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: **проф. д-р Татяна Атанасова**

1. **Актуалност на разработвания в дисертационния труд проблем в научно и научноприложно отношение**.

Бъдещите развития в пространството на киберсигурността не могат да бъдат разглеждани без участието на изкуствения интелект за усъвършенствано откриване на заплахи, проактивна защита срещу евентуални атаки и по-нататъшна автоматизация на процесите при реагиране на нежелани инциденти. Възприемането на изкуствения интелект като ключов фактор за подобряване на киберсигурността и адаптиране към променящите се враждебни стратегии определя актуалността и значението на тази дисертация в научен и приложен план. Анализът на големи данни за откриване на кибератаки с помощта на изкуствен интелект и машинно обучение, предложен в тази дисертация, е несъмнено необходим за изграждането на автономни и адаптивни защитни системи.

2. **Степен на познаване състоянието на проблема и творческа интерпретация на литературния материал.**

Дисертационният труд е съставен от 3 глави в общ обем от 129 страници, със списък от 108 литературни източници и уеб адреси.

Очертани са перспективите за развитие на киберсигурността с използване на изкуствен интелект и са разгледани етапите от механизмите за кибератаки, вариращи от пасивно събиране на информация до активни действия. Представена е схема и общи характеристики на най-популярните видове кибератаки. Щетите от кибератаките са класифицирани по категории и последици. Особено внимание е обърнато на социалното инженерство и неговите техники, както и на видовете зловреден софтуер.

Направен е преглед на технологиите и решенията, свързани с откриване на кибератаки и предотвратяване на проникванията. Извършен е кратък анализ на IDS и IPS системите и най-разпространените антивирусни програми. Изследвано е текущото състояние на киберсигурността от различни страни с акцент върху нарастващата сложност на кибератаките. Подчертава се двойствената роля на ИИ като инструмент за защита и средство за атака. Като ефективно решение за многослойна защита на мрежите и устройствата се посочва комбинацията от IDS, IPS и антивирусни решения.

3. **Съответствие на избраната методика на изследване и поставената цел и задачи на дисертационния труд с постигнатите приноси.**

Целта на дисертацията е да предложи и валидира метод за анализ на големи данни за откриване на кибератаки с помощта на изкуствен интелект. За постигане на тази цел са

посочени изисквания за изграждане на проактивна система за откриване на кибератаки, използваща бинарна класификация.

След направения анализ на класическите алгоритми за машинно обучение е предложен метод за откриване на кибератаки чрез поетапно обработване на данните. Реалната имплементация на разработения метод е реализирана с предложената софтуерна архитектура на компонентна модулна система. Експерименталните изследвания демонстрират подобрение в точността спрямо традиционните методи чрез многостепенно анализиране на данните и оптимизиране на моделите.

4. **Научни и/или научноприложни приноси на дисертационния труд.**

Приемам и оценявам положително научно-приложните приноси, формулирани в дисертацията. Основните приноси в дисертационния труд могат да се отнесат към обогатяване на съществуващите знания, създаване на нови методи на изследване и приложение на научни постижения в практиката. Считам, че постигнатите резултати са лично дело на докторанта под вещото ръководство на научния ръководител.

5. **Преценка на публикациите по дисертационния труд.**

По дисертационния труд са представени 3 публикации в платформата на AIP Conference Proceedings, реферирани и индексирани в Scopus и Web of Sciences. Всички публикации са в съавторство с научния ръководител, като докторантът е на първо място. Общият брой точки по показател Г7 от минимални национални изисквания надхвърля изискуемия минимум от 30 точки. Публикациите отразяват резултатите от изследванията в дисертацията, с което е демонстрирана необходимата публичност на постигнатите резултати пред научната общност.

6. **Мнения, препоръки и бележки.**

Нямам съществени забележки, които да оспорят основните научноприложни приноси на дисертационния труд, с изключение на няколко от редакционен и технически характер. Получени са резултати, които се отличават със значима практическа важност.

7. **Заключение с ясна положителна или отрицателна оценка на дисертационния труд.**

Считам, че представеният дисертационен труд отговаря на изискванията на Закона за развитието на академичния състав в Република България, Правилника за неговото прилагане, а също така и на Правилника за условията и реда за придобиване на научни степени в Технически университет - София за получаването на образователна и научна степен ДОКТОР. Постигнатите резултати ми дават основание да дам положителна оценка и препоръчвам на почитаемото Научно жури да присъди образователната и научна степен „Доктор“ на маг. Пламен Людмилов Спахиев в професионално направление 4.6 „Информатика и компютърни науки“ по научна специалност „Информатика“.

