ФКСТ44-НС1-076
13.01.2026г.

ТЕХНИЧЕСКИ УНИВЕРСИТЕТ ФКСТ СОФИЯ

С Т А Н О В И Щ Е

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**

Член на научното жури: **проф. д-р инж. Александър Богданов Бекярски**

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

Научната област, свързана с машинното обучение и изкуствения интелект, е особено актуална и свързана с почти всички дейности на човека. В настоящата дисертация тази актуалност се отнася до научната област киберсигурност, в която машинното обучение има първостепенно значение при решаване на проблеми на сигурността, както в компютърните системи, така и в широка гама от области изискващи висока степен на сигурност и защита от кибератаки.

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

Реална представа и обосновка за научното ниво или степен на познаване състоянието на проблема и съответна творческа интерпретация на литературния материал може да се формира на базата на изложението в Глава 1 на дисертационния труд. В тази глава, на базата на многобройни и актуални в настоящия момент научни публикации, е извършен обстоен преглед и е направен анализ на съществуващите методи и средства за приложението на машинно обучение в сферата на киберсигурността. Използваните при анализа и включени в библиографията към дисертацията 111 литературни източници на латиница, кирилица и интернет адреси, са изцяло научни публикации, доклади и статии от реномирани списания, издания от международни конференции и източници от сайтове в Интернет, с имена на достатъчен на брой автори като водещи, изтъкнати в настоящия момент и близкото минало, чужди и наши учени и специалисти в областта на машинното обучение и изкуствения интелект.

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

От напълно основателно дефинираната значимост и необходимост в научно и научно-приложно отношение от изследване в областта на приложението на машинното обучение следва обосноваността на целите и

задачите в дисертационния труд. Докторантът много точно и конкретно е формулирал целта и задачите в своя дисертационен труд.

Основната цел на настоящия дисертационен труд е проучване на методи и алгоритми, свързани с киберсигурността, въз основа на което да се предложи софтуерно решение, на базата на метод с изкуствен интелект за класифициране на зловредни файлове, за да се улесни техния първичен и вторичен анализ.

За изпълнението на тази цел, са формулирани **следните задачи**:

- да се проучи и изследва възможността за прилагане на методи на машинното обучение при анализа на инциденти с киберсигурността, с цел решаване на задача за класификация, която да е в помощ на експертите по киберсигурност в присвояване на зловредни файлове и методология на работа към различни хакерски групи;
- да се намерят характеристики, които адекватно да отразяват обективните зависимости от класификационния статус;
- да се предложи и оптимизира модел за решаване на класификационната задача и да се приложи този модел за определяне на класификационния статус на анализираните артефакти;
- да се направи експериментален анализ за приложение на предложения модел, на базата на който да се преценят неговите възможности.

4. Научни и/или научноприложни приноси на дисертационния труд

В дисертационния труд са представени 1 научен, 2 научно-приложни и 2 приложни приноси, както следва:

Научно приноси:

- предложен е модел базиран на Random Forest класификатор 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 екперти по киберсигурност.

5. Преценка на публикациите по дисертационния труд

Основните постижения в дисертационния труд са популяризирани в 5 научни публикации в съавторство с научните ръководители, в престижни научни конференции. От тях 4 са индексирани в Scopus. Има 3 цитирания на публикациите. Всички публикации са с теоретично и приложно значение, свързани са с дисертацията и с професионалното направление 5.3. Комуникационна и компютърна техника. Приемам публикационната дейност като напълно достатъчна по обем, на високо научно ниво и популяризирана в достатъчна степен в национален и международен научен план.

6. Мнения, препоръки и бележки

В научно отношение представеният за рецензиране дисертационен труд е много добре оформен, реализиран и структуриран и затова могат да се посочат главно следните по важни редакционни и други незначителни забележки:

- в списъкът на цитираната литература няма номерация и нейното съответствие с цитирането в текста на дисертацията чрез имената на авторите е затруднено, например в текста на стр.16 има цитиране (Busulu et al., 2015), което липсва в списъка т на цитираната литература;

- в изводите към четвърта глава са представени числови данни от експерименталните резултати, например „класификацията на хакерски групи достига 100% или почти 100%, докато точността на атрибуцията по държава е около 70%“, които е препоръчително да бъдат посочени в приложните приноси за по-доброто им аргументиране.

Посочените препоръчителни забележки имат реален смисъл на колегиални пожелания за бъдещата научна дейност на докторанта в перспективната научна област на дисертацията.

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

В заключение считам, че дисертационният труд е оформен в съответствие с изискванията, има определени и потвърдени практически и дефинирани като научно-приложни и приложни приноси, отразени и популяризирани в достатъчен на брой научни публикации и в подходящи научни списания и конференции. Предлагам на Уважаемото научно жури да присъди образователната и научна степен „доктор" на маг. Гроздан Костадинов Христов в професионалното направление 5.13. Комуникационна и компютърна техника, научна специалност: „Системи с изкуствен интелект".

