ФКСТ44 – НС1 – 077
12.01.2026г.

ТЕХНИЧЕСКИ УНИВЕРСИТЕТ ФКСТ СОФИЯ

СТАНОВИЩЕ

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“**

Член на научното жури: **проф. д-р инж. Мариана Евстатиева Горанова**

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

   Съвременното развитие на информационните технологии и тяхната приложимост в съвременния дигитален свят е свързано със защитата на информацията и сигурността на софтуерните системи. Дисертационният труд е посветен на техниките за моделиране на заплахи с цел идентифициране, анализиране и оценяване на потенциалните рискове и тестовете за статично и динамично идентифициране на уязвимости.

   В научно отношение актуалността на изследването се състои в разработката на автоматизирани решения, които интегрират моделирането на заплахи и внедряване на статични и динамични тестове на уязвимости, намаляват времето за откриване и отстраняване на уязвимости, увеличават точността и намаляват влиянието на човешкия фактор.

   В научноприложно отношение са разработени методи за моделиране на заплахи въз основа на рамката STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) – подмяна на самоличност, подправяне, отричане на действие, разкриване на информация, отказ от услуга и повишаване на привилегии. Използвани са инструментите Irius Risk за моделиране на потенциални заплахи и OWASP ZAP (Open Worldwide Application Security Project Zed Attack Proxy) за динамично сканиране за сигурност, подходящи за производствени DevSecOps (Development, Security, and Operations) тръбопроводи – сигурност във всеки етап на процеса за разработване на програми – от първоначалното проектиране през интегриране, тестване, доставка и внедряване.

   За постигане на основната цел са дефинирани следните конкретни задачи: 1) изследване на методи за сигурност на данни в уеб приложения; 2) тестване на уеб приложения за киберсигурност; 3) разработване на методи за моделиране на заплахи, статично и динамично тестване на уязвимости; 4) разработване на методи за интегритет и защита на данните срещу различни атаки.

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

   Обзорът е посветен на съвременното състояние на проблемите, свързани с решенията за управление на сигурността в софтуерните разработки. Разгледани са положителните и отрицателните аспекти при статичното (SAST – Static Application Security Testing) и динамичното (DAST – Dynamic Application Security Testing) тестване. Обърнато е особено внимание на нерешените проблеми – по-прецизни механизми за статичен анализ, подобряване на динамичните тестове, автоматизиране на моделирането на заплахи.

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

   Стандартно практиките за сигурността включват статичен анализ на кода и динамично тестване на работещо приложение. Моделирането на заплахи, с което се намаляват потенциалните рискове още в началните етапи на разработка, е ключов аспект на DevSecOps. Автоматизирането на откриването на заплахи и интегрирането на данните за заплахите в база от данни гарантира разработването на сигурни софтуерни системи в среда на непрекъснато внедряване.

Предложени са три подхода за моделиране на заплахи и динамично тестване на уязвимости: ръчно моделиране, полуавтоматично моделиране чрез стандартни инструменти и автоматизирано моделиране чрез разработен скрипт.

4. Приноси на дисертационния труд.

Приносите на дисертационния труд могат да се обобщят в следните направления:

Научноприложни:

1. Предложен е подход за управление на сигурността в уеб приложения чрез интегриране на инструменти за статично и динамично тестване в DevSecOps рамка.
2. Извършен е сравнителен анализ на ръчни, полуавтоматични и автоматизирани методи за моделиране на заплахи.
3. Извършен е сравнителен анализ на резултатите от моделирането на заплахи и резултатите от статично и динамично тестване на уязвимости.
4. Създаден е автоматизиран метод за моделиране на заплахи и динамично тестване на уязвимости с цел подобряване на сигурността на уеб приложенията.

Приложни:

1. Създаден е автоматизиран конвейер за моделиране на заплахи чрез Irius Risk и динамично тестване чрез OWASP ZAP за управление на сигурността в ранните етапи от разработката.
2. Създадена е DevSecOps рамка за статичен анализ чрез инструмента Snyk, моделиране на заплахи чрез инструмента Irius Risk и динамично тестване чрез инструмента OWASP ZAP.
3. Разработен е скрипт за автоматизиране на процеса за моделиране на заплахи и динамично тестване на уязвимости.

5. Преценка на публикациите по дисертационния труд.

Публикациите се разпределят по рубрики в страната и чужбина, както следва:

1. Публикувани в научни списания в чужбина – 1 бр.
2. Публикувани в сборници на научни конференции в чужбина – 1 бр.
3. Публикувани в сборници на научни конференции в чужбина, реферирани в световно известни бази от данни – 1 бр., 3 бр. цитирания.
4. Публикувани в сборници на научни конференции у нас, реферирани в световно известни бази от данни – 1 бр., 5 бр. цитирания.

Всички публикации са съвместни с научния ръководител. Изпълнени са всички минимални изисквания за броя на публикациите.

6. Мнения, препоръки и бележки.

Тъй като са използвани много техники и инструменти, не навсякъде е обяснено тяхното значение при първото им срещане в текста. Има несъответствие на номерацията на фигурите в дисертационния труд и автореферата.

Считам, че дисертантът успешно се е справил с поставените в дисертацията задачи и набелязани цели. Научните публикации, които отразяват написаното в дисертацията, са приети и положително оценени от научната общност.

Моите препоръки към кандидата са свързани с още по-успешни изследвания в областта на киберсигурността на софтуерните приложения с цел намаляване на времето за целия процес на разработка на софтуер.

