ОПСУ-НС-1-093
22.06.2026

СТАНОВИЩЕ

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

Автор на дисертационния труд: **маг. инж. Мариан Христов**

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

Член на научното жури: **проф. д-р инж. Станимир Садинов**

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

Разработването на облачно-базирана система за наблюдение и анализ на събития е актуален научно-приложен проблем, поради това че облачният подход предоставя възможности за централизация, мащабируемост, интеграция на множество източници на телеметрия, аналитика в реално време и автоматизация на реакцията. Също така това види до повишаване ефективността, мащабируемостта и автоматизацията на процесите, но едновременно с това разширява възможните точки за атака и увеличава вероятността от киберинциденти с оперативен и физически ефект. Затова събирането и анализът на събития се превръщат в ключов фактор за киберустойчивост.

По този начин необходимостта от разработването и валидирането на архитектура и механизми за облачно-базиран мониторинг и анализ на събития, приложими към Индустриалните мрежи, представлява значим и актуален принос към повишаване на киберустойчивостта на критични среди.

В научно-приложно отношение в дисертационния труд са решени множество задачи, свързани с разработването и изграждането на цялостна система за наблюдение и анализ на събитията в индустриални мрежи (OT/ICS), като се стреми да подобри нивото на сигурност на организациите, чрез повишаване на мрежовата видимост и своевременно откриване на заплахи.

Използвани са научни методи, като сравнителен анализ, моделиране и експериментално валидиране. В структурно отношение дисертационния труд обхваща теоретичен преглед, разработване на система за наблюдение на OT/ICS, оценка на ефективността, експериментални резултати и разработване на методология за оценка на риска в ОТ среди.

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

Дисертационният труд включва съдържание, списъци на фигури, таблици, увод, четири глави за решаване на формулираните основни задачи, като след всяка глава е направено заключение, и са представени основните научни и научно-приложни приноси, а накрая има списък на използвани 240 научни източника. В дисертационния труд са цитирани и 6 публикации на докторантът в съавторство, като в 4 от тях той е на първо място. Всички литературни източници са подбрани така, че да отразяват съвременните научни достижения в областта на тематиката на дисертационния труд.

Цитирани са онлайн достъпни материали, като статии от научни списания, конференции и стандарти. Извършеният аналитичен обзор позволява на докторантът да дефинира коректно целта и основните задачи за изследване, които той решава успешно в отделните глави.

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

В дисертационния труд е извършен анализ на съвременните заплахи и системни слабости в OT/ICS, който служи като основа за дефиниране на архитектурни принципи и функционални изисквания към системата за мониторинг и анализ на събития. Като научна новост се разглежда и разработването на многокомпонентен подход за повишаване надеждността на мониторинга чрез независими механизми за откриване на деградация или загуба на видимост. Допълнително, представена е аналитична логика, съобразена с версиите, - version-aware - която позволява разграничаване на легитимни фърмуерни промени от потенциално злонамерени firmware downgrade действия, въпреки високата прилика между процесите. Предложените подходи демонстрират практическа ефективност чрез валидиране в тестова и/или реална индустриална - производствена - среда и водят до по-бързо откриване и реакция при инциденти и до намаляване на нерелевантни аларми, като по този начин се повишава устойчивостта на наблюдението и управляемостта на риска в OT/ICS инфраструктури.

Получените резултати са анализирани и илюстрирани с много работни екрани, таблици и фигури, които потвърждават действието на разработените механизми и компоненти на предложената облачно-базирана система за наблюдение и анализ на събития. Предложените

решения могат да бъдат реализирани в реални Индустриални мрежи, където са налице ограничения за активни сканирания и инсталиране на агенти, и където се изисква надеждно уведомяване и бърза реакция при инциденти.

В този смисъл формулираната цел и задачи на дисертацията са изпълнени, като в синтезиран вид те са изложени в изводите и заключенията, като това потвърждава коректността на избрания научноизследователския подход и неговата приложимост.

4. **Приноси на дисертационния труд.**

Приемам формулираните и декларирани от докторантът приноси и техния научен, научно-приложен и приложен характер. Приносните моменти имат значимост на новост в разглежданата проблематика и се явяват разширение на съществуващите знания. От получените резултати може да се установи, че новосъздадените и модифицираните методи, системи за наблюдение и подходи са подходящи за прилагане и имат ясно изразен потенциал за реална употреба в множество практически контексти, с възможност за доразвиване спрямо конкретните нужди на различни сектори и приложения.

