Univerzitet Crne Gore
Prirodno-matematički fakultet

Džordža Vašingtona b.b.
1000 Podgorica, Crna Gora

tel: +382 (0)20 245 204
fax: +382 (0)20 245 204
www.pmf.ac.me

Broj: 2024/01-1924/1
Datum: 05.09.2024

UNIVERZITET CRNE GORE

-CENTAR ZA DOKTORSKE STUDIJE-

U prilogu akta dostavljamo odluku Vijeća Prirodno matematičkog fakulteta sa CXX sjednice održane 3.9.2024.godine.

DEKAN
Prof. dr Miljan Bigović

Univerzitet Crne Gore
Prirodno-matematički fakultet

Džordža Vašingtona b.b.
1000 Podgorica, Crna Gora

tel: +382 (0)20 245 204
fax: +382 (0)20 245 204
www.pmf.ac.me

Broj: 2024/01-1924/2
Datum: 05.09.2024

Na osnovu člana 64 Statuta Univerziteta Crne Gore, a u vezi sa članom 41 stav 1 Pravila doktorskih studija, na CXX sjednici Vijeća Prirodno-matematičkog fakulteta, održanoj dana 3.9.2024.godine, je donijeta je

O D L U K A

I

Utvrđuje se da su ispunjeni uslovi iz člana 38 Pravila doktorskih studija za doktoranda Msc Krenara Kepusku.

II

Predlaže se Odboru za doktorske studije sastav komisije za ocjenu doktorske disertacije:

1. Dr Srđan Kadić, docent na Prirodno-matematičkom fakultetu Univerziteta Crne Gore (naučna oblast: Softverski inžinjerstvo);
2. Dr Milo Tomašević, redovni profesor Elektrotehničkog faklteta Univerziteta u Beogradu (naučna oblast: Paralelni sistemi, Algoritimi, Kriptografija);
3. Dr Savo Tomović, redovi profesor Prirodno-matematičkog fakulteta Univerziteta Crne Gore (naučna oblast: Analiza i obrada podataka. Data mining);
4. Dr Maja Vukasović, docent na Elektrotehničkom fakultetu Univerziteta u Beogradu (naučna oblast: Zaštita podataka, prevodioci) i
5. Dr Aleksandar Popović, vanredni profesor Prirodno-matematičkog fakulteta Univerziteta Crne Gore (naučna obvlast: Softversko inžinjerstvo)

III

Odluka se dostavlja Odboru za doktorske studije Univerziteta Crne Gore.

DEKAN
Prof. dr Miljan Bigović

ISPUNJENOST USLOVA DOKTORANDA

OPŠTI PODACI O DOKTORANDU			
Titula, ime, ime roditelja, prezime	MSc, Krenar, Xhelal, Kepuska		
Fakultet	Prirodno-matematički fakultet		
Studijski program	Računarske nauke		
Broj indeksa	1/2016		
NAZIV DOKTORSKE DISERTACIJE			
Na službenom jeziku	Pristup penetracionog testiranja u veb aplikacijama kao proaktivna i odbrambena tehnologija		
Na engleskom jeziku	Penetration test approach in web applications as a proactive and defensive technology		
Naučna oblast	Računarske nauke		
MENTOR/MENTORI			
Prvi mentor	Milo Tomašević	Elektrotehnički fakulet Univerziteta u Beogradu, Srbija	Paralelni sistemi, adlogritmi, kriptografija
Drugi mentor	(Titula, ime i prezime)	(Ustanova i država)	(Naučna oblast)
KOMISIJA ZA PREGLED I OCJENU DOKTORSKE DISERTACIJE			
Doc. dr Srđan Kadić		Prirodno-matematički fakultet, Univerzitet Crne Gore, Crna Gora	Softversko inženjerstvo
Prof. dr Milo Tomašević		Elektrotehnički fakulet Univerziteta u Beogradu, Srbija	Paralelni sistemi, alogritmi, kriptografija
Prof. dr Savo Tomović		Prirodno-matematički fakultet, Univerzitet Crne Gore, Crna Gora	Analiza i obrada podataka - data mining
Doc. dr Maja Vukasović		Elektrotehnički fakulet Univerziteta u Beogradu, Srbija	Zaštita podataka, prevodioci
Prof. dr Aleksandar Popović		Prirodno-matematički fakultet, Univerzitet Crne Gore, Crna Gora	Softversko inženjerstvo
Datum značajni za ocjenu doktorske disertacije			
Sjednica Senata na kojoj je data saglasnost na ocjenu teme i kandidata	07-08.05.2020.		

Dostavljanja doktorske disertacije organizacionoj jedinici i saglasanost mentora	11.07.2024.god
Sjednica Vijeća organizacione jedinice na kojoj je dat prijedlog za imenovanje komisija za pregled i ocjenu doktorske disertacije	03.09.2024.god

ISPUNJENOST USLOVA DOKTORANDA

U skladu sa članom 38 pravila doktorskih studija kandidat **je** cjelokupna ili dio sopstvenih istraživanja vezanih za doktorsku disertaciju publikovao u časopisu sa **(SCI/SCIE)/(SSCI/A&HCI)** liste kao prvi autor.

Spisak radova doktoranda iz oblasti doktorskih studija koje je publikovao u časopisima sa (upisati odgovarajuću listu)

Kepuška K., Tomašević M., "A lightweight framework for cyber risk management in Western Balkan higher education institutions, ", *PEERJ Computer Science*, April 2024, pp. 1-3, DOI: http://doi.org/10.7717/peerj-cs.1958, ISSN: 1532-0626, Impact factor (2022): 3.8

Obrazloženje mentora o korišćenju doktorske disertacije u publikovanim radovima

U radu objavljenom u vodećem međunarodnom časopisu *PEERJ Computer Science* autor je koncipirao i predožio lagani okvir namenjen povećanju sigurnosti veb aplikacija u akademskim institucijama. Ovaj okvir je zasnovan na proaktvnoj metodologiji penetracionog testiranja koja je glavna tema ove disertacije. Disertacija se posebno fokusira na zemlje zapadnog Balkana, prepoznajući jedinstvene potrebe i izazove u oblasti sajber bezbednosti sa kojima se suočavaju akademske institucije u ovom regionu.

Datum i ovjera (pečat i potpis odgovorne osobe)

U Podgorici,
2. 7. 2024.

UNIVERZITET CRNE GORE Prirodno-matematički fakultet UCG MP

DEKAN

Prilog dokumenta sadrži:

1. Potvrdu o predaji doktorske disertacije organizacionoj jedinici
2. Odluku o imenovanju komisije za pregled i ocjenu doktorske disertacije
3. Kopiju rada publikovanog u časopisu sa odgovarajuće liste
4. Biografiju i bibliografiju kandidata
5. Biografiju i bibliografiju članova komisije za pregled i ocjenu doktorske disertacije sa potvrdom o izboru u odgovarajuće akademsko zvanje i potvrdom da barem jedan član komisije nije u radnom odnosu na Univerzitetu Crne Gore

Univerzitet Crne Gore
Prirodno-matematički fakultet

Džordža Vašingtona b.b.
1000 Podgorica, Crna Gora

tel: +382 (0)20 245 204
fax: +382 (0)20 245 204
www.pmf.ac.me

Broj: 2024/01-1881
Datum: 11.07.2024

Na osnovu člana 33 Zakona o upravnom postupku, nakon uvida u službenu evidenciju, Prirodno-matematički fakultet izdaje

P O T V R D U

MSc Krenar Kepuska, student doktorskih studija na Prirodno-matematičkom fakultetu u Podgorici, dana 11.07.2024.godine dostavio je ovom fakultetu doktorsku disertaciju pod nazivom ***"Penetration test approach in web applications as a proactive and defensive technology"*** na dalje postupanje.

UNIVERZITET CRNE GORE Prirodno-matematički fakultet

D E K A N
Prof. dr Miljan Bigović

Univerzitet Crne Gore

Prirodno-matematički fakultet

Na osnovu člana 37 Pravila doktorskih studija Univerziteta Crne Gore dajem

SAGLASNOST

da doktorska disertacija pod naslovom "Pristup penetracionog testiranja u veb aplikacijama kao proaktivna i odbrambena tehnologija" (Penetration test approach in web applications as a proactive and defensive technology) kandidata MSc Krenara Kepuske zadovoljava kriterijume propisane Statutom Univerziteta Crne Gore I pravilima doktorskih studija.

Beograd, 2.7.2024.

Mentor

Prof. dr Milo Tomašević

PeerJ Computer Science

A lightweight framework for cyber risk management in Western Balkan higher education institutions

Krenar Kepuska[1] and Milo Tomasevic[2]

[1] Computing and Information Technology, Rochester Institute of Technology - Kosovo, Pristina, Kosovo
[2] Faculty of Electrical Engineering, University of Belgrade, Belgrade, Serbia

ABSTRACT

Higher education institutions (HEIs) have a significant presence in cyberspace. Data breaches in academic institutions are becoming prevalent. Online platforms in HEIs are a new learning mode, particularly in the post-COVID era. Recent studies on information security indicate a substantial increase in cybersecurity attacks in HEIs, because of their decentralized e-learning structure and diversity of users. In Western Balkans, there is a notable absence of incident response plans in universities, colleges, and academic institutions. Moreover, e-learning management systems have been implemented without considering security. This study proposes a cybersecurity methodology called a lightweight framework with proactive controls to address these challenges. The framework aims to identify cybersecurity vulnerabilities in learning management systems in Western Balkan countries and suggest proactive controls based on a penetration test approach.

Subjects Algorithms and Analysis of Algorithms, Computer Education, Cryptography, Security and Privacy
Keywords Information security management, Software simulations, Higher education institution, Western Balkan countries

Submitted 21 December 2023
Accepted 4 March 2024
Published 10 April 2024

Corresponding author
Krenar Kepuska, krkcad@rit.edu

Academic editor
Sedat Akleylek

Additional Information and Declarations can be found on page 20

DOI 10.7717/peerj-cs.1958

INTRODUCTION

In the context of higher education institutions (HEIs), the learning management system (LMS) assumes a pivotal role, serving as a vital tool utilized by a diverse range of individuals, as observed (*Maryam & Mostafa, 2021*; *Josac et al., 2019*). These platforms store sensitive data, including personally identifiable information (PII) of students, email account particulars, intellectual property (I.P.), funding details, medical records, employment contracts, academic transcripts, research data, and other vital information, as underscored (*Ulven & Wangen, 2021*; *Pinheiro, 2020*). Recent investigations into information security emphasize a discernible increase in cybersecurity threats within HEIs, primarily ascribed to the decentralized structure of e-learning and the diverse composition of the user base. The primary factors behind incidents in HEIs are identified as social engineering tactics and vulnerabilities within e-learning platforms, as articulated (*Pinheiro, 2020*; *Wangen, 2019*). 35% of all data breaches in the world occur in HEIs. In addition, between 2019 and 2020, 54% of an astounding 35% of global data breaches are concentrated within HEIs, underscoring the severity of the prevailing situation. Notably, the period

spanning 2019 to 2020 witnessed a substantial 54% of HEIs in the United States reporting data breaches, as substantiated (*OpenSSF, 2022*; *Irwin, 2022*; *Chapman, 2021*). Consequently, the exigency for effective cybersecurity management has assumed paramount significance within universities and other academic establishments. This urgency is driven by the realization that the computer systems of these institutions serve as repositories for sensitive data emanating from a diverse array of users, including students, instructors, and various other personnel, as elucidated (*Pinheiro, 2020*; *OpenSSF, 2022*).

HEIs in the Western Balkan region encounter distinct cybersecurity challenges, especially in crafting and executing incident response strategies. These difficulties are influenced by the region's specific financial, technological, and educational contexts. A notable scarcity of cybersecurity expertise in the area further complicates matters. This lack of skilled professionals undermines the institutions' abilities to respond swiftly and effectively to cybersecurity incidents, leaving them vulnerable to timely threat identification, containment, and mitigation. An overarching challenge is the prevalent underestimation of cybersecurity's significance within these educational communities. The deficiency in awareness and training among faculty and students augments the risk, as the human element often becomes the weakest link in cybersecurity. Untrained individuals are more susceptible to deceptive tactics like phishing or social engineering. A pivotal aspect of cybersecurity in HEIs is protecting the confidentiality and integrity of student and staff data. The institutions often grapple with aligning their data management practices with regional and international data protection statutes, further complicating their cybersecurity landscape. To navigate these challenges effectively, a multi-dimensional strategy is essential. This strategy should bolster IT infrastructure, recruit and train cybersecurity personnel, develop versatile and robust incident response plans, and cultivate a pervasive culture of cybersecurity awareness within the academic ecosystem. Such a holistic approach is crucial for mitigating cyber risks and enhancing the overall cybersecurity posture of HEIs in the Western Balkans.

The lack of cybersecurity resilience in HEIs in Western Balkan countries can be attributed to various factors, ranging from economic constraints to infrastructural and educational challenges. HEIs in Western Balkan countries often face budgetary constraints, limiting their ability to invest in advanced cybersecurity infrastructure, tools, and technologies. There is frequently a gap in skilled cybersecurity professionals in the region. This shortage affects the institutions' capacity to manage and respond to cyber threats effectively and hampers the development of comprehensive cybersecurity strategies and training programs. Many HEIs may operate with outdated IT systems that are more susceptible to cyber-attacks. Upgrading these systems requires significant investment, which can be challenging under limited budgets. Developing and enforcing cybersecurity policies and regulations might be inconsistent or lacking. Some institutions may not have the guidance or mandate to implement robust cybersecurity measures. Political and economic instabilities in the region can impact the focus and resources allocated to cybersecurity initiatives. To address these issues and enhance cybersecurity resilience, HEIs in Western Balkan countries must focus on increasing IT infrastructure investment, improving cybersecurity education and

training, developing robust institutional policies, and fostering collaborations within the region and with international partners.

The lack of a cybersecurity incident response plan in HEIs in Western Balkan countries can be attributed to several factors that are often interrelated and stem from internal and external challenges these institutions face. One of the primary challenges is limited financial and human resources. Many HEIs in Western Balkan countries may not have the necessary funding to invest in robust cybersecurity infrastructure, including developing an incident response plan. This limitation also affects the hiring and retention of skilled cybersecurity personnel. There is often a shortage of staff adequately trained in cybersecurity practices, including incident response. This gap makes it difficult for institutions to plan for and respond to cyber incidents effectively. Cybersecurity might not be a top priority at the administrative and management levels within HEIs. This lack of awareness and understanding of cyber risks leads to less prioritization of cybersecurity measures, including incident response planning. HEIs often rely on external digital services and platforms for various functions. This interconnectivity can complicate developing an incident response plan that effectively addresses all potential points of vulnerability. HEIs may operate with outdated IT infrastructure that is more vulnerable to cyberattacks. Developing an effective incident response plan is challenging without modern and secure systems. Addressing the lack of cybersecurity incident response plans in HEIs in Western Balkan countries requires a comprehensive approach, including increased funding for cybersecurity, enhancing cybersecurity education and training, developing and enforcing relevant policies and regulations, modernizing IT infrastructure, and fostering a culture of cybersecurity awareness.

