ФКСТ-НС1-077
08.01.2026 г.

ТЕХНИЧЕСКИ УНИВЕРСИТЕТ ФКСТ СОФИЯ

СТАНОВИЩЕ

върху дисертационен труд за придобиване на научна степен „доктор“
професионално направление 5.3 „Комуникационна и компютърна техника“
научна специалност „Компютърни системи, комплекси и мрежи“

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. Атанас Велков Атанасов, ХТМУ-София

1. Актуалност на дисертационния труд

В последните години се отбелязва рязко повишаване на ръста на киберпрестъпността, на течовете на данни и на броя на засегнатите потребители. Увеличените възможности за кибератаки и уязвимости, възникващи още в началните етапи на разработката на софтуера, създават сериозни рискове за информационната сигурност, особено при използване на уеб приложения, облачни услуги, IoT технологии и изкуствения интелект. В този контекст става все по-наложително прилагането на интегрирани и автоматизирани подходи за сигурност, които обединяват моделирането на заплахите със статично и динамично тестване с цел навременно откриване и ефективно смекчаване на уязвимости в съвременните софтуерни системи.

Настоящият дисертационен труд е свързан именно с такива подходи и решения, които могат да намалят времето за откриване и валидиране на уязвимости, като същевременно увеличат точността и намалят зависимостта от човешки фактор.

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

Докторантът маг. инж. Любен Николов демонстрира задълбочено познаване на проблемите, свързани с идентифицирането на киберуязвимостите и заплахите на всички етапи от жизнения цикъл на разработка на софтуер за уеб приложения, базирани на DevOps и DevSecOps технологията. В дисертацията са цитирани общо 109 литературни източници и 5 интернет адреси, като всичките са на английски. От направения литературен анализ в областите на статичното (SAST) и динамичното (DAST) тестване на сигурността на уеб приложения и тяхната интеграция с допълнителни подходи като интерактивното тестване (IAST), защита по време на работа на приложението (RASP) и техниките за моделиране на заплахи, се вижда, че темата на дисертацията е значима и актуална.

Въз основа на анализа правилно са формулирани целите и задачите на дисертационния труд. Позицията и творческите приноси на автора са ясно изразени, както в дисертационния труд така и в представените публикации.

3. Съответствие на предложената методика на изследване и поставените цел и задачи на дисертационния труд

Целта на дисертационния труд е да изследва практиките и методите, които се използват от злонамерени потребители в интернет за генерирането на уеб хакерски атаки, както и да предложи и изследва подход за автоматизирано моделиране на заплахите. Този подход е ориентиран към откриване и минимизиране на уязвимости на различни етапи от жизнения цикъл на разработка на уеб-базиран софтуер, както и значително намаляване на времето за целия процес на разработка. Това включва използването на софтуерни инструменти и статични и динамични тестове на уязвимости за подобряване на сигурността и надеждността на съвременните софтуерни системи, работещи в динамични и разпределени среди.

От така дефинираната цел и подцели произтичат и основните задачи на дисертационния труд, които са ясно формулирани и обосновани: -Проучване и изследване на подходи, методи и алгоритми за сигурност на данни, които се съдържат в уеб приложения, както и естеството на атаките и тяхното въздействие върху сигурността; Изследване на 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; Разработване и интегриране на методи за моделиране на заплахите, както и статично и динамично тестване на уязвимости, с цел подобряване на сигурността на уеб приложения, базирани на DevOps модела. Разработка на методи и решения за сигурност, които имат за цел да осигурят интегритет и защита на данните срещу различни атаки.

За решаване на поставените задачи са използвани подходящи модели, методи и инструменти за моделиране на заплахи и оценяване на риска като модела STRIDE, платформата IriusRisk, приложенията Microsoft Threat Modeling Tool (MTMT), OWASP Threat Dragon и инструмента Trike. Всички тези софтуерни инструменти са използвани при разработката на уеб-базирано приложение в средата на DevSecOps конвейер.

Считам, че използваните в дисертацията методи, подходи и средства за анализ са адекватни на поставената цел и задачи.

4. Научни, научно-приложни и приложни приноси на дисертационния труд

Приемам всички заявени от маг. инж. Любен Николов приноси, формулирани като:

Научни:

– Разработен е автоматизиран метод за моделиране на заплахи и динамично тестване, който съкращава времето с 82% за идентификация и валидиране на уязвимости в уеб приложения спрямо полуавтоматичния метод за моделиране на заплахи.;

Научно-приложни:

– Извършен е сравнителен анализ на методите за моделиране на заплахи, както и ръчните, полуавтоматичните и автоматизираните подходи, като са идентифицирани техните силни и слаби страни.