Направените изводи след всяка глава, синтезираните методологии и разработените подходи, процедури и експерименти, могат да се приемат като полезни препоръки за внедряване в съвременните комуникационни и информационни системи.

5. **Преценка на публикациите по дисертационния труд.**

По темата на дисертацията са представени 6 авторски публикации, една от които е публикувана в международно научно списание в Q2. Пет от научните публикации са представени и публикувани в сборници от международни научни конференции и национални конференции с международно участие.

Пет от публикациите са в съавторство с научните ръководители. Статиите имат общо 49 цитирания в индексирани издания Scopus, WoS и Google scholar. В тях са публикувани и са станали достояние на научната общност голяма част от резултатите на проведените експерименти, представени в дисертацията. Всичко това ми дава основание да заявя, че научните постижения на автора са значими и са станали известни като се цитират от научната общност в страната и чужбина.

6. **Мнения, препоръки и бележки.**

Считам, че дисертационният труд постига заявената цел, а дефинираните задачи са изпълнени на добро научно ниво и дисертацията има завършен характер. Би било добре да се даде информация и за образователните и научноизследователски проекти, в които докторантът е взел участие. Адмирации за големия брой представени сертификати, чрез които той демонстрира придобитите знания и компетентност в областта на киберсигурността. Препоръчвам в бъдещата се работа да продължи на работи по тематиката в екип и да публикува резултатите в списания, които се отразяват в базите данни на Scopus и Web of Science, както и да развива своята експертна и внедрителска дейност, която да реализира в участия в проекти.

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

Считам, че представеният дисертационен труд **отговаря** на изискванията на Закона за развитие на академичния състав в Република България и оценката ми за него е напълно **положителна**. Постигнатите резултати ми дават основание **да предложа** да бъде придобита образователната и научна степен „доктор" от **маг. инж. Мариан [redacted] Христов.**

в област на висше образование - 5. Технически науки,

професионално направление - 5.3 „Комуникационна и компютърна техника",

докторска програма - „Осигурителна техника и системи".

Дата: 18.06.2026 г.

ЧЛЕН НА ЖУРИТО: [redacted]

(проф. д-р инж. Станимир Садинов)

[illegible]-НС-09
22.06.2026

OPINION

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

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

Topic of the dissertation: **Investigation of a Cloud-based Security Information and Event Management Sistem**

Member of the scientific jury: **Prof. eng. Stanimir [redacted] Sadinov, PhD**

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

The development of a cloud-based event monitoring and analysis system represents a relevant scientific and applied research problem, as the cloud approach provides opportunities for centralization, scalability, integration of multiple telemetry sources, real-time analytics, and automated response mechanisms. At the same time, while this approach improves operational efficiency, scalability, and process automation, it also expands the potential attack surface and increases the likelihood of cyber incidents with both operational and physical consequences. Therefore, the collection and analysis of events have become key factors in achieving cyber resilience.

In this context, the development and validation of an architecture and mechanisms for cloud-based event monitoring and analysis applicable to industrial networks constitute a significant and timely contribution to enhancing the cyber resilience of critical environments.

From a scientific and applied perspective, the dissertation addresses numerous challenges related to the design and implementation of a comprehensive event monitoring and analysis system for industrial networks (OT/ICS). The proposed solution aims to improve the security posture of organizations by increasing network visibility and enabling the timely detection of threats.

Scientific methods such as comparative analysis, modeling, and experimental validation have been employed throughout the research. Structurally, the dissertation includes a theoretical review, the development of an OT/ICS monitoring system, an evaluation of its effectiveness, experimental results, and the development of a risk assessment methodology for OT environments.

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

The dissertation consists of a table of contents, lists of figures and tables, an introduction, and four chapters dedicated to addressing the formulated research objectives. Each chapter concludes with a summary of the findings, and the dissertation presents its main scientific and scientific-applied contributions. The work concludes with a bibliography comprising 240 scientific references.The dissertation also cites six publications co-authored by the PhD candidate, with the candidate listed as the first author in four of them. All references have been carefully selected to reflect the current state of the art and contemporary scientific achievements in the field of the dissertation topic.

The cited sources include publicly available online materials such as articles published in scientific journals, conference proceedings, and standards. The conducted analytical review enabled the PhD candidate to accurately define the research objective and the main research tasks, which have been successfully addressed throughout the individual chapters.

3. **Compliance of the chosen research methodology and the set goal and objectives of the dissertation with the contributions achieved.**

The dissertation presents an analysis of contemporary threats and systemic vulnerabilities in OT/ICS environments, which serves as the foundation for defining the architectural principles and functional requirements of the proposed event monitoring and analysis system. A notable scientific contribution is the development of a multi-component approach aimed at increasing the reliability of monitoring through independent mechanisms for detecting degradation or loss of visibility. Furthermore, the dissertation introduces a version-aware analytical framework that enables the distinction between legitimate firmware updates and potentially malicious firmware downgrade activities, despite the high degree of similarity between these processes. The proposed approaches demonstrate practical effectiveness through validation in both test and/or real industrial production environments, leading to faster incident detection and response, as well as a reduction in irrelevant alerts. Consequently, the resilience of monitoring processes and the effectiveness of risk management within OT/ICS infrastructures are significantly enhanced.

The obtained results are thoroughly analyzed and illustrated through numerous screenshots, tables, and figures, which confirm the functionality of the developed mechanisms and components of the proposed cloud-based event monitoring and analysis system. The proposed solutions can be

implemented in real industrial networks, where restrictions on active scanning and agent installation are common, and where reliable notification mechanisms and rapid incident response are essential requirements.

In this regard, the stated objective and research tasks of the dissertation have been successfully accomplished. Their fulfillment is clearly synthesized in the findings and conclusions of the dissertation, thereby confirming the validity of the selected research methodology and its practical applicability.

4. **Contributions of the dissertation work.**

I accept the contributions formulated and declared by the PhD candidate, as well as their scientific, scientific-applied, and practical nature. The identified contributions demonstrate a significant degree of novelty within the investigated research area and represent a valuable extension of the existing body of knowledge. Based on the obtained results, it can be concluded that the newly developed and enhanced methods, monitoring systems, and approaches are suitable for practical implementation and possess a clear potential for real-world application across a wide range of contexts. Furthermore, they offer opportunities for further development and adaptation to meet the specific requirements of various sectors and application domains.

The conclusions drawn at the end of each chapter, together with the synthesized methodologies and the developed approaches, procedures, and experimental frameworks, may be regarded as valuable recommendations for implementation in modern communication and information systems.

5. **Evaluation of dissertation publications.**

A total of six author publications related to the dissertation topic have been presented, one of which has been published in an international scientific journal ranked in the Q2 quartile. Five of the publications have been presented and published in the proceedings of international scientific conferences and national conferences with international participation.

Five of the publications have been co-authored with the scientific supervisors. The publications have received a total of 49 citations in indexed sources, including Scopus, Web of Science, and Google Scholar. A substantial portion of the results obtained from the experiments conducted within the scope of the dissertation has been published in these works and made available to the scientific community. This provides sufficient grounds for concluding that the author's scientific achievements are significant and have gained recognition both nationally and internationally, as evidenced by citations from members of the scientific community in Bulgaria and abroad.

6. **Opinions, Recommendations, and Remarks.**

I consider that the dissertation successfully achieves its stated objective and that the defined research tasks have been accomplished at a good scientific level. The dissertation demonstrates completeness and coherence as a scholarly work. It would have been beneficial to include information regarding the educational and research projects in which the PhD candidate has participated. I would also like to express my appreciation for the large number of certificates presented, through which the candidate demonstrates the knowledge and competencies acquired in the field of cybersecurity.

For future work, I recommend continuing research in this area through collaborative teamwork and publishing the obtained results in journals indexed in the Scopus and Web of Science databases. Furthermore, I encourage the candidate to continue developing their expertise and practical implementation activities through active participation in research and development projects.

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

I consider that the presented dissertation **meets** the requirements of the Law for the Development of the Academic Staff in the Republic of Bulgaria, and my overall assessment of it is fully **positive**. The achieved results give me grounds **to propose** that the educational and scientific degree "**Doctor (PhD)**" be awarded to **M.Sc. Eng. Marian** [redacted] **Hristov** in the field of higher education:

Field of Higher Education - 5. Technical Sciences

Professional Field - 5.3 Communication and Computer Engineering

Doctoral Program - Security systems engineering.

Date: 22.06.2026 r.

JURY MEMBER [redacted]
(Prof. eng. Stanimir Sadinov, PhD)