Дата: 13.01.2026 г. **ЧЛЕН НА ЖУРИТО:.....**

(проф. д-р Александър Бекярски)

OPINION

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

Author of the dissertation: M.Eng. Grozdan Kostadinov Hristov

Topic of the dissertation: Methods and algorithms for machine learning in cybersecurity

Member of the scientific jury: Prof. Dr. Eng. Alexander Bogdanov Bekyarski

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

The scientific field related to machine learning and artificial intelligence is particularly relevant and related to almost all human activities. In the present dissertation, this relevance refers to the scientific field of cybersecurity, in which machine learning is of paramount importance in solving security problems, both in computer systems and in a wide range of areas requiring a high degree of security and protection from cyberattacks.

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

A real idea and justification for the scientific level or degree of knowledge of the state of the problem and a corresponding creative interpretation of the literary material can be formed on the basis of the presentation in Chapter 1 of the dissertation. In this chapter, based on numerous and currently relevant scientific publications, a comprehensive review and analysis of the existing methods and tools for the application of machine learning in the field of cybersecurity has been carried out. The 111 literary sources in Latin, Cyrillic and Internet addresses used in the analysis and included in the bibliography to the dissertation are entirely scientific publications, reports and articles from reputable journals, issues of international conferences and sources from Internet sites, with the names of a sufficient number of authors as leading, prominent at the present time and in the recent past, foreign and domestic scientists and specialists in the field of machine learning and artificial intelligence.

3. Compliance of the selected research methodology and the set goal and tasks of the dissertation with the achieved contributions

From the fully justified definition of the significance and necessity in scientific and scientific-applied terms of research in the field of machine learning application, the validity of the goals and tasks in the dissertation follows. The doctoral student has very precisely and specifically formulated the goal and tasks in his dissertation.

The main goal of this dissertation is to study methods and algorithms related to cybersecurity, on the basis of which to propose a software solution based on an artificial intelligence method for classifying malicious files in order to facilitate their primary and secondary analysis.
To achieve this goal, the following tasks have been formulated:
- to study and investigate the possibility of applying machine learning methods in the analysis of cybersecurity incidents, in order to solve a classification task that would assist cybersecurity experts in assigning malicious files and work methodology to various hacker groups;
- to find characteristics that adequately reflect the objective dependencies on the classification status;
- to propose and optimize a model for solving the classification task and to apply this model to determine the classification status of the analyzed artifacts;
- to conduct an experimental analysis for the application of the proposed model, on the basis of which to assess its capabilities.

4. Scientific and/or applied scientific contributions of the dissertation
The dissertation presents 1 scientific, 2 applied scientific and 2 applied contributions, as follows:
Scientific contributions:
- a model based on a Random Forest classifier is proposed for assigning a class of belonging of malicious code to a specific country, sponsoring the activities and development of hacker groups directed against the communication and information infrastructure of other countries and/or organizations;
Scientific and applied contributions:
- the use of a taxonomy is proposed for performing precision procedures in the processing of 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 determination of incidents in cybersecurity;
- the use of evaluation techniques for optimizing classification characteristics and selecting hyperparameters for the Random Forest classifier is proposed, which evaluate over-representation of samples for minority classes and reduce the representation coefficient of samples for over-represented classes.

Applied contributions:
- an experimental prototype using the proposed model with the Random Forest classifier was developed, which implements an automated process for classifying characteristics of files containing malicious code to a definition of hacker groups and/or sponsoring countries and facilitates the analysis and assessment activities of cybersecurity experts;
- the proposed model was experimentally evaluated using the developed experimental prototype to validate the capabilities of the model for improving file classification and facilitating the work of cybersecurity experts.

5. Assessment of publications on the dissertation work

The main achievements in the dissertation work have been popularized in 5 scientific publications co-authored with the scientific supervisors, at prestigious scientific conferences. Of these, 4 are indexed in Scopus. There are 3 citations of the publications. All publications are of theoretical and applied importance, related to the dissertation and the professional field 5.3. Communication and computer technology. I accept the publication activity as completely sufficient in volume, at a high scientific level and sufficiently popularized in the national and international scientific plan.

6. Opinions, recommendations and notes

In scientific terms, the dissertation work submitted for review is very well designed, implemented and structured, and therefore the following important editorial and other minor remarks can be indicated:

- the list of cited literature is not numbered and its correspondence with the citation in the text of the dissertation, through the names of the authors is difficult, for example, in the text on p.16 there is a citation (Busulu et al., 2015), which is missing in the list of cited literature;
- the conclusions to the fourth chapter present numerical data from the experimental results, for example, "the classification of hacker groups reaches 100% or almost 100%, while the accuracy of attribution by country is about 70%", which it is advisable to indicate in the applied contributions for their better argumentation.

The indicated recommended remarks have a real meaning of collegial wishes for the future scientific activity of the doctoral student in the prospective scientific field of the dissertation.

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

In conclusion, I believe that the dissertation work is designed in accordance with the requirements, has certain and confirmed practical and defined as scientifically applied and applied contributions, reflected and popularized in a sufficient number of scientific publications and in appropriate scientific journals and conferences. I propose to the Honorable Scientific Jury to award the educational and scientific degree "doctor" to Mag. Grozdan Kostadinov Hristov in the professional field 5.13. Communication and computer technology, scientific specialty: "Artificial intelligence systems".

Date: 13.01.2026 JURY MEMBER:.....

(Prof. Dr. Alexander Bekyarski)