Vulnerabilities in higher education e-learning management systems (eLMSs) are another concern. As reported in *Scerbakov, Scerbakov & Kappe (2019)*, the design of these platforms is defined by the utilization of intricate hierarchical content, accommodating a wide range of users, catering to various types of materials, and a variety of programming languages. The most common learning management platforms' features include uploading and downloading of posting students' assignments, test papers, test scores, project reports, and other resources from instructors; forum discussions on various themes; databases with grading systems and actual grades; and incorporation of third-party into online learning (*Ramani, 2017*). Some of the most web application vulnerabilities are: improper input validation such as cross-site scripting, cross-site request forgery, structured query language injection, improper authentication, improper privilege management, certificate validation, and uploading of files of a potentially hazardous nature is permitted (*SANS Institute, 2021*). In addition, according to *OWASP (2021a)* and *Riadi, Umar & Sukarno (2018)*, the most prevalent web application vulnerabilities in 2021 are the following: injection flaws, broken authentication and access control, security misconfigurations, and sensitive data exposure. Furthermore, LMSs can be affected by various logical and technical vulnerabilities, for example, input validations, cross-site scripting, insecure configuration, and broken authentication (*Invicti, 2021*; *Imperva, 2021*).

Data breaches are one of the most severe concerns in HEIs, and they report increasing security incidents. Reports from the cybersecurity industry (*Cisco, 2023*; *Invicti, 2021*;

StealthLabs, 2021) claimed that HEIs have the highest rate of ransomware and phishing fraud compared to all other attacks in recent years. According to *McKenzie (2021)*, in 2021, critical data from a number of U.S. universities was recently revealed on the dark web. Ransomware attacks have increased by seven times in 2020 compared to 2019 in HEIs (*Liluashvili, 2021*; *IBM, 2021*). In recent years, there has been an increasing amount of literature on cybersecurity data breaches. Various studies (*Chapman, 2021*; *Bongiovanni, 2019*; *Riadi, Umar & Sukarno, 2018*; *StealthLabs, 2021*) have shown that the most prevalent flaws in HEIs include social engineering or ransomware attacks, vulnerabilities in LMS platforms, and a lack of cybersecurity standards in place.

The migration from traditional classroom instruction to virtual learning environments has precipitated a myriad of cybersecurity conundrums for scholastic entities. This evolution, hastened by the global health crisis, has augmented the breadth of educational engagements within the digital realm, consequently amplifying the susceptibility to cyber incursions. As pedagogical modalities pivot to online platforms, there is an observable augmentation in the diversity and volume of devices interfacing with educational repositories, thus expanding the vectors accessible to malevolent cyber entities. Learners and educators interfacing with pedagogic content *via* domiciliary or public internet conduits may encounter compromised network integrity, heightening exposure to nefarious activities such as interception attacks, clandestine surveillance, and illegitimate system access. Virtual learning infrastructures are repositories of copious amounts of sensitive data, encompassing the personal particulars of students, scholarly records, and secure access credentials. The proliferation of digital correspondence has been accompanied by an escalation in deceptive stratagems, such as phishing and complex social engineering tactics designed to exfiltrate sensitive information or deploy malicious software. Adopting personal apparatuses under the "Bring Your Own Device" (BYOD) introduces complexities in orchestrating and safeguarding these devices from a plethora of security perils, including but not restricted to malware and unmediated system flaws. A potential deficit in cybersecurity awareness exists among the scholastic populace, rendering them more prone to digital threats. A regiment of ongoing enlightenment and training is necessitated. Academic institutions employ an array of software ecosystems to facilitate remote learning, with inherent vulnerabilities that could be exploited to secure unauthorized ingress or disrupt educational operations. Notably, smaller educational institutions might be challenged by a paucity of resources or specialized knowledge to counteract these cybersecurity adversities sufficiently. In response to these exigencies, it is imperative for educational establishments to enact comprehensive cybersecurity frameworks encompassing the fortification of network defenses, the institutionalization of periodic security evaluations, extensive training for the academic community, utilization of secure and authenticated virtual learning interfaces, and stringent adherence to data privacy statutes.

The absence of established cybersecurity standards and governance poses a noteworthy challenge for higher education institutions, particularly within the context of Western Balkan countries. Higher education institutions are increasingly facing ransomware attacks, with a report indicating that nearly two-thirds (64%) of institutions experienced such attacks last year. The impact can be substantial, leading to operational disruptions

and financial losses. To defend against these, a Zero Trust security model is recommended, which emphasizes the need for explicit verification, least privileged access, and the assumption that a breach has already occurred or will soon occur (*Scholz, Hagen & Lee, 2021*). Many higher education institutions are in the early stages of their IAM journey, struggling with piecemeal approaches and the need to aggregate solutions from multiple vendors or address gaps from a single IAM vendor. The complexity of managing a large number of identities, especially in the context of remote learning, adds to these challenges (*Bio-Key International, 2022*). The pandemic has exacerbated budget cuts in the education sector, limiting the funds available for cybersecurity investments. This financial strain, combined with the challenge of protecting expansive and open college networks, makes institutions vulnerable to cyberattacks (*Miller, 2022*).

In accordance with the findings reported by *Stojanovic et al. (2021)* and *Gecevska, Lombardi & ČUŠ (2009)*, Western Balkan governments, while ostensibly demonstrating preparedness at a conceptual level, manifest a practical effectiveness deficit in handling cybersecurity attacks. The incidence of data breaches is on the rise across organizations within Western Balkan countries, with a pronounced emphasis on HEIs. The advent of the COVID-19 pandemic has further facilitated threat actors in infiltrating higher education networks, given the widespread provision of remote access to students and staff. *Chapman (2021)* highlight that a majority of Western Balkan countries have either established or lack an e-learning system.

Moreover, there is an identified inadequacy in cybersecurity expertise and incident response capabilities within HEI administrations. Observations indicate a notable vulnerability in a substantial proportion of eLMSs, characterized by the absence of robust cybersecurity processes for conducting vulnerability assessments. Additionally, the various technologies integrated into LMSs across Western Balkan countries lack a security-oriented design, and the absence of integrated standards exacerbates the overall susceptibility to cyber attacks. The imperative nature of risk management within HEIs is underscored by *Chapman (2021)*, who delineates essential inquiries for the evaluation of cybersecurity risk:

1. Are systems adequately patched and maintained with up-to-date security measures?
2. Is there a systematic implementation of routine vulnerability scans as part of a comprehensive vulnerability management policy?
3. Is there a well-defined incident response plan in place to address potential security breaches?
4. Do the monitoring and mitigation systems encompass relevant cybersecurity risks effectively?
5. Is the network provider proficiently mitigating denial-of-service attacks in alignment with cybersecurity objectives?

As a result, it is imperative to develop a specialized incident response strategy tailored to individual instances of eLMS in Western Balkan countries, as underscored by *Ramani (2017)* and *Invicti (2021)*. The deficiency of proactive cybersecurity controls within HEIs in the Western Balkan countries poses a direct threat to information security. Moreover, the scarcity of proficient personnel and dedicated security operation centers (SOCs) manifests as a pervasive challenge in the context of Western Balkan countries.

There is a focus on enhancing cybersecurity governance and capabilities, as evidenced by a rapid response project initiated by the European Union (EU), which includes Albania, Montenegro, and North Macedonia. This project involves strengthening cybersecurity governance, adjusting cybersecurity legislation, and enhancing the training of Computer Security Incident Response Teams (CSIRTs). The effort is not only aimed at improving the cybersecurity stance of these countries but also at achieving EU and international standards to foster better opportunities and regional exchanges on digital and cybersecurity cooperation. Higher education institutions in western Balkan were increasingly encountering cyber threats, and attacks are becoming more sophisticated, tailoring malicious content to local languages and contexts. Cybercrime remains the main threat, particularly malware, phishing, ransomware, and Distributed Denial of Service (DDoS) attacks. Furthermore, these efforts reflect a growing awareness and commitment to cybersecurity in the Western Balkans' higher education sector, acknowledging the importance of resilience in the face of evolving digital threats (*Jin & Klopfer, 2021*; *ISAC, 2022*; *Plantera, 2023*; *Maigre, 2022*).

Motivations and contributions

This research endeavors to present a lightweight cybersecurity framework, encompassing proactive controls, with the aim of fortifying the security of eLMS within HEIs situated in Western Balkan countries. The primary aim is to employ a penetration test approach for the systematic identification of vulnerabilities within eLMS platforms, subsequently devising proactive controls tailored to address each identified vulnerability. This study addresses the following research questions:

- What vulnerabilities and weaknesses characterize the cybersecurity landscape of eLMSs in HEIs in Western Balkan countries?
- What methodologies can be employed to implement proactive measures based on the identified vulnerabilities?

In addressing these inquiries, a penetration testing methodology is adopted, leveraging the MITRE Attack framework and the Open Web Application Security Project (OWASP) methodology. Additionally, the primary contribution of this study lies in proposing a model for a lightweight framework designed to assist HEIs in prioritizing and identifying vulnerabilities, subsequently facilitating the implementation of proactive controls identified during the penetration testing process. Importantly, this lightweight framework is intended to provide support to inexperienced and understaffed HEIs, thereby enhancing their cybersecurity infrastructure. A penetration testing methodology is employed to tackle these issues, utilizing the MITRE Attack framework and the OWASP methodology. Furthermore, the primary contribution of this study is to propose a lightweight framework model to assist HEIs in prioritizing and discovering vulnerabilities and implementing proactive controls found during the penetration test process. Furthermore, the lightweight framework will support inexperienced, understaffed HEIs and improve their cybersecurity infrastructure.

Article organization

The rest of the article is structured as follows. 'Methodology' describes the proposed methodology for penetration tests usable to find the vulnerabilities in eLMSs of HEIs. 'Proposed Lightweight Framework with Proactive Controls for ELMS' discusses the details of implementing the proposed lightweight framework for cybersecurity attack management. 'Results and Discussions' discusses the simulation of the proposed framework. 'Conclusion' concludes the article with some valuable remarks and suggestions.

METHODOLOGY

A penetration test is one of the most common methodologies for determining vulnerabilities in different platforms. According to *Alghamdi (2021)*, penetration testing is crucial for identifying security vulnerabilities, but it is becoming sophisticated and time-consuming, resulting in poor reporting. An HEI can use various penetration test principles and procedures for such purposes. Penetration testing methodologies, such as PTES, are used by organizations to identify and evaluate the security of their systems, networks, and applications. Some use cases for penetration testing are given below.

- **Risk management:** Penetration testing can identify potential vulnerabilities and risks that attackers could exploit, allowing organizations to prioritize and address the most critical issues.
- **Auditing:** Organizations may conduct regular penetration testing as part of their internal audit processes to ensure that their security controls are working as intended.
- **Incident response:** Penetration testing can be used to simulate real-world attacks and test an organization's incident response procedures to identify any gaps and make improvements (*Alexei, Nistiriuc & Alexei, 2020*).
- **Insider threat identification:** Penetration testing can help to find potential insider attacks by testing user access controls and evaluating the impact of compromised credentials.

Penetration testing methodologies, such as PTES, are used by organizations to identify and evaluate the security of their systems, networks, and applications. Some use cases for penetration testing are given below.

- **Risk management:** Penetration testing can identify potential vulnerabilities and risks that attackers could exploit, allowing organizations to prioritize and address the most critical issues.
- **Auditing:** Organizations may conduct regular penetration testing as part of their internal audit processes to ensure that their security controls are working as intended.
- **Incident response:** Penetration testing can be used to simulate real-world attacks and test an organization's incident response procedures to identify any gaps and make improvements (*Alexei, Nistiriuc & Alexei, 2020*).
- **Insider threat identification:** Penetration testing can help to find potential insider attacks by testing user access controls and evaluating the impact of compromised credentials.

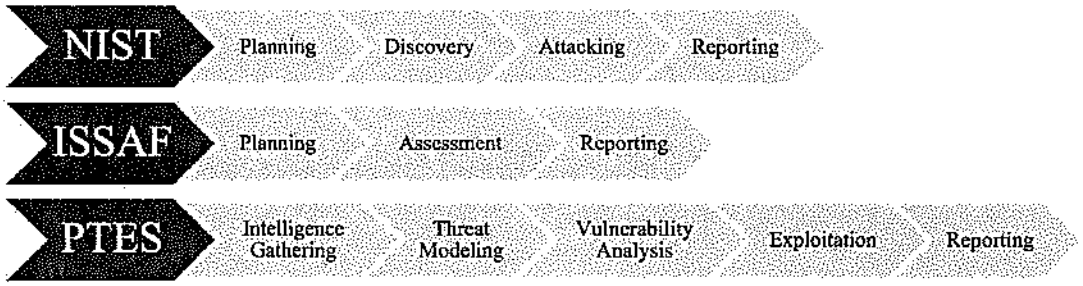

Figure 1 **Penetration test phases NIST, ISAAF, and PTES.**
Full-size DOI: 10.7717/peerjcs.1958/fig-1

- **Internal network testing:** OSSTMM provides a comprehensive methodology for testing internal networks, including guidelines for information gathering, vulnerability scanning, vulnerability assessment, and penetration testing.

The Open-Source Security Testing Methodology Manual (OSSTMM) is a systematic and structured security testing methodology used in various contexts to evaluate the security of systems, networks, and applications. Some use cases for OSSTMM include:

- **Web application testing:** OSSTMM provides a methodology for testing web applications, including guidelines for identifying and exploiting vulnerabilities in web applications.
- **Third-party testing:** Organizations may use OSSTMM to conduct security testing of third-party vendors, such as service providers, to ensure that they meet the organization's security standards (*Sekulovic, 2018*).

Open Information Systems Security Group (OISSG) is a community-driven organization that provides guidelines, methodologies, and best practices for security testing. The OISSG's guidelines can be used in a variety of contexts. Some of the use cases for OISSG include:

- **Penetration testing:** OISSG provides guidelines for conducting penetration testing and identifying vulnerabilities attackers could exploit.
- **Risk management:** OISSG provides guidelines for identifying and evaluating the risks associated with different systems, networks, and applications and developing strategies for mitigating those risks.
- **Incident response:** OISSG provides guidelines for incident response procedures and identifying vulnerabilities that attackers could exploit (*Abu-Dabaseh & Alshammari, 2018*).

In addition, penetration test as a security mechanism are limited to only finding vulnerabilities, not fixing them or proposing specific preventive strategies (*Doyle et al., 2020*; *Korniyenko et al., 2021*). An overview of penetration test phases from various standards such as NIST, ISAAF, and PTES is shown in Fig. 1.

The comparison of different cybersecurity frameworks or methodologies, specifically NIST, ISSAF, and PTES:

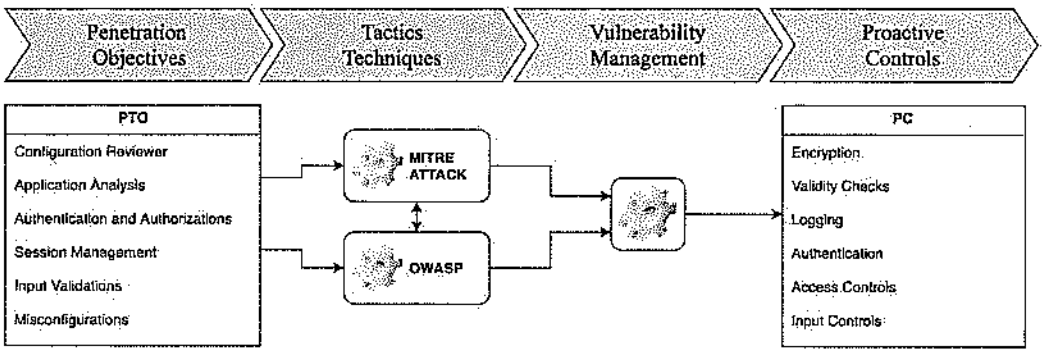

Figure 2 **Proposed lightweight framework with proactive controls for LMS.**
Full-size DOI: 10.7717/peerjcs.1958/fig-2

- **National Institute of Standards and Technology (NIST)** follows a series of steps, starting with Planning, moving to discovery, then Attacking, and finally, Reporting. This approach is very structured and is known for its comprehensive nature, focusing on protecting and maintaining the security of information systems.
- **Information Systems Security Assessment Framework (ISSAF)** is simplified into three stages: Planning, Assessment, and Reporting. It provides a streamlined approach to evaluating information system security, which can benefit organizations with limited cybersecurity resources.
- **Penetration Testing Execution Standard (PTES)** outlines a more detailed approach, starting with Intelligence Gathering, moving to Threat Modeling, then Vulnerability Analysis, followed by exploitation, and concluding with Reporting.

