ФКСТЧ4 – НС1 – 076
13.01.2026 г.

РЕЦЕНЗИЯ

върху дисертационен труд

за придобиване на образователна и научна степен "**доктор**"

Автор на дисертационния труд: **маг. инж. Гроздан Костадинов Христов**

Тема на дисертационния труд:

„Методи и алгоритми за машинно обучение в киберсигурността "

Рецензент: **проф. д-р Милена Кирилова Лазарова–Мицева**

катедра Компютърни системи, ФКСТ, Технически университет–София

Настоящата рецензия е изготвена в качеството ми на член на научно жури, назначено със Заповед № ОЖ–5.3–58/30.10.2025 г. на Ректора на Технически университет–София и протокол от първо заседание на научното жури от 12.11.2025 г.

Докторантът маг. инж. Гроздан Костадинов Христов е зачислен в задочна докторантура по докторска програма „Системи с изкуствен интелект" в професионално направление 5.3 Комуникационна и компютърна техника към катедра „Компютърни системи" във Факултет по Компютърни системи и технологии при Технически университет–София на 1.03.2022 г. Докторантът е изпълнил индивидуалния си план и е положил всички изпити от докторантския минимум. Отчислен е с право на защита на 21.10.2025 г. с решение на ФС на ФКСТ (Протокол №11/21.10.2025 г.). По предложение на Катедрения съвет на катедра „Компютърни системи" (Протокол №2/20.10.2025 г.) с решение на Факултетния съвет на ФКСТ (Протокол №2/21.10.2025 г.) е взето решение за разкриване на процедура за публична защита на дисертационния му труд.

1. Актуалност на разработвания в дисертационния труд проблем в научно и научно-приложно отношение

Представеният дисертационен труд е насочен към изследване на актуална и динамично развиваща се област свързана с използването на методи и алгоритми от машинното обучение за анализ, класификация и предотвратяване на кибератаки. Актуалността на разглеждания проблем произтича от нарастващата зависимост на съвременното общество от информационните и комуникационните технологии и съпътстващото я увеличение на честотата и сложността на кибератаките. В условията на глобална дигитализация традиционните подходи за осигуряване на киберсигурност се оказват недостатъчни за своевременно откриване и неутрализиране на заплахите. Това обуславя необходимостта от прилагане на интелигентни методи базирани на машинно обучение, които позволяват автоматизирано разпознаване, класификация и адаптивна реакция при инциденти. В този контекст изследването в дисертационния труд представлява актуална и значима научна и приложна задача с висока практическа стойност.

Целта на дисертационния труд е да се проучат методи и алгоритми за класифицикация на зловредни файлове към хакерски групи/индивиди свързани с пробиви в киберсигурността. Във връзка с формулираната цел на дисертационния труд и на базата на анализ на текущото състояние на проблемната област са формулирани конкретни задачи за постигане на поставената цел: (1) Да се проучат и изследват

възможностите за прилагане на методи на машинното обучение при анализ на инциденти с киберсигурността за решаване на класификационни задачи за присвояване на зловредни файлове към различни хакерски групи; (2) Да се определят характеристики, които адекватно отразяват обективните зависимости от класификационния статус; (3) Да се предложи и оптимизира модел за решаване на класификационната задача, който да се приложи модел за определяне на класификационния статус на анализираните артефакти; (4) Да се проведе експериментален анализ за приложение на предложения модел на базата, на който да се оценят неговите възможности. Определянето на целта и конкретните задачи, свързани с постигането ѝ, са обосновани от автора коректно и изчерпателно.

