ФКСТ 44-НС1-060
28.11.2023 г.

ТЕХНИЧЕСКИ УНИВЕРСИТЕТ ФКСТ СОФИЯ

СТАНОВИЩЕ

върху дисертационен труд за придобиване на образователна и научна степен „доктор”

Автор на дисертационния труд: **маг. инж. Евгени Веселинов Събев**

Тема на дисертационния труд: ***„Изследване възможностите за повишаване киберсигурността на системите в Индустрия 4.0 посредством изкуствен интелект”***

Член на научното жури: **проф. дтн Димитър Неделчев Карастоянов**

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

Развитието на индустриалното производство е в етап Индустрия 4.0, в който се създава интегрирана, интелигентна и гъвкава индустриална среда за да е по-ефективна. От друга страна се увеличава и възможността за кибератаки. Използваните в индустриалните системи традиционните методи за киберсигурност не винаги са достатъчни за справяне със сложността на новите заплахи. В дисертацията е направено задълбочено изследване за намиране на решение на проблема с киберсигурността в Индустрия 4.0 като са предложени различни методи за машинно обучение за киберсигурност в индустриалните системи и използване на изкуствения интелект. Смятам, че пробелмът разработен в дисертационния труд е много актуален в научно и научно-приложно отношение.

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

Докторантът е посочил 152 актуални литературни източници, които е цитирал коректно в дисертацията. Целта на дисертациионния труд е анализ на особеностите на Киберсигурността в Индустрия 4.0 и доразвиване на методите за повишаване на киберсигурността на системите в Индустрия 4.0 с използване на изкуствен интелект. За постигането на целта са формулирани 5 задачи, които са последователно решени в отделните глави на дисертацията.

Авторът познава много добре състоянието на проблема и умее да прави аналитични и критични интерпретации на използвания литературен материал, което е видно от направените критични анализи и изследвания.

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

Изследванията в областта на киберсигурността в Индустрия 4.0 изискват използването на различни методи за анализ на уязвимостите и защитата на компютърните системи. Използваните в дисертацията методи включват: Моделиране на заплахи, Анализ на риска, Машинно обучение, Системи за

засичане и предотвратяване на инциденти, Разработване на политики и процедури за сигурност.

Резултатите получените в дисертационния труд обосновават пълното съответствие на избраната методика на изследване с поставената цел и задачи на дисертационния труд.

4. Научни и/или научно-приложни приноси на дисертационния труд

Дисертацията има няколко значителни приноса към научната общност. Разглежда се пресечната точка на две динамично развиващи се области - Индустрия 4.0 и машинно обучение - и се изследва как те могат да бъдат интегрирани за подобряване киберсигурността на индустриалните процеси.

Приемам формулираните от докторанта приноси, които са разделени на:
Научни: Анализирани са различните референтни модели; Извършен е критичен анализ и синтез на съществуващи кибератаки; Обобщаване и анализиране на вече съществуващи стандарти и регулации в индустриалната киберсигурност, в международен и държавен аспект.
Научно-приложни: Анализирани са различните модели за машинно обучение и тяхната приложимост в сферата на Индустрия 4.0; Предложен е модел за машинно обучение, за откриване на кибератака над приложния физически модел; Предложен е модел за машинно обучение, който да може да бъде обучен да класифицира потенциалните атаки с по-голяма точност от обобщителните модели в предходния принос; Генериран е тестова база от данни, която е използвана в моделите за машинно обучение. Тя може да бъде използвана и за допълнителни изследвания и следващи валидации от изследователи в сферата на Индустрия 4.0.
Приложни: Проектиран и е изграден модел на вятърни турбини, който наподобява системите за вятърни турбини в реалния свят; Обобщаване на стъпките необходими за създаване на физически модел и тяхното опростено систематизиране с цел бъдещо използване от други изследователи в сферата на Индустрия 4.0; Дефиниран е набор от сценарии за кибератаки над физическия модел, които потенциално могат да бъдат насочени към системи за вятърни турбини; Обобщаване на сигурни протоколи и техните технически спецификации. Извършено е практическо сравнение между двата протокола Modbus/TCP и Secure Modbus/TCP.

5. Преценка на публикациите по дисертационния труд:

Маг. инж. Евгени Събев е представил общо пет публикации на английски език по дисертационния труд - четири в съавторство и една самостоятелна. Резултатите от дисертацията са докладвани на международни научни конференции: InfoTech(2021), ICAI(2021), APSAC(2023), COMSCI(2023), EEPES(2023). Всички 5 публикации се реферират и индексират в световноизвестните бази данни Scopus и/или Web of Science.

Тези публикации дават достатъчна публичност сред научната общност на голяма част от резултатите от дисертационния труд.

6. Мнения, препоръки, забележки

Нямам съществени забележки към дисертационния труд.

Препоръчвам на маг.инж. Евгени Събев да продължи изследванията си в тази научна област, която има перспектива за нови научни резултати.

7. Заключение

Имайки в предвид извършените изследвания и анализи, представените резултати, отразени в научни публикации смятам, че дисертацията напълно отговаря на изискванията в Закона за развитие на академичния състав в Република България и Правилника за неговото прилагане, както и в Правилника за условията и реда за придобиване на научни степени в Технически университет – София.

