ОИСТ-НС1-093
07.07.2026г.

Р Е Ц Е Н З И Я

върху дисертационен труд за придобиване на образователна и научна степен „доктор"
Професионално направление 5.3. Комуникационна и компютърна техника
Научна специалност: Осигурителна техника и системи

Автор на дисертационния труд: **маг. инж. Мариан [redacted] Христов**

Тема на дисертационния труд: **Изследване на облачно-базирана система за наблюдение и анализ на събития**

Рецензент: **проф. д-р инж. Габриела [redacted] Атанасова**

1. Актуалност на разработвания в дисертационния труд проблем в научно и научноприложно отношение. Степен и нива на актуалността на проблема и конкретните задачи, разработени в дисертацията.

През последните години бързото развитие на Индустрия 4.0 и дигиталната трансформация на критичната инфраструктура доведоха до значителна интеграция между информационните технологии (ИТ) и оперативните технологии (ОТ). Макар че тази интеграция води до несъмнени ползи, като повишена ефективност, автоматизация и възможност за анализ на данни в реално време, тя същевременно поражда значителни рискове за сигурността, излагайки критичната инфраструктура на киберзаплахи, които досега бяха характерни предимно за средите на ИТ. Свидетелство за това са множеството успешни атаки срещу индустриални системи през последното десетилетие.

С навлизането на Индустрия 5.0, конвергенцията между ИТ и ОТ поставя нови предизвикателства пред киберсигурността. Сред най-критичните проблеми се очертават ограничената видимост в индустриалните мрежи, липсата на адекватни механизми за мониторинг, съобразени със спецификата на средите за ОТ и сложността при своевременно откриване и разследване на инциденти. Именно тези проблеми са в центъра на настоящия дисертационен труд, който се фокусира върху разработването и практическото внедряване на системи за наблюдение и анализ на събития, базирани на съвременни SIEM решения в реална индустриална среда.

Настоящият дисертационен труд е фокусиран върху реализиране на техническо решение, изследване и разработване на методология за оценка на риска в среди за оперативни технологии.

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

Докторантът демонстрира познаване на спецификите на OT/ICS средите, разликите спрямо ИТ, както и съществуващите технологии за мониторинг.

Литературният обзор обхваща общо 240 печатни и електронни източника. Повечето от тях са техническа документация, доклади и годишни отчети на CISA, Dragos, NIST, Microsoft Lear и други, както научните статии от рецензирани издания и конференции (IEEE Xplore и др.). Въз основа на направеният преглед и анализ на особеностите на индустриалните мрежи, съществуващите предизвикателства, сравнението с информационните технологии, наблюдението и анализа на събития в индустриалните мрежи и приложението на механизъм за уведомяване при откриване на зловреден софтуер, е формулирана целта на дисертацията, поставени и решени са задачи, свързани с реализация на предложеното техническо решение в реална индустриална среда, оценена е ефективността и е разработена методология за оценка на риска в средите с оперативни технологии.

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

Избраната от докторанта методика за прилагане на многослоен модел за надеждност на наблюдението на оперативните технологии, както и въвеждането на концептуален модел на симетрия на сигурността при злонамерено действие, детектирането на понижаването на версията на фърмуера и анализ на протоколите, детектиране на фазите на кибератаката, в реално време посредством класификация на постъпилите аларми, съответства на поставените в дисертационния труд задачи, като отчита сложността на разглеждания проблем.

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

Структурата на дисертационния труд съответства на темата му, отделните глави са добре балансирани по обем и притежават логическа обвързаност.

Дисертационният труд е разработен в обем от 187 страници, включващ 156 фигури и 5 таблици. Структуриран е в следните раздели: въведение, четири глави, списъци на използваните съкращения и означения, фигури, таблици и списък на използваната литература.

В **първа глава** е направен обзор на индустриалните мрежи, съществуващите предизвикателства, основните определения използвани в индустриалните мрежи, съпоставянето между информационните технологии и индустриалните мрежи (оперативните технологии), видовете протоколи използвани в оперативните технологии, наблюдението и анализа на събитията в индустриалните мрежи, както и приложението на механизми за уведомяване при откриване на зловреден софтуер. Формулирана е целта на дисертационния труд и задачите, които трябва да бъдат решени за постигането ѝ.

Втора глава е посветена на регистрираните събития в индустриалните мрежи, наличната информация, системите за наблюдаване и съхраняване на събитията,

прилагането им за наблюдение в IoT мрежи. Представено е реализирано техническо решение и са извършени тестове за работоспособността му.

В **трета глава** са разгледани механизмите за откриването на атаки срещу индустриални мрежи целящи понижаване на версията на фърмуера. Представено и реализирано е техническо решение за известяване чрез аларми при този тип атаки. Извършени са тестове за потвърждаване на работоспособността на предложеното решение.

Четвърта глава е посветена на разработване на система за наблюдение и анализ на събитията. Представени са архитектура, приложение за откриване на DDoS атаки, конфигуриране и правила за генериране на аларми и тестване на работоспособността на системата.

5. Научни и/или научноприложни приноси на дисертационния труд.