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

Дисертационният труд обхваща тематика, която включва необходимост от познаване съвременното състояние на предметните области машинно обучение и киберсигурност, както и на особеностите на съществуващите методи и алгоритми за машинно обучение и спецификата на приложението им за решаване на класификационни задачи в областта на киберсигурността. Авторът коректно интерпретира основните тенденции и ограничения на традиционните подходи за защита и ги съпоставя с възможностите, които предоставят интелигентните алгоритми за анализ и класификация на киберинциденти. Литературното проучване е в основата на формулираната цел и свързаните с нея задачи за постигането ѝ. Библиографската справка по дисертационния труд съдържа общо 110 източника, в това число 67 Интернет адреса. На базата на направения литературен обзор и сравнителен анализ на релевантната научна литература са очертани ключовите предизвикателства при автоматизираното откриване и атрибутиране на кибератаки, което позволява ясно позициониране на изследването в актуален научен контекст. Литературните източници са систематизирани и творчески интерпретирани чрез извеждане на обективни зависимости между характеристиките на зловредните артефакти и тяхната принадлежност към конкретни хакерски групи. Това показва аналитичен подход и способност за критична оценка и надграждане на съществуващите научни резултати, което придава на изследването оригиналност и висока научна стойност.

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

Избраната методика за провеждане на научните изследвания се базира на системен сравнителен анализ на особеностите и различните аспекти на разглежданата тематична област, на основата на който е направен обоснован избор на методи и средства за решаване на поставените задачи. Предложените, разработени и изследвани подходи, методи и алгоритми се основават на аргументиран избор, теоретична обосновка, експериментална оценка и верификация на възможностите за практическото им използване, което осигурява не само постигане на целта на дисертацията, но позволява обективна оценка на предложените решения и постигнатите резултати. Методически дисертационният труд е логически последователен и адекватен по отношение на избраната и приложена методика на провеждане на научните изследвания, което обуславя успешно изпълнение на поставените цел и задачи на дисертационния труд.

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

Представеният дисертационен труд е структуриран в увод, четири глави, заключение, списък с приноси по дисертационния труд, списък с публикации по дисертационния труд с посочени цитирания, списък с участие в научно-изследователски проекти, списък с фигури, списък с таблици, списък с използвани съкращения, библиографска справка на използваните литературни източници и едно приложение с програмен код. Общият обем на дисертационния труд е 148 страници. Дисертационният труд съдържа 21 фигури и 8 таблици. Цитирани са 110 литературни източника, в това число 5 на български език, останалите на английски език, от които 67 Интернет адреса.

Първа глава представя изследване и анализ на съвременните тенденции и заплахи в киберпространството, разглежда основните типове кибератаки и взаимовръзката между изкуствения интелект и киберсигурността, като очертава актуалните предизвикателства в областта. Втора глава е посветена на анализа на APT (Advanced Persistent Threat) хакерските групи и на видовете методи на изкуствения интелект, използвани при анализа на зловредни файлове. Описани са подходите за подбор, обработка и подготовка на обучителните множества от данни. Трета глава представя разработването на модел за машинно обучение за класификация на зловредни файлове основан на алгоритъма Random Forest. Представени са класификационните характеристики, архитектурата на експерименталния прототип и приложението му към реални системи в сферата на образованието. Четвърта глава включва анализ и оценка на резултатите от експериментално валидиране, сравнение с други съществуващи решения и обсъждане на практическата приложимост на предложения модел като завършва с изводи относно неговата ефективност и възможности за бъдещо развитие.

От представеното изложение, формулираната цел на дисертационните изследвания и поставените във връзка с нея задачи, както и използваните средства за реализиране на целта, може да се направи заключение, че докторантът добре познава състоянието на разглежданите проблеми. Съдържанието на отделните глави показва логическа последователност и методологична обоснованост – от анализа на съвременните заплахи и концептуалните взаимовръзки между изкуствения интелект и киберсигурността, през систематизиране на знанията за APT групите и методите за обработка на данни, до разработване и експериментална валидация на авторски модел за класификация. Това позволява извеждането на приноси, основани както на утвърдени научни концепции, така и на емпирично проверими резултати. Достоверността на използвания материал се подкрепя от прилагането на утвърдени алгоритми за машинно обучение, използването на реални набори данни и сравнителен анализ с други съществуващи решения. Това ми дава основание да определя получените резултати и свързаните с тях приноси като достоверни и практически полезни.

