ФКСТ44-НС1-077
06.04.2026г.

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"
по научно направление 5.3"Комуникационна и компютърна техника" и специалност „Автоматизирани системи за обработка на информация и управление"

Рецензент: проф. д-р Нина Василевна Синягина

1. Общи положения

Дисертационният труд съдържа 180 стр. основен текст, фигури , таблици и диаграми. Състои се от увод, 4 глави, заключение , библиографска справка, справка за приносите , списък на публикации, свързани дисертацията,списък за участие в научни проекти, декларация за оригиналност и 6 приложения Цитираната литература включва над 100 източника на английски език.

2 Актуалност на проблема

Темата на дисертацията е свързана с изследвания в областта на *Методи и средства за дсигуряване на защита на уеб приложения.* С развитието на информацонните технологии и нарастващата им роля в съвременния свят, сигурността на софтуерните системи и по-специално уеб приложения става все по-важна. Ускореното внедряване на нови технологии, като *облачни услуги,инернет на нещата, изкуствен интелект* поставя под заплаха критичните информационни инфраструктури и личните данни. Тяхната защита изисква изследването и внедряването на нови подходи и инструменти, които биха могли да намалят заплахите както по време на разработката, така и на внедряването на съответния софтуер.
В последните години са постигнати значителни успехи при приложение на техниките на моделиране на заплахите и тестове за сигурност (статични и динамични). В настоящия труд докторантът прави опит да намери решения, които интегрират моделирането на заплахите със статично и динамично тестване. Считам че темата на дисертацията е много интересна и актуална.

3. Степен на познаване на състоянието на проблема

Докторантът прави много задълбочен обзор на съвременното състояние на проблематиката, свързана с методи и средства за защита на уеб приложения, като отразява особеностите на статично и динамично сканиране за сигурност (SAST и DAST) и разликите между тях. В дисертацията подробно са разгледани принципите на моделирането на заплахите, като е показана методологията на изследването и различни видове решения за моделирането (Irius Risk, Microsoft Treat Modeling Tool, OWASP Treat Dragon,Trike)

Докторантът демонстрира дълбокото си запознаване с основните понятия и проблеми, свързани с проблематиката, показва,че познава много добре изследваната област, като същевременно отразява и критичното си отношение към някои нерешени задачи.
Библиографската справка включва над 100 заглавия на литературни източници в периода от 2013г. до 2025г., което показва, че той е запознат много добре с известните постижения в избраното научно направление. Направено е подробно разглеждане на резултатите от изследванията, отразени в известните литературни източници, което показва неговите възможности за творческата интерпретация на литературния материал.

4. Цел на дисертацията и избраната методика

Докторантът си поставя следните цели на изследването :
1. *Изследване на практиките и методите, използвани от злонамерени потребители в ИНТЕРНЕТ за генериране на уеб хакерски атаки.*
2. Да бъди предложен подход за автоматизирано моделиране на заплахите, включващ интеграция на статични и динамични тестове на уязвимости и даващ възможност за подобрения в процеса на жизнения цикъл на разработка на софтуера за уеб приложения.
За решаване на поставените цели се формулират следните по-конкретни задачи:

1. Да се проучат и изследват подходи, методи и алгоритми за сигурността на данни в уеб приложенияи, както и естеството на атаките и тяхното въздействие върху сигурността.
2. Да се изследва възможността за експлоатация на уеб приложения чрез тестване на базата на софтуерни решения, използващи оценка на риска и уязвимост при уеб приложения.
3. Да се разработят и интегрират методи за моделиране на заплахите и статично (SAST) и динамично (DAST) тестване, с цел подобряване на сигурнотта при жизнения цикл на разработка на софтуера (SDLC) за уеб приложения.
4. Да се предложат методи и решения за сигурност, даващи възможност за интегритет и защита на данните срещу различни атаки.

За решаване на поставените задачи се използват методи и подходи за моделиране на заплахите, както и алгоритми за статично и динамично тестване.
Считам, че избраните методи и методики за изследване съответстват с поставената цел и конкретните задачи.