This article suggests a lightweight framework to protect higher education assets from various cybersecurity attacks. A lightweight framework can be a practical methodology for developing proactive controls based on a penetration testing approach to effectively protect the eLMS from various cybersecurity attacks, as illustrated in Fig. 2. The framework is divided into two parts. The first part pertains to the offensive aspect and encompasses penetration test objectives and tactics based on the MITRE ATT&CK framework and OWASP methodologies. The second part focuses on vulnerability management, including filtering and implementing proactive controls based on the vulnerabilities identified.

This framework can be implemented in several ways, including:

- **Vulnerability identification:** The framework can be used to identify vulnerabilities in systems, networks, and applications through penetration testing. This can consist of identifying known vulnerabilities, such as those listed in the Common Vulnerabilities and Exposures (CVE) database, and discovering new vulnerabilities.
- **Risk prioritization:** The framework can be used to prioritize the identified vulnerabilities based on their likelihood and potential impact. This allows organizations to focus on addressing the most critical vulnerabilities first.
- **Proactive controls:** The framework can be used to develop and implement proactive controls to mitigate the identified vulnerabilities. This can include implementing

security controls such as firewalls, intrusion detection and prevention systems, and patch management.

- **Continuous monitoring:** The framework can be used to continuously monitor systems, networks, and applications for vulnerabilities and threats, allowing organizations to identify and respond to new or emerging threats quickly.
- **Reports and metrics:** The framework can be used to generate reports and metrics that provide visibility into the organization's security posture, allowing them to track the effectiveness of their security controls over time.

The diagram suggests a comprehensive strategy that aligns cybersecurity objectives with the institution's infrastructure, utilizing well-known cybersecurity frameworks to structure the institution's approach to managing cyber risks. The framework emphasizes a balance between proactive measures to prevent incidents and reactive measures to respond to them, with an underlying acknowledgment of the need for resource allocation, including personnel and budget considerations. The framework is structured in three layers, suggesting a hierarchical approach to cybersecurity.

Layer 1: strategic overview

- Penetration test objectives establishing the goals of penetration testing to identify security weaknesses.
- Tactics, Techniques, Tools, and Procedures (TTTP) define the methods and tools that will be used in penetration testing and incident response.
- Vulnerability management consists of identifying, classifying, prioritizing, remediating, and mitigating software vulnerabilities.
- Proactive controls prevent security incidents before they occur, such as patch management, strong authentication, and user education.

Layer 2: operational details

- Reconnaissance testing scope determines the scope of the security testing, likely focused on gathering information about potential targets and vulnerabilities.
- MITRE ATT & CK and OWASP established cybersecurity frameworks (MITRE ATT & CK) and guidelines (OWASP) for known tactics, techniques, and procedures attackers use.
- Assessment analysis prioritizes the results of the security assessments to focus on the most critical vulnerabilities or areas of improvement.
- Control type, implementation actor, and costs consist of the control measures to be implemented, who will be responsible for implementation, and the associated costs.

Layer 3: implementation and approach

- HEIs objectives guide the choice of security measures and priorities.
- HEIs infrastructure needs to be secured according to the framework.
- Framework approaches (Offensive and Defensive) incorporate both offensive measures (*e.g.*, ethical hacking, penetration testing) to identify vulnerabilities and defensive measures (*e.g.*, firewalls, intrusion detection systems) to protect against threats.

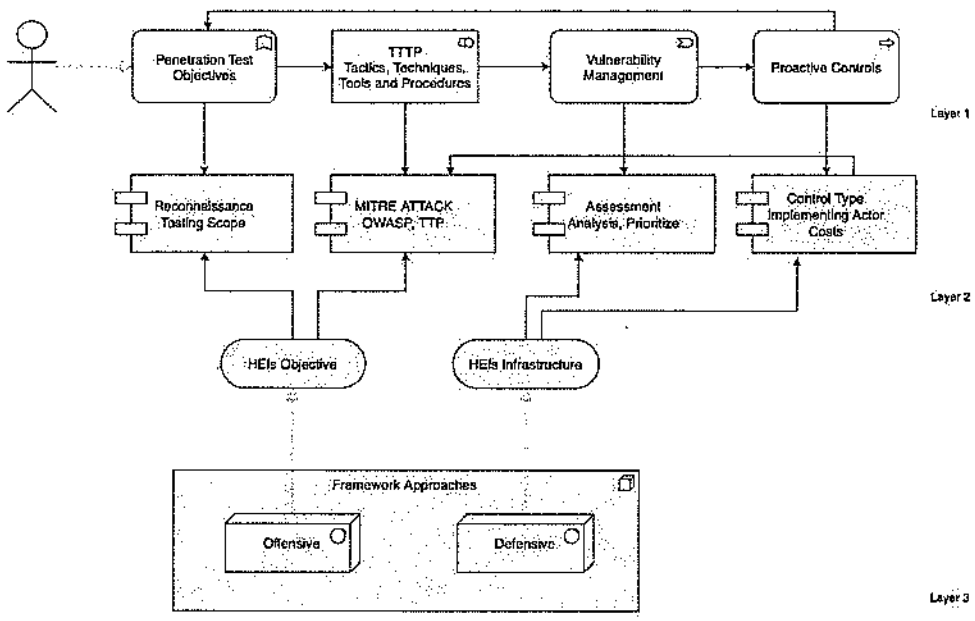

Figure 3 The structure of the proposed framework.

Full-size DOI: 10.7717/peerjcs.1958/fig-3

Overall, a lightweight framework can be a valuable tool for HEIs to identify and mitigate cybersecurity risks and proactively protect their assets from various cyberattacks, as shown in Fig. 2.

PROPOSED LIGHTWEIGHT FRAMEWORK WITH PROACTIVE CONTROLS FOR ELMS

The methodology of the proposed framework encompasses four distinct implementation levels.Illustrated in Layer 1 (See Figs. 3, 4 and 5) is a comprehensive depiction of the lightweight framework, delineated by its constituent elements: penetration test objectives (PTO), penetration test processes (PTP), vulnerability management (VM), and proactive controls (PC).

The proposed diagram suggests a strategic approach to cybersecurity, starting with penetration testing to identify vulnerabilities and using established frameworks to structure the approach to threat mitigation.

It emphasizes the importance of managing vulnerabilities and implementing proactive controls to improve overall security posture. The flow from penetration objectives to tactics and techniques, then on to vulnerability management and proactive controls, indicates a comprehensive process from identifying vulnerabilities to implementing measures to address them. The conceptual diagram is organized into four main components: PTO, tactics technique, vulnerability management, and PC.

- PTO list elements that are likely objectives or targets for penetration testing within an organization. These areas within an IT system or application would be scrutinized

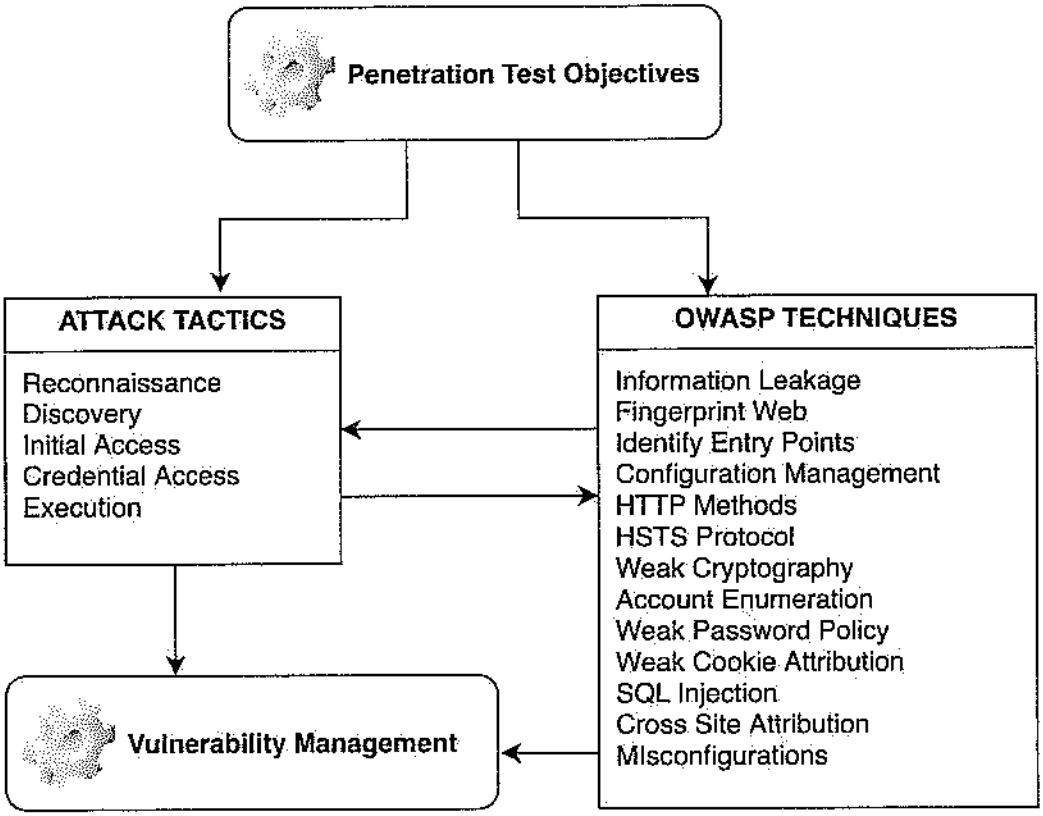

Figure 4 **The offensive approach of lightweight framework.**
Full-size DOI: 10.7717/peerjcs.1958/fig-4

during a penetration test to identify security weaknesses. It includes configuration review, application analysis, authentication and authorization, session management, input validations, and misconfigurations.

- Tactics technique refers to the specific tactics and methods employed during testing or as part of the security strategy. These frameworks provide structured approaches to identifying potential threats and the means to mitigate them. It might link to two well-known cybersecurity frameworks: MITRE ATT&CK and the Open Web Application Security Project (OWASP).
- Vulnerability management involves identifying, evaluating, prioritizing, and remedying software vulnerabilities to prevent exploitation.
- Proactive controls (PC) lists proactive measures that can be implemented to prevent security breaches, such as, encryption, validity checks, logging, authentication, access control, and input controls.

The diagram shows a feedback loop between the ATT & CK tactics and OWASP techniques and vulnerability management, suggesting that the outcomes of using these tactics and techniques feed into the process of managing vulnerabilities. This reflects a proactive approach to cybersecurity, where continuous penetration testing and assessment inform the ongoing process of managing and mitigating risks. The diagram represents

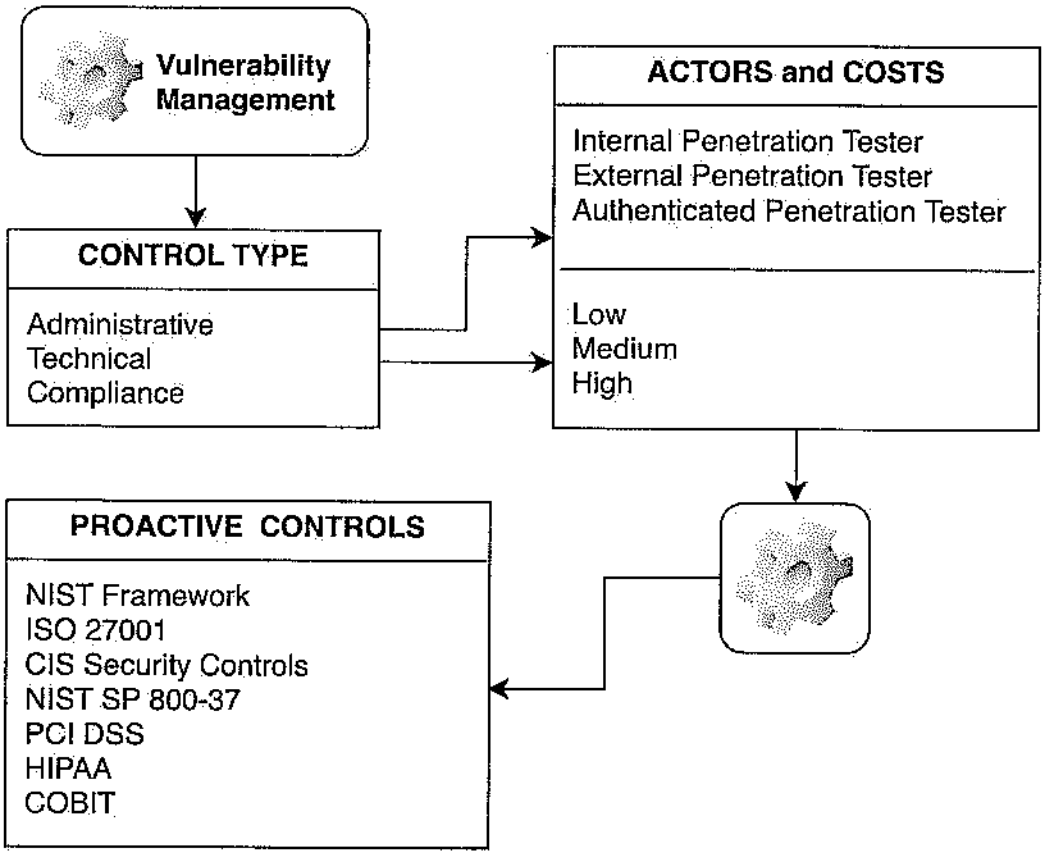

Figure 5 **The defensive approach of the proposed framework.**
Full-size DOI: 10.7717/peerjcs.1958/fig-5

a cybersecurity approach focusing on penetration testing objectives, tactics, techniques, and vulnerability management. Penetration test objectives typically identify and exploit vulnerabilities to understand the security posture of a system. ATT & CK Tactics listed tactics—reconnaissance, discovery, initial access, credential access, and execution—stages an attacker might go through to compromise a system. These tactics help to structure penetration testing efforts by simulating real-world attack scenarios. OWASP techniques list common web application security issues identified by the Open Web Application Security Project (OWASP). These include problems like information leakage, weak cryptography, and common vulnerabilities such as SQL injection and Cross-Site Scripting (XSS). Penetration testers use these techniques to try and exploit vulnerabilities in web applications. Vulnerability Management is the process that follows the identification of vulnerabilities. It includes the prioritization, remediation, and mitigation of discovered vulnerabilities to enhance the security of the system.

The flowchart demonstrates how vulnerability management is informed by understanding the types of controls that can be applied, the actors involved, and the associated costs. It also shows that the process is underpinned by a range of industry frameworks and standards that guide the establishment of proactive controls

to prevent security breaches. Vulnerability management is the central element of the diagram, indicating that it is the core process being described. Vulnerability management encompasses identifying, classifying, prioritizing, remedying, and mitigating vulnerabilities. Control type breaks down the types of controls that can be implemented as part of vulnerability management into three categories:

- **Administrative:** Policies, procedures, and other managerial controls.
- **Technical:** Hardware or software mechanisms that enforce or monitor security.
- **Compliance:** Controls to ensure adherence to laws, regulations, and policies.