Основните научни и научно-приложни приноси могат да се обобщят, както следва:

- Методология за прилагане на многослоен модел за наблюдение на индустриалните мрежи;
- Въвеждане на концептуален модел за симетрия на сигурността при злонамерено действие;
- Представяне на метод за детектиране на злонамерени действия след понижаване на версията на фърмуера;
- Създаване на модел за детектиране на фазите на традиционната кибератака;
- Дефиниране на измерим подход за детектиране в реално време, посредством класификация на алармите и обосноваване на избора спрямо оперативната стойност на индикаторите;
- Предложена е аналитична методология за потвърждаване на злонамерено действие.

Считам, че тези приноси правилно отразяват постигнатото от автора в процеса на проведените изследвания и несъмнено ще намерят своята приложимост.

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

Въз основа на дисертационния труд, постигнатите научни резултати и публикационната дейност на маг. инж. Мариан [redacted] Христов считам, че формулираните научни и научно-приложни приноси са резултат от неговата самостоятелна изследователска работа.

7. Преценка на публикациите по дисертационния труд.

По материалите на дисертационния труд докторантът представя списък от 6 публикации, които включват статия в списание Symmetry (MDPI), както и пет доклада представени на конференции. Всичките авторски публикации са индексирани от базата данни Scopus и три в Web of Science, което доказва високото качество и значимост на проведените изследвания. В четири от публикациите маг. инж. Мариан Христов е първи автор. Две от авторските публикации имат 28 цитирания (Scopus) с изключени самоцитирания.

Считам, че представените научни публикации, индексирането им в базите данни Scopus и Web of Science, както и получените цитирания от други автори, представляват убедително доказателство, че резултатите от дисертационния труд са получили научно признание и са достигнали до научната общност. Съдържанието и обемът на представените публикации и доклади напълно отразяват разработените проблеми в дисертационния труд.

8. Мнения, препоръки и бележки.

Представеният за рецензиране дисертационен труд представлява цялостно, задълбочено и завършено научно изследване, разработено на високо научно и методично ниво. Трудът е логически структуриран, добре аргументиран и коректно оформен.

Научната област на дисертацията е перспективна и с висока значимост за развитието на индустриалните мрежите, поради което препоръчвам на маг. инж. Мариан [redacted] Христов да продължи своята научноизследователска дейност в разглежданата научна област.

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

В резултат на представените публикации и приноси в дисертационния труд смятам, че той съответства на изискванията на „Закона за развитие на академичния състав в Република България", Правилника за неговото приложение и Правилника за условията и реда за придобиване на научни степени в Технически университет – София. Давам **положителна оценка** на дисертационния труд и предлагам на уважаемото Научно жури да присъди на **маг. инж. Мариан [redacted] Христов** образователната и научна степен **„доктор"** по професионално направление 5.3 Комуникационна и компютърна техника, научна специалност „Осигурителна техника и системи".

06.07.2026 г.
гр. София

РЕЦЕНЗЕНТ: [redacted]
/проф. д-р инж. Габриела Атанасова/

ВКС 38-НС-093
07.08.2026

REVIEW

on a doctoral thesis for the award of an educational and scientific degree "Doctor"
Professional field: 5.3 Communication and Computer Engineering
Scientific speciality: Security Equipment and Systems

Author of the dissertation: **Marian I [redacted] Hristov, M.Sc. Eng.**

Dissertation topic: **Investigation of a Cloud-based Security Information and Event Management System**

Reviewer: **Prof. Gabriela I [redacted] Atanasova, PhD Eng.**

1. Relevance of the problem and the specific tasks developed in the doctoral thesis.

In recent years, the rapid development of Industry 4.0 and the digital transformation of critical infrastructure have led to significant integration between Information Technology (IT) and Operational Technology (OT). While this integration offers undeniable benefits – such as increased efficiency, automation, and real-time data analysis capabilities – it also introduces substantial security risks, exposing critical infrastructure to cyber threats that were previously largely confined to IT environments. The numerous successful attacks on industrial systems over the past decade bear witness to this.

With the advent of Industry 5.0, the convergence of IT and OT presents new cybersecurity challenges. Key issues include limited visibility within industrial networks, a lack of adequate monitoring mechanisms tailored to the specific nature of OT environments, and the complexity of timely incident detection and investigation. These challenges constitute the central focus of the present doctoral dissertation, which is dedicated to the development and practical deployment of event monitoring and analysis systems based on modern Security Information and Event Management (SIEM) solutions within a real-world industrial environment.

The present doctoral thesis is focused on the implementation of a technical solution, and the research and development of a risk assessment methodology for operational technology environments.

2. Degree of topic knowledge and creative interpretation of the literary material.

The PhD student demonstrates knowledge of the specifics of OT/ICS environments, the differences compared to IT, and existing monitoring technologies.