5. Аналитичната характеристика на дисертационния труд

В **първата** глава на дисертацията е изложено направеното проучване на съвременното състояние на проблема, свързан с темата на изследването. Разгледани са основните особености на статичен (SAST) и динамичен (DAST) анализ на сигурността. SAST идентифицира уязвимости в ранните етапи, анализирайки изходния код, а DAST тества изпълнимото приложение в реална

среда, като симулира хакерски атаки. Комбинираното им приложение води до по-високо ниво на сигурност, което намалява риска от кибератаки.
В главата също така се акцентира върху моделирането на заплахите, което представлява методология за идентифициране, анализ и класификация на потенциални рискове в информационните системи.Разгледани са редица методи, които дават аналитична рамка за оценка на заплахите и са описани инструменти, осигуряващи автоматизация на процесите на моделирането.

Втората глава е посветена на задача, свързана с моделирането на заплахите въз основа на рамката STRIDE за уеб приложения. Направен е анализ на цялостния подход за създаване на архитектура, включваща като компоненти уеб приложения, разположени върху уеб сървър и свързаната с него база данни. Предложени са четири решения за моделиране на заплахи, като се използват различни инструменти (Irius Risk, Microsoft Threat Modeling Tool, OWASP Threat Dragon, Trike). Всеки инструмент има силни и слаби страни. Докторантът е направил подробен сравнителен анализ.

В **третата** глава се описва подход за интегриране на процеса на моделирането на заплахите в DevSecOps тръбопровод с цел подобрено разработване на софтуера . Представена е рамка за моделирането включваща следните технологии:

1. Виртуална среда с инсталиран Дженкинс сървър върху виртуална машина с инсталиран Window Server, като цялата среда е изградена върху облачна платформа на Microsoft - Azure.
2. Моделиране на заплахите чрез платформата Irius Risk.
3. Динамично сканиране за сигурност с Owasp ZAP.

Интеграцията на заплахите в DevOps тръбопровода представлява значителен напредък в осигуряването на съвременните практики при разработка на софтуера.

В четвъртата глава е представен анализ на експериментални резултати и методи за създаване на диаграми за моделиране на заплахи. Направено е сравнение на подходи за ръчни и автоматизирани начини за моделиране на заплахите. Описан е предложения метод , водещ до подобрение и автоматизиране на процеса на моделиране на заплахите и динамично сканиране за уязвимост. Показани са резултатите от проведените експерименти на моделирането на заплахите и динамично тестване за уязвимост.
В **заключението** е направено резюме на основните резултати от проведеното изследване и са описани перспективи за бъдещото развитие на тематиката.

6.Приноси на дисертационния труд

Приносите в дисертационния труд могат да бъдат обобщени по следния начин:

Научни:

-Предложен е автоматизиран метод за моделиране на заплахи и динамично тестване, съкращаващ времето за идентификация и валидиране на уязвимости в уеб приложения с 82% спрямо полуавтоматизиран метод.

Този принос се отнася към група " **Доказване с нови средства на съществени нови страни не вече съществуващи научни области".**

Научно-приложни:

- Извършен е сравнителен анализ на методите за моделиране на заплахи, включващи ръчни, полуавтоматизирани и автомтизирани подходи.
- Предложен е подход за управление на сигурността в CI/CD тръбопроводи чрез интегриране на инструменти за статично (SAST) и динамично(DAST) тестване в DevSecOps рамка.
- Направено е сравнение на резултатите от моделирането на заплахите с резултатите от тестване за уязвимост, което потвърждава валидност на анализа.

Тези приноси си отнасят към група "**Създаване на нови методи и класификации."**

Приложни:

- Създаден е софтуерен прототип на автоматиирян конвейер за моделиране на заплахи и динамично тестване с използване на инструменти Irius Risk и OWAST ZAP.
- Разработена е DevSecOps рамка, която комбинира инструментите SAST и DAST с моделиране на заплахи, като осигурява мониторинг на сигурността в CI/CD тръбопроводи.
- Проведени са експерименти с уеб приложението Spring PetClinic, демонстриращи ефективнотта на предложените методи.
- Разработен е скрипт, който автоматизира процеса на моделиране на заплахи, като предоставя възможност за бъдещо надграждане с PYTM.

Тези приноси си отнасят към група " **Получаване на потвърдителни факти"**

7. Публикации, свързани с дисертацията

Във връзка с дисертациятата са публикувани 4 труда. От тях единият труд е публикация в " Transaction on Systems and Control , два труда представляват доклади на международни конференции. И четирите труда са в съавторство с други специалисти , като маг. инж. Любен Николов е посочен на първо място
Не са ми известни цитирания на посочените публикации от други автори.

8. Реферат

Авторфератът е написан съгласно изискванията. Съдържанието му изяснява актуалността на тематиката на дисертацията, формулира основната цел и задачи на изследването и отразява получените резултати.

9. Личното участие

Анализ на десертационния труд и представения списък на публикации, свързани с дисертационния труд ми дава основание да направя заключение дисертантът познава много добре състоянието на проблема и нямам никакво основание да се съмнявам в личното му участие в проведените изследвания и в написване на дисертацията.

10.Забележки, мнения и препоръки

Имах възможността да прегледам дисертационния труд преди обсъждането му в катедрата, в резултат на което направих редица принципни и редакционни забележки. Тези забележки и откритите грешки и пропуски са частично отстранени. По настоящия вариант на дисертацията могат да се направят следните забележки и препоръки :

- Стилът на дисертацията на места не е много удачен , излишно усложен и на места трудно разбираем.
- Текстът в много фигури е на английски , а би трябвало да е на български (фиг 13, 14 и др.)
- Алгоритмите на стр 40, 91, 98 , 111 и др.са представени в описателен вид. Графичното представяне е по нагледно и обикновено е прието в научните трудове.
- Фигурите 8, 9, 13, 22 са неясни и липсва обяснение.
- Не е казано ясно, кой е създал модела DevSecOps (стр. 68) и неговата валидация (стр.88).
- На фиг 41 текстът не се чете.
- Цитиранията не са направени в общоприетия вид. Липсва номерация на източници, което затруднява сравнение на текста и съответната литература,

11. Заключение

Независимо от направените забележки, които имат главно редакционен характер,оценката на дисертационния труд е положителна.Като имам предвид съдържащите се в дисертацията безспорни научен, научно-приложни и приложни приноси, актуалността и значимостта на изследваната проблематика, разгласата на постиженията на докторанта в медиите и задълбочените му познания в изследваната област, считам, че дисертационният труд отговаря на изискванията на Закона за развитие на академичния състав в република България и на Правилника за условията и реда за придобиване на научните степени в ТУ-София , поради което предлагам на **маг. инж. Любен Асенов Николов** да бъде присъдена образователната и научна степен "доктор" по научно направление Комуникационна и компютърна техника и научна специалност **"**Автоматизирани системи за обработка на информация и управление**".**

20.12.2025г.

София

РЕЦЕНЗЕНТ:
/проф. д-р Нина В. Синягина/

REVIEW

on a dissertation work for acquisition of the educational and scientific degree "Doctor".

Author of the dissertation work: MSc Eng. Lyuben Asenov Nikolov
Title of the dissertation work: **"Methods and resources for ensuring the security and protection of web applications"**
Scientific field: 5.3 "Communication and Computer Engineering"
Specialty: Automated information processing and management systems"
Reviewer: Prof. Dr. Nina Sinyagina.

1. General remarks

The dissertation work contains 180 pages of main text, figures, tables, and diagrams. It consists of an introduction, four chapters, a conclusion, a bibliographic reference, a statement of contributions, a list of publications related to the dissertation, a list of participation in scientific projects, a declaration of originality and six appendices. The cited literature includes more than 100 sources in the English language.

2 RELEVANCE OF THE TOPIC

The dissertation topic concerns research on *Methods and resources for ensuring the security and protection of web applications*. With the development of information technologies and their increasing role in the modern world, the cybersecurity of software systems, particularly web applications, becomes increasingly important. The Internet of Things and artificial intelligence put critical information infrastructure and personal information at risk. Their protection requires the development and implementation of new approaches and tools that could reduce threats during both the development and deployment of the respective software.