Actors and costs suggest that implementing the controls from the "Control Type" box involves different actors, such as internal or external penetration testers and authenticated testers (who test the system with valid access credentials). Costs are considered on a scale of low, medium, to high, indicating that the choice of actor and the type of control implemented will affect the overall cost of the vulnerability management process. Proactive controls lists various established cybersecurity frameworks and standards organizations can use to inform their proactive control measures. These include NIST Framework, CIS Critical Security Control, ISO 27001 Information Security Management, NIST SP 800-37, NIST SP 800-37, PCI DSS, HIPAA rules, and COBIT.

A lightweight cybersecurity framework can be effectively applied globally, providing HEIs worldwide with the guidance needed to protect their information assets and the privacy of their students and staff in a cost-effective and pragmatic manner. The framework is designed to scale with the size and complexity of different institutions, from small colleges to large universities with multiple campuses, accommodate various types of educational institutions with different IT infrastructures, resources, and regulatory environments, and maximize cybersecurity benefits while minimizing costs and resource use, which is crucial for institutions with limited budgets. The framework is designed to help institutions comply with a range of international and local regulations, leverage internationally recognized standards and best practices, such as those from ISO, NIST, and OWASP, which are globally applicable and respected, and allow for regional customization to address specific threat landscapes effectively.

In subsequent iterations, this methodology endeavors to automate and integrate a broader spectrum of vulnerabilities and proactive controls through an in-depth analysis of eLMSs situated in Western Balkan countries. This risk assessment process is tailored to be lightweight by focusing on the most significant threats and vulnerabilities that could affect eLMS platforms rather than a comprehensive assessment of all possible risks. The goal is to maintain a balance between thorough risk management and the practical constraints of the HEIs in the Western Balkans. Risk assessment can be seen as a critical first step in the defense mechanism in the context of the proposed lightweight framework model for protecting eLMS in HEIs. The assessment would typically involve identifying, analyzing, and evaluating the potential risks that eLMS platforms might face. The model includes a structured approach to risk assessment. Determine which assets are critical to the eLMS platform's operations. This includes software, data, hardware, and services essential for the eLMS to function. Identify potential cybersecurity threats that could affect the eLMS, such

as malware, phishing, DDoS attacks, or insider threats. This can be informed by threat intelligence and historical data. Use tools and techniques, possibly including those from the framework like open-source vulnerability scanners or checklists, to identify existing vulnerabilities within the eLMS, like outdated software or weak configurations. Evaluate the potential impact of each identified threat exploiting a vulnerability. This includes considering the consequences of data breaches, service interruptions, and compliance violations. Determine the probability of each threat materializing by considering factors such as the HEI's location, the sophistication of potential attackers, and the current geopolitical climate. Combine the impact and likelihood to rate the level of risk each threat poses to the eLMS platform. Risks are often categorized as low, medium, or high. Review current cybersecurity controls to assess their effectiveness against identified risks. Determine if additional measures are needed and what those might be. Based on the evaluation, prioritize the risks that require immediate attention and those that can be monitored over time. Resource allocation should focus on high-priority risks. Cybersecurity is dynamic, so the risk assessment process should be iterative. Regularly review and update the risk assessment to account for new threats, vulnerabilities, and changes in the HEI's environment. The proposed lightweight framework fortifies eLMS against cybersecurity threats in HEIs, particularly within the context of the Western Balkans (*Maigre, 2022*; *Henry, 2020*; *Castelo, 2020*).

Managing access control and identity management through appropriate cryptographic protocols and schemes ensures the security of the eLMS platform. Using firewalls and network monitoring is a necessary part of a defensive strategy to protect against external threats. Resource optimization is a strategic imperative to ensure that limited financial and computational resources are used effectively and efficiently, providing the best possible security posture with the available assets. Access control and identity management are pivotal in ensuring that only authorized individuals can access educational institutions' systems and data. Utilizing strong authentication protocols like OAuth 2.0 for authorizing and authenticating users who are accessing the systems. Implementing MFA to add an extra layer of security. Define user roles and assign access rights accordingly. Use Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), for secure communication over a computer network. Ensuring that only necessary hardware and software are purchased and maintained, avoiding unnecessary expenditures. Leveraging cloud services can reduce costs related to on-premises data centers, such as power, cooling, and maintenance.

RESULTS AND DISCUSSIONS

The eLMSs within the Western Balkan countries govern a diverse array of student activities, encompassing assignments, file transfers, faculty interactions, and subject-related engagements. These systems comprise stored data, including student and lecturer profile pages, functionalities for the management of files through downloading and uploading various documents, and virtual learning-relevant forum pages. The present research employs a qualitative and descriptive methodology (*Invicti, 2021*) based on penetration

Table 1 **Vulnerabilities discovered in Western Balkan HEIs eLMS.**

Common Vulnerabilities	T1	T2	T3	T4	T5	T6	T7	T8
Fingerprint web-server	×		×		×	×		×
Trace method enabled		×						×
SSL support v2	×		×		×	×		×
SSL weak cipher		×				×		×
SSL expired certificate			×		×	×		
SSL self-signed certificate			×				×	
Credentials over GET methods	×				×			×
Lack of client-side validations	×				×			×
Lack of server-Side validations			×				×	
Weak lockout mechanism		×				×	×	
Session ID prediction		×	×	×		×		
Weak password Policy								×
Weak cookie settings	×		×			×		×
Email Enumerations through Forms	×			×				
XSS in URL parameters				×	×			×
Lack of "http-only" and "security" flags		×						×
Cookie expires		×			×	×		
SQL Injections					×		×	×
Unnecessary features		×		×		×		×
Unpatched software	×		×		×			

testing techniques (*Al-Shaer, Spring & Christou, 2020*; *Korniyenko et al., 2021*; *The MITRE Corporation, 2021*; *OWASP, 2021b*; *Yosifova, 2021*) to identify essential vulnerabilities in eLMS in Western Balkan HEIs. The primary objective is to discern critical vulnerabilities within eLMSs in HEIs situated in the Western Balkan region. The study focuses on eight HEIs spanning four Western Balkan countries: Albania, Kosovo, Montenegro, and North Macedonia. The process of penetration testing (*Zakaria et al., 2019*) involves passive analysis of eLMS for weaknesses, technical flaws, or vulnerabilities. According to MITRE ATT&CK and OWASP (*Al-Shaer, Spring & Christou, 2020*; *Korniyenko et al., 2021*; *Pham & Dang, 2018*; *Zare, Zare & Azadi, 2018*), the primary purpose of penetration tests is to find more effective attack vectors as well as exploit vulnerabilities.

The methodology outlined is utilized to obtain all of the results listed in Table 1, which pertain to eight targets from countries in the Western Balkans. Most eLMS targets are vulnerable due to untrustworthy inputs, weak cryptography, lack of client/server-side controls, weak authentication mechanisms, misconfigurations, and open unnecessary features.

Table 1 represents a summary of common vulnerabilities found across various systems, as identified through a series of tests (T1 through T8) conducted as part of a cybersecurity audit within the context of a lightweight framework for higher education institutions in the Western Balkan countries. Table 1 lists several types of vulnerabilities, such as issues with Secure Sockets Layer (SSL) configurations, problems with session management (like Session ID Prediction), and other common web application vulnerabilities like SQL

Injections and Cross-Site Scripting (XSS). Each "X" in Table 1 indicates the presence of the vulnerability in the corresponding test.

- Fingerprint web server refers to the ability to detect the type and version of a web server by sending it requests and analyzing the responses, which could give attackers information on potential vulnerabilities.
- The trace method enabled is used for diagnostic purposes and can be exploited by attackers to gain access to information in HTTP headers, such as cookies and authentication data.
- SSL support v2 indicates that the outdated and insecure version 2 of the SSL protocol, which has known vulnerabilities, is supported.
- SSL weak cipher refers to the use of encryption algorithms that are no longer considered strong and can be easily broken by attackers.
- SSL expired certificate use an expired SSL certificate can lead to man-in-the-middle attacks as the website's identity cannot be confirmed.
- SSL self-signed certificates are not trusted by default and can be a sign of a potential man-in-the-middle attack.
- Credentials over GET methods consist of passing sensitive information such as login credentials in the URL (*via* GET requests) that can expose them to anyone with access to the URL.
- Without client-side/server-side validation, an application may accept malicious input that can lead to various attacks.
- A weak lock-out mechanism does not lock out users after multiple failed login attempts, making it vulnerable to brute force attacks.
- Session ID Prediction makes it easier for attackers to hijack user sessions.
- A weak password policy may choose passwords that are easy to guess or brute force.
- Weak cookie settings can allow attackers to intercept or manipulate cookies.
- Email enumerations through forms reveal whether an email address is associated with an account; it could aid an attacker in crafting a targeted attack.
- XSS in URL parameters refers to cross-site scripting vulnerabilities that occur when an application includes unvalidated or unescaped user input in URLs.
- Lack of "http-only" and "security" flags can be accessed by client-side scripts, which could lead to cross-site scripting attacks.
- SQL injections can insert or manipulate SQL queries through the application, potentially gaining access to or manipulating the database.
- Unnecessary features can introduce additional security risks
- Unpatched software has not been updated with the latest patches and may have known vulnerabilities that can be exploited.

In terms of the lightweight cybersecurity framework's application to the Western Balkan HEIs, this table shows that there are multiple common points of weakness that need to be addressed. The recurrence of "X" marks across the tests for each vulnerability indicates a pattern that may suggest systemic flaws in their e-learning platform web applications. Considering the potential lack of skilled cybersecurity professionals in the

region, a lightweight framework would prioritize addressing these vulnerabilities in a cost-effective and resource-efficient manner. The results suggest that Western Balkan HEIs could significantly improve their cybersecurity resilience by focusing on these common vulnerabilities and using a tailored lightweight framework that considers the region's specific challenges and constraints.

As asserted by *Alexei, Nistiriuc & Alexei (2020)*, within a survey encompassing thirty scholarly articles, five researchers within the academic domain advocate for the integration of the ISO27001 standard in HEIs, while two recommend the adoption of the COBIT framework. In addition, two articles suggest the utilization of the COBIT framework, one advocates for the incorporation of ITIL best practices, and another proposes a hybrid approach. Conversely, a significant proportion of researchers present their individualized strategies for enhancing cybersecurity within HEIs. Moreover, the envisaged methodology tailored for HEIs in the Western Balkans seeks to identify vulnerabilities within eLMSs and proactively establish controls. This approach integrates the MITRE ATT&CK framework, the OWASP methodology, CIS controls, and the NIST framework to formulate a comprehensive set of proactive controls. Based on a real-world scenario, we will propose many approaches to avoid failed login attempts to an eLMS. Implement account lockout to limit the number of consecutive failed login attempts and lock the account for a certain period. Implement a CAPTCHA system to prevent automated attempts to login. Implement multi-factor authentication by requiring multiple forms of authentication. Block I.P. addresses that have a high number of failed login attempts. Implement a security information and event management (SIEM) system to monitor the system for unusual login patterns and alert the administrator if there are too many failed login attempts. Asking security questions, such as personal information, after a certain number of unsuccessful attempts can help verify the user's identity. Implementing two-factor authentication (2FA) in a learning management system can help to improve security by adding an extra layer of protection. Keep track of all login attempts, both successful and unsuccessful, and regularly review the logs to detect any suspicious activity. The framework is designed to be flexible and salable to adapt to the changing threat landscape and the evolving needs of educational institutions. It aims to provide a balanced approach that ensures the security of assets without imposing excessive administrative or financial burdens on the institutions. Under the proposed lightweight cybersecurity framework for HEIs in the Western Balkans, the protection of assets would be approached through several strategic layers: asset identification and classification, access control, data encryption, regular security audits and vulnerability assessments, patch management, security awareness training, incident response plan, backup and recovery, network security, and compliance with legal and regulatory requirements.

CONCLUSION

Implementing e-learning management systems (eLMS) without due consideration for security can lead to many challenges, especially in regions like the Western Balkans, where resources may be limited and cybersecurity awareness may not be widespread. Addressing

these challenges requires a comprehensive approach involving policy development, investment in technology, training and awareness programs, and collaboration between educational institutions, government bodies, and cybersecurity experts. E-learning systems store significant personal data from students and staff, such as names, addresses, academic records, and sometimes even payment information. Inadequate security measures can lead to data breaches, risking the exposure of sensitive information. An eLMS without robust security features is an attractive target for cyberattacks, ranging from denial-of-service attacks disrupting access to learning materials to more severe ransomware attacks that encrypt valuable data. Without a proper security framework, an institution may not have an incident response plan in place. This can severely hamper its ability to respond to and recover from cyber incidents quickly. E-learning platforms host proprietary course materials and research data. Without adequate security, there is a risk of unauthorized access and intellectual property theft. The eLMS must continuously update and maintain to address new security threats. Neglecting this can leave systems vulnerable to new types of cyberattacks. There is a lack of awareness or a cultural barrier to understanding the importance of cybersecurity. This can result in a casual approach to security among students and staff, exacerbating vulnerabilities. In the Western Balkans, financial and human resources might be scarce to invest in advanced cybersecurity infrastructure and to train staff adequately on cybersecurity best practices. In the context of academic research, the proposal of a lightweight framework model to protect eLMS in HEIs in the Western Balkans is predicated on several core academic concepts and methodologies. The proposed lightweight framework designed for the Western Balkans higher education institutions, compared to NIST, ISSAF, and PTES, highlights the advantages:

- The lightweight framework might be specifically tailored to the common threats and resources available in the Western Balkan higher education environment, providing a more focused and relevant approach than the general methodologies.
- Given the resource constraints in the region, a lightweight framework would likely simplify the process to focus on the most impactful activities, reducing the complexity and cost associated with more comprehensive standards.
- It could emphasize essential controls that offer the most significant security benefit, particularly valuable in an environment where institutions may not be able to implement a broad array of measures.
- The framework could incorporate education and cybersecurity awareness elements, which are crucial in environments where cybersecurity knowledge may not be widespread.
- The lightweight framework is likely designed for rapid deployment and agility, allowing institutions to improve their cybersecurity posture in response to emerging threats quickly.
- By focusing on the most significant risks and implementing key controls efficiently, a lightweight cybersecurity framework can provide a practical and cost-effective solution for improving cybersecurity resilience in resource-constrained environments like those of higher education institutions in the Western Balkans.

In conclusion, the article proposes a novel, lightweight cybersecurity framework designed to safeguard eLMS platforms in Western Balkan HEIs. This framework is grounded in an open-source methodology, allowing customization, community support, and cost-effectiveness. By integrating the framework as a self-assessment tool, HEIs can actively gauge and enhance their cybersecurity maturity. The iterative penetration testing process, a key component of the framework, is informed by empirical findings that underscore the prevalent vulnerabilities within eLMS platforms. The proposed model facilitates the implementation of proactive controls, emphasizing preventive measures over-reactive responses, aligning with best cybersecurity management practices.

ADDITIONAL INFORMATION AND DECLARATIONS

Funding

No funding was used in this study.

Competing Interests

The authors declare there are no competing interests.

Author Contributions

- Krenar Kepuska conceived and designed the experiments, performed the experiments, analyzed the data, performed the computation work, prepared figures and/or tables, authored or reviewed drafts of the article, and approved the final draft.
- Milo Tomasevic conceived and designed the experiments, performed the experiments, analyzed the data, performed the computation work, prepared figures and/or tables, authored or reviewed drafts of the article, and approved the final draft.

Data Availability

The following information was supplied regarding data availability:

The data used to support the findings of this study are included in the article. The code is available in the Supplementary File.

Supplemental Information

Supplemental information for this article can be found online at http://dx.doi.org/10.7717/peerj-cs.1958#supplemental-information.