5. Научни и/или научноприложни приноси на дисертационния труд

Приемам формулираните от автора приноси, постигнати в резултат на извършените научни изследвания. Приносите могат да се отнесат към категориите обогатяване на съществуващо научно знание и научни постижения в практиката, както и създаване на

нови и модифициране на съществуващи методи, подходи, модели и алгоритми за решаване на поставените в дисертационния труд задачи.

На базата на получените в дисертационната работа резултати постигнатите приноси могат да бъдат систематизирани като научни, научно-приложни и приложни както следва:

- ***научни приноси:***
  - Предложен е модел базиран на класификатор Random Forest за присвояване на клас на принадлежност на зловреден код към определена държава, спонсорираща дейности и развитие на хакерски групи, насочени срещу комуникационна и информационна инфраструктура на други държави и/или организации;
- ***научно-приложни приноси:***
  - Предложено е използването на таксономия за извършване на прецизиращи процедури при обработката на данни свързани със зловреден код, хакерски групи и спонсориращи държави, избрана на базата на проучване на международни практики в класифицирането на хакерски групи и определянето на инциденти в киберсигурността;
  - Предложено е използването на оценъчни техники за оптимизация на класификационните характеристики и избор на хиперпараметри за класификатора Random Forest, които оценяват свръх представяне на извадките за малцинствените класове и намаляване на коефициента на представяне на извадките за свръх представените класове;
- ***приложни приноси:***
  - Разработен е експериментален прототип, използващ предложения модел с класификатор Random Forest, който реализира автоматизиран процес по класифициране на характеристики на файлове, съдържащи зловреден код към определение хакерски групи и/или спонсориращи държави и улеснява дейностите за анализ и оценка на експерти по киберсигурност;
  - Предложеният модел е експериментално оценен с използване на разработения експериментален прототип за валидиране на възможностите на модела за подобряване на класификацията на файлове и улесняването на работата на експерти по киберсигурност.

6. Оценка за степента на личното участие на дисертанта в приносите

Представеното съдържание и структура на дисертационния труд показват отличното познаване на третираната проблематика от страна на докторанта. Една от петте научни статии публикувани във връзка с дисертацията е самостоятелна, а останалите са в съавторство с неговите научни ръководители, като в две от тях докторантът е първи автор. Представените материали по дисертационния труд и публикациите към него правят добро впечатление за научната работа на маг. инж. Гроздан Христов, която се характеризира с аналитична задълбоченост и прецизност. Считам, че личния му принос при постигане на представените научни резултати и приноси е безспорен.

7. Преценка на публикациите по дисертационния труд

Получените от автора резултати от дисертационното изследване са публикувани в 5 научни статии. Една от статиите е публикувана в научно списание (International Journal of Innovative Research and Scientific Studies), а другите четири са докладвани на научни конференции, проведени в България (2023 International Scientific Conference on Computer Science, Youth Scientific Conference „Machines Innovation and Technology", 2020 International Scientific Conference Computer Science, 2023 31st National Conference with International Participation „TELECOM"). Публикациите са направени в периода 2020–2025 година и покриват тематиката на представената дисертационна работа като отразяват основните постигнати резултати и приноси. Всички статии са на английски език. Една от статиите е самостоятелна, останалите са в съавторство с научните ръководители на докторанта. Две от публикациите са индексирани в Scopus и имат общо 4 цитирания, в това число в 3 статии индексирани в Scopus.

8. Използване на резултатите от дисертационния труд в научната практика

Във връзка с научните изследвания по дисертационния труд докторантът е участвал в научно-изследователски проект, финансиран от ФНИ към МОН.

Не са представени данни за пряко практическо използване на получените резултати от научните изследвания в дисертационния труд, но считам, че получените резултати имат съществен практически потенциал за приложение в системите за киберсигурност.

Разработеният модел за класификация на зловредни файлове може да бъде внедрен в съвременни системи за откриване и предотвратяване на кибератаки, антивирусни решения и платформи за анализ на зловреден код, както и да се използва за подпомагане на работата на специализирани центрове и екипи по кибер отбрана. Разработеното решение има потенциал за използване за образователни и изследователски цели, както и за създаване на интелигентни адаптивни защитни системи, повишаващи устойчивостта на цифровите инфраструктури.

