ФТС78-НС1-093
08.06.2026

[redacted]

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 на събития**"
Член на научното жури: **доц. д-р инж. Ивелина Балабанова**, Технически университет - Габрово

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

Ефективността на наблюдението и установяването на легитимни и злонамерени активности при мониторинг, диагностика и оценка на състоянието на събития е значимо предизвикателство пред корпоративни и индустриални центрове при обработка на потоци от информационни ресурси. Основната задача пред мрежовите администратори е изискването за „Киберустойчивост" чрез интегриране на комплексни и адаптивни механизми за технологично управление на информационна сигурност с висока надеждност и бързодействие. Неимоверна е актуалността на проблематиката на дисертационният труд, свързана с разработване на облачно-базирана техническа рамка и методология за анализ на заплахи и рискове за обезпечаване на киберсигурността при зловреден достъп в индустриална среда.

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

Дисертационният труд е с обем от 194 страници и напълно изпълнява дефинираните основни задачи, отразяващи проведените дейности по анализ на състоянието на разглежданата проблематика в съответната предметна област. Силно положително впечатление е значителният обем от анализирана научна информация, обхващаща 240 чуждестранни източнина, отразяващи съвременните нововъведения в областта. Изложението на дисертационния труд се характеризира с висока степен на адекватна интерпретация на научното съдържание и формулиране на насоките на изследванията.

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

В дисертационният труд са съчетани комплексни подходи на основата на аналитични, симулационни и експериментални похвати в качеството на приложими инструменти за систематизиране на:

- Критериите, които трябва да изпълнява облачно-базираната система за оперативен мониторинг на високорискови събития;
- Инструментите и механизмите при проектиране, имплентиране и верифициране на работоспособността на предложената система при различни сценарии в индустриално-производствена среда.

4. Научно-приложни приноси на дисертационния труд.

Според мен може да бъде приложена следната категоризация на приносите по дисертационния труд:

- Разработване на Real-Time Notification Pipeline метод и модели за анализ на OT/ICS детекции с алармени събития и система за автоматизирано уведомяване при детектиране на събития за нарушаване на интегритета на

данните със злонамерени манипулации върху съхранявани информационни ресурси и хардуерно оборудване от D4IoT в индустриални среди с Sentinel интеграция;

- Дефиниране на система от индикатори, аналитични правила и многослоен модел в парадигмата „оперативен мониторинг", анализиращи факторите на мрежовата среда, изработващи независими уведомления при високорискови събития;
- Създаване на модели за оперативен мониторинг, интегриращи механизми за изработване на уведомления при прекъсната облачна свързаност при киберзаплахи;
- Разработване на технически подходи за управление на симетрия на сигурността при Firmware Lifecycle и Version-Aware детекция на понижаване на Firmware;
- Създаване на SIEM-ориентиран модел за установяване и анализ на последствията в отделните фази на зловредни кибератаки към информационни ресурси в индустриални мрежи;
- Синтезиране на рамка от аналитични правила за разпределение, анализ на състоянието и обновяванията на Firmware ресурсите за откриване на потенциални аномалии, както и SPL-базирани правила за изработване на аларми в реално време.

5. Преценка на публикациите по дисертационния труд.

Във връзка със запознаване на научната общност с постигнатите резултати по дисертационния труд по отношение на комплекс от емпирични и експериментални изследвания са реализирани общо шест научни публикации. Представените трудове са индексирани в световно известни бази данни Scopus и IEEE, изнесени на организирани форуми като:

- Национални конференции „TELECOM – [A1], [A3]", "Electronics – [A4]", "ELECTRONICA – [A5]";
- Международни симпозиуми „Symmetry – [A2]"„Network Computing and Applications (NCA), Бостън – [A6]",

и са изготвени в съавторство с научен колектив. В голяма част от публикациите кандидатът е първи автор, което е свидетество за неговото лично дело и висок принос.

Забележителен е броя на цитиранията в издания с висока научна стойност. В предоставените материали е дадена информация за 1 цитиране на публикации [A2], [A3] и 47 цитирания на научен труд [A6]. Според проведена справка в световно известни бази данни Scopus към момента са налични 28 цитирания, което потвърждава, че научните постижения на докторанта са достъпни и известни за широк обхват от изследователи в областта, в страната и чужбина.

6. Мнения, препоръки и бележки.

Не познавам лично кандидата маг. инж. Мариан Христов. Нямам съществени забележки към изложението на дисертационния труд. Предстаните материали свидетелстват за изследовател с висока професионална компетентност и умения за прилагане на най-съвременните технологични достижения в сферата на сигурността. Силно положително впечатление правят множеството сертификати за завършени професионални курсове и обучения с високи технически познания в направление „Киберсигурност и информационна сигурност", издадени от водещи международни организации като "International Sociaty of Automation","Microsoft", "Cisco", "Fortinet

Training Institute", "IACET Accredited Provider", "Claroty", "Технологично училище „Електронни системи"."

Препоръчвам на кандидата да поддържа и награжда основите на своята активна научноизследователска дейност. Налице са силни възможности пред маг. инж. Мариан Христов да профилира своите научни интереси в значително повече професионални направления сред научната общност. Също така да разшири обсега на участие в големи национални и международни проекти и изследователски програми, и своята публикационна дейност в издания с IF референция с висока научна стойност.

1. **Заключение.**

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

- в област на висше образование - 5. Технически науки;
- професионално направление - 5.3 „Комуникационна и компютърна техника";
- докторска програма - „Осигурителна техника и системи".

Дата: 03.06.2026 г. **ЧЛЕН НА ЖУРИТО:**

ОПК78-НС1-023
08.06.2026

[redacted]

OPINION

on dissertation for the awarding
of the educational and scientific degree **"doctor"**

Dissertation Author: **M. Eng. Marian Hristov**
Dissertation Subject: " **Investigation of Cloud-Based System for Events Observation and Analysis** "
Member of Scientific Jury: **Assoc. Prof. Ivelina Balabanova, PhD** – Technical University of Gabrovo

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

The effectiveness of monitoring and identifying legitimate and malicious activities in monitoring, diagnosing and assessing the state of events is a significant challenge for corporate and industrial centers when processing flows of information resources. The main task for network administrators is the requirement for "Cyber Resilience" by integrating complex and adaptive mechanisms for technological management of information security with high reliability and speed. The relevance of the issues of the dissertation work, related to the development of a cloud-based technical framework and methodology for analyzing threats and risks to ensure cybersecurity in the event of malicious access in an industrial environment, is incredibly relevant.

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

The dissertation labor in a volume of 194 pages it effortlessly fulfills the defined basic tasks reflecting conducted activities by analysis on the state on the one under consideration issues in the relevant subject field. A strongly positive impression is the significant volume of analyzed scientific information, covering 240 foreign sources, reflecting modern innovations in the field. The presentation of the dissertation work is characterized by a high degree of adequate interpretation of the scientific content and formulation of the research directions.

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

In the dissertation labor complex approaches based on analytical, simulation and experimental methods are combined quality concepts on applicable tools to systematize:

- The criteria that the cloud-based operational monitoring system for high-risk events must meet;
- The tools and mechanisms for designing, implementing and verifying the performance of the proposed system under various scenarios in an industrial production environment.

4. Contributions of the dissertation work.

In my opinion, the following categorization of contributions to the dissertation can be applied:

- Development of a Real-Time Notification Pipeline method and models for analyzing OT/ICS detections and alarm events and a system for automated notification upon detection of data integrity violation events, malicious manipulations on stored

information resources and hardware equipment from D4IoT in industrial environments with Sentinel integration;

- Defining a system of indicators, analytical rules and a multilayer model in the "Operational monitoring" paradigm, analyzing network environment factors and producing independent notifications for high-risk events;
- Creation of operational monitoring models integrating mechanisms for generating notifications in case of interrupted cloud connectivity due to cyber threats;
- Development of technical approaches for security symmetry management in the Firmware Lifecycle and Version - Aware detection of Firmware downgrades;
- Creation of a SIEM-oriented model for identifying and analyzing the consequences in the individual phases of malicious cyberattacks on information resources in industrial networks;
- Synthesizing a framework of analytical rules for allocation, status analysis and firmware resource updates to detect potential anomalies, as well as SPL-based rules for generating real-time alarms.

5. Assessment of dissertation publications.

In connection with acquaintance on scientific community with the achieved results by the dissertation labor by attitude on complex from empirical and experimental research are realized total six scientific publications. The presented works with indexing in world-renowned databases Scopus and IEEE, exported to organized:

- National conferences "TELECOM - [A1], [A3]" , "Electronics - [A4]", "ELECTRONICA - [A5]";
- International Symposia "Symmetry – [A2]" "Network Computing and Applications (NCA), Boston – [A6]",

are prepared in co-authorship with a scientific team. In a large part of the publications, the candidate is the first author, which is a testament to his personal work and high contribution.

The number of citations in publications of high scientific value is remarkable. The submitted materials provide information about 1 citation of publications [A2], [A3] and 47 citations of a scientific paper [A6]. According to a search conducted in the world-famous Scopus databases, 28 citations are currently available, which confirms that the doctoral student's scientific achievements are accessible and known to a wide range of researchers in the field in the country and abroad.

6. Opinions, recommendations and notes.

I do not personally know the candidate, M. Eng. Marian Hristov. I have no significant comments on the presentation of the dissertation. The materials presented testify to a researcher with high professional competence and skills in applying the most modern technological achievements in the field of security. The numerous certificates for completed professional courses and trainings with high and technical knowledge in the field of "Cybersecurity and Information security" issued from leading international organizations such as "International Society of Automation" , "Microsoft", "Cisco", "Fortinet Training Institute", "IACET Accredited Provider", "Claroty", "Technological School "Electronic Systems".

I recommend that the candidate maintain and reward the foundations of his active research activity. There are strong opportunities for M. Eng. Marian Hristov to profile his scientific interests in significantly more professional areas among the scientific community. Also, to expand the scope of participation in large national and international projects and research programs, and his publication activity in IF- referenced publications of high scientific value.

7. Conclusion.

In conclusion, I can be said that the presented dissertation meets the requirements of the Law on the Development of the Academic Staff in the Republic of Bulgaria and the assessment I summarize for it is completely **positive** . The achieved results give me reason to propose to be awarded the educational and scientific degree "**doctor**" from **M. Eng. Marian Hristov**:

- field of higher education - 5. Technical Sciences;
- in scientific specialty 5.3. "Communication and Computer Technology";
- Doctoral program "Security systems engineering".

Date: 03.06.2026 **MEMBER OF SCIENTIFIC JURY: ..**

/Assoc. Prof. Ivelina Balabanova, PhD/