The literature review covers a total of 240 print and electronic sources. Most of these consist of technical documentation, reports, and annual statements from CISA, Dragos,

NIST, Microsoft Learn, and others, as well as research articles from peer-reviewed journals and conferences (IEEE Xplore, etc.). Based on the review and analysis of the characteristics of industrial networks, existing challenges, comparisons with information technology, the monitoring and analysis of events within industrial networks, and the application of a malware detection notification mechanism, the objective of the dissertation was formulated; tasks related to implementing the proposed technical solution in a real-world industrial environment were defined and addressed; the solution's effectiveness was evaluated; and a risk assessment methodology for operational technology environments was developed.

3. Consistency of the selected research methodology with the dissertation goal and tasks.

The methodology selected by the doctoral candidate, which is based on the application of a multilayer monitoring reliability model for operational technology environments, together with the introduction of a conceptual security symmetry model for malicious activities, the detection of firmware downgrade attacks through protocol analysis, and the real-time detection of cyberattack phases by classifying incoming security alerts, is fully consistent with the objectives and research tasks defined in the dissertation. The proposed approach appropriately reflects the complexity of the problem under investigation.

4. Brief analytical description of the nature and assessment of the credibility of the material on which the contributions of the dissertation are based.

The structure of the PhD thesis is fully consistent with its research topic. The individual chapters are well balanced in terms of content and length, and logically interconnected.

The PhD thesis comprises 187 pages, including 156 figures and 5 tables. It is structured into the following sections: an introduction, four chapters, lists of abbreviations and notations, lists of figures and tables, and a bibliography.

Chapter 1 provides an overview of industrial networks, existing challenges, and key definitions used in the field. It compares information technology with industrial networks (operational technology) and discusses the types of protocols employed in operational technology, the monitoring and analysis of events within industrial networks, and the implementation of notification mechanisms for malware detection. The objective of the PhD thesis is formulated, along with the tasks required to achieve it.

The second chapter is dedicated to events recorded in industrial networks, available information, systems for monitoring and storing events, and their application for monitoring in IoT networks. A technical solution is presented, and tests verifying its functionality have been conducted.

Chapter 3 examines mechanisms for detecting attacks on industrial networks aimed at downgrading firmware versions. A technical solution for issuing alarms in response to such attacks is presented and implemented. Tests were conducted to verify the functionality of the proposed solution.

Chapter 4 is dedicated to developing a system for event monitoring and analysis. It presents the system architecture, an application for detecting DDoS attacks, configuration and alarm generation rules, and system performance testing.

5. Scientific and/or applied research contributions of the dissertation.

The main scientific and applied scientific contributions can be summarized as follows:

- Methodology for implementing a multi-layer monitoring model for industrial networks.
- Introduction of a conceptual model for security symmetry in the event of malicious action.
- Presentation of a method for detecting malicious actions following a firmware downgrade.
- Development of a model for detecting the phases of a traditional cyberattack.
- Defining a measurable approach for real-time detection through alarm classification and justifying the choice based on the operational value of the indicators.
- An analytical methodology for confirming malicious activity has been proposed.

I believe that these contributions accurately reflect the achievements attained by the author throughout the course of the conducted research and will undoubtedly find practical application.

6. Evaluation of the degree of personal participation of the PhD candidate.

Based on the PhD thesis, the scientific results achieved, and the publication record of MSc Eng. Marian [redacted] Hristov, I consider that the formulated scientific and applied-scientific contributions are the result of his independent research work.

7. Assessment of dissertation publications.

Based on the dissertation research, the PhD candidate presents a list of six publications, including an article in the journal Symmetry (MDPI) and five conference papers. All the publications are indexed in the Scopus database, with three also indexed in Web of Science, demonstrating the high quality and significance of the research conducted. Marian Hristov (MSc Eng.) is the first author on four of these publications. Two of the publications have received 28 citations (Scopus), excluding self-citations.

I consider that the submitted scientific publications, their indexing in the Scopus and Web of Science databases, and the citations received from other authors constitute convincing evidence that the results of the PhD thesis have gained scientific recognition and reached the scientific community. The content and scope of the submitted publications and reports fully reflect the issues addressed in the PhD thesis.

8. Comments, recommendations, and remarks.

The PhD thesis submitted for review constitutes a comprehensive, in-depth, and complete scientific study, conducted at a high scientific and methodological level. The work is logically structured, well-argued, and properly presented.

The scientific field of the PhD thesis is promising and of great significance for the development of industrial networks; therefore, I recommend that Marian Hristov, M. Sc. Eng., continue his research activities in this field.

9. Conclusion with a positive or negative dissertation assessment

As a result of the presented publications and contributions in the PhD thesis, I believe that it meets the requirements of the "Law on the Development of the Academic Staff in the Republic of Bulgaria", the Regulations for its Application, and the Regulations for the Conditions and Procedures for Obtaining Scientific Degrees at the Technical University in Sofia. I give a positive assessment of the PhD thesis and propose to the Honourable Scientific Jury to award **Mari Hristov, M.Sc. Eng.** educational and scientific degree "Doctor" in professional field 5.3 Communication and Computer Engineering, scientific speciality Security Equipment and Systems.

06.07.2026 **REVIEWER:**

Sofia **/Prof. Gabriela Atanasova, PhD Eng./**