Убедено давам **положителна оценка** на дисертационния труд и предлагам на уважаемото Научно жури да **присъди образователната и научна степен „доктор“ на маг. инж. Евгени Веселинов Събев** в професионално направление 5.3 Комуникационна и компютърна техника по научна специалност „Системи с изкуствен интелект“.

27.11.2023 г. ЧЛЕН НА ЖУРИТО:.....

гр.София /проф. дтн Димитър Неделчев Карастоянов/

STATEMENT

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

Author of the dissertation: **M.Sc. Engineer Evgeni Veselinov Sabev**
Topic of the dissertation: ***"Investigating the possibilities of increasing the cyber security of the systems in Industry 4.0 by means of artificial intelligence"***
Member of the scientific jury: **Prof. Dr. Dimitar Nedelchev Karastoyanov**

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

The development of industrial production is in the Industry 4.0 stage, in which an integrated, intelligent and flexible industrial environment is created to be more efficient. On the other hand, the possibility of cyber attacks also increases. Traditional cyber security methods used in industrial systems are not always sufficient to deal with the complexity of new threats. In the dissertation, a thorough research has been done to find a solution to the problem of cyber security in Industry 4.0 by proposing different machine learning methods for cyber security in industrial systems and using artificial intelligence. I think that the problem developed in the dissertation work is very relevant in a scientific and scientific-applied sense.

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

The PhD student indicated 152 current literary sources, which he cited correctly in the dissertation. The aim of the dissertation work is to analyze the features of Cybersecurity in Industry 4.0 and to further develop the methods of increasing the cyber security of the systems in Industry 4.0 using artificial intelligence. To achieve the goal, 5 tasks have been formulated, which are successively solved in the individual chapters of the dissertation.

The author knows very well the state of the problem and is able to make analytical and critical interpretations of the used literary material, which is evident from the critical analyzes and research done.

3. Correspondence of the chosen research methodology with the set goal and tasks of the dissertation work.

Research in the field of cyber security in Industry 4.0 requires the use of various methods for analyzing vulnerabilities and protecting computer systems. Methods used in the dissertation include: Threat Modeling, Risk Analysis, Machine Learning, Incident Detection and Prevention Systems, Development of Security Policies and Procedures.

The results obtained in the dissertation justify the complete compliance of the chosen research methodology with the set goal and tasks of the dissertation.

4. Scientific and/or scientific-applied contributions of the dissertation work

The dissertation makes several significant contributions to the scientific community. It looks at the intersection of two dynamically developing fields - Industry 4.0 and machine learning - and explores how they can be integrated to improve the cyber security of industrial processes.

I accept the contributions formulated by the doctoral student, which are divided into:

Scientific: The various reference models are analyzed; A critical analysis and synthesis of existing cyberattacks was performed; Summarizing and analyzing already existing standards and regulations in industrial cyber security, in an international and national aspect.

Scientific-applied: The different models for machine learning and their applicability in the field of Industry 4.0 are analyzed; A machine learning model is proposed to detect a cyber attack over the applied physical model; A machine learning model is proposed that can be trained to classify potential attacks with greater accuracy than the generalization models in the previous contribution; A test database was generated which was used in the machine learning models. It can also be used for further research and subsequent validations by researchers in the field of Industry 4.0.

Applied: A wind turbine model is designed and built to resemble real-world wind turbine systems; Summarizing the steps necessary to create a physical model and their simplified systematization for future use by other researchers in the field of Industry 4.0; A set of cyber-attack scenarios over the physical model that could potentially target wind turbine systems are defined; Summary of secure protocols and their technical specifications. A practical comparison was made between the two protocols Modbus/TCP and Secure Modbus/TCP.

5. Evaluation of publications on the dissertation work:

M.Sc. Eng. Evgeni Sabev presented a total of five publications in English on his dissertation - four co-authored and one independent. The results of the dissertation have been reported at international scientific conferences: InfoTech(2021), ICAI(2021), APSAC(2023), COMSCI(2023), EEPES(2023). All 5 publications are referenced and indexed in the world-renowned databases Scopus and/or Web of Science.

These publications give sufficient publicity among the scientific community to a large part of the results of the dissertation work.

6. Opinions, recommendations, remarks

I have no significant remarks on the dissertation work.

I recommend to M.Eng. Evgeni Sabev to continue his research in this scientific field, which has the prospect of new scientific results.

7. Conclusion

Bearing in mind the research and analysis carried out, the presented results,

reflected in scientific publications, I believe that the dissertation fully meets the requirements of the Law on the Development of the Academic Staff in the Republic of Bulgaria and the Rules for its Implementation, as well as the Rules for the Conditions and Procedures for Acquiring scientific degrees at Technical University - Sofia.

I confidently give a positive assessment of the dissertation work and propose to the respected Scientific Jury to award the educational and scientific degree "doctor" to M.Sc. Eng. Evgeni Veselinov Sabev in professional direction 5.3 Communication and computer technology in scientific specialty "Systems with artificial intelligence".

27.11.2023 MEMBER OF THE JURY:.....
Sofia / Prof. Dr. Dimitar Nedelchev Karastoyanov /