С Т А Н О В И Щ Е

върху дисертационен труд за придобиване на образователна и научна степен „**доктор**”

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**

Член на научното жури: **Доц. д-р Анна Розева** съгласно заповеди **ОЖ-4.6-11/10.03.2025г., ОЖ-4.6-13/ 18.03.2025г. и ОЖ-4.6-16/ 26.03.2025г.**

1. **Актуалност** на разработвания в дисертационния труд проблем и задачи. Обект на изследване в дисертационния труд са киберзаплахи и механизми за защита и предотвратяване на нанасяне на потенциални вреди и щети. В съвременния непрекъснато дигитализиращ се свят актуалността на изследвания и решения за своевременното откриване на злонамерени атаки към софтуерна и информационна инфраструктура и за прилагане на адекватни мерки за минимализиране на вредите от тях, са безспорно актуални. Факт е ежедневното генериране на големи обеми данни в интернет и средства за съхраняването им, както и на развитието и усъвършенстването на технологията изкуствен интелект за обработка на тези големи данни за анализ, откриване на полезни закономерности и прогнозиране на бъдещо поведение. Така методите на изкуствения интелект съдействат за подобряване ефективността на мерките за киберсигурност и интегрирането им в бизнес и административна софтуерна инфраструктура. В този смисъл изследванията, свързани със задачите в дисертационния труд са актуални и с потенциал за получаване на полезни и значими резултати.

2. **Степен на познаване** състоянието на проблема и творческа интерпретация на литературния материал. В дисертационния труд е включена библиография от повече от сто източника. Те са изцяло свързани с изследваната проблематика на киберсигурност, изкуствен интелект, машинно обучени модели и съответен набор от алгоритми. Направеният в началните глави обзор на представената литература показва натрупани знания в изследваните области и налични към момента решения на проблемите, които са във фокуса на изложението. Съдържанието на следващите глави, свързано с проектиране архитектурата на проактивна система за откриване на кибератаки, обосновката на структурата и функционалността на отделните компоненти, както и самото й изграждане и верификация показват креативност при интерпретацията на литературните източници.

3. **Съответствие на избраната методика** на изследване и поставената цел и задачи на дисертационния труд с постигнатите приноси. За постигане на поставената в дисертацията цел за изграждане на система за киберсигурност основана на прилагане на машинно обучени модели е използвана класическа методика, която осигурява реализацията на жизнения цикъл на система с методи на изкуствен интелект.

Предложени са иновативни решения по отношение на потока данни за обучение и функционалност на съответните модули в архитектурата, както и на използване на специфичен тип алгоритми за определяне на подходящи хиперпараметри за настройка на точността. Реализацията на изградената система и нейната верификация с конкретни получени резултати доказват правилността на избора на методиката за изследване и проектиране.

4. **Научни и/или научноприложни приноси** на дисертационния труд: Дисертационният труд съдържа научноприложни и приложни приноси. Считам за основен **научноприложен** принос предложената многослойна архитектура на изгражданата система с модулен характер, която включва вложени слоеве и използване на прогнозирани резултати от първия слой за обучение на модела в следващия. Така се гарантира неразпознати образци да бъдат подложени на последваща класификация, което повишава ефективността на проактивната система за откриване на атаки. Друг принос е свързан с използването на генетичен алгоритъм за откриване на подходящите хиперпараметри за настройка на модела. **Приложни** (приноси за внедряване): Софтуерната система за верификация на предложения метод.

Получената като принос архитектура с машинно обучени модели е с потенциал да допринесе за развитието на изследванията в така важната област на постигане на киберсигурност с използване на методи на изкуствен интелект.

5. **Преценка на публикациите** по дисертационния труд. Представени са 3 публикации, от които две са в AIP Conference Proceedings с SJR и са индексирани в Scopus. Третата е в процес на публикуване, за което е представено потвърждение. Те съдържат основните резултати, изложени в отделните глави на дисертационния труд. Не са отчетени цитирания на тези публикации от други автори.

6. **Мнения, препоръки и бележки**. Кандидатът е навлязъл успешно в проблематиката на киберсигурността и е намерил творческо решение на приложението на изкуствен интелект за откриване на кибератаки. В дисертацията липсва ясно дефиниране на задачи за изследване, те са дадени само в автореферата. Неправилно е използван терминът претоварване за “overfitting”. Приноси 1 и 3 могат да се обединят в метод за проективна система. Би могло да се представят конкретни резултати от прилагането на генетичен алгоритъм за откритите подходящи хиперпараметри. Обзорната глава би могло да бъде по-непосредствено ориентирана към съществуващи решения на изследвания проблем, за сметка на описания на използвани алгоритми за обучение на модели. Бележките и препоръките целят подпомагане и насочване на кандидата в бъдещи изследвания.

7. **Заключение.** Оценката ми за представения дисертационен труд е **положителна**. Приносите са лично дело на кандидата и покриват изискванията на образователна и научна степен. Препоръчвам на **Пламен Людмилов Спахиев** да бъде присъдена степен „доктор“ в професионално направление 4.6 Информатика и компютърни науки.

Дата: 22.05.2025 Член на журито:

OPINION

on a thesis for acquiring a **PhD** degree

Thesis author: **Plamen Ljudmilov Spahiev**

Thesis theme: **Method and proactive system for analyzing big data for discovering cyberattacks by means of artificial intelligence**

Jury member: **Assoc. Prof. Anna Rozeva, PhD**

1. **Actuality** of the investigated problem and tasks. Research focus of the thesis are cyberattacks and mechanisms for protection and prevention of potential harm and losses. In a continuously digitalizing world, the actuality of performing research and finding solutions of on time discovery of harmful attacks to any software and information infrastructure and the application of adequate actions for eliminating or minimizing the eventual losses due to the attacks are doubtlessly actual. Obvious fact is the daily generation of enormous amounts of various data in the internet and means for their storage, as well as the development and refinement of the artificial intelligence technology for manipulating these big data for explorative analysis, pattern discovery and forecasting future behavior. In this way the artificial intelligence methods provide for improving the efficacy of cybersecurity measures and their integration in business and public administrative software infrastructure. In this context the investigations on the tasks of the research goal are actual and have the potential for obtaining useful and valuable results.
2. **Acquaintance** with the problem's state of the art and creative interpretation of the surveyed literature. The bibliography included in the thesis contains more than hundred sources. They are closely related to cybersecurity, artificial intelligence, machine learnt models and respective algorithms for training the models as research topics. The literary survey presented in the initial chapters reveals the knowledge acquired by the candidate on the research areas state of the art as well as on solutions to the investigated problems that are currently available. The content of the next chapters addresses the design of an architecture of a proactive system for cyberattacks discovery, the justification of the structure and functionality of its components and finally the development and test of the system present the author's creativity when interpreting the literature sources.

3. **Compliance of the implemented research methodology and the research goal and tasks to the contributions claimed.** For the achievement of the thesis goal, i.e. the design of a cybersecurity system by implementing machine learnt models, a classic methodology has been implemented which enables the realization of the lifecycle of a system involving artificial intelligence functionality. Within the methodology implementation innovative solutions have been proposed concerning the training data flow, the functionality of the modules of the architecture and the implementation of specific algorithms for determining the most suitable

hyperparameters for tuning the models. The development of the system according to the selected methodology and the obtained results during the testing prove its suitability and sound basis for accomplishing the research goal.

4. **Scientific and/or scientific and application contributions of the thesis**: The thesis has achieved **scientific and application value contributions**. The basic scientific and application value contribution I consider is the multilayer modular architecture of the designed system involving nested layers and use of predictions of the initial layer for training the model at the next layer. In this way it will be guaranteed that unrecognized inputs will be subjected to further classifications, which raises the efficacy of the proactive system to discover cyberattacks. Another contribution refers to the implementation of a genetic algorithm for discovering the most appropriate hyperparameters for model tuning. **Contribution with application value:** The developed system for testing the proposed model and architecture.

The architecture implementing machine learnt models claimed as a contribution has the potential for facilitating the research in the challenging area of enhancing cybersecurity by means of artificial intelligence methods and solutions.

5. **Evaluation of the publications on the thesis**. In relation to the thesis a list of three publications has been presented. Two of them have been published in AIP Conference Proceedings, an edition with SJR and they are indexed in Scopus. The third one has been accepted for publications for which an acceptance letter has been provided. All of them contain the main results described in the thesis chapters. No citations by other authors have been observed so far.

6. **Overall impression, recommendations, remarks**. The candidate has become adequately involved in the basic cybersecurity problems and has elaborated a creative solution of artificial intelligence application for attacks discovery. The thesis lacks precise formulation of research tasks, they have been mentioned in the summary only. The Bulgarian translation of “overfitting” is incorrect. Contributions 1 and 3 could be generalized as method for a proactive system. The explicit presentation of results from the application of the genetic algorithm for hyperparameter selection would add value to the thesis content. The literature review could be more closely oriented to analysis of existing solutions to the investigated problem than to descriptions of used algorithms for model training. These remarks and recommendations aim to guide and support the candidate in future research work.

7. **Conclusion.** My opinion of the thesis is **positive**. The claimed contributions have been achieved by the candidate himself and they satisfy the requirements for acquiring an educational and scientific degree. Therefore, I recommend **Plamen Ljudmilov Spahiev** to be awarded a PhD degree in Professional area 4.6. Informatics and Computer Science.

Date: 22.05.2025 Jury member: