ФКСТЧЧ- Вх1-076
16.12.2025г.

ТЕХНИЧЕСКИ УНИВЕРСИТЕТ ФКСТ СОФИЯ

РЕЦЕНЗИЯ

на дисертационен труд за получаване на образователна и научна степен " доктор " на тема:
"Методи и алгоритми за машинно обучение в киберсигурността"
Професионално направление: 5.3" Комуникационна и компютърна техника"
научна специалност: "Системи с изкуствен интелект"

Автор: маг.инж. Гроздан Костадинов Христов
от проф. д-р Нина Василевна Синягина

1. ОБЩИ ПОЛОЖЕНИЯ

Текстът на дисертационния труд включва 147 страници текст, фигури, таблици, графици и диаграми и се състои от увод, 4 глави, заключение, списък с публикации, свързани с дисертацията, списък с приносите, списък на използваната литература, декларация за оригиналност, приложение и списък за участие в научни-изследователските проекти. Цитираната литература включва над 100 източника на английски и български език.

2. АКТУАЛНОСТ НА ПРОБЛЕМА

Темата на дисертацията *е* ***Методи и алгоритми за машинно обучение в Киберсигурността.*** По тази тематика се работи интиензивно в целия свят.

През последните десетилетия сферата на комуникационни и информационни технологии претърпяват бурно развитие. Един от важните проблеми е сигурността на използваните информационни системи. Основната тежест от установяване на зловредните действия и последващото им ограничаване се пада върху експертите по киберсигурност, които са натоварени със задачата да анализират и класифицират настъпилите инциденти. За повишване ефективността на тяхната работа в последните години започват да се използват методи и подходи на изкуствения интелект. Предлагането и разработването на нови ефективни начини с използване на изкуствен интелект е много важна и сложна задач.

Предмет на дисертационния труд е ефективното използване на класификационни алгоритми и софтуерни приложения, осигуряващи защита на комуникационн и информационни системи от кибератаки. Считам, че темата на дисертацията е **актуална.**

3. АНАЛИЗ НА ДИСЕРТАЦИОННИЯ ТРУД

Авторът поставя следната цел на своето изследване
Проучване на различни методи, алгоритми и подходи от изкуствения интелект за класифициране на зловредни файлове, свързани с пробиви в киберсигурността, в резултат на което да бъде предложено софтуерно решение за ефективното им класифициране.
За реализиране на поставената цел са формулирани следните конкретни задачи :
1. ***Изследване на възможността за прилагане на методи на машинно обучение при анализа на инциденти с киберсигурността, като основната им функция е решаване на задача за класификация на зловредните файлове, свързани с различни хакерски групи.***
2. ***Определяне на харктеристики, които адекватно отразяват обективните зависимости от класификационния статус.***

3. ***Разработка на оптимален модел за класификационната задача.***
4. ***Провеждане на експериментален анализ на разработеното приложение.***

В **първата глава** е изложено направеното проучване за съвременното състояние на проблема. Извършен е анализ на тенденциите и заплахите в киберпространството и взаимовръзката им със сферата на изкуствения интелект.

Във **втората глава** е представено изследване на видовете методи на изкуствен интелект, свързани с анализа на зловредните файлове, като е избрано и подготвено множеството данни, приложими за обучение.

Третата глава е посветена на изследвания, свързани с определяне на класификационни характеристики, като е представен нов подход към използване на метода Random Forest за отнасяне на зловредни файлове към определени хакерски групи и/или свързани с тях държави. Описано е създаденото софтуерно приложение, демонстриращо функциониране на избрания метод за машинно обучение при класификация на APT зловредни файлове, използвани при кибератаки.

В четвъртата глава е представен извършеният анализ на предложения модел и степен на полезност по отношение на бъдещата му употреба в реални ситуации, наблюдавани в практиката.

В **Заключението** е направен кратък анализ на направените изследвания и са дадени насоки за бъдещото развитие на проблемите.

4. СТЕПЕН НА ПОЗНАВАНЕ НА ПРОБЛЕМА

Докторантът е направил много задълбочен обзор на съвременното състояние на проблематиката, свързана с *Машинно обучение в киберсигурността*
Считам, че избраните методи и методики за изследване съответстват на поставената цел и конкретните задачи, свързани с целта.

5. ЛИЧНОТО УЧАСТИЕ

Анализ на дисертационния труд и представения списък на публикации, свързани с дисертационния труд ми дава основание да направя заключение, че авторът познава много добре състоянието на проблема, и нямам никакво основание да се съмнявам в личното му участие в проведените изследвания и в написване на дисертацията.

6. ПУБЛИКАЦИИ, СВЪРЗАНИ С ДИСЕРТАЦИЯТА

Представен е списък на публикации, свързани с дисертацията , който включва 5 наименования. В три публикации докторантът е посочен на първо място. Четири публикации са в сборници от международни конференции, а една е статия в " International Jourrnal.of Innovative Research and Scientific Studies ".

За две публикации има три цитирания. Трябва да се отбележи и участие на маг.-инж Гроздан Христов в научно-изследователслите проекти.