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

Авторефератът към дисертацията съответства на дисертационния труд – вярно и точно отразява целите, задачите, съдържанието по глави, постигнатите приноси. Авторефератът е подготвен и оформен съгласно изискванията за изготвянето му и считам, че безспорно носи същностните черти на дисертационния труд, като отразява в адекватен обем и по коректен начин неговото съдържание.

10. Мнения, препоръки и бележки

Нямам забележки към представения дисертационен труд. Направените забележки при запознаването ми с версията на дисертационния труд, представена за предварително обсъждане в катедрата, са взети под внимание и са отразени в представената дисертация. Към дисертационния труд имам техническа забележка по отношение пълното и точно библиографско описание на литературните източници с използването на единен стил.

Дисертационният труд показва голям обем на извършените научни изследвания. Той е оформен внимателно и старателно с високо ниво на представяне на научните изследвания и свидетелства за отлично запознаване на автора с предметната област, илюстрира задълбоченост на извършените научни изследвания и дава възможност за развитието им и практическото им използване.

Препоръките ми към докторанта са да продължи научните си изследвания по темата на дисертационния труд и да насочи усилията си към внедряване на разработените алгоритми и модели в практиката с цел постигане на преки приложни резултати.

Към докторанта имам следните въпроси:

1. До колко използваните източници на данни и методите за тяхната подготовка осигуряват представителност и устойчивост на резултатите, получени при експерименталната валидация на предложения модел?

2. Какво е влиянието на използваните техники за балансиране на класовете върху точността и надеждността на модела с класификатор Random Forest?

3. В каква степен използваната методология за оптимизация на хиперпараметри гарантира обобщаващата способност и практическата приложимост на предложения модел при реални сценарии за анализ на киберинциденти?

11. Заключение

На основание на изложеното считам, че дисертационния труд отговаря на изискванията на Закона за развитие на академичния състав в Република България, на Правилника за прилагане на закона и съответния правилник на Технически университет–София и на изискванията за придобиване на образователната и научна степен „доктор". Проведените научни изследвания са в актуална област и третират проблематика, която е обект на засилен изследователски интерес. Авторът е постигнал поставените цели и задачи в дисертационния труд. Получените резултати съдържат научни, научно-приложни и приложни приноси, които са значими, действително са получени и са негово дело. Съществените приноси на дисертационния труд са отразени в научни публикации, които са адекватно разпространени и направени достояние на заинтересованата научна общност чрез публикуването им в научни доклади на конференции и статии в научни списания.

Ето защо давам своята положителна оценка на представения дисертационен труд и предлагам на уважаемите членове на Научното жури да бъде присъдена образователната и научна степен „доктор" на **маг. инж. Гроздан Костадинов Христов** по научна специалност „Системи с изкуствен интелект" в професионално направление 5.3 Комуникационна и компютърна техника.

12.01.2026 г.

Рецензент:
/ проф. д-р Милена Лазарова–Мицева /

REVIEW

on a dissertation for "Doctor of Philosophy" degree

Author of the dissertation: **MSc. Eng. Grozdan Kostadinov Hristov**

Title of the dissertation:

"Methods and algorithms from machine learning in cybersecurity"

Reviewer: **Prof. Milena Kirilova Lazarova–Mitseva**, PhD

Dept. Computer Systems, FCST, Technical University of Sofia

This review is prepared in my capacity as a member of the Scientific Jury appointed by Order № ОЖ-5.3-58/30.10.2025 of the Rector of the Technical University of Sofia and Protocol No.1/12.11.2025 from the first meeting of the Scientific Jury.

MSc. Eng. Grozdan Kostadinov Hristov was enrolled as a part-time PhD student in doctoral program "Artificial Intelligence Systems", professional field 5.3 Communication and Computer Engineering" at the Department "Computer Systems" of the Faculty of Computer Systems and Technologies at The Technical University of Sofia on 1.09.2021. The PhD student has fulfilled all the requirements in the individual plan of his PhD study and has successfully passed all the required exams. He was discharged as a PhD with the right to defend his thesis on 21.10.2025 by decision of the Faculty Council of the Faculty of Computer Systems and Technologies (Protocol №11/21.10.2025). The procedure for the public defence of his dissertation has started by a decision of the Department Council of the Department of Computer Systems (Protocol №2/20.10.2025) and the Faculty Council of the Faculty of Computer Science and Technology (Protocol №2/21.10.2025).

