ФКСТЧУ- НС1-076
12.01.2026г.

СТАНОВИЩЕ

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 Даниела Асенова Гоцева

1. Актуалност на проблема

Темата на дисертацията е изключително актуална и се извършват множество изследвания по тематиката в целия свят и от изследователи и организации от различни научни, правителствени и икономически организации. Разгледани са различни въпроси, свързани с бурното развитие на комуникационни и информационни технологии, в частност информационните системи, където основен проблем е установяването и предотвратяването на зловредни действия върху тях и информацията, съхранявана в тях. В този контекст докторантът е предложил разработване и развиване на решение, чрез използване на изкуствен интелект, което да подпомогне дейностите по киберзащитата на информационните системи.

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

Докторантът е извършил обширен преглед на актуалното състояние на въпросите, свързани с машинното обучение в киберсигурността. Извършен е преглед на киберзаплахите, тенденциите на развитие и връзката им със сферата на изкуствения интелект. Направено е проучване на типовете методи на изкуствен интелект, свързани с прегледа на зловредните файлове, като е подбран и подготвен наборът данни, приложим за обучение.

Литературният преглед е съвременен, включващ научни публикации от последните сезони, което показва добрата осведоменост по материята. Чрез прилагане на критична оценка и разбор на обхванатите източници, авторът стига до формулиране на собствени изводи и иновативни решения.

3. Съответствие на методиката с целта, задачите и приносите

Избраният подход напълно съответства на заложената цел и задачите на дисертационния труд. Той обединява теоретичен преглед, сравнително проучване

и опитна верификация чрез експериментален прототип. Докторантът прилага различни метрики (F1 score, Precision, Recoil) и графично представяне на резултатите, включително чрез използвана на Confusion Metrix, за валидация на предложеното решение.

Методиката е адекватна и ефективна, като осигурява връзка между теоретичната постановка, изпълнение на задачите и постигнатите приноси.

4. Научни и научно-приложни приноси на дисертационния труд

Докторската дисертация съдържа ясно изложени и аргументирани научни и приложни приноси, които са директно обвързани с дисертационния труд. Те се изразяват в представяне на концепция за модел за категоризация на зловреден софтуер, основана на класификатор Random Forest за определяне на този софтуер към конкретна държава, подкрепяща активността на хакерски групи и създаване на експериментален прототип, който осъществява автоматизиран процес по класифициране на файлове, експлоатиращи зловреден код. Достигнатите резултати са смислово свързани с целта и задачите на проучването и допринасят за развитието на актуалните методики в сферата на киберсигурността.

5. Преценка на публикациите по дисертационния труд

Публикациите на докторанта по темата на дисертационния труд отразяват главните научни резултати и утвърждават тяхната оригиналност и научна стойност. Те са осъществени в реномирани конференции и издания, рецензирани на национално и международно ниво. Съдържанието на публикациите е в пълно съответствие с тематиката и приносите на дисертацията, като демонстрира системност, научна аргументация и умения за самостоятелна изследователска дейност.

6. Мнения, препоръки и бележки

Дисертацията е логически структурирана, последователна и ясно аргументирана. Авторът е осъществил задълбочено и последователно проучване в актуална и важна научна материя, представяйки добре организиран и обоснован труд. Дисертационният труд се отличава с висока степен на научна обосновка, приносен образ и приложна насоченост, които показват сериозна изследователска дейност и професионална експертиза на автора.

7. Заключение

Дисертационният труд на маг. инж. Гроздан Костадинов Христов е завършено, оригинално и висококачествено изследване с ясни приноси. Авторът демонстрира отлична подготовка и самостоятелност в решаването на сложни научно-технически проблеми.

Предлагам на уважаемото научно жури ДА ПРИСЪДИ на маг. инж. Гроздан Костадинов Христов образователна и научна степен ДОКТОР в професионално направление „5.3 Комуникационна и компютърна техника“.

Дата: 09.01.2026 г. Член на журито:

/проф. Даниела Гоцева/

SCIENTIFIC OPINION

On the occasion of the dissertation work for the award of the educational and scientific degree of PhD on the topic:
"Methods and algorithms for machine learning in cybersecurity"
In the professional field: 5.3 "Communication and Computer Engineering"
Scientific specialty: "Systems with artificial intelligence"

Author: M.Eng. Grozdan Kostadinov Hristov
From Prof. Daniela Asenova Gotseva

1. Relevance of the topic

The topic of the dissertation is extremely current and there is a lot of research on the subject around the world and by researchers and organizations from various scientific, governmental and economic organizations. Various issues related to the rapid development of communication and information technologies, in particular information systems, where the main problem is the detection and prevention of malicious actions on them and the information stored in them, are discussed. In this context, the doctoral student has proposed the development and development of a solution, using artificial intelligence, to support the cyber protection activities of information systems.

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

The PhD student has conducted an extensive review of the current state of machine learning issues in cybersecurity. An overview of cyber threats, development trends and their relationship with the field of artificial intelligence is carried out. A study of the types of artificial intelligence methods involved in the examination of malicious files was carried out, and the dataset applicable for training was selected and prepared.

The literature review is up-to-date, including scientific publications from recent seasons, which indicates a good awareness of the subject matter. By applying a critical evaluation and analysis of the covered sources, the author arrives at the formulation of his own conclusions and innovative solutions.

3. Compliance of the methodology with the goal, objectives and contributions

The chosen approach fully corresponds to the set goal and tasks of the dissertation work. It combines a theoretical review, a comparative study and experimental verification through an experimental prototype. The PhD student applies various metrics (F1 score, Precision, Recoil) and graphical representation of the results, including by using the Confusion Metrix, to validate the proposed solution.

The methodology is adequate and effective, ensuring a connection between the theoretical formulation, the implementation of the tasks and the achieved contributions.

4. Scientific and applied scientific contributions of the dissertation work

The doctoral dissertation contains clearly presented and argued scientific and applied contributions that are directly related to the dissertation work. They are expressed in presenting a concept for a malware categorization model based on a Random Forest classifier to assign this software to a specific country supporting the activity of hacker groups and creating an experimental prototype that implements an automated process for classifying files exploiting malicious code. The achieved results are meaningfully related to the purpose and tasks of the study and contribute to the development of current methodologies in the field of cyber security.

5. Assessment of the dissertation work

The doctoral student's publications on the topic of the dissertation reflect the main scientific results and confirm their originality and scientific value. They have been carried out in renowned conferences and publications, reviewed at national and international level. The content of the publications is in full accordance with the topic and contributions of the dissertation, demonstrating systematicity, scientific argumentation and skills for independent research.

6. Opinions, recommendations and notes

The dissertation is logically structured, consistent and clearly argued. The author has carried out a thorough and consistent study in a current and important scientific subject, presenting a well-organized and substantiated work. The dissertation is distinguished by a high degree of scientific justification, contribution and applied focus, which demonstrate serious research activity and professional expertise of the author.

7. Conclusion

The dissertation of M.Eng. Grozdan Kostadinov Hristov is a complete, original and high-quality study with clear scientific and applied contributions. The author demonstrates excellent preparation and independence in solving complex scientific and technical problems.

I propose to the esteemed scientific jury TO AWARD to M.Eng. Grozdan Kostadinov Hristov the educational and scientific degree PhD in the professional field 5.3 “Communication and Computer Engineering”

Date: 09.01.2026 г. Jury member:

/Prof. Daniela Gotseva/