7. Заключение.

Въз основа на запознаването ми с дисертационния труд на тема „Методи и средства за осигуряване на защита на уеб приложения“ и съдържащите се в него научноприложни и приложни приноси, намирам за основателно да предложа на Уважаемото жури да присъди образователната и научна степен ДОКТОР на маг. инж. Любен Асенов Николов по научна специалност „Компютърни системи, комплекси и мрежи“ от професионално направление 5.3. Комуникационна и компютърна техника.

София, 12.01.2026 г.

ЧЛЕН НА ЖУРИТО:

/проф. д-р инж. Мариана Горанова/

POSITION

On a Dissertation Thesis for Obtaining
the Educational and Scientific Degree "PhD"

Author of the dissertation: **Lyuben Asenov Nikolov, M. Sc.**

Title of the dissertation: **„Methods and Tools for Securing Web Applications"**

Member of the Scientific Jury: **Prof. Mariana Evstatieva Goranova, PhD**

1. Relevance of the problem developed in the dissertation.

The modern development of information technologies and their applicability in today's digital world is closely connected with information protection and the security of software systems. The dissertation focuses on threat modeling techniques aimed at identifying, analyzing, and evaluating potential risks, as well as tests for the static and dynamic detection of vulnerabilities.

From a scientific perspective, the relevance of the research consists in the development of automated solutions that integrate threat modeling and the implementation of static and dynamic vulnerability tests, reduce the time required to detect and remediate vulnerabilities, improve accuracy, and minimize the influence of the human factor.

From a scientific and applied perspective, methods have been developed for threat modeling based on the STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) framework. The tools Irius Risk for modeling potential threats and OWASP ZAP (Open Worldwide Application Security Project Zed Attack Proxy) for dynamic security scanning have been used, suitable for production DevSecOps (Development, Security, and Operations) pipelines – ensuring security at every stage of the software development process – from initial design through integration, testing, delivery, and deployment.

To achieve the main objective, the following specific tasks have been defined: 1) studying data security methods in web applications; 2) testing web applications for cybersecurity; 3) developing methods for threat modeling, as well as static and dynamic vulnerability testing; 4) developing methods to ensure data integrity and protect against various attacks.

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

The review focuses on the current state of issues related to security management solutions in software development. The positive and negative aspects of static (SAST – Static Application Security Testing) and dynamic (DAST – Dynamic Application Security Testing) testing are analyzed. Particular attention is paid to unresolved problems – more precise mechanisms for static analysis, improving dynamic testing, and automating threat modeling.

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

Standard security practices include static code analysis and dynamic testing of a running application. Threat modeling, which mitigates potential risks early in the development process, is a key aspect of DevSecOps. Automating threat detection and integrating threat data into a database ensures the development of secure software systems in a continuous deployment environment.

Three approaches to threat modeling and dynamic vulnerability testing are proposed: manual modeling, semi-automated modeling using standard tools, and automated modeling using a custom-developed script.

4. Contributions of the dissertation.

The contributions of the dissertation can be summarized in the following areas:

Scientific-applied:

1. An approach for managing security in web applications has been proposed by integrating static and dynamic testing tools within a DevSecOps framework.
2. A comparative analysis of manual, semi-automated, and automated threat modeling methods has

been performed.

3. A comparative analysis of threat modeling results and the results of static and dynamic vulnerability testing has been conducted.
4. An automated method has been created for threat modeling and dynamic vulnerability testing to enhance the security of web applications.

Applied:

1. An automated pipeline has been created for threat modeling using Irius Risk and dynamic testing using OWASP ZAP to manage security in the early stages of development.
2. A DevSecOps framework has been established for static analysis using the Snyk tool, threat modeling with the Irius Risk tool, and dynamic testing with the OWASP ZAP tool.
3. A script has been developed to automate the process of threat modeling and dynamic vulnerability testing.

5. Evaluation of the publications on the dissertation.

The publications are categorized by type in the country and abroad as follows:

1. Published in scientific journals abroad – 1 item.
2. Published in conference proceedings abroad – 1 item.
3. Published in conference proceedings abroad, indexed in internationally recognized databases – 1 item, 3 citations.
4. Published in conference proceedings in the country, indexed in internationally recognized databases – 1 item, 5 citations.

All publications are co-authored with the scientific supervisor. All minimum requirements for the number of publications have been met.

6. Opinions, recommendations and remarks.

Since many techniques and tools have been used, their significance is not explained everywhere at their first mention in the text. There is a discrepancy in the figure numbering between the dissertation and the abstract.

I believe that the doctoral candidate has successfully addressed the tasks and objectives set out in the dissertation. The scientific publications reflecting the dissertation's content have been accepted and positively evaluated by the scientific community.

My recommendations to the candidate concern conducting even more successful research in the field of cybersecurity for software applications, aiming to reduce the time required for the entire software development process.

7. Conclusion.

Based on my review of the dissertation entitled "Methods and Tools for Securing Web Applications" and the scientific-applied and applied contributions contained therein, I find it appropriate to recommend to the Honorable Jury to award the educational and scientific degree of PhD to Lyuben Asenov Nikolov, M. Sc., in the scientific specialty "Computer Systems, Complexes, and Networks" from the professional field 5.3. Communication and Computer Equipment.

Sofia, 12.01.2026

Member of the Scientific Jury:

/Prof. Mariana Goranova, PhD/