1. Relevance of the dissertation topic in scientific and applied aspects

This dissertation addresses a contemporary and dynamically developing field related to the use of machine learning methods and algorithms for analyzing, classifying, and preventing cyberattacks. The relevance of the problem under consideration stems from the growing dependence of modern society on information and communication technologies and the accompanying increase in the frequency and complexity of cyber attacks. In the context of global digitalization, traditional approaches for ensuring cybersecurity are proving insufficient for the timely detection and neutralization of threats. This necessitates the application of intelligent methods based on machine learning that enable automated recognition, classification and adaptive response to incidents. In this context the research in the dissertation represents an important and significant scientific and applied task with high practical value.

The aim of the dissertation is to study methods and algorithms for classifying malicious files associated with hacker groups/individuals involved in cybersecurity breaches. Based on the analysis of the current state of the art in the problem area several research tasks are defined related to the dissertation aim: (1) To investigate the possibilities for applying machine learning methods in the analysis of cybersecurity incidents to solve classification tasks for assigning malicious files to different hacker groups; (2) To determine features that adequately reflect the objective dependencies on the classification status; (3) To propose

and optimize a model for solving the classification task and to apply it in order to determine the classification status of the analyzed artefacts; (4) To conduct an experimental analysis of the proposed model, based on which its capabilities will be evaluated. The dissertation aim and the objectives related to its achievement are correctly and thoroughly formulated and defined.

2. Degree of knowledge on the dissertation topic and constructive interpretation of the bibliography

The research in the dissertation covers topics that include the need to understand the current state of the subject areas of machine learning and cybersecurity as well as the characteristics of the existing machine learning methods and algorithms and the specifics of their application for solving classification tasks in the field of cybersecurity. The author correctly interprets the main trends and limitations of the traditional protection approaches and compares them with the possibilities offered by intelligent algorithms for the analysis and classification of cyber incidents. The literature review is the basis for the stated dissertation aim and the objectives related to its achievement. The bibliographic reference of the dissertation contains a total of 110 sources, including 67 Internet addresses. Based on the literature review and comparative analysis of the relevant scientific literature sources, the key challenges in the automated detection and attribution of cyber attacks are outlined that allows for a clear positioning of the research in the current scientific context. The literature sources are systematized and creatively interpreted by drawing objective connections between the features of malicious artefacts and their affiliation with specific hacker groups. This demonstrates an analytical approach and the author's ability to critically evaluate and build solutions on the existing scientific results which gives the research originality and high scientific value.

3. Consistency of the used research methodology with the dissertation aim and objectives

The chosen methodology for conducting the research study is based on systematic comparative analysis of the features and the different aspects of the research field under consideration. On that basis consistent decisions and selection of methods, algorithms and means are made for solving the dissertation tasks and objectives. The proposed, developed, and investigated approaches, methods, and algorithms are based on well-reasoned decisions, theoretical justification, experimental evaluation, verification and validation of the possibilities of their practical utilization which ensures not only the achievement of the dissertation goals but also the allows objective evaluation of the proposed solutions and the achieved contributions. Methodologically the dissertation is logically consistent and adequate in terms of the chosen and applied methodology of conducting research which determines the successful achievement of the goals and tasks set in the dissertation.

4. Brief analytical characteristic of the dissertation and assessment of the reliability of the material on which the contributions of the dissertation are built

The presented dissertation is structured in an introduction, four chapters, a conclusion, a list of contributions, a list of publications on the dissertation with citations of the publications on the dissertation, a list of participation of the PhD student in research projects, a list of figures, a list of tables, a list of used abbreviations and terms a list of bibliographic references of the used literature sources and one appendix with program code. The

dissertation has 148 pages. The dissertation comprises 21 figures and 8 tables. The list of cited bibliographic references comprises 110 sources, including 5 references in Bulgarian, the rest in English, 67 of them are Internet addresses.