REFERENCES

Abu-Dabaseh F, Alshammari E. 2018. Automated penetration testing: an overview. In: *The 4th international conference on natural language computing, Copenhagen, Denmark.* 121–129 DOI 10.5121/csit.2018.80610.

Alexei A, Nistiriuc P, Alexei A. 2020. Analysis of security frameworks implemented in HEI's. In: *Scientific collection interconf: scientific trends and trends in the context of globalization.* 347–359 DOI 10.51582/interconf.7-8.06.2021.036.

Alghamdi AA. 2021. Effective penetration testing report writing. In: *Proceedings of the 2021 international conference on electrical, computer, communications and mechatronics engineering (ICECCME)*. Piscataway: IEEE, 1–5 DOI 10.1109/ICECCME52200.2021.9591097.

Al-Shaer R, Spring JM, Christou E. 2020. Learning the Associations of MITRE ATT&CK Adversarial Techniques. ArXiv arXiv:2005.01654.

Bio-Key International. 2022. EDUCAUSE 2022: Key Trends in Higher Education Cybersecurity. *Available at https://blog.bio-key.com/educause-2022-key-trends-in-higher-education-cybersecurity*.

Bongiovanni I. 2019. The least secure places in the universe? A systematic literature review on information security management in higher education. *Computers & Security* **86**:350–357 DOI 10.1016/j.cose.2019.07.003.

Castelo M. 2020. Best practices for securing a learning management system. *Available at https://edtechmagazine.com/k12/article/2020/08/best-practices-securing-learning-management-system*.

Chapman J. 2021. How safe is your data? Cyber-security in higher education. *Available at https://www.hepi.ac.uk/2019/04/04/how-safe-is-your-data-cyber-security-in-higher-education/* (accessed on 00 October 2021).

Cisco. 2023. Cybersecurity threat trends report. Cisco Umbrella. *Available at https://umbrella.cisco.com/info/cybersecurity-threat-trends-report*.

Doyle L, McCabe C, Keogh B, Brady A, McCann M. 2020. An overview of the qualitative descriptive design within nursing research. *Journal of Research in Nursing* **25(5)**:443–455 DOI 10.1177/1744987119880234.

Gecevska V, Lombardi F, ČUŠ F. 2009. E-learning opportunity in high education for engineers. *Annals of the Faculty of Engineering Hunedoara–Journal of Engineering* **7(2)**:26–33.

Henry J. 2020. 5 Key eLearning platform security components. *Available at https://www.absorblms.com/blog/5-key-elearning-platform-security-components*.

IBM. 2021. Cost of a data breach report 2021. *Available at https://info.techdata.com/rs/946-OMQ-360/images/Cost_of_a_Data_Breach_Report_2021.PDF* (accessed on 11 February 2022).

Imperva. 2021. Imperva: application security OWASP top-10. *Available at https://www.imperva.com/learn/application-security/owasp-top-10/* (accessed on 15 March 2021).

Invicti. 2021. Acunetix: OWASP top-10 compliance. *Available at https://www.acunetix.com/vulnerability-scanner/owasp-top-10-compliance/* (accessed on 5 July 2021).

Irwin L. 2022. List of data breaches and cyberattacks in January 2020. *Available at https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-january-2020-1-5-billion-records-breached* (accessed on 12 February 2022).

ISAC. 2022. Western Balkans: emerging cyber threats—cybersecurity ecosystem report. International and Security Affairs Centre. *Available at https://www.isac-fund.org/en/publication/western-balkans-emerging-cyber-threats-cybersecurity-ecosystem-report*.

Jin J, Klopfer F. 2021. Developing national cybersecurity strategies in the Western Balkans. National Cybersecurity Strateg. *Available at https://ncsguide.org/2021/11/22/developing-national-cybersecurity-strategies-in-the-western-balkans/.*

Josac M, Frederico B, Ramiro G, Manuel A-Y-O, Tiago O, Mijail N-Z, Frederico C-J. 2019. Assessing the success behind the use of education management information systems in higher education. *Telematics and Informatics* 38:182–193 DOI 10.1016/j.tele.2018.10.001.

Korniyenko B, Ladieva L, Galata L, Yakovenko O, Nesteruk A, Ivannikova V. 2021. Web application critical resources protection. In: *2021 IEEE 3rd international conference on advanced trends in information theory (ATIT).* Piscataway: IEEE, 256–261 DOI 10.1109/ATIT54053.2021.9678541.

Liluashvili GB. 2021. Cyber risk mitigation in higher education. *International Journal of Law* 7(2):15–27 DOI 10.36475/7.2.2.

Maigre M. 2022. Cybersecurity study on the Western Balkans. *Available at https://ega.ee/project/cybersecurity-study-western-balkans/.*

Maryam NA, Mostafa A. 2021. Learning management systems and technology acceptance models: a systematic review. *Education and Information Technologies* 26:5499–5533 DOI 10.1007/s10639-021-10513-3.

McKenzie L. 2021. University affected by IT security company data breach. Inside Higher Ed. *Available at https://www.insidehighered.com/quicktakes/2021/04/05/universities-affected-it-security-company-data-breach.*

Miller E. 2022. The state of higher education cybersecurity: top insights and trends. *Available at https://www.bitlyft.com/resources/the-state-of-higher-education-cybersecurity-insights-trends.*

OpenSSF. 2022. Open source software. *Available at https://openssf.org/blog/2023/09/06/strengthening-open-source-software-best-practices-for-enhanced-security/* (accessed on 05 February 2022).

OWASP. 2021a. The open web application security project. *Available at https://owasp.org/Top10/* (accessed on 15 November 2021).

OWASP. 2021b. OWASP cookies attributes. *Available at https://owasp.org/www-community/controls/SecureCookieAttribute* (accessed on 19 September 2021).

Pham V, Dang T. 2018. CVExplorer: multidimensional visualization for common vulnerabilities and exposures. In: *2018 IEEE international conference on big data (big data).* 1296–1301 DOI 10.1109/BigData.2018.8622092.

Pinheiro J. 2020. Review of cyber threats on educational institutions. In: *Proceedings of the digital privacy and security conference.* 43–51.

Plantera F. 2023. Safeguarding digital systems in the Western Balkans. *Available at https://ega.ee/blog_post/western-balkan-digital-security/.*

Ramani R. 2017. Learning management system trends archives. ELearning industry. *Available at https://elearningindustry.com/tags/learning-management-system-trends.*

Riadi I, Umar R, Sukarno W. 2018. Vulnerability of injection attacks against the application security of framework based websites open web access security project (OWASP). *Jurnal Informatika* 12(2):53 DOI 10.26555/jifo.v12i2.a8292.

SANS Institute. 2021. CWE TOP 25 most dangerous software errors. *Available at https://www.sans.org/top25-software-errors/* (accessed on 08 November 2021).

Scholz S, Hagen W, Lee C. 2021. The Increasing threat of ransomware in higher education. Educause review. *Available at https://er.educause.edu/articles/2021/6/the-increasing-threat-of-ransomware-in-higher-education.*

Scerbakov N, Scerbakov A, Kappe F. 2019. Security vulnerabilities in modern LMS. In: *Proceedings of the international conference E-LEARNING 2019.* 242–246.

Sekulovic R. 2018. NIST: penetration test. *Available at https://csrc.nist.gov/* (accessed on 7 January 2022).

StealthLabs. 2021. Cyber security threats and attacks: all you need to know. *Available at https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/* (accessed on 8 August 2021).

Stojanovic M, Stojkovski B, Kajosevic S, Kuloglija N, Mejdini N. 2021. Cyber-attacks a growing threat to unprepared Balkan states. *Available at https://balkaninsight.com/2021/03/10/cyber-attacks-a-growing-threat-to-unprepared-balkan-states/* (accessed on 11 February 2022).

The MITRE Corporation. 2021. Application layer protocol; Web protocols. *Available at https://attack.mitre.org* (accessed on 14 September 2021).

Ulven JB, Wangen G. 2021. A systematic review of cybersecurity risks in higher education. *Future Internet* 13(2):1–40 DOI 10.3390/fi13020039.

Wangen G. 2019. Quantifying and analyzing information security risk from incident data. *Graphical models for security.* Cham: Springer International Publishing DOI 10.1007/978-3-030-36537-0_7.

Yosifova V. 2021. Vulnerability type prediction in common vulnerabilities and exposures database with ensemble machine learning. In: *2021 international conference automatics and informatics (ICAI).* Piscataway: IEEE, 146–149 DOI 10.1109/ICAI52893.2021.9639588.

Zakaria MN, Phin PA, Mohmad N, Ismail SA, Kama MN, Yusop O. 2019. A review of standardization for penetration testing reports and documents. In: *2019 6th international conference on research and innovation in information systems (ICRIIS).* 1–5 DOI 10.1109/ICRIIS48246.2019.9073393.

Zare H, Zare MJ, Azadi M. 2018. Cybersecurity vulnerabilities assessment (a systematic review approach). In: *Information technology-new generations: 15th international conference on information technology.* Cham: Springer, 61–68.

Krenar Kepuska

Cyber Security Engineer

- **Ph.D** in Cyber Security
- **M.Sc. Eng.** in Engineering of Mathematics and IT
- Certified from **SANS** Institute, **GIAC** and **CompTIA**
- **Fulbright** & George C. **Marshall** alumnus
- > 10 years in Cybersecurity

CONTACT ME

+383 44 970097

krenar.kepuska@fulbrightmail.org

krkcad@rit.edu

SKILLS

- Cyber Security
- Information Security
- Cryptography
- Cyber Forensics
- Data Security
- Incident Handling
- Incident Response
- Malware Investigations
- Network Security
- Penetration Testing
- Ethical Hacking
- Threat Detection
- Vulnerability Assessment
- Web Application Security

WORK EXPERIENCE

Lecturer — 2022 - Present
Rochester Institute of technology (RIT-K) | Kosovo

Accreditation Expert - Special Service Agreement (SSA) — 2024 - Present
National Qualification Authority | Kosovo

Cyber Security Analyst — 2022 - 2024
National Unit for Cyber Security | Kosovo

Cyber Security Instructor — 2021 - 2022
Haking Magazine | Poland

Cyber Security Researcher — 2021 - 2021
Rochester Institute of technology (RIT) | Rochester, USA

Cyber Security Instructor — 2021 - 2021
University of Colorado (UCCS) | Colorado Springs, USA

Lecturer — 2014 - 2021
University AAB | Kosovo

EDUCATION

Doctor of Science (PhD) in Cyber Security — 2018 - 2024
University of Monenegro | Podgorica, Montenegro

PhD Research in Cyber Security — 2021 - 2021
Rochester Institute of Technology | Rochester, USA
University of Colorado in Colorado Springs | Colorado Springs, USA

Master of Science (MSc. Eng.) in Engineering of Math and Computer Science — 2012 - 2014
University of Tirana | Faculty of Natural Science | Tirana, Albania

Bachelor of Science (BSc. Eng.) in Engineering of Electronics and IT — 2009 - 2012
Polytechnic University of Tirana | Tirana, Albania

FELLOWSHIPS

CRDF Global and U.S. Department of State — 2022
Purdue University | Indiana, USA

Fulbright Association and U.S. Department of State — 2021
Rochester Institute of Technology | Rochester, USA
University of Colorado in Colorado Springs | Colorado, USA

CERTIFICATE

GIAC Certified Incident Handler (GCIH) | **Advanced Certificate in Cyber Security** — 2023 - 2027
SANS Institute | Rockville, Maryland, USA

CompTIA Security+ — 2022 - 2026
CompTIA - Accredited by ANSI | Illinois, USA

MILITARY CERTIFICATE

Program on Cyber Security Studies (PCSS) — 2023
European Center for Security Studies
George C. Marshall | Garmisch-Partenkirchen, Germany

CONFERENCES

Cyber Threat Intelligence Conference — 2024
Organized by FIRST | Berlin, Germany

Threat Inteligence Pipelines for Information Exchange — 2024
Organized by Trusted Introducer | Durres, Albania

Information Exchange using OSINT for Cyber Investigations — 2023
Organized by European Union | Mauritius, South Africa

Ensuring Cyber Resilience: Securing Our Connected Future — 2023
Organized by European Union | Chisinau, Moldova

Task Force for Computer Security Incident Response Team — 2022
Organized by FIRST | Tirane, Albania

TRANSITS II - Workshop on Incident Response (CSIRT) — 2022
Organized by Trusted Introducer | Prague, Czech Republic

TRAININGS

Perfecting Academic Skills — 2019
Radboud University | Nijmegen, Netherland

Computer and Information Systems Security/Information Assurance — 2019
Algebra University | Zagreb, Croatia

PROJECTS

Cybersecurity Awareness among High School Students — 2023
Supported by Kosovo United States Alumni (KUSA) and U.S. Embassy in Kosovo

Hosting Fulbright Specialist — 2023
Supported by U.S. Embassy in Kosovo

PUBLICATION

Web of Science - SCI - Scopus - Peerj - Computer Science — 2024
A lightweight framework for Cyber Risk Management in Western Balkan

KRENAR KEPUSKA

Phone number: (+383) 44970097 (Mobile) | **Email address:** krenar.kepuska@fulbrightmail.org |

Email address: kkepuska@auk.org | **Email address:** krkcad@rit.edu | **LinkedIn:**

https://www.linkedin.com/in/krenarkepuska/ | **WhatsApp Messenger:** +38344970097 |

Address: Rechep Krasniqi, Kalabria, 10000, Prishtine, Kosovo (Home) |

Address: 162 East Lewis Ave Pearl River NY, 10965, New York, United States (Work)

ABOUT ME

- **PhD** in Cyber Security
- Cyber Security Engineer certified from **SANS** Institute, **GIAC** and **CompTIA**
- **Fulbright** & George C. **Marshall** alumnus

WORK EXPERIENCE

2024 – CURRENT

LECTURER (FULL-TIME) ROCHESTER INSTITUTE OF TECHNOLOGY RIT-K (A.U.K)

- Develop syllabi, lectures, assignments, and exams.
- Deliver lectures, lead classroom discussions, and conduct lab sessions
- Design and grade assignments, exams, and projects
- Conduct original research in the field of CIT.
- Subject 1: **Information Assurance and Security**
- Subject 2: **Computer Systems Concepts**
- Subject 3: **Task Automation Using Interpretive Languages**

2022 – 2024 Prishtine, Kosovo

SENIOR CYBER SECURITY ANALYST CYBER SECURITY NATIONAL UNIT (KOS-CERT)

- Provide technical support to resolve cyber incidents
- Develop cybersecurity awareness campaigns for different audiences
- Developing national cybersecurity policies and strategies.
- Correlate incident data to identify specific vulnerabilities
- Analysis of log files to identify possible threats to security.
- Real-time cyber defense and incident handling tasks
- Tools: **MISP, TheHive, Nessus, Kali linux, Snort**

2022 – 2024 Prishtine, Kosovo

ADJUNCT LECTURER ROCHESTER INSTITUTE OF TECHNOLOGY RIT-K (A.U.K)

- Deliver lectures, lead classroom discussions, and conduct lab sessions
- Preparing students for assessments and providing performance feedback.
- Answering students' questions and providing feedback on assignments.
- Subject 1: **Task automation using interpretive language**
- Subject 2: **Information Security and Assurance**

2021 – 2022 Rochester, United States

CYBER SECURITY RESEARCHER ROCHESTER INSTITUTE OF TECHNOLOGY

- Threat intelligence analysis and end-point security protection
- Incident handling, memory analysis and malware investigations
- Incident response and cyber investigation with Power Shell
- Tools: **Wireshark, Snort, Splunk, MISP, Nessus, OpenVAS, Hashcat**