– Предложен е цялостен подход за управление на сигурността в CI/CD конвейери чрез интегриране на инструменти за статично и динамично тестване в DevSecOps рамка.

– Съпоставени са резултатите от моделирането на заплахи с резултатите от статично и динамично тестване за уязвимости, гарантиращо последователност и валидност на анализа.

Приложни:

– 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 конвейери.

– Проведени са експерименти с уеб приложението Spring PetClinic, демонстриращи 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.

5. Преценка на публикациите по дисертационния труд

Докторантът маг. инж. Л. Николов е представил 4 публикации, които са вързани с проблемите и задачите решавани в дисертационния труд. Три от тях са представени в български и международни научни конференции, реферирани в Scopus, а четвъртата е представена в международно научно списание, като всичките са отпечатани в пълен текст.

Всички публикации на докторанта са в съавторство с научния му ръководител, като във всички докторантът е първи съавтор. Към този момент са известни седем цитата на публикациите, като три от цитиранията са в статии, индексирани в Scopus, което подчертава значимостта на постиженията на докторанта. Сборът от точките на публикациите надвишава двукратно изискуемия минимум, заложен в Правилника за условията и реда за придобиване на научната степен "Доктор" на ТУ-София по съответното професионално направление.

6. Мнения, препоръки и бележки

Към представената дисертация нямам съществени забележки.

Считам, че докторантът има научен потенциал за провеждане на самостоятелни изследвания, както в областта на компютърните системи и мрежи, така и в защитата на уеб-базирани софтуерни системи.

Имам една забележка свързана с използвания в дисертацията термин „DevOps pipeline“, и неговия превод „DevOps тръбопровод“. Тъй като DevOps е един от гъвкавите модели, описващ етапите на разработка на софтуер, смятам, че по-точният превод е „DevOps конвейер“.

ЗАКЛЮЧЕНИЕ

Оценката ми относно съдържанието на дисертационния труд и приносите на маг. инж. **Любен Асенов Николов е положителна**. Дисертантът е извършил значителна по обем и съдържание изследователска работа. Дисертационният труд отговаря напълно на изискванията на Закона за развитие на академичния състав на Република България, на Правилника за неговото приложение и на Правилника за условията и реда за придобиване на научни степени в Техническия Университет – София.

Гореизложеното ми дава основание да препоръчам на Уважаемото Научно жури **да присъди на инж. Любен Асенов Николов образователната и научната степен „доктор“** по професионално направление 5.3 Комуникационна и компютърна техника, научна специалност „Компютърни системи, комплекси и мрежи“.

София, 08. 01. 2026 г.

Член на журито:

/проф. д-р инж. А. Атанасов/

OPINION

**on a dissertation work for obtaining a scientific degree "Doctor"
professional direction 5.3 "Communication and computer technology"
scientific specialty "Computer systems, complexes and networks"**

Author of the dissertation: MSc, Lyuben Asenov Nikolov
Dissertation title: "Methods and means for ensuring the protection of WEB applications"
Member of the scientific jury: Prof. Dr. Eng. Atanas Velkov Atanassov, UCTM-Sofia

1. **Actuality of the dissertation**

In recent years, there has been a sharp increase in the growth of cybercrime, data leaks and the number of affected users. The increased opportunities for cyberattacks and vulnerabilities, arising even in the initial stages of software development, create serious risks for information security, especially when using web applications, cloud services, IoT technologies and artificial intelligence. In this context, the implementation of integrated and automated security approaches that combine threat modeling with static and dynamic testing is becoming increasingly urgent in order to timely detect and effectively mitigate vulnerabilities in modern software systems.

The current dissertation work is related to such approaches and solutions that can reduce the time for detecting and validating vulnerabilities, while increasing accuracy and reducing dependence on the human factor.

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

The PhD. student MSc. Eng. Lyuben Nikolov, demonstrates in-depth knowledge of the problems related to the identification of cyber vulnerabilities and threats at all stages of the software development life cycle for web applications based on DevOps and DevSecOps technology. The dissertation cites a total of 109 literary sources and 5 Internet addresses, all of which are in English. From the literature analysis in the areas of static (SAST) and dynamic (DAST) security testing of web applications and their integration with additional approaches such as interactive testing (IAST), runtime application protection (RASP) and threat modeling techniques, it is clear that the topic of the dissertation is significant and relevant.

Based on the analysis, the goals and objectives of the dissertation are correctly formulated. The author's position and creative contributions are clearly expressed, both in the dissertation and in the presented publications.