The first chapter presents a study and analysis of the current trends and threats in cyberspace, examines the main types of cyberattacks and the interrelations between artificial intelligence and cybersecurity outlining the current challenges in the field. The second chapter is devoted to the analysis of APT (Advanced Persistent Threat) hacker groups and the types of artificial intelligence methods used in the analysis of malicious files. Several approaches for the selection, processing and preparation of training data sets are described. The third chapter presents the development of a machine learning model for the classification of malicious files based on the Random Forest algorithm. The classification features, the architecture of the experimental prototype and its application to real systems in the field of education are presented. The fourth chapter comprises an analysis and evaluation of the results of experimental validation, a comparison with other existing solutions and a discussion of the practical applicability of the proposed model resolving with conclusions about its effectiveness and possibilities for future development.

Based on the dissertation content, the formulated dissertation aim and the research objectives defined in the dissertation as well as the means used for their accomplishment, a conclusion can be made that MSc. Eng. Grozdan Hristov is well aware of the state of the art of the scientific topics under consideration. The content of the individual chapters shows logical consistency and methodological soundness – from the analysis of contemporary threats and the conceptual interrelations between artificial intelligence and cybersecurity, through the systematization of knowledge about APT groups and data processing methods, to the development and experimental validation of an author's classification model. This allows for contributions based on both established scientific concepts and empirically verifiable results. The reliability of the material used is supported by the application of established machine learning algorithms, the use of real data sets, and comparative analysis with other existing solutions. This gives me reason to consider the results obtained and the related contributions to be reliable and practically useful.

5. Scientific and applied contributions of the dissertation

I accept the research contributions formulated by the author in his dissertation as a result of the research carried out. The contributions can be related to enrichment of the existing scientific knowledge and scientific achievements in practice as well as development of new and modification of existing approaches, methods, models and algorithms for their application for solving the problems investigated in the dissertation.

On the base of the results obtained in the dissertation the contributions of the dissertation can be classified as scientific, applied-scientific and applied as follows:

- ***scientific contributions:***
  - A model based on a Random Forest classifier is proposed for assigning a class of malicious code belonging to a specific country that sponsors activities and the development of hacker groups targeting the communications and information infrastructure of other countries and/or organizations;

- ***applied-scientific contributions:***
  - Utilization of a taxonomy is proposed in order to perform refinement procedures when processing data related to malicious code, hacker groups and sponsoring countries, selected on the basis of a study of international practices in the classification of hacker groups and the identification of cybersecurity incidents;
  - Utilization of evaluation techniques is proposed in order to optimize the classification features and the selection of hyperparameters for the Random Forest classifier, which evaluate the over-representation of samples for minority classes and reduce the representation coefficient of samples for over-represented classes;
- ***applied contributions:***
  - An experimental prototype is developed using the proposed model based on a Random Forest classifier that implements an automated process for classifying the features of files containing malicious code to specific hacker groups and/or sponsoring countries and facilitates the analysis and assessment activities of cybersecurity experts;
  - The proposed model is experimentally evaluated using the developed experimental prototype to validate the model's capabilities for improving the file classification and facilitating the work of cybersecurity experts.

6. Assessment of the extent of author's personal participation in the dissertation contributions

The presented content and the structure of the dissertation reveals the author's excellent comprehension on the dissertation topic and the presented field of study. One out of the five research papers published in connection with the research presented in the dissertation is single authored by the applicant and the others are co-authored with his scientific supervisors, in two of which the PhD student is the first author. The presented dissertation and the research papers on its topic make a good impression of the scientific work of MSc. Eng. Grozdan Hristov which is characterized by analytical thoroughness and precision. His personal contribution to the achievement of the presented scientific results and contributions is undoubted.