2021 – 2022 Colorado Springs, United States

CYBER SECURITY RESEARCHER UCCS - UNIVERSITY OF COLORADO, COLORADO SPRINGS

- Analyze network evidence for Indicator of Compromise (IOC).
- Investigate windows programs and ports for Indicator of Compromise (IOC).
- Incident handling and malware investigations
- Tools: **Wireshark, Snort, Splunk, MISP, Nessus, OpenVAS, Hashcat**

2021 – 2022 Warsaw, Poland

CYBER SECURITY INSTRUCTOR HAKING MAGAZINE

- Client-Side Exploitation
- Skills and principles of client remote exploitation
- Simulating different types of vulnerabilities in client-side
- Social Engineering, backdoors and cookie attacks
- Tools: **Kali Linux, Metasploit, Nmap, Armitage, John the Ripper, Maltego**

2014 – 2022 Prishtine, Kosovo

CYBER SECURITY LECTURER COLLEGE AAB

- Deliver lectures, lead classroom discussions, and conduct lab sessions
- Preparing students for assessments and providing performance feedback.
- Subject 1: **Penetration Testing and Vulnerability Assessment**
- Subject 2: **Cyber Security Investigations**
- Subject 3: **Linux Operating System**

EDUCATION AND TRAINING

2018 – 2024 Podgorica, Montenegro

DOCTOR OF COMPUTER SCIENCE / DOCTOR OF PHILOSOPHY (PHD.) University of Montenegro

Level in EQF EQF level 8 | **Type of credits** ECTS | **Number of credits** 180 |

Thesis A Lightweight Framework for Cyber Risk Management in Western Balkan HEIs

2023 – 2023 Garmisch-Partenkirchen, Germany

PROGRAM ON CYBER SECURITY STUDIES (PCSS) George C. Marshall - European Center for Security Studies

- Knowledge of the technical aspects, concepts, and terminology of cyberspace
- Comprehensive awareness of the emerging and future threats posed by state
- Established standards and frameworks for conducting cybersecurity assessments
- Understanding best practices for the implementation of international law

Address Garmisch-Partenkirchen, Garmisch-Partenkirchen, Germany | **Website** https://www.marshallcenter.org

2023 United States

GIAC CERTIFIED INCIDENT HANDLER (GCIH) SANS Institute

Abilities:

- Apply a dynamic approach to incident response
- Identify threats using host, network, and log analysis
- Leverage PowerShell for data collection and cyber threat analysis
- Cyber investigation processes using live analysis and memory forensics
- Defense spotlight strategies to protect critical assets

Skills:

- **Incident Handling, Incident Response, Information Security, Malware Investigations**
- **Network Security, Penetration Testing, Reconnaissance, Security Policy**
- **Vulnerability Assessment, Web Application Security**

Address Washington, D.C, United States | **Website** https://www.sans.org

2022 United States
CERTIFIED COMPTIA SECURITY+ CompTIA - Accredited by ANSI (Verification Code "KVSDMHW8FQ3PVP95")

Abilities:

- Understand various types of threats, attacks, and vulnerabilities
- Analyze malware, ransomware, phishing, and social engineering
- Implement secure network architecture and principles
- Manage authentication, authorization, and accounting (AAA)
- Conduct risk assessments to evaluate risks to information assets

Skills:

- **Access Control, Cryptography, Cyber Forensics, Data Security**
- **Malware Identification, Network Security, Threat Analysis**

Address Chicago, United States | **Website** https://www.comptia.org

2012 – 2014 Tirane, Albania
M.SC. ENG. ENGINEERING OF MATHEMATICS AND COMPUTER SCIENCE Public University of Tirana / Faculty of Natural Science

Level in EQF EQF level 7 | **Type of credits** ECTS | **Number of credits** 120 |

Thesis Parallel Computations Through Different Algorithms

2009 – 2012 Tirane, Albania
B.SC. ENG. ENGINEERING OF ELECTRONICS Polytechnic University of Tirana / Faculty of Information Technology

Level in EQF EQF level 6 | **Type of credits** ECTS | **Number of credits** 180 | **Thesis** Analyzing and Exploiting Weak Wi-Fi Protocols

LANGUAGE SKILLS

Mother tongue(s): **ALBANIAN**

Other language(s):

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken production	Spoken interaction	
ENGLISH	B2	B2	B2	B2	B2

Levels: A1 and A2: Basic user; B1 and B2: Independent user; C1 and C2: Proficient user

DIGITAL SKILLS

Cyber Investigation and Cyber Security | Penetration Testing | Linux | Network Security | Linux (Terminal Commands, Bash/Shell) | Incident Response | Malware Analysis | Ethical Hacking . | Web Application Security | IT Security | Vulnerability Assestment | Programming with Python, Node js, Ruby, Bash, React, Js

CONFERENCES AND SEMINARS

2024 – 2024 Berlin, Germany
Cyber Threat Intelligence Conference

Organized by FIRST

2024 – 2024 Durres, Albania
Threat Inteligence Pipelines for Information Exchange

Organized by Trusted Introducer

2023 – 2023 Tirane, Albania
Task Force Computer Security Incident Response Team (CSIRT)

2023 – 2023 Mauritius, South Africa
Information Exchange using OSINT for Cyber Investigations

Organized by European Union

2023 – 2023 Chisinau, Moldova
Ensuring Cyber Resilience: Securing Our Connected Future

Organized by European Union

2022 – 2022 Vilnius, Lithuania
Task Force Computer Security Incident Response Team (CSIRT)

2022 – 2022 Prague, Czech Republic
TRANSITS II - Workshop on Incident Response (CSIRT)

Organized by Trusted Introducer

PROJECTS

2022 – 2023
Cybersecurity Awareness among High School Students

Supported by Kosovo United States Alumni (KUSA) and U.S. Embassy in Kosovo

2022 – 2022
Hosting Fulbright Specialist

Supported by U.S. Embassy in Kosovo

2021 – 2021
Cyber Security Consultants

Project "EU vs Virus Covid-19" organized by European Commission

2019 – 2019
Perfecting Academic Skills

Radboud University | Nijmegen, Netherland

2019 – 2019
Computer and Information Systems Security

Algebra University | Zagreb, Croatia

FELLOWSHIPS

2022 – 2022
International Cybersecurity Fellowship for Western Balkan

Purdue University I Indiana, USA

2021 – 2022
Fulbright Association and U.S. Department of State

Rochester Institute of Technology I Rochester, USA
University of Colorado in Colorado Springs I Colorado, USA

DRIVING LICENCE

Driving Licence: A

Krenar Kepuska has completed **PhD research** in Cyber Security as a Fulbright scholar at the University of Colorado in Colorado Springs (UCCS) and at the Rochester Institute of Technology (RIT). He is a **PhD candidate** at the University of Montenegro, where he proposes a framework for cyber risk management in Western Balkan higher education institutions. Furthermore, he earned an M.Sc. in Engineering of Mathematics and Computer Science from the Public University of Tirana, focusing on the efficiency of parallel computing algorithms.

In 2022, he participated in a fellowship with CRDF Global and the U.S. Department of State at **Purdue University** in Indiana. Additionally, he was part of the Fulbright Association and U.S. Department of State fellowship program in 2021, which included research and collaboration at **Rochester Institute of Technology** in New York and the **University of Colorado** in Colorado Springs. These fellowships highlight his commitment to advancing cybersecurity through academic and practical engagements.

Mr. Kepuska holds several notable certifications and training in cybersecurity. He became a GIAC Certified Incident Handler (**GCIH**) from the **SANS** Institute in 2023, enhancing his skills in dynamic incident response and cyber threat analysis. In 2022, he earned the Certified **CompTIA** Security+ credential, which solidified his understanding of threats, attacks, and vulnerabilities, as well as secure network architecture. Additionally, he completed the Program on Cyber Security Studies (**PCSS**) at the George C. Marshall European Center for Security Studies in 2023, gaining comprehensive knowledge of cyberspace concepts, emerging threats, and international cybersecurity standards.

Mr. Kepuska is currently a full-time lecturer at Rochester Institute of Technology in Kosovo (A.U.K), where he develops and delivers various cybersecurity course materials. From **2022 to 2024**, he served as a Senior Cyber Security Analyst at KOS-CERT, providing technical support for cyber incidents and developing national cybersecurity policies and strategies. In **2021-2022**, Krenar worked as a Cyber Security Researcher at Rochester Institute of Technology, focusing on threat intelligence analysis and malware investigations. He also held a similar position at the University of Colorado, Colorado Springs, where he analyzed network evidence and conducted incident handling. Additionally, he served as a Cyber Security Instructor at Haking Magazine, teaching skills and principles of client-side exploitation and social engineering. From **2014 to 2022**, he was a Cyber

Security Lecturer at College AAB, where he taught penetration testing, cyber investigations, and Linux operating systems. His extensive experience in both academia and the cybersecurity industry highlights his expertise and dedication to advancing the field.

Mr. Kepuska possesses a comprehensive set of skills in incident handling, response, information security, and malware investigations. His expertise extends to vulnerability assessment and web application security, with programming proficiency in Python. He is familiar with tools such as Wireshark, Snort, Splunk, MISP, Nessus, OpenVAS, Hashcat, Kali Linux, Metasploit, Nmap, Armitage, John the Ripper, and Maltego.

Mr. Kepuska has actively participated in various international conferences focused on cybersecurity. In **2024**, he attended the Cyber Threat Intelligence Conference organized by FIRST in Berlin, Germany, and the Threat Intelligence Pipelines for Information Exchange organized by Trusted Introducer in Durres, Albania. In **2023**, he took part in the Information Exchange using OSINT for Cyber Investigations conference organized by the European Union in Mauritius, South Africa, and the Ensuring Cyber Resilience: Securing Our Connected Future event in Chisinau, Moldova. In **2022**, Krenar participated in the Task Force for Computer Security Incident Response Team event organized by FIRST in Tirane, Albania, and the TRANSITS II - Workshop on Incident Response organized by Trusted Introducer in Prague, Czech Republic. These conferences highlight his engagement with the global cybersecurity community and his commitment to staying updated on the latest developments in the field.

Mr. Kepuska has completed advanced trainings at **Radboud University** in the Netherlands and **Algebra University** in Croatia, focusing on academic skills and computer security, respectively. His publication on "A lightweight framework for Cyber Risk Management in Western Balkan Higher Education Institutions" has been featured in renowned journals like **Scopus**, **Web of Science**, SCI, and PeerJ, reflecting his significant contributions to cybersecurity research.

Krenar is passionate about cybersecurity education and awareness in the Western Balkan region, committed to enhancing cybersecurity resilience through his research, teaching, and practical efforts. He led a project on cybersecurity awareness among high school students, supported by Kosovo United States Alumni (KUSA) and the U.S. Embassy in Kosovo in 2022. He hosted a Fulbright

Specialist, also supported by the U.S. Embassy in Kosovo, during the same year. Additionally, he contributed to the "EU vs Virus Covid-19" project organized by the European Commission in 2021.

Univerzitet Crne Gore
adresa / address_Cetinjska br. 2
81000 Podgorica, Crna Gora
telefon / phone_00382 20 414 255
fax_00382 20 414 230
mail_rektorat@ucg.ac.me
web_www.ucg.ac.me
University of Montenegro

Broj / Ref 03-3548
Datum / Date 28.10.2019

3256
05.11.19

Na osnovu člana 72 stav 2 Zakona o visokom obrazovanju („Službeni list Crne Gore" br 44/14, 47/15, 40/16, 42/17, 71/17, 55/18, 3/19, 17/19, 47/19) i člana 32 stav 1 tačka 9 Statuta Univerziteta Crne Gore, Senat Univerziteta Crne Gore na sjednici održanoj 28.10.2019. godine, donio je

O D L U K U
O IZBORU U ZVANJE

Dr Srđan Kadić bira se u akademsko zvanje docent Univerziteta Crne Gore za **oblast Računarstvo i programiranje**, na Prirodno-matematičkom fakultetu Univerziteta Crne Gore, na period od pet godina.

SENAT UNIVERZITETA CRNE GORE
PREDSJEDNIK

Prof. dr Danilo Nikolić, rektor

BIOGRAFIJA

Rodjen sam 11.09.1968.godine u Beogradu. Osnovnu i srednju školu završio sam u Podgorici sa odličnim uspjehom. Diplomirao sam na prirodno-matematičkom fakultetu u Podgorici na Odjseku za matematiku i računarske nauke, smjer računarstvo. Postdiplomske studije sam upisao na Odsjeku za matematiku i računarske nauke, smjer računarstvo Matematičkog fakulteta u Beogradu. Zbog specifičnosti teme dio ispita sa postdiplomskih studija sam polagao na Elektro-tehničkom fakultetu u Beogradu. Magistarski rad pod nazivom "Algoritam sortiranja za hardverski akcelerator obrade podataka" odbranio sam na Matematičkom fakultetu u Beogradu. Doktorske studije upisao sam na na prirodno-matematičkom fakultetu u Podgorici na Odjseku za matematiku i računarske nauke, smjer računarstvo. Disertaciju pod nazivom "Algoritam provjere serijalizovanosti konkuretnog izvršavanja transakcija" odbranio sam na Prirodno-matematičkom fakultetu u Podgorici.

Od oktobra 1994.godine radim u nastavi na Odsjeku za matematiku i računarske nauke Prirodno-matematičkog fakulteta u Podgorici. U nastavi držim predavanja/ vježbe iz predmeta: Računari i programiranje, Principi programiranja, Vizuelizacija i računarska grafika, Uvod u informacione sisteme, Softver inžinjering, Napredne progamske tehnike i Razvoj aplikacija na prenosvim uređajima.

Funkciju prodekana za finansije na Prirodno-matematičkom fakultetu u Podgorici obavljao sam u periodu 2013-2016.

prof. M. Томашевић

УНИВЕРЗИТЕТ У БЕОГРАДУ ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ
БЕОГРАД

Адреса: Студентски трг 1, 11000 Београд, Република Србија
Тел.: 011 3207400; Факс: 011 2638818; E-mail: office@etf.bg.ac.rs

Примљено: 13 -07- 2015
Орг. јед. | Број | Прилог | Вредност
63/7

СЕНАТ УНИВЕРЗИТЕТА
У БЕОГРАДУ

Београд, 08.07.2015. године
06-01 Број: 61202-2450/3-15
МЦ

На основу чл. 65. ст. 2. Закона о високом образовању ("Службени гласник РС", број 76/05, 100/07-аутентично тумачење, 97/08, 44/10 и 93/12), чл. 42. ст. 1. тач. 23. и чл. 43. ст. 4. Статута Универзитета у Београду ("Гласник Универзитета у Београду", број 162/11-пречишћени текст и 167/12), чл. 25. ст. 1. и ст. 2. тач. 1. Правилника о начину и поступку стицања звања и заснивања радног односа наставника Универзитета у Београду ("Гласник Универзитета у Београду", број 142/08, 150/09 и 160/11) и Критеријума за стицање звања наставника на Универзитету у Београду ("Гласник Универзитета у Београду", број 140/08, 144/08, 160/11, 161/11, 165/11), а на предлог Изборног већа Електротехничког факултета, број: 63/5 од 21.04.2015. године и мишљења Већа научних области техничких наука, број: 61202-2450/2-15 од 08.05.2015. године, Сенат Универзитета, на седници одржаној 08.07.2015. године, донео је

О Д Л У К У

БИРА СЕ др Мило Томашевић у звање редовног професора на Универзитету у Београду-Електротехнички факултет, за ужу научну област Рачунарска техника и информатика.

О б р а з л о ж е њ е

Електротехнички факултет је дана 14.01.2015. године у листу „Послови" објавио конкурс за избор у звање редовног професора, за ужу научну област Рачунарска техника и информатика, због истека потреба Факултета.