In recent years, significant progress has been made in the area of threat modeling and security testing (static and dynamic). In this work, the doctoral candidate seeks solutions that integrate threat modeling with static and dynamic application security testing. I believe the dissertation topic is very interesting and relevant.

3. Level of familiarity with the state of the problem

The PhD candidate conducts a very in-depth review of the current state and problems related to methods and resources for the cyber protection of web applications, including the specifics of static and dynamic security scanning (SAST and DAST) and their differences. In the dissertation, the principles of threat modeling are examined in detail, and the research methodology and various threat modeling solutions (Irius Risk, Microsoft Threat Modeling Tool, OWASP Threat Dragon, Trike) are presented.

The doctoral candidate demonstrates deep familiarity with the basic concepts and problems related to the studied problematics which confirms his high level of

competence in the researched domain, while at the same time expressing a critical attitude toward some unresolved issues.

The bibliographic reference includes more than 100 literature sources from 2013 to 2025, indicating that he is well informed about the known achievements in the selected scientific field. A detailed analysis of the research results presented in well-known literature sources is carried out, demonstrating his capabilities for creative interpretation of the reviewed literature.

4. Purpose of the dissertation and the chosen methodology

The doctoral candidate sets the following research goals:

1. *Research into the practices and methods used by malicious actors on the INTERNET to generate web hacking attacks.*

2. To propose an approach for automated threat modeling, combined with the integration of static and dynamic vulnerability testing and enabling improvements in the software development lifecycle process for web applications.

For achieving the goals, the following more specific tasks are formulated:

1. To study and research the approaches, methods and algorithms for data security in web applications, as well as the nature of attacks and their impact on security.
2. To investigate the exploitability of web applications through testing based on software solutions using risk and vulnerability assessment methods in web applications.
3. To develop and integrate threat modeling methods, including static (SAST) and dynamic (DAST) security testing to improve the security posture in the software development life cycle (SDLC) for web applications.
4. Propose security methods and solutions to strengthen the data integrity and protection against various types of attacks.

To solve the formulated tasks, threat modeling methods and approaches are used, along with algorithms for static and dynamic security testing.

I consider that the selected methods and research methodologies correspond to the defined research aim and the specific tasks related to this objective.

5. Analytical characteristics of the dissertation work

In the **first** chapter of the dissertation, a study is presented of the current state of the problem related to the research topic. The main characteristics of static (SAST) and dynamic (DAST) security analysis are examined. SAST identifies vulnerabilities at an early stage of the software development lifecycle by analyzing the source code while DAST tests the runtime application in a real environment by simulating hacker attacks. The chapter also emphasizes threat modeling, which represents a methodology for the identification, analysis, and classification of potential risks in information systems. A number of methods are reviewed that provide an analytical framework for threat modeling assessment, along with tools that automate the threat modeling activities.

The **second** chapter is devoted to a task related to threat modeling based on the STRIDE framework for web applications. An analysis of the overall approach for

designing an architecture is carried out, including web applications deployed on a web server and the associated database represented as components on a diagram. Four threat modeling solutions are proposed using different tools (Irius Risk, Microsoft Threat Modeling Tool, OWASP Threat Dragon, Trike). Each tool has its advantages and disadvantages. The PhD candidate has made a detailed comparative analysis.

In the **third** chapter, an approach for integrating the threat modeling process into a DevSecOps pipeline is described with the aim of improved software development process. A threat modeling framework is presented which includes the following technologies:

1. Virtual environment consisted of a Jenkins web server hosted on a Windows Server virtual machine, deployed in the cloud environment Azure supported by Microsoft.
2. Threat modeling through the Irius Risk Software-as-a-Service platform.
3. Dynamic application security testing using the tool Owasp ZAP.

The integration of the threat modeling process into the DevOps pipeline represents a significant advancement, ensuring modern practices in the software development.

The **fourth** chapter presents an analysis of experimental results and methods for creating threat modeling diagrams. A comparison of approaches for manual and automated threat modeling is presented. The proposed method is described, leading to improvement and automation of the threat modeling process and dynamic vulnerability scanning. The results of the conducted experiments on threat modeling and dynamic vulnerability testing are also presented.