7. Evaluation of the author's publications on the dissertation's topic

The results of the dissertation research obtained by the author have been published in 5 scientific papers. One of the papers is published in an international scientific journal (International Journal of Innovative Research and Scientific Studies) and the other four papers are presented at scientific conferences held in Bulgaria (2023 International Scientific Conference on Computer Science, Youth Scientific Conference „Machines Innovation and Technology", 2020 International Scientific Conference Computer Science, 2023 31st National Conference with International Participation „TELECOM"). The publications are made in the period 2020–2025 and cover the topics of the presented dissertation reflecting the main achieved results and contributions. All papers are in English. One of the papers is single authored by the PhD student and the others are co-authored with his scientific supervisors. Two of the publications are indexed in Scopus and have a total of 4 citations by foreign authors, including 3 citations in papers indexed in Scopus.

8. Utilization of the dissertation's results and contributions in scientific and social practice

In connection with the research in the dissertation, the PhD student participated in a scientific project funded by the National Science Fund at the Ministry of Education and Science.

No data on the direct practical application of the results obtained from the scientific research in the dissertation has been presented, but I believe that the results obtained have significant practical potential for application in cybersecurity systems.

The developed model for classification of malicious files can be implemented in modern systems for detecting and preventing cyber attacks, antivirus solutions and platforms for analyzing malicious code as well as used to support the work of specialized cyber defence centers and teams. The developed solution has the potential to also be used for educational and research purposes as well as for creating intelligent adaptive defence systems that increase the resilience of digital infrastructures.

9. Assessment of the compliance of dissertation's autoreferat with the requirements for its preparation as well as its accurate presentation of the dissertation's content and contributions

The dissertation's autoreferat corresponds to the dissertation thesis – correctly and accurately reflects the dissertation aims and objectives, the content by chapters and the research contributions achieved. The autoreferat is prepared and formatted in accordance with the requirements and I consider that it presents the essential features of the dissertation reflecting in an adequate volume and in a correct manner its content.

10. Comments, recommendations and remarks

I have no comments on the presented dissertation. The comments I made on the version of the thesis submitted for preliminary discussion in the department are taken into account and are reflected in the submitted thesis. I only have a technical remark to the dissertation regarding the complete and accurate bibliographic description of the references using a uniform style.

The dissertation presented for a review reveals a large amount of research studies carried out, demonstrates the author's excellent research comprehension on the addressed scientific problems, reveals the thoroughness of the research carried out and provides an opportunity for its further development and practical utilization.

I would recommend the author to continue his research on the dissertation topic and to focus his efforts towards the implementation of the developed algorithms and models in practice in order to achieve direct applied results.

I have the following questions for the PhD student:

1. How do the data sources used and the methods for their preparation ensure the representativeness and sustainability of the results obtained in the experimental validation of the proposed model?

2. What is the impact of the used class balancing techniques on the accuracy and reliability of the Random Forest classifier model?

3. To what extent do the used methodology for hyperparameter optimization guarantee the generalizability and practical applicability of the proposed model in real-world cyber incident analysis scenarios?

11. Conclusion

Based on the above said I consider the dissertation presented for review in the procedure for awarding the "Doctor of Philosophy" degree as fully corresponding to and fulfilling all the requirements of the Act on the Academic Staff Development in Republic of Bulgaria and the Regulations governing the application of the Act as well as the Regulations for the application of the Act in the Technical University of Sofia. The dissertation topic falls in a relevant scientific field subject to intensive research studies. The author fulfilled the dissertation goals and the objectives. The results obtained contain scientific and applied contributions that are significant for both science and practice and are achieved by the applicant himself. The contributions of the dissertation are published in scientific papers that are adequately disseminated and made available to the international scientific community through presentation and publication in research conference proceedings.

Therefore I am convinced of my positive assessment of the dissertation presented and propose to the honourable members of the Scientific Jury **MSc. Eng Grozdan Kostadinov Hristov** to be awarded a "Doctor of Philosophy" degree in the professional field 5.3 "Communication and Computer Engineering", scientific specialty "Artificial Intelligence Systems".

Date: 12.01.2026

REVIEWER:

/ Prof. Milena Lazarova-Mitseva, PhD /