovska)