ФКСТ44-НСЛ-077
13.01.2026 г.

ТЕХНИЧЕСКИ УНИВЕРСИТЕТ ФКСТ СОФИЯ

РЕЦЕНЗИЯ

върху дисертационен труд

за придобиване на образователна и научна степен "**доктор**"

Автор на дисертационния труд: **маг. инж. Любен Асенов Николов**

Тема на дисертационния труд: **„Методи и средства за осигуряване на защита на уеб приложения "**

Рецензент: **проф. д-р Милена Кирилова Лазарова–Мицева**

катедра Компютърни системи, ФКСТ, Технически университет–София

Настоящата рецензия е изготвена в качеството ми на член на научно жури, назначено със Заповед № ОЖ–5.3–59/30.10.2025 г. на Ректора на Технически университет–София и протокол от първо заседание на научното жури от 12.11.2025 г.

Докторантът маг. инж. Любен Асенов Николов е зачислен в задочна докторантура по докторска програма „Компютърни системи, комплекси и мрежи" в професионално направление 5.3 Комуникационна и компютърна техника към катедра „Компютърни системи" във Факултет по Компютърни системи и технологии при Технически университет–София на 1.09.2021 г. Докторантът е изпълнил индивидуалния си план и е положил всички изпити от докторантския минимум. Отчислен е с право на защита на 1.09.2024 г. с решение на ФС на ФКСТ (Протокол №11/26.06.2024 г.) и Заповед №2130/22.07.2024 г. на Ректора на ТУ–София. По предложение на Катедрения съвет на катедра „Компютърни системи" (Протокол №2/20.10.2025 г.) с решение на Факултетния съвет на ФКСТ (Протокол №2/21.10.2025 г.) е взето решение за разкриване на процедура за публична защита на дисертационния му труд.

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

Представеният дисертационен труд е насочен към изследване на методи и средства за осигуряване на защита на уеб приложения и автоматизирано моделиране на заплахи чрез интеграция на статични и динамични тестове на уязвимости за подобряване на сигурността в жизнения цикъл на разработка на софтуер за уеб приложения. Темата на дисертационния труд е изключително актуална, тъй като сигурността на уеб приложенията е сред най-критичните предизвикателства в съвременната информационна среда. С нарастващата дигитализация, внедряването на облачни технологии и DevOps/DevSecOps практики, нуждата от ефективни и автоматизирани решения за откриване и предотвратяване на уязвимости става все по-належаща. Изследването представено в дисертационния труд намира пресечната точка между софтуерното инженерство и киберсигурността, две области с ключово значение за развитието на съвременното информационно общество.

Целта на дисертационния труд е да изследват практиките и методите, използвани за генерирането на уеб хакерски атаки и да се предложи и изследва подход за автоматизирано моделиране на заплахите с интеграция на инструменти за статични и динамични тестове на уязвимости за подобряване на сигурността в жизнения цикъл на разработка на софтуер за уеб приложения с цел постигане на оптимална сигурност и надеждност на приложенията в съвременните динамични и разпределени среди.

Във връзка с формулираната цел на дисертационния труд и на базата на анализ на текущото състояние на проблемната област са формулирани конкретни задачи за постигане на поставената цел: (1) Да бъдат проучени и изследвани подходи, методи и алгоритми за сигурност на данни, които се съдържат в уеб приложения, както и естеството на атаките и тяхното въздействие върху сигурността; (2) Да се изследва възможността за експлоатация на уеб приложения чрез тестване от софтуерни решения за киберсигурност, които се използват за оценка на риска и уязвимостта в уеб приложенията; (3) Да се изследват, разработят и интегрират методи за моделиране на заплахите, статично и динамично тестване на уязвимости, с цел подобряване на сигурността в жизнения цикъл на разработка на софтуер за уеб приложения; (4) Да се предложат методи и решения за сигурност, които имат за цел да осигурят интегритет и защита на данните срещу различни атаки. Определянето на целта и конкретните задачи, свързани с постигането ѝ, са обосновани от автора коректно и изчерпателно.

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

Дисертационният труд обхваща тематика, която включва необходимост от познаване на особеностите на предметните области софтуерно инженерство и киберсигурност, както и спецификата на съществуващите подходи и методи за защита на уеб приложения и автоматизирано моделиране на заплахи. Целта на дисертационния труд и поставените за решаване задачи изискват задълбочено проучване и познаване на съществуващите подходи за статично и динамично тестване на уязвимости, както и на практиките в DevSecOps среда. Литературното проучване е в основата на формулираната цел и свързаните с нея задачи за постигането ѝ. Библиографската справка по дисертационния труд съдържа общо 114 източника, в това число 5 Интернет адреса. Цитираните литературни източници, на които е базиран сравнителния литературен анализ, обхващат научни изследвания и статии в научни издания и международни конференции, като повече от половината от тях са публикувани в последните 5 години. Направеният литературен обзор и сравнителен анализ показват умело интерпретиране от автора на релевантните научни източници от областите софтуерно инженерство и киберсигурност. Чрез критичен анализ на съществуващите подходи и методи за защита на уеб приложения и автоматизирано моделиране на заплахи са определени техните ограничения и възможности за надграждане и е изградена аргументирана основа за разработване на интегриран и иновативен подход за повишаване на сигурността в жизнения цикъл на разработка на уеб приложения. Това свидетелства за отлично познаване на проблематиката и съвременните постиженията в областта от страна на докторанта.

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

Избраната методика за провеждане на научните изследвания се базира на системен сравнителен анализ на особеностите и различните аспекти на разглежданата тематична област, на основата на който е направен обоснован избор на методи и средства за решаване на поставените задачи. Предложените, разработени и изследвани подходи, методи и алгоритми се основават на аргументиран избор, теоретична обосновка, експериментална оценка и верификация на възможностите за практическото им използване, което осигурява не само постигане на целта на дисертацията, но позволява обективна оценка на предложените решения и

постигнатите резултати. Методически дисертационният труд е логически последователен и адекватен по отношение на избраната и приложена методика на провеждане на научните изследвания, което обуславя успешно изпълнение на поставените цел и задачи на дисертационния труд.

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

Представеният дисертационен труд е структуриран в увод, четири глави, заключение, списък с приноси по дисертационния труд, списък с публикации по дисертационния труд, списък с участие в научно-изследователски проекти, списък с фигури, списък с таблици, списък с използвани съкращения, речник за използвани термини, библиографска справка на използваните литературни източници и шест приложения. Общият обем на дисертационния труд е 181 страници. Дисертационният труд съдържа 47 фигури и 15 таблици. Цитирани са 114 литературни източника.

В първа глава първа е представен преглед на съществуващите методи и средства за сигурност на уеб приложенията. Анализирани са подходите за статично (SAST) и динамично (DAST) тестване, както и тяхната интеграция в DevOps и DevSecOps модели. Втора глава е посветена на моделирането на заплахи въз основа на рамката STRIDE. Разгледани са различни инструменти (IriusRisk, Microsoft Threat Modeling Tool, OWASP Threat Dragon и Trike), като са анализирани резултатите от тяхното приложение и сравнителната им ефективност. В трета глава е представен авторски метод за интегриране на моделирането на заплахите в DevSecOps тръбопровод, като са описани експериментални постановки, примери с инструменти като Jenkins, Snyk, OWASP ZAP и Burp Suite, както и резултати от практическото прилагане на метода. Четвърта глава съдържа анализ на експерименталните резултати и сравнение между ръчни, полуавтоматични и автоматизирани методи за моделиране на заплахите. Предложен е усъвършенстван подход за автоматизация и интеграция на моделирането на заплахи с динамичното тестване за уязвимости. В заключението са обобщени основните резултати и приноси, очертани са възможности за бъдещо развитие и практически приложения на изследването в областта на сигурност на уеб приложения.

От представеното изложение, формулираната цел на дисертационните изследвания и поставените във връзка с нея задачи, както и използваните средства за реализиране на целта, може да се направи заключение, че докторантът добре познава състоянието на разглежданите проблеми. На базата на направения анализ на утвърдени теоретични модели и съвременни практически решения за сигурност на уеб приложения е предложен цялостен и автоматизиран DevSecOps-ориентиран подход за управление на сигурността на уеб приложения, който интегрира моделиране на заплахи със статично и динамично тестване. Разработени са метод, рамка и софтуерен прототип, осигуряващи непрекъсната интеграция и валидиране на уязвимости в CI/CD тръбопроводи. Ефективността на предложените решения е доказана чрез експериментална оценка с реално уеб приложение и чрез сравнителен анализ на ръчни, полуавтоматични и автоматизирани техники за моделиране на заплахи. Това ми дава основание да определя получените резултати и свързаните с тях приноси като достоверни и практически полезни.

5. Научни и/или научноприложни приноси на дисертационния труд

Приемам формулираните от автора приноси, постигнати в резултат на извършените научни изследвания. Приносите могат да се отнесат към категориите обогатяване на съществуващо научно знание и научни постижения в практиката, както и създаване на нови и модифициране на съществуващи методи, подходи, модели и алгоритми за решаване на поставените в дисертационния труд задачи.

На базата на получените в дисертационната работа резултати постигнатите приноси могат да бъдат систематизирани като научни, научно-приложни и приложни както следва:

- ***научни приноси:***
  - Разработен е автоматизиран метод за моделиране на заплахи и динамично тестване, който съкращава времето за идентификация и валидиране на уязвимости в уеб приложения с 82% спрямо полуавтоматичния метод за моделиране на заплахи;
- ***научно-приложни приноси:***
  - Извършен е сравнителен анализ на методите за моделиране на заплахи, включително ръчни, полуавтоматични и автоматизирани подходи, като са идентифицирани техните силни и слаби страни;
  - Предложен е цялостен подход за управление на сигурността в CI/CD тръбопроводи чрез интегриране на инструменти за статично (SAST) и динамично (DAST) тестване в DevSecOps рамка;
  - Направена е съпоставка на резултатите от моделирането на заплахи с резултатите от статично и динамично тестване за уязвимости, което гарантира последователност и валидност на анализа;
- ***приложни приноси:***
  - Създаден е софтуерен прототип на автоматизиран конвейер за моделиране на заплахи и динамично тестване, който използва Irius Risk и OWASP ZAP, позволявайки ефективно управление на сигурността в ранните етапи от разработката;
  - Създадена е DevSecOps рамка, която комбинира инструменти за SAST (Snyk), DAST (OWASP ZAP) и моделиране на заплахи и осигурява непрекъсната интеграция и мониторинг на сигурността в CI/CD тръбопроводи;
  - Проведена е експериментална оценка с уеб приложението Spring PetClinic, демонстрираща ефективността на предложените методи и инструменти в реални условия;
  - Разработен е скрипт, който автоматизира процеса на моделиране на заплахи и DAST, като същевременно предоставя възможност за бъдещо надграждане с PYTM за напълно кодова автоматизация.

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

Представеното съдържание и структура на дисертационния труд показват отличното познаване на третираната проблематика от страна на докторанта. Публикуваните четири научни статии във връзка с дисертацията са в съавторство с научния му ръководител като докторантът е водещ автор.

Представените материали по дисертационния труд и публикациите към него правят отлично впечатление за научната работа на маг. инж. Любен Николов, която се характеризира с интердсициплинарност, аналитичност, задълбоченост и прецизност. Считам, че личния му принос във всички етапи на изследването – от концептуалното моделиране до практическата валидация на предложените решения и постигане на резултатите по дисертационния труд е безспорен.

7. Преценка на публикациите по дисертационния труд

Получените от автора резултати от дисертационното изследване са публикувани в 4 научни статии. Една от статиите е публикувана в международно научно списание (WSEAS Transactions on Systems and Control), а другите три са докладвани на международни научни конференции, две от които проведени в чужбина (International Conference on Applied Physics, Simulation and Computing, Рим, Италия, 2024; International Conference on Software, Telecommunications and Computer Networks, Сплит, Хърватия, 2024) и една в България (2023 International Scientific Conference on Computer Science, Созопол). Публикациите са направени в периода 2023–2025 година и покриват тематиката на представената дисертационна работа като отразяват основните постигнати резултати и приноси. Всички статии са на английски език, в съавторство с научния ръководител на докторанта. Всичките публикации са индексирани в Scopus, а едната и в WoS. Две от публикациите имат общо 9 цитирания от чуждестранни автори, в това число в 6 статии индексирани в Scopus.

8. Използване на резултатите от дисертационния труд в научната практика

Във връзка с научните изследвания по дисертационния труд докторантът е участвал в научно-изследователски проект, финансиран от ФНИ към МОН. Не са представени данни за пряко практическо използване на получените резултати от научните изследвания в дисертационния труд, но считам, че получените резултати отговарят на реални потребности на индустрията за подобряване на надеждността и устойчивостта на софтуерните системи срещу киберзаплахи. Приносите по дисертационния труд имат съществен практически потенциал за приложение и внедряване с цел автоматизация на процеса чрез единна непрекъсната верига от идентифициране на заплахи, валидиране чрез динамично сканиране и автоматично генериране на коригиращи действия за постигане на високо ниво на сигурност още на етапа на проектиране и разработване на софтуерните решения. Наред с това резултатите от дисертационния труд имат потенциал за използване за образователни и изследователски цели и биха били полезни на изследователи, докторанти и студенти при провеждане на научни изследвания и при обучение в областта на дисертационните изследвания.

9. Оценка на съответствието на автореферата с изискванията за изготвянето му, както и на адекватността на отразяване на основните положения и приносите на дисертационния труд

Авторефератът към дисертацията съответства на дисертационния труд – вярно и точно отразява целите, задачите, съдържанието по глави, постигнатите приноси. Авторефератът е подготвен и оформен съгласно изискванията за изготвянето му и считам, че безспорно носи същностните черти на дисертационния труд, като отразява в адекватен обем и по коректен начин неговото съдържание.

10. Мнения, препоръки и бележки

Нямам забележки към представения дисертационен труд. Направените забележки при запознаването ми с версията на дисертационния труд, представена за предварително обсъждане в катедрата, са взети под внимание и са отразени в представената дисертация.

Дисертационният труд показва голям обем на извършените научни изследвания. Той е оформен внимателно и старателно с високо ниво на представяне на научните изследвания и свидетелства за отлично запознаване на автора с разгледаните научни проблеми, илюстрира задълбоченост на проведените научни изследвания и дава възможност за по-нататъшното им развитие и практическо използване.

Препоръките ми към докторанта са да продължи научните си изследвания по темата на дисертационния труд и да насочи усилията си към внедряване на разработените подходи и методи в практиката с цел постигане на преки приложни резултати.

Към докторанта имам следните въпроси:

1. Съществуват ли ограничения и специфични изисквания за практическо приложение на разработения автоматизиран метод за моделиране на заплахи и динамично тестване в широк кръг случай на употреба?

2. До колко предложените в дисертационния труд решения са приложими за микросървизни архитектури и необходимо ли е съответно адаптиране за такива приложения?

11. Заключение

На основание на изложеното считам, че дисертационния труд отговаря на изискванията на Закона за развитие на академичния състав в Република България, на Правилника за прилагане на закона и съответния правилник на Технически университет–София и на изискванията за придобиване на образователната и научна степен „доктор". Проведените научни изследвания са в актуална област и третират проблематика, която е обект на засилен изследователски интерес. Авторът е постигнал поставените цели и задачи в дисертационния труд. Получените резултати съдържат научни, научно-приложни и приложни приноси, които са значими, действително са получени и са негово дело. Съществените приноси на дисертационния труд са отразени в научни публикации, които са адекватно разпространени и направени достояние на заинтересованата научна общност чрез публикуването им в научни доклади на конференции и статии в научни списания.

Ето защо давам своята положителна оценка на представения дисертационен труд и предлагам на уважаемите членове на Научното жури да бъде присъдена образователната и научна степен „доктор" на **маг. инж. Любен Асенов Николов** по научна специалност „Компютърни системи, комплекси и мрежи" в професионално направление 5.3 Комуникационна и компютърна техника.

12.01.2026 г.

Рецензент:

/ проф. д-р Милена Лазарова–Мицева /

REVIEW

on a dissertation for "Doctor of Philosophy" degree

Author of the dissertation: **MSc. Eng. Lyuben Asenov Nikolov**

Title of the dissertation: **"New algorithms and models for intelligent agents-assistants in risk environments"**

Reviewer: **Prof. Milena Kirilova Lazarova–Mitseva**, PhD

Dept. Computer Systems, FCST, Technical University of Sofia

This review is prepared in my capacity as a member of the Scientific Jury appointed by Order № ОЖ-5.3-59/30.10.2025 of the Rector of the Technical University of Sofia and Protocol No.1/12.11.2025 from the first meeting of the Scientific Jury.

MSc. Eng. Lyuben Asenov Nikolov was enrolled as a part-time PhD student in doctoral program "Computer systems, complexes, and networks", professional field 5.3 Communication and Computer Engineering" at the Department "Computer Systems" of the Faculty of Computer Systems and Technologies at The Technical University of Sofia on 1.09.2021. The PhD student has fulfilled all the requirements in the individual plan of his PhD study and has successfully passed all the required exams. He was discharged as a PhD with the right to defend his thesis on 1.09.2024 by decision of the Faculty Council of the Faculty of Computer Systems and Technologies (Protocol №11/26.06.2024) and Order № 2130/22.07.2024 of the Rector of the TU–Sofia. The procedure for the public defence of his dissertation has started by a decision of the Department Council of the Department of Computer Systems (Protocol №2/20.10.2025) and the Faculty Council of the Faculty of Computer Science and Technology (Protocol №2/21.10.2025).

1. Relevance of the dissertation topic in scientific and applied aspects

This dissertation addresses a relevant topic related to the methods and means for ensuring web application security and automated threat modeling through integration of static and dynamic vulnerability testing to improve security in the web application software development lifecycle. The topic of the dissertation is extremely relevant as web application security is one of the most critical challenges in today's information environment. With the intensified digitization and the wide implementation of cloud technologies as well as DevOps/DevSecOps practices, the need for effective and automated solutions for detecting and preventing vulnerabilities is becoming increasingly urgent. The research presented in the dissertation finds the intersection between software engineering and cybersecurity, two areas of key importance for the development of the modern information society.

The thesis aim is to explore the practices and methods used to generate web hacking attacks and to propose and investigate an approach for automated threat modeling with the integration of static and dynamic vulnerability testing tools to improve security in the software development lifecycle for web applications in order to achieve optimal security and reliability reliability of applications in today's dynamic and distributed environments.

Based on the analysis of the current state of the art in the problem area several research tasks are defined related to the dissertation aim: (1) Investigate the approaches, methods, and algorithms for data security of web applications as well as the nature of attacks and their impact on security; (2) Investigate the possibility of exploiting web applications by testing them with cybersecurity software solutions used to assess risk and vulnerability in web applications; (3) Investigate, develop and integrate methods for threat modeling, static and dynamic vulnerability testing aimed at improving security in the software development life cycle for web applications; (4) Propose security methods and solutions aimed at ensuring data integrity and protection against various attacks. The dissertation aim and the objectives related to its achievement are correctly and thoroughly formulated and defined.

2. Degree of knowledge on the dissertation topic and constructive interpretation of the bibliography

The dissertation demonstrates a thorough knowledge of the current state of the art in the fields of software engineering and cybersecurity as well as the specifics of existing approaches and methods for protecting web applications and automated threat modeling. The aim of the dissertation and the fulfilment of the defined objectives require in-depth study and knowledge of the existing approaches for static and dynamic vulnerability testing as well as the practices in the DevSecOps environment. The literature review is the basis for the stated dissertation aim and the objectives related to its achievement. The bibliographic reference of the dissertation contains a total of 114 sources, including 5 Internet addresses. The cited literature sources on which the literature analysis is based include research papers and articles in scientific journals and international conferences, more than half of them published in the last 5 years. The literature review and the comparative analysis demonstrate the author's comprehensive interpretation of the relevant scientific sources in the fields of software engineering and cybersecurity. Through critical analysis of the existing approaches and methods for protecting web applications and automated threat modeling, their limitations and opportunities for improvement have been identified and a well-reasoned basis has been established for developing an integrated and innovative approach to enhance the security in the web application development lifecycle. This demonstrates the author's excellent knowledge of the subject matter and contemporary achievements in the field.

3. Consistency of the used research methodology with the dissertation aim and objectives

The chosen methodology for conducting the research study is based on systematic comparative analysis of the features and the different aspects of the research field under consideration. On that basis consistent decisions and selection of methods, algorithms and means are made for solving the dissertation tasks and objectives. The proposed, developed, and investigated approaches, methods, and algorithms are based on well-reasoned decisions, theoretical justification, experimental evaluation, verification and validation of the possibilities of their practical utilization which ensures not only the achievement of the dissertation goals but also the allows objective evaluation of the proposed solutions and the achieved contributions. Methodologically the dissertation is logically consistent and adequate in terms of the chosen and applied methodology of conducting research which determines the successful achievement of the goals and tasks set in the dissertation.

4. Brief analytical characteristic of the dissertation and assessment of the reliability of the material on which the contributions of the dissertation are built

The presented dissertation is structured in an introduction, four chapters, a conclusion, a list of contributions, a list of publications on the dissertation, a list of citations of the publications on the dissertation, a list of participation of the PhD student in research projects, a list of bibliographic references of the used literature sources, a list of figures, a list of tables, a list of used abbreviations and a glossary of used terms and six appendices. The dissertation has 181 pages. The dissertation comprises 47 figures and 15 tables. The list of cited bibliographic references comprises 114 references.

The first chapter of the dissertation presents an overview of the existing methods and tools for web application security and analyzes the approaches for static (SAST) and dynamic (DAST) testing as well as their integration into DevOps and DevSecOps models. The second chapter is devoted to threat modeling based on the STRIDE framework. Various tools (IriusRisk, Microsoft Threat Modeling Tool, OWASP Threat Dragon, and Trike) are examined, and the results of their application and comparative effectiveness are analyzed. The third chapter presents an author's method for integrating threat modeling into the DevSecOps pipeline describing experimental setups, examples with tools such as Jenkins, Snyk, OWASP ZAP, and Burp Suite as well as results from the practical application of the method. The fourth chapter contains an analysis of the experimental results and a comparison between manual, semi-automatic and automated methods for threat modeling. An improved approach for automating and integrating threat modeling with dynamic vulnerability testing is proposed. The conclusion summarizes the main results and contributions of the dissertation, outlines the opportunities for future development and practical applications of the research contributions in the field of web application security.

Based on the dissertation content, the formulated dissertation aim and the research objectives defined in the dissertation as well as the means used for their accomplishment, a conclusion can be made that PhD student is well aware of the state of the art of the scientific topics under consideration.

On the basis of the analysis of established theoretical models and modern practical solutions for web application security, a comprehensive and automated DevSecOps-oriented approach to web application security management is proposed that integrates threat modeling with static and dynamic testing. An automated method, a framework and a software prototype are developed to ensure continuous integration and validation of vulnerabilities in CI/CD pipelines. The effectiveness of the proposed solutions is validated through experimental evaluation with a real web application and comparative analysis of manual, semi-automated, and automated threat modeling techniques. This gives me reason to conclude that the achieved results and the research contributions obtained in the dissertation are reliable and practically valuable.

5. Scientific and applied contributions of the dissertation

I accept the research contributions formulated by the author in his dissertation as a result of the research carried out. The contributions can be related to enrichment of the existing scientific knowledge and scientific achievements in practice as well as development of new and modification of existing approaches, methods, models and algorithms for their application for solving the problems investigated in the dissertation.

On the base of the results obtained in the dissertation the contributions of the dissertation can be classified as scientific, applied-scientific and applied as follows:

- ***scientific contributions:***
  - An automated threat modeling and dynamic testing method is developed that reduces the time required to identify and validate vulnerabilities in web applications by 82% compared to the semi-automated threat modeling method;
- ***applied-scientific contributions:***
  - A comparative analysis of threat modeling methods is performed including manual, semi-automated and automated approaches and their strengths and weaknesses are identified;
  - A comprehensive approach to security management in CI/CD pipelines is proposed by integrating static (SAST) and dynamic (DAST) testing tools into a DevSecOps framework;
  - A comparison is made between the results of threat modeling and the results of static and dynamic vulnerability testing ensuring consistency and validity of the analysis;
- ***applied contributions:***
  - A software prototype of an automated threat modeling and dynamic testing pipeline is developed using Irius Risk and OWASP ZAP that enables effective security management in the early stages of development;
  - A DevSecOps framework is developed that combines tools for SAST (Snyk), DAST (OWASP ZAP) and threat modeling and provides continuous integration and security monitoring in CI/CD pipelines.
  - An experimental evaluation is performed with Spring PetClinic web application that demonstrates the effectiveness of the proposed methods and tools in real-world conditions;
  - A script is developed that automates the threat modeling and DAST process while providing the possibility for future upgrades with PYTM for full code automation.

6. Assessment of the extent of author's personal participation in the dissertation contributions

The presented content and the structure of the dissertation reveals the author's excellent comprehension on the dissertation topic and the presented field of study. The four scientific papers published in connection with the research presented in the dissertation are co-authored with his scientific supervisor with the PhD student as the lead author. The presented dissertation and the research papers on its topic make an excellent impression of the scientific work of MSc. Eng. Lyuben Nikolov, which is characterized by interdisciplinarity, analytical thoroughness and precision. I consider that his personal contribution to all stages of the research – from conceptual modelling to practical validation of the proposed solutions and achievement of the results in the dissertation is undoubted.

7. Evaluation of the author's publications on the dissertation's topic

The results of the dissertation research obtained by the author have been published in 4 scientific papers. One of the papers is published in an international scientific journal (WSEAS Transactions on Systems and Control) and the other three papers are presented at international scientific conferences, two of which are held abroad (International Conference on Applied Physics, Simulation and Computing, Rome, Italy, 2024; International Conference on Software, Telecommunications and Computer Networks, Split, Croatia, 2024) and one is held in Bulgaria (2023 International Scientific Conference on Computer Science, Sozopol). The publications are made in the period 2023–2025 and cover the topics of the presented dissertation reflecting the main achieved results and contributions. All papers are in English and are co-authored with the PhD student's scientific supervisor. All publications are indexed in Scopus and one of them is also indexed in WoS. Two of the publications have a total of 9 citations by foreign authors, including 6 citations in papers indexed in Scopus.

8. Utilization of the dissertation's results and contributions in scientific and social practice

In connection with the research in the dissertation, the PhD student participated in a scientific project funded by the National Science Fund at the Ministry of Education and Science. No data are presented for direct practical utilisation of the results obtained from the research in the dissertation, but I consider the results obtained as relevant to the real needs of the industry for improvement of the reliability and resilience of software systems against cyber threats. The dissertation contributions have significant practical potential for application and implementation for automating the process through a single continuous chain of threat identification, validation through dynamic scanning and automatic generation of corrective actions to achieve a high level of security as early as the design and development stage of software solutions. In addition the dissertation contributions have the potential to be used for educational and research purposes and would be useful to both researchers, PhD students and undergraduates in research and training in the scientific field under consideration.

9. Assessment of the compliance of dissertation's autoreferat with the requirements for its preparation as well as its accurate presentation of the dissertation's content and contributions

The dissertation's autoreferat corresponds to the dissertation thesis – correctly and accurately reflects the dissertation aims and objectives, the content by chapters and the research contributions achieved. The autoreferat is prepared and formatted in accordance with the requirements and I consider that it presents the essential features of the dissertation reflecting in an adequate volume and in a correct manner its content.

10. Comments, recommendations and remarks

I have no comments on the presented dissertation. The comments I made on the version of the thesis submitted for preliminary discussion at the department council are taken into account and are reflected in the submitted thesis.

The dissertation presented for a review reveals a large amount of research studies carried out. It is carefully and thoroughly structured with a high level of presentation of scientific research and demonstrates the author's excellent research comprehension on the addressed scientific problems, reveals the thoroughness of the research carried out and provides an opportunity for its further development and practical utilization.

I would recommend the author to continue his research on the dissertation topic and to focus his efforts towards the implementation of the developed approaches and methods in practice in order to achieve direct applied results.

I have the following questions for the PhD student:

1. Are there any restrictions and specific requirements for the practical application of the developed automated method for threat modeling and dynamic testing in a wide range of use cases?

2. To what extent are the proposed solutions in the dissertation applicable to microservice architectures and is it necessary to adapt them for such applications?

11. Conclusion

Based on the above said I consider the dissertation presented for review in the procedure for awarding the "Doctor of Philosophy" degree as fully corresponding to and fulfilling all the requirements of the Act on the Academic Staff Development in Republic of Bulgaria and the Regulations governing the application of the Act as well as the Regulations for the application of the Act in the Technical University of Sofia. The dissertation topic falls in a relevant scientific field subject to intensive research studies. The author fulfilled the dissertation goals and the objectives. The results obtained contain scientific and applied contributions that are significant for both science and practice and are achieved by the applicant himself. The contributions of the dissertation are published in scientific papers that are adequately disseminated and made available to the international scientific community through presentation and publication in research conference proceedings.

Therefore I am convinced of my positive assessment of the dissertation presented and propose to the honourable members of the Scientific Jury **MSc. Eng Lyuben Asenov Nikolov** to be awarded a "Doctor of Philosophy" degree in the professional field 5.3 "Communication and Computer Engineering", scientific specialty "Computer systems, complexes, and networks".

Date: 12.01.2026

REVIEWER:

/ Prof. Milena Lazarova-Mitseva, PhD /