Дата: 27.05.2025 **ЧЛЕН НА ЖУРИТО:**

/проф. д-р Татяна Атанасова/

O P I N I O N

on a dissertation for the acquisition of an educational and scientific degree "Doctor"

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

Dissertation topic: **Method and proactive system for big data analysis for detecting cyberattacks using artificial intelligence**

Member of the Scientific Jury: **Prof. Dr. Tatiana Atanasova**

1. **Actuality of the problem developed in the dissertation in scientific and applied terms**.

Future developments in the cybersecurity space cannot be considered without the involvement of artificial intelligence for advanced threat detection, proactive protection against possible attacks and further automation of processes in responding to unwanted incidents. The perception of artificial intelligence as a key factor in improving cybersecurity and adapting to changing hostile strategies determines the relevance and importance of this dissertation in scientific and applied terms. The analysis of big data to detect cyberattacks using artificial intelligence and machine learning, proposed in this dissertation, is undoubtedly necessary for the construction of autonomous and adaptive defense systems.

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

The dissertation is composed of 3 chapters in a total volume of 129 pages, with a list of 108 literature sources and web addresses.

The prospects for the development of cybersecurity using artificial intelligence are outlined and the stages of cyberattack mechanisms, ranging from passive information collection to active actions, are considered. A scheme and general characteristics of the most popular types of cyberattacks are presented. The damage from cyberattacks is classified by categories and consequences. Particular attention is paid to social engineering and its techniques, as well as the types of malwares.

An overview of technologies and solutions related to the detection of cyberattacks and the prevention of intrusions is made. A brief analysis of IDS and IPS systems and the most common antivirus programs is performed. The current state of cybersecurity from different countries is examined with an emphasis on the increasing complexity of cyberattacks. It highlights the dual role of AI as a tool of protection and a means of attack. As an effective solution for multi-layer protection of networks and devices, the combination of IDS, IPS and antivirus solutions is indicated.

3. **Compliance of the chosen research methodology and the set goals and objectives of the dissertation with the achieved contributions.**

The purpose of the dissertation is to propose and validate a method for analyzing big data to detect cyberattacks using artificial intelligence. To achieve this goal, requirements are specified for the construction of a proactive system for detecting cyberattacks using binary classification.

After the analysis of the classical machine learning algorithms, a method for detecting cyberattacks by step-by-step data processing is proposed. The actual implementation of the developed method is realized with the proposed software architecture of a component modular system. Experimental studies have demonstrated an improvement in accuracy over traditional methods through multi-level data analysis and model optimization.

4. **Scientific and/or scientifically applied contributions of the dissertation.**

I accept and evaluate positively the scientific and applied contributions formulated in the dissertation. The main contributions to the dissertation can be attributed to the enrichment of existing knowledge, the creation of new research methods and the application of scientific achievements in practice. I believe that the results achieved are a personal work of the PhD student under the expert guidance of the supervisor.

5. **Evaluation of the publications on the dissertation.**

The dissertation presents 3 publications in the AIP Conference Proceedings platform, refereed and indexed in Scopus and Web of Sciences. All publications are co-authored with the supervisor, with the PhD student in the first place. The total number of points under indicator D7 of minimum national requirements exceeds the required minimum of 30 points. The publications reflect the results of the research in the dissertation, which demonstrates the necessary publicity of the achieved results to the scientific community.

6. **Notes, recommendations and remarks.**

I have no significant remarks that would dispute the main scientific and applied contributions of the dissertation, with the exception of a few of editorial and technical nature. Results of essential practical importance have been obtained.

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

I believe that the submitted dissertation meets the requirements of the Act on the Development of the Academic Staff in the Republic of Bulgaria, the Regulations for its implementation, as well as the Regulations on the terms and conditions for acquiring scientific degrees at the Technical University of Sofia for obtaining the educational and scientific degree of DOCTOR. The achieved results give me grounds to give a positive assessment and I recommend to the honorable Scientific Jury to award the educational and scientific degree "Doctor" to MSc. Plamen Lyudmilov Spahiev in the professional field 4.6 "Informatics and Computer Science" in the scientific specialty "Informatics".

Date: 27.05.2025 **JURY MEMBER:**

/Prof. Dr. Tatiana Atanasova/