7. АВТОРЕФЕРАТ

Авторефератът е написан съгласно изискванията. Съдържанието му изяснява актуалността на тематиката на дисертацията, формулира основната цел и задачи на изследването и отразява постигнатите резултати.

8. НАУЧНО-ПРИЛОЖНИ И ПРИЛОЖНИ ПРИНОСИ

След анализа на проведените изследвания и получените резултати считам, че те могат да бъдат обобщени по следния начин:

За Научна-приложни се приемат

- Предложен е модел на система за класификация на злонамерен код, базиран на класификатор Random Forest за присвояване на този код към определена държава, спонсорираща дейността на хакерски групи, насочени срещу комуникационна и информационна инфраструктура на други държави и/или организации.

- Предложено е използване на таксономия за извършване на процедури по обработка на данни, свързани със зловреден код, хакерски групи и спонсориращи държави чрез проучване на международни практики.

- Предложени са оценъчни техники за оптимизация на класификационни характеристики при избора на хиперпараметри за класификатора Random Forest.

. За ***Приложни*** се приемат:

- Разработен е експериментален прототип на базата на предложения модел с класификатор Random Forest, който реализира автоматизиран процес по класифициране на файлове, съдържащи зловреден код.

- Извършена е експериментална оценка на предложения модел с цел възможните подобрения на класификацията на файлове и улесняването на работата на експертите по киберсигурност.

9. ЗАБЕЛЕЖКИ И ПРЕПОРЪКИ ПО ДИСЕРТАЦИОННИЯ ТРУД

Имам редица забележки, които открих в процеса на преглеждането на дисертацията:

- В дисертацията се описват много подробно известните неща. В резултат на това се получава дисбаланс на дисертационния труд - обзорът заема значителна част от общия обем. Би било по-добре да бъде обърнато повече внимание на собствените изследвания.

- За съжаление, дисертантът не обърнал достатъчно внимание на моите забележки в предварителното мнение:

1/ Заглавието на дисертацията не съвсем точно отразява същността на проведеното изследване,т.к. би могло да се разбере, че той претендира върху новите методи на машинното обучение, а не на тяхното използване в киберсигурността.

2/ Цитиранията не са направени в общоприетия вид, липсва номерация на източници, което затруднява сравняване на текста и съответната литература.

- Дисертантът оперира доста произволно по отношение на терминологията. Например, за термина "данни" се използват понятия "сурови", :"нови ""поглъщане " и др., което не е общоприето и понякога представляват не много удачен превод от английски.

- Не се посочват ясно в много места на текста личните приноси на дисертанта.

- Имам редица редакционни и стилови забележки, които отразяват грешки, пропуски и неточности, но които не намаляват важността на дисертацията.

10. ЗАКЛЮЧЕНИЕ

В представения дисертационен труд се съдържат нови и оригинални идеи, които могат да се използват за създаване на нови модели за машинно обучение в киберсигурността.

Докторантът показва задълбочени познания в изследваната област, за което говори както дългият списък на използваната литература, така и собствените публикации.

Като цяло дисертационният труд е изпълнен на добро професионално ниво и отговаря на изискванията за получаване на образователната и научната степен "**доктор** ".

Имайки предвид изложеното, предлагам на почитаемото Научно жури при ТУ- София да вземе решение за присвояване на маг. инж. Гроздан Костадинов Христов образователната и научна степен **доктор** по научно направление 5.3 „ Комуникационна и компютърна техника", научна специалност „Системи с изкуствен интелект".

15.12.2025 год. Подпис:

/ проф. д-р Нина Синягина/

REVIEW

of a dissertation for the award of the educational and scientific degree "Doctor," entitled:
"Methods and algorithms for machine learning in cybersecurity"
Professional field: 5.3 "Communication and Computer Engineering"
Scientific specialty: "Systems with artificial intelligence"

Author: M.Sc. Grozdan Kostadinov Hristov
Reviewer: Prof. Dr. Nina Sinyagina

1. GENERAL REMARKS

The dissertation comprises 147 pages of text, figures, tables, charts, and diagrams. It consists of an introduction, 4 chapters, a closing list of publications related to the dissertation, a list of contributions, a list of used literature, a declaration of originality, an appendix and a list of participation in the necessary research projects. The cited literature includes over 100 sources in English and Bulgarian.

2. RELEVANCE OF THE TOPIC

The topic of the dissertation is Machine Learning Methods and Algorithms in Cybersecurity. This topic is being worked on intensively all over the world.
In recent decades, the field of communication and information technologies has undergone rapid development. One of the important problems is the security of the information systems used. The main burden of identifying malicious actions and subsequently limiting them falls on cybersecurity experts, who are tasked with analyzing and classifying the incidents that have occurred. To increase the efficiency of their work, in recent years, artificial intelligence methods and approaches have begun to be used. Proposing and developing new effective ways using artificial intelligence is a very important and complex task.
The subject of the dissertation is the effective use of classification algorithms and software applications that provide protection of communication and information systems from cyberattacks. I believe that the topic of the dissertation is relevant.