Извештај Комисије за припрему извештаја о пријављеним кандидатима стављен је на увид јавности дана 23.02.2015. године преко сајта Факултета.

На основу предлога Комисије за припрему извештаја о пријављеним кандидатима, Изборно веће Електротехничког факултета, на седници одржаној дана 21.04.2015. године, донело је одлуку о утврђивању предлога да се кандидат др Мило Томашевић изабере у звање редовног професора.

Електротехнички факултет је дана 21.05.2015. године доставио Универзитету комплетан захтев за избор у звање на прописаним обрасцима.

Универзитет је комплетну документацију коју је доставио Факултет ставио на web страницу Универзитета дана 01.06.2015. године.

Веће научних области техничких наука, на седници одржаној дана 08.06.2015. године дало је мишљење да се др Мило Томашевић може изабрати у звање редовног професора.

Сенат Универзитета, на седници одржаној дана 08.07.2015. године разматрао је захтев Електротехничког факултета и утврдио да кандидат испуњава услове прописане чл. 64. и 65. Закона о високом образовању, чланом 124. Статута Универзитета у Београду, као и услове прописане Критеријумима за стицање звања наставника на Универзитету у Београду, па је донета одлука као у изреци.

ПРЕДСЕДНИК СЕНАТА
Ректор
Проф. др Владимир Бумбаширевић

Достављити:
- Факултету (2)
- архиви Универзитета
- сектору 06

Мило В. Томашевић

I. НАУЧНО-ИСТРАЖИВАЧКИ РЕЗУЛТАТИ

М10 – Монографије, монографске студије, тематски зборници, лексикографске и картографске публикације међународног значаја

М14 Рад у тематском зборнику међународног значаја

1. Tomašević M., Milutinović V., *Hardware Solutions for Cache Coherence Problem in SharedMemory Multiprocessors* in *Cache Coherence Problem in SharedMemory Multiprocessors: Hardware Solutions,* IEEE Computer Society Press, Los Alamitos, CA, USA, July 1993.
2. Protić, J., Tomašević M., Milutinović V., *An Overview of Distributed Shared Memory* in *Distributed Shared Memory: Concepts and Systems,* IEEE Computer Society Press, Los Alamitos, CA, USA, July 1997.
3. Milutinović, V., Tomašević, M., Protić, J., Savić, S., Jovanović, M., and Grujić, A., "A Reflective Memory System for Personal Computers" in *Surviving the Design of Microprocessor and Multimicroprocessor Systems – Lessons Learned by Milutinović, V., John Wiley & Sons,* 2000.

М17 Уређивање тематског зборника, лексикографске и картографске публикације водећег међународног значаја

1. Tomašević M., Milutinović V., *Cache Coherence Problem in SharedMemory Multiprocessors: Hardware Solutions*, IEEE Computer Society Press, Los Alamitos, CA, USA, July 1993.
2. Protić, J., Tomašević M., Milutinović V., *Distributed Shared Memory: Concepts and Systems,* IEEE Computer Society Press, Los Alamitos, CA, USA, July 1997.

М20 – Радови међународног значаја

М21а Рад у међународном часопису изузетних вредности

1. Dundjerski D., Tomašević M., "Automatic Database Troubleshooting of Azure SQL Databases", *IEEE Transaction on Cloud Computing*, DOI: 10.1109/TCC.2020.3007016, Vol. 10, No. 3, July-September 2022, pp. 1604-1619, ISSN: 2168-7161, IF(2020): 5.938, citiran 1 put
2. Trobec R., Vasiljević R., Tomašević M., Milutinović V., Beivide R., Valero M., "Interconnection Networks in Petascale Computer Systems: a Survey", *ACM Computing Surveys*, Vol. 49, No. 3, September 2016, pp. 1-25, ISSN: 0360-0300, IF(2016): 6.748, citiran 19 puta

М21 Рад у врхунским међународним часописима

1. Kepuška K., Tomašević M., "A lightweight framework for cyber risk management in Western Balkan higher education institutions, ", *PEERJ Computer Science*, April 2024, DOI: 10.7717/peerj-cs.1958, ISSN: 2376-5992, IF(2022): 3.8, citiran 0 puta

2. Protić J., Tomašević M., Milutinović V., "Distributed Shared Memory: Concepts and Systems," *IEEE Parallel & Distributed Technology*, Vol. 4, No. 2, Summer 1996, pp. 6379, ISSN: 1063-6552, IF(1998): 1.727, citiran 118 puta
3. Grujić A., Tomašević M., Milutinović V., "A Simulation Study of Hardware-Oriented DSM Approaches", *IEEE Parallel & Distributed Technology*, Vol. 4, No. 1, Spring 1996, pp. 7483, ISSN: 1063-6552, IF(1998): 1.727, citiran 17 puta

M22 Рад у истакнутом међународном часопису

1. Mišić M., Tomašević M., "Comparison of Parallel Central Processing Unit- and Graphics Processing Unit-based Implementations of Greedy String Tiling Algorithm for Source Code Plagiarism Detection", *Concurrency and Computation: Practice and Experience*, Vol. 27, Issue 1, June 2022, pp. 1-12, DOI: 10.1002/cpe.7135, ISSN: 1532-0626, IF(2021): 1.831, citiran 1 put
2. Mišić M., Kovačev P, Tomašević M., "Improving Performance of Background Subtraction on Mobile Devices: a Parallel Approach" *Journal of Real-Time Image Processing*, November 2021, DOI: 10.1007/s11554-021-01184-x, ISSN: 1861-8200, IF(2021): 1.935, citiran 1 put
3. Blagojević V., Bojić D., Bojović M., Cvetanović M., Đorđević J., Đurđević Đ., Furlan B., Gajin S., Jovanović Z., Milićev D., Milutinović V., Nikolić B., Protić J., Punt M., Radivojević Z., Stanisavljević Ž., Stojanović S., Tartalja I., Tomašević M., Vuletić P., "A Systematic Approach to Generation of New Ideas for PhD Research in Computing", *Advances in Computers*, Vol. 104, January 2017., pp. 1-32, 10.1016/bs.adcom.2016.09.001 ISSN: 0065-2458, IF(2017): 1.514, citiran 18 puta
4. Dundjerski D., Tomašević M., "GPU-Based Parallelization of the OSPF and BGP Routing Protocols", *Concurrency and Computation: Practice and Experience*, Vol. 27, Issue 1, January 2015, pp. 237-251, ISSN: 1532-0626, IF(2015): 0.942, citiran 2 puta
5. Punt M., Tomašević M., Đorđević J., "Evaluation and Analysis of an On-line Error Detection Monitoring Technique", *Computers and Electrical Engineering*, Vol. 39, Issue 2, February 2013, pp. 261-273, ISSN: 0045-7906, IF(2013): 0.992, citiran 0 puta
6. Tomašević M., Milutinović V., "Hardware Approaches to Cache Coherence in Shared-Memory Multiprocessors, Part 2," *IEEE Micro*, Vol.14., No.6, December 1994., pp. 61-66, ISSN: 0272-1732, IF: 0.43, citiran 0 puta
7. Tomašević M., Milutinović V., "Hardware Approaches to Cache Coherence in Shared-Memory Multiprocessors, Part 1," *IEEE Micro*, Vol.14., No.5, October 1994., pp. 52-59, ISSN: 0272-1732, IF: 0.43, citiran 33 puta

M23 Рад у међународном часопису

1. Tomašević V., Tomašević M., "Double TimeMemory TradeOff in OSK RFID Protocol", *Wireless Personal Communication*, 108(1), August 2019, pp. 551-568, DOI: 10.1007/s11277-019-06417-8, ISSN: 0929-6212, IF(2019): 1.061, citiran 1 put
2. Tomašević V., Tomašević M., Bojanić S., "Interval-based Recording of Generated Pseudo-Random Numbers", *Revista Internacional de Métodos Numéricos para*

Cálculo y Diseño en Ingeniería, Vol 35 (2), 33, 2019., DOI:10.23967/j.rimni.2019.06.003, ISSN: 0213-1315, IF(2019): 0.338, citiran 1 put

3. Radulović M., Girbal S., Tomašević M., "Low-level Implementation of the SISC Protocol for Thread-level Speculation on a Multi-core Architecture", *Parallel Computing*, vol. 67, Issue C, September 2017, pp. 119, DOI: 10.1016/j.parco.2017.07.007, ISSN: 0167-8191, IF(2017): 0.938, citiran 0 puta
4. Radulović M., Tomašević M., Milutinović V., "Register-Level Communication in Speculative Chip Multiprocessors", *Advances in Computers*, vol. 92, January 2014, pp. 166, ISSN: 0065-2458, IF: 0.489 (2013), citiran 3 puta
5. Vitorović A., Tomašević M., Milutinović V., "Manual Parallelization versus State-of-the-art Parallelization Techniques: the SPEC CPU2006 as a Case Study", *Advances in Computers*, vol. 92, January 2014, pp. 203-251, ISSN: 0065-2458, IF: 0.489 (2013), citiran 4 puta
6. Tomašević V., Tomašević M., "An Analysis of Chain Characteristics in the Cryptanalytic TMTO Method", *Theoretical Computer Science*, Vol. 501, August 2013, pp. 52-61, ISSN: 0304-3975, IF(2013): 0.516, citiran 4 puta
7. Tomašević M., Bojović M., Đorđević J., "A Hardware Implementation of the Mechanism of Multiprocessing", *Microprocessors and Microsystems*, Vol. 23, December 1999, pp. 471479, ISSN: 0141-9331, IF(1999): 0.151, citiran 0 puta
8. Bojović M., Tomašević M., Đorđević J., "The Interactive Development and Testing System for a RISC-Style Processor," *The Computer Journal*, Vol. 42, No. 5, 1999., ISSN: 0010-4620, IF(1999): 0.349, citiran 0 puta
9. Đorđević J., Tomašević M., Bojović M., Potić V., Ranđić S., "An Operating System Accelerator," *Journal of Systems Architecture*, Vol. 44, No. 9-10, June 1998, pp. 737-754, ISSN: 1383-7621, IF(1998): 0.029, citiran 3 puta
10. Tomašević M., Milutinović V. "The Word-invalidate Cache Coherence Protocol," *Microprocessors and Microsystems*, Vol. 20, No. 1, March 1996, pp. 3-16, ISSN: 0141-9331, IF(1997): 0.163, citiran 6 puta
11. Savić, S., Tomašević M., Milutinović V. "Improved RMS for the PC Environment," *Microprocessors and Microsystems*, Vol. 19, No. 10, December 1995, pp. 609-619, ISSN: 0141-9331, IF(1997): 0.163, citiran 3 puta

Радови у међународним научним часописима ван JCR листе (часописи који немају *impact factor*)

1. Đorđević J., Bojović M., Tomašević M., Lazić B., Velašević D., "A RISC-Style Hardware Accelerator for Operating Systems," *International Journal of Computers and Applications*, Vol. 21, No. 2, 1999, pp. 50-55, ISSN: 1206-212X.
2. Radulović M., Tomašević M., "A Proposal for Register-level Communication in a Speculative Chip Multiprocessor", *ETF Journal of Electrical Engineering, University of Montenegro,* Vol. 15, No. 1, May 2006, pp. 91-98. ISSN 0352 – 5207.
3. Tomašević M., Protić J., Savić S., Jovanović M., Grujić A., Milutinović V. "A Reflective Memory System for Personal Computers", *The IPSI Transactions on Internet Research*, Vol. 2, No. 2, July 2006, pp. 7-12. ISSN: 1820-4503

4. Radulović M., Tomašević M. "On Reducing Overheads in CMP TLS Integrated Protocols", *The IPSI Bgd Transactions on Internet Research*, Vol. 3, No. 1, January 2007, pp. 11-17. ISSN: 1820-4503

M30 Међународни научни скупови

M31 – Предавање по позиву са међународног скупа штампано у целини

1. Mišić M., Protić J., Tomašević M. "Improving Source Code Plagiarism Detection: Lessons Learned", *25th Telecommunications Forum (TELFOR)*, Belgrade, Serbia, November 2017.
2. Šuštran Ž., Protić J., Tomašević M. "Towards an Improved Implementation of Hardware Transactional Memory on Asymmetric Processors", *30th Telecommunications Forum (TELFOR)*, Belgrade, Serbia, November 2022.

M32 – Предавање по позиву са међународног скупа штампано у изводу

1. Tomašević M., Milutinović V., "Shared-Memory Multiprocessors", *2nd International Conference on Parallel Processing and Applications (PPAM'97)* Zakopane, Poland, September 1997.
2. Tomašević M., Protić, J., Milutinović V., "Contemporary Issues in Shared-Memory Multiprocessors", *HIPC-97 Asian High Performance Conference,* Seoul, Korea, April 97.
3. Protić J., Tomašević M., Milutinović V., "Distributed Shared Memory: Concepts and Systems," *23th International Symposium on Computer Architecture (ISCA 23),* Philadelphia, PA, USA, May 1996.
4. Tomašević M., Tartalja I., Milutinović V., "Hardware and Software Approaches to Cache Coherence in Shared-Memory Multiprocessors", *Specialized workshop on cache consistency problem*, University of Pisa, Pisa, Italy, January 96.
5. Tomašević M., Milutinović V., "Tutorial on Hardware Approaches to Cache Coherence in Shared-Memory Multiprocessors", *2th International Symposium on High-Performance Computer Architecture (HPCA),* San Jose, CA, USA, February 1996.
6. Tomašević M., Milutinović V., "Hardware Approaches to Cache Coherence in Shared-Memory Multiprocessors", *22th International Symposium on Computer Architecture (ISCA 22),* Santa Margherita Ligure, Italy, June 1995.

M33 – Саопштење са међународног скупа штампано у целини

1. Smiljković L., Radonjić M., Mišić M., Tomašević M. "Comparing Python Code Parallelization Techniques for Spatial Transcriptomics Data", *30th Telecommunications Forum (TELFOR)*, Belgrade, Serbia, November 2023.
2. Šuštran Ž., Protić J., Tomašević M. "Towards an Improved Implementation of Hardware Transactional Memory on Asymmetric Processors", *30th Telecommunications Forum (TELFOR)*, Belgrade, Serbia, November 2022.