In the conclusion, the main results of the research are summarized, and perspectives for future development of the topic are described.

6. Contributions of the dissertation

The contributions of the dissertation can be summarized as follows:

SCIENTIFIC:

- An automated method for threat modeling and dynamic security testing is proposed which reduces the time required for the identification and validation of vulnerabilities in web applications by 82% compared to a semi-automated method. This contribution falls within the group "**Demonstration, using new means of significant new aspects of already existing scientific fields**".

SCIENTIFIC-APPLIED:

- A comparative analysis of threat modeling methods and practices has been conducted including manual, semi-automated and automated approaches.
- An approach for security management in CI/CD pipelines is proposed through the integration of static (SAST) and dynamic (DAST) security testing tools within a DevSecOps framework.
- A comparison between the results of threat modeling and the results of vulnerability testing has been done confirming the validity of the analysis.

These contributions fall within the group "**Creation of new methods and classifications**".

APPLIED:

- A software prototype of an automated pipeline for threat modeling and dynamic vulnerability testing has been developed using the IriusRisk and OWASP ZAP tools.
- A DevSecOps framework has been developed that combines SAST and DAST tools with threat modeling, providing security monitoring within CI/CD pipelines.
- Experiments were conducted using the Spring PetClinic web application, demonstrating the effectiveness of the proposed methods.
- A script has been developed that automates the threat modeling process, providing the possibility for future extension using the PyTM framework. These contributions fall within the group "**Obtaining confirmatory facts.**"

7. PUBLICATIONS CONNECTED TO THE DISSERTATION

In connection with the dissertation, four publications have been published. One of them is a journal publication in "Transactions on Systems and Control," and two are papers presented at international conferences. All four publications are co-authored with other specialists, with M.Eng. Lyuben Nikolov listed as the first author.
No citations of the listed publications by other authors are known to me.

8. AUTHOR'S ABSTRACT

The abstract is written in accordance with the requirements. Its content clarifies the dissertation topic's relevance, formulates the research's main goal and objectives, and reflects the results obtained.

9. PERSONAL PARTICIPATION

An analysis of the dissertation work and the presented list of publications related to the dissertation leads me to conclude that the doctoral candidate understands the state of the problem very well, and I have no reason to doubt his personal participation in the research and in writing the dissertation.

10. REMARKS AND RECOMMENDATIONS REGARDING THE DISSERTATION

I had the opportunity to review the dissertation prior to its discussion in the department, as a result of which I made a number of substantive and editorial comments. These comments, as well as the identified errors and omissions, have been partially addressed. With regard to the current version of the dissertation, the following remarks and recommendations can be made:

- The style of the dissertation in some places is not very appropriate, unnecessarily complicated and at times difficult to understand.
- The text in many figures is in the English language and it should be in Bulgarian (fig 13, 14 etc.)

- The algorithms on pages 40, 91, 98, 111, and others are presented in a descriptive form. Using a graphical representation is more illustrative and is generally accepted in scientific works.
- Figures 8, 9, 13, 22 are not clear and the explanation is missing
- It is not clear who created the DevSecOps model (page 68) and its validation (page 88).
- At figure 41 the text is very difficult to read
- The citations are not presented in a generally accepted format. The absence of source numbering makes it difficult to correlate the text with the corresponding literature.

11. CONCLUSION

Despite the remarks, which are mainly of an editorial nature, the overall assessment of the dissertation is positive. Taking into account the indisputable scientific, scientific-applied, and applied contributions contained within the dissertation, the relevance and significance of the researched topic, the dissemination of the doctoral candidate's achievements in the media, and his in-depth knowledge in the studied field, I consider that the dissertation is in compliance with the requirements based on the Law on the Development of the Academic Staff in the Republic of Bulgaria and the Regulations on the Terms and Procedure for the Acquisition of Academic Degrees at the Technical University of Sofia, therefore, I propose that MEng Lyuben Asenov Nikolov be awarded the educational and scientific degree „Doctor" in the scientific field of **„Communication and Computer Engineering**" and scientific specialty **„Automated information processing and management systems".**

05.01.2026г.
Sofia

Signature:
/ Prof. Dr. Nina Sinyagina /