3. ANALYSIS OF THE DISSERTATION

The author sets the following goal for his research:
Investigating various methods, algorithms and artificial intelligence approaches for classifying malicious files related to cybersecurity breaches, as a result of which a software solution for their effective classification will be proposed.
To achieve the set goal, the following specific tasks have been formulated:
1. Researching the possibility of applying machine learning methods in the analysis of cybersecurity incidents, with their main function being to solve the task of classifying malicious files associated with various hacker groups
2. Determination of characteristics that adequately reflect the objective dependencies on the classification status
3. Development of an optimal model for the classification task
4. Conducting experimental analysis of the developed application
The first chapter presents a study of the current state of the problem. An analysis of trends and threats in cyberspace and their relationship with the field of artificial intelligence is carried out.

The second chapter presents a study of the types of artificial intelligence methods related to the analysis of malicious files, selecting and preparing the set of data applicable for training.
The third chapter is dedicated to research related to determining classification characteristics, presenting a new approach to using the Random Forest method to attribute malicious files to certain hacker groups and/or countries associated with them. The created software application is described, demonstrating the functioning of the selected machine learning method in classifying APT malicious files used in cyberattacks.
The fourth chapter presents the analysis of the proposed model and the degree of usefulness in terms of its future use in real situations observed in practice.
The Conclusion provides a brief analysis of the research conducted and provides guidelines for the future development of the problems.

4. DEGREE OF FAMILIARITY WITH THE PROBLEM

The PhD student has made a very thorough overview of the current state of the issues related to Machine Learning in Cybersecurity
I believe that the selected methods and research methodologies correspond to the set goal and the specific tasks related to the goal.

5. PERSONAL INVOLVEMENT

An analysis of the dissertation and the presented list of publications related to the dissertation gives me reason to conclude that the author knows the state of the problem very well, and I have no reason to doubt his personal participation in the research conducted and in writing the dissertation.

6. PUBLICATIONS RELATED TO THE DISSERTATION

A list of publications related to the dissertation is presented, which includes 5 articles. In three articles the PhD student is listed first. Four publications are in proceedings of international conferences and one is an article in the "International Journal of Innovative Research and Scientific Studies".
There are three citations for two publications. It should also be noted the participation of M.Eng. Grozdan Hristov in scientific research projects.

7. AUTHOR'S ABSTRACT

The abstract is written according to the requirements. Its content clarifies the relevance of the dissertation topic, formulates the main goal and objectives of the research, and reflects the achieved results.

8. SCIENTIFIC-APPLIED AND APPLIED CONTRIBUTIONS

Following analysis of the studies conducted and the results obtained, I believe they can be summarized as follows:

Scientific-applied contributions:

A model of a malicious code classification system based on a Random Forest classifier is proposed to assign this code to a specific country sponsoring the activities of hacker groups targeting the communication and information infrastructure of other countries and/or organizations.

The use of a taxonomy has been proposed to perform data processing procedures related to malicious code, hacker groups and sponsoring states by studying international practices.

Estimation techniques for optimizing classification features in the selection of hyperparameters for the Random Forest classifier are proposed.

Applied contributions:

An experimental prototype based on the proposed model with a Random Forest classifier has been developed, which implements an automated process for classifying files containing malicious code.

An experimental evaluation of the proposed model was performed with the aim of making improvements in file classification and facilitating the work of cybersecurity experts.

9. REMARKS AND RECOMMENDATIONS REGARDING THE DISSERTATION

I have a number of remarks discovered during my review of the dissertation:

The dissertation describes in great detail what is known. As a result, the dissertation work is unbalanced - the review takes up a significant part of the total volume. It would be better to pay more attention to one's own research.
Unfortunately, the dissertation author did not pay sufficient attention to my remarks in the preliminary opinion:

The title of the dissertation does not quite accurately reflect the essence of the research conducted, as it could be understood that it claims new machine learning methods, and not their use in cybersecurity.
The citations are not made in the generally accepted form, there is no numbering of sources, which makes it difficult to compare the text and the relevant literature.

The dissertationist operates quite arbitrarily in terms of terminology. For example, for the term “data” the terms “raw”, “new”, “absorption”, etc. are used, which is not generally accepted and sometimes represents a not very good translation from English.
The personal contributions of the dissertation candidate are not clearly stated in many places in the text

I have various editorial and stylistic remarks that reflect errors, omissions, and inaccuracies; however, these do not diminish the importance of the dissertation.

10. CONCLUSION

The dissertation presented contains new and original ideas that can be used to develop models for authentication in web systems. The doctoral candidate has demonstrated a deep knowledge of the field under study, as evidenced both by the extensive list of references used and by his own publications. Overall, the dissertation is executed at a good professional level and meets the requirements for the award of the educational and scientific degree “Doctor.”

In view of the above, I propose that the esteemed Academic Jury of TU–Sofia decide to confer upon M.Sc. Eng. Grozdan Kostadinov Hristov the educational and scie]ntific degree Doctor in Professional Field 5.3 “Communication and Computer Engineering”, scientific specialty “Systems with artificial intelligence.”

15.12.2025 Signature:

/ Prof. Dr. Nina Sinyagina /