3. Đukić J., Jocović V., Mišić M., Tomašević M. "Automated Grading System for Picocomputer Assembly Codes Integrated within E-Learning Platform", *6th International Conference on Electrical, Electronic and Computing Engineering (IcETRAN)*, Novi Pazar, Serbia, June, 2022.
4. Kovačev P., Mišić M., Tomašević M. "Parallelization of the Mixture of Gaussians Model for Motion Detection on the GPU", *Zooming Innovation in Consumer Electronics International Conference 2018 (ZINC)*, Novi Sad, Serbia, May, 2018.
5. Dundjerski D., Lazić S., Tomašević M., Bojić D., "Improving Schema Issue Advisor in the Azure SQL Database", *25th Telecommunications Forum (TELFOR)*, Belgrade, Serbia, November 2017.
6. Mišić M., Protić J., Tomašević M. "Improving Source Code Plagiarism Detection: Lessons Learned", *25th Telecommunications Forum (TELFOR)*, Belgrade, Serbia, November 2017.
7. Vlahović T., Mišić M., Tomašević M., Karadžić A., Rikalo A., "Extending Valgrind framework with the MIPS MSA Support", *Zooming Innovation in Consumer Electronics International Conference 2017 (ZINC)*, Novi Sad, Serbia, May, 2017.
8. Dunđerski D., Nikolić B., Tomašević M., "A New CUDA Web-based Learning Environment", *3rd International Conference on Electrical, Electronic and Computing Engineering (IcETRAN)*, Zlatibor, Serbia, June 2016.
9. Vesović M., Smiljanić A., Tomašević M., "Speeding-up IP Lookup Procedure in Software Routers by Means of Parallelization", *24th Telecommunications Forum (TELFOR)*, Belgrade, Serbia, November 2016.
10. Nikolov D., Mišić M., Tomašević M., "GPU-based Implementation of Reverb Effect", *23th Telecommunications Forum (TELFOR)*, Belgrade, Serbia, November 2015.
11. Mišić M., Bethune I., Tomašević M., "Automated Regression Testing and Code Coverage Analysis of the CP2K Application", *7th IEEE International Conference on Software Testing, Verification, and Validation*, Cleveland, USA, April 2014.
12. Milić U., Gelado I., Puzović N., Ramirez A., Tomašević M., "Parallelizing General Histogram Application for CUDA Architecture", *International Conference on Embedded Computer Systems: Architectures, Modeling, and Simulation*, Samos, Greece, July 2013.
13. Štrbac-Savić S., Tomašević M., "Comparative Performance Evaluation of the AVL and RedBlack Trees", *V Balcan Conference in Informatics*, Novi Sad, Serbia, September 2012.
14. Mišić M., Đurđević Đ., Tomašević M., "Evolution and Trends in GPU Computing", *35th International Convention on Information, Communication and Electronics Technology (MIPRO)*, Opatija, Croatia, Maj 2012.
15. Punt M., Djordjević J., Tomašević M., "A Simulation Environment for the On-Line Monitoring of a Fault Tolerant Flight Control Computer", *IEEE Eastern European Regional Conference on the Engineering of Computer Based Systems*, Novi Sad, September 2009.
16. Radulović M., Tomašević M., "Towards an Improved Integrated Coherence and Speculation Protocol", *IEEE EUROCON2007*, Warsaw, Poland, September 2007.

17. Radulović M., Tomašević M., "Support for Thread-Level Speculationin Chip Multiprocessors", *Proceedings of the ACACES (Advanced Computer Architecture and Compilation for Embedded Systems)*, L'Aquila, Italy, July 2007.

18. Radulović M., Tomašević M., "An Agressive Register-level Communication in a Speculative Chip Multiprocessor", *IEEE EUROCON2005*, Belgrade, Serbia, November 2005.

19. Elahresh M., Djordjević J., Tomašević M., Aleksić M., "An Improved On-Line Monitoring Technique for a Fault-Tolerant Computing Node", *Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering*, Toronto, Canada, 2004.

20. Tončev M., Tomaševic M., Djordjević J., Aleksić M., "Improving Performance of a DSM System by the Communication Controller Organization", *Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering*, Toronto, Canada, 2004.

21. Tončev M., Djordjević J.,Tomaševic M., Aleksić M., "Multithreaded Communication Controller For Efficient DSM Multiprocessors", *Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering*, Toronto, Canada, 2001.

22. Tončev M., Tomaševic M., Aleksić M., "The Impact of Out-of-Order Message Delivery on Cache Coherence Protocols", *Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering*, Toronto, Canada, 2001.

23. Milutinović V., Marković B., Tomašević M., Tremblay M. "The Split Temporal/Spatial Cache: A Complexity Analysis," *Proceedings of 6th SCIzzL*, Santa Clara, USA, September 1996,

24. Milutinović V., Marković B., Tomašević M., Tremblay M. "The Split Temporal/Spatial Cache: A Performance Analysis," *Proceedings of 5th SCIzzL*, Santa Clara, USA, March 1996,

25. Protić J., Tartalja I., Tomašević M., "Memory Consistency Models for Shared Memory Multiprocessors and DSM Systems," *Proceedings of the MELECON96*, Bari, Italy, May 1996.

26. Milutinović V., Tomašević M., Marković B., Tremblay M. "A New Cache Architecture Concept: The Split Temporal/Spatial Cache," *Proceedings of the MELECON96*, Bari, Italy.

27. Protić J., Tomašević M., Milutinović V., "A Survey of Distributed Shared Memory Systems," *28th Hawaii International Conference on System Sciences*, Maui, USA, January 1995.

28. Jovanović M., Tomašević M., Milutinović V., "A Simulation Analysis of Two Reflective Memory Approaches," *28th Hawaii International Conference on System Sciences*, Maui, USA, January 1995.

29. Protić J., Tomašević M., Milutinović V., "A Survey of Distributed Shared Memory Approaches," *Proceedings of XVI Int. Symposium on Nuclear Electronics and Computing*, Varna, Bulgaria, September 1994.

30. Jovanović M., Tomašević M., Milutinović V., "Design Issues in Block-Oriented Reflective Memory System," *Proceedings of XVI Int. Symposium on Nuclear Electronics and Computing*, Varna, Bulgaria, September 1994.

31. Grujić A., Tomašević M., Milutinović V., "A Simulation Study of Hardware-Oriented DSM Approaches", *IEEE Region 10's 9th Annual International Conference,* Singapore, August 1994.
32. Graovac S., Tomašević M., Benčik R., Radosavljević A., "Train Driving Simulator," *5th International Training Equipment Conference,* Hague, Netherland, April 1994.
33. Tomašević M., Milutinović V., "A Survey of Hardware Solutions for Maintenance of Cache Coherence in Shared-Memory Multiprocessors", *26th Hawaii International Conference on System Sciences*, Maui, USA, January 1993.
34. Tomašević M., Milutinović V., "A Simulation Study of Snoopy Cache Coherence Protocols", *25th Hawaii International Conference on System Sciences*, Maui, USA, January 1992.

M34 – Саопштење са међународног скупа штампано у изводу

1. Mišić M., Tomašević M., "Analysis of Parallel Sorting Algorithms on Different Parallel Platforms", *Proceedings of the ACACES (Advanced Computer Architecture and Compilation for Embedded Systems)*, Fiuggi, Italy, July 2011.
2. Radulović M., Girbal S., Tomašević M., "Evaluating the SISC TLS Protocol through Structural Simulation", *Proceedings of the ACACES (Advanced Computer Architecture and Compilation for Embedded Systems)*, Terrasa, Barcelona, Spain, July 2009.
3. Stojanović S., Furlan B., Tomašević M., Milutinović V., "An Overview of Concurrency Support in Accessing Shared Data in SMPs," *Proceedings of the ACACES (Advanced Computer Architecture and Compilation for Embedded Systems)*, L'Aquila, Italy, July 2008.
4. Radulović M., Girbal S., Tomašević M., "Simulation Support for Speculative Multithreading Processors", *Proceedings of the ACACES (Advanced Computer Architecture and Compilation for Embedded Systems)*, L'Aquila, Italy, July 2008.
5. Tomašević M., Puzović N., Leković S., "Analysis and Improvement of Replacement Algorithms in SMP cache memory systems", *Proceedings of the ACACES (Advanced Computer Architecture and Compilation for Embedded Systems)*, L'Aquila, Italy, July 2005.

M40 – Монографије националног значаја

M45 Поглавље у књизи M42 или рад у тематском зборнику националног значаја

1. V.Tomašević and M.Tomašević, Application of the innovative IT technologies in insurance, in *Contemporary challenges and sustainability of the insurance industry*, Chapter 23, University of Belgrade - Faculty of Economics, 2021, pp. 283-298.
2. V.Tomašević and M.Tomašević, Insurance issues regarding cyber security threats, in *Insurance market after COVID-19*, Chapter 23, University of Belgrade - Faculty of Economics, 2020, pp. 421-440.

M50 – Национални часописи

M52 – Рад у истакнутом часопису националног значаја

1. Tomašević V., Tomašević M., "Analysis and Evaluation of Three Methods for Tag Identification in OSK RFID Protocol", *Telfor Journal*, Vol. 11, No. 1, 2019., ISSN: 1821-3251.
2. Dundjerski D., Lazić S., Tomašević M., Bojić D., "An Extended Evaluation of Schema Issue Advisor in the Azure SQL Database," *Telfor Journal*, Vol. 10, No. 2, 2017., pp. 91-96, 2018., ISSN: 1821-3251.
3. Vesović M., Smiljanić A., Tomašević M., "Speeding up IP Lookup Procedure in Software Routers by Means of Parallelization," *Telfor Journal*, Vol. 9, No. 1, 2017., pp. 2-7, 2017. ISSN: 1821-3251.
4. Mišić M., Nikolov D., Tomašević M., "Analysis of CPU and GPU Implementations of Convolution Reverb Effect", *Telfor Journal*, Vol. 8, No. 2, 2016., pp. 121-126. ISSN: 1821-3251.
5. Mišić M., Dašić D., Tomašević M., "An Analysis of OpenACC Programming Model: Image Processing Algorithms as a Case Study", *Telfor Journal*, Vol. 6, No. 1, 2014., pp. 53-58. ISSN: 1821-3251.
6. Mišić M., Tomašević M., "Data Sorting Using Graphics Processing Units", *Telfor Journal*, Vol. 4 No.1, 2012, ISSN: 1821-3251.
7. Milivojević M., Đurđević Đ., Tomašević M., "Architecture of a System for Interactive Training and Testing in Algorithms and Data Structures", *Telfor Journal*, Vol.3 No.1 (2011). ISSN: 1821-3251.

М53 – Рад у часопису националног значаја

1. Tomašević V., Tomašević M., "Pregled i analiza kriptoanalitičkih TMTO metoda", *Singidunum revija*, Beograd, oktobar 2010., pp. 141-152. ISSN: 1820-8819.
2. Štrbac-Savić S., Tomašević M., Maček N., Minchev Z. "Comparative Performance Evaluation of Suboptimal Binary Search Trees", *Journal of Computer And Forensic Sciences*, Vol.1, No. 1, 2022, pp. 29-45, ISSN 2956-0799.
3. Radulović M., Tomašević M. "On Reducing Overheads in CMP TLS Integrated Protocols", *The IPSI Bgd Transactions on Internet Research*, Vol. 3, No. 1, January 2007, pp. 11-17. ISSN: 1820-4503
4. Tomašević M., Protić J., Savić S., Jovanović M., Grujić A., Milutinović V. "A Reflective Memory System for Personal Computers", *The IPSI Bgd Transactions on Internet Research*, Vol. 2, No. 2, July 2006, pp. 7-12. ISSN: 1820-4503.

М55 – Уређивање научног часописа националног значаја

1. Члан Уређивачког одбора часописа *TELFOR Journal*
2. Одговорни уредник сепарата Електротехника у оквиру часописа *Техника*

<u>М60 –Национални скупови</u>

М63 – Саопштење са скупа националног значаја штампано у целини

1. Mišić M., Jovanović K., Drašković D., Žarković M., Tomašević M., "Godine partnerstva: saradnja sa privredom na Elektrotehničkom fakultetu Univerziteta u Beogradu u periodu 2016.-2021.", *XXVIII skup „Trendovi razvoja"*, Univerzitet u Novom Sadu, Fakultet tehničkih nauka, Kopaonik, Februar 2021

2. Drašković D., Šekularac T., Srbljanović A., Nikolić B., Protić J., Cvetanović M., Ivaniš P., Tomašević M., "Novi pristupi u daljinskoj nastavi i radu stručnih tela Elektrotehničkog fakulteta u Beogradu tokom pandemije Covid-19", *XXVII skup „Trendovi razvoja"*, Univerzitet u Novom Sadu, Fakultet tehničkih nauka, Kopaonik, Februar 2021.
3. Tomašević V., Tomašević M., "Ubrzanje postupka identifikacije taga kod OSK RFID protokola", *XXVI Telekomunikacioni forum TELFOR*, Beograd, Novembar 2018.
4. Mišić M., Protić J., Tomašević M., "Pravci unapređenja softverskih sistema za detekciju plagijarizma u izvornom programskom kodu u akademskom okruženju", *XXIII skup „Trendovi razvoja"*, Univerzitet u Novom Sadu, Fakultet tehničkih nauka, Kopaonik, Februar, 2017
5. Mišić M., Dacić A., Jovanović V., Protić J., Tomašević M., "Disciplinska odgovornost studenata kroz pravilnike, disciplinske mere, stavove studenata i analizu podataka", *XXIII skup „Trendovi razvoja"*, Univerzitet u Novom Sadu, Fakultet tehničkih nauka, Kopaonik, Februar, 2017.
6. Mišić M., Nikolov D., Protić J., Tomašević M., "Paralelizacija GST algoritama za detekciju sličnosti u programskom kodu", *XXIV Telekomunikacioni forum TELFOR*, Beograd, Novembar 2016.
7. Tomašević V., Tomašević M., "Time-Memory Trade-Off in RFID Systems", *SINTEZA2016 International Scientific Conference*, Belgrade, April 2016.
8. Mišić M., Živković M., Protić J., Tomašević M., "Detekcija sličnosti u programskom kodu korišćenjem GST algoritma", *YUINFO 2016*, Kopaonik, Mart 2016.
9. Francuski M., Mišić M., Tomašević M., "Simulacija računarskog protivnika u igri potapanje brodova na Android platformi", *YUINFO 2013*, Kopaonik, 2013.
10. Mišić M., Dašić D., Tomašević M., "Analiza primene OpenACC direktiva u implementaciji algoritama za obradu slike", *XXI Telekomunikacioni forum TELFOR*, Beograd, Novembar 2013.
11. Miletić S., Mišić M., Tomašević M.,"Implementacija grafovskih algoritama korišćenjem grafičkih procesora", *Konferencija za ETRAN*, Zlatibor, Jun 2013.
12. Ilić V., Mišić M., Tomašević M., "Primena grafičkih procesora u obradi zvučnih signala", *XX Telekomunikacioni forum TELFOR*, Beograd, Novembar 2012.
13. Tomašević V., Tomašević M., " Kompromis između vremenskih i memorijskih zahteva u kriptoanalitičkom postupku", *XX Telekomunikacioni forum TELFOR*, Beograd, Novembar 2012. (Predavanje po pozivu)
14. Mišić M., Tomašević M.,"Analiza performansi memorijske hijerarhije na CUDA grafičkim procesorima", *Konferencija za ETRAN*, Zlatibor, Jun 2012.
15. Štrbac-Savić S., Tomašević M., "Analiza performansi skoro balansiranih stabala binarnog pretraživanja", *Konferencija za ETRAN*, Zlatibor, Jun 2012.
16. Štrbac-Savić S., Tomašević M., "Analiza tehnika za reorganizaciju samopodešavajućih stabala", *XI Naučno-stručni simpozijum Infoteh*, Jahorina, Mart 2012.
17. Mišić M., Tomašević M., "Sortiranje podataka korišćenjem grafičkih procesorskih jedinica" *XIX Telekomunikacioni forum TELFOR*, Beograd, Novembar 2011.

18. Dunđerski D., Tomašević M., "Paralelizacija izbora najboljih ruta u BGP protokolu pomoću grafičkog procesora", *XIX Telekomunikacioni forum TELFOR*, Beograd, Novembar 2011.
19. Milivojević M., Đurđević Đ., Tomašević M., "Sistem za interaktivnu obuku i testiranje znanja iz algoritama i struktura podataka", *XVIII Telekomunikacioni forum TELFOR*, Beograd, Novembar 2010.
20. Radulović M., Tomašević M., "A Proposal for Register-level Communication in a Speculative Chip Multiprocessor", *XLIX Konferencija za ETRAN*, Budva, Jun 2005.
21. Tomašević M., Radulović M., "Speculative Chip Multiprocessors", *Proceedings of International Workshop devoted to the 25th Anniversary of Faculty of Natural Sciences*, Podgorica, September 2005, pp. 168-186.
22. Elahresh M., Đorđević J., Tomašević M., "Evaluation of a Fault-Tolerant Computing Node", *XLIV Konferencija za ETRAN*, Sokobanja, Jun 2