3. **Correspondence of the chosen research methodology with the set goal and tasks of the dissertation work.**

The goal of the dissertation is to investigate the practices and methods used by malicious users on the Internet to generate web hacking attacks, as well as to propose and research an approach for automated threat modeling. This approach is oriented towards detecting and minimizing vulnerabilities at different stages of the web-based software development life cycle, as well as significantly reducing the time for the entire development process. This includes the use of software tools and static and dynamic vulnerability testing to improve the security and reliability of modern software systems operating in dynamic and distributed environments.

From the thus defined goal and subgoals, the main tasks of the dissertation arise, which are clearly formulated and justified: -Research and investigation of approaches, methods and algorithms for data security contained in web applications, as well as the nature of attacks and their impact on security; Research into the possibility of exploiting web applications through testing by cybersecurity software solutions used to assess risk and vulnerability in web applications; Development and integration of threat modeling methods, as well as static and dynamic vulnerability testing, in order to improve the security of web applications based on the DevOps model. Development of security methods and solutions that aim to ensure data integrity and protection against various attacks.

To solve the tasks set, appropriate models, methods and tools for threat modeling and risk assessment were used, such as the STRIDE model, the IriusRisk platform, the Microsoft Threat Modeling Tool (MTMT) applications, OWASP Threat Dragon and the Trike tool. All of these software tools were used in the development of a web-based application in the DevSecOps pipeline environment.

I believe that the methods, approaches and analysis tools used in the dissertation are adequate to the set goal and tasks.

4. Scientific and/or applied science contributions of the dissertation.

I accept all contributions stated by MSc. L. Nikolov, which he formulated as:

The scientific:

– An automated method for threat modeling and dynamic testing has been developed, which reduces the time by 82% for identifying and validating vulnerabilities in web applications compared to the semi-automatic method for threat modeling;

The scientific and applied:

– A comparative analysis of threat modeling methods, as well as manual, semi-automatic and automated approaches, has been performed, identifying their strengths and weaknesses;

– A comprehensive approach to security management in CI/CD pipelines has been proposed by integrating static and dynamic testing tools into the DevSecOps framework;

– The results of threat modeling have been compared with the results of static and dynamic vulnerability testing, ensuring consistency and validity of the analysis.

The applied:

– A software prototype of an automated threat modeling and dynamic testing pipeline was created, which uses Irius Risk and OWASP ZAP, enabling effective security management in the early stages of development;

– A DevSecOps framework was created, which combines SAST (Snyk), DAST (OWASP ZAP) and threat modeling tools and provides continuous integration and security monitoring in CI/CD pipelines;

– Experiments were conducted with the Spring PetClinic web application, demonstrating the effectiveness of the proposed methods and tools in real-world conditions;

– A script was developed that automates the threat modeling and DAST process, while providing the ability to be future-proofed with PYTM for full code automation.

5. Evaluation of the publications on the dissertation

The PhD student, MSc. Eng. L. Nikolov, has presented 4 publications related to the problems and tasks solved in the dissertation. Three of them have been presented at Bulgarian and international scientific conferences, referenced in Scopus, and the fourth has been presented in an international scientific journal, all of which have been printed in full text. All of the doctoral student's publications are co-authored with his scientific supervisor, and in all of them the doctoral student is the first co-

author. At this moment, seven citations of the publications are known, with three of the citations being in articles indexed in Scopus, which emphasizes the significance of the doctoral student's achievements. The sum of the points of the publications exceeds twice the required minimum set out in the Regulations on the conditions and procedure for acquiring the scientific degree "Doctor" of TU-Sofia in the relevant professional field.

6. Notes, opinions and recommendations

I have no significant comments on the presented dissertation.

I believe that the doctoral student has the scientific potential to conduct independent research, both in the field of computer systems and networks, and in the protection of web-based software systems.

CONCLUSION

My assessment of the content of the dissertation and the contributions **of MSc. Eng. Lyuben Asenov Nikolov is positive.** The dissertation candidate has carried out significant research work in terms of volume and content. The dissertation fully meets the requirements of Law on the Development of the Academic Staff of the Republic of Bulgaria, the Regulations for its Application and the Regulations for the Conditions and Procedures for Acquiring Scientific Degrees at the Technical University - Sofia.

The above gives me reason to recommend to the Honorable Scientific Jury **to award MSc. Eng. Lyuben Asenov Nikolov the educational and scientific degree "Doctor"** in professional direction 5.3 Communication and Computer Engineering, scientific specialty "Computer systems, complexes and networks".

Sofia, 08. 01. 2026

Jury member:

/Prof. Dr. Eng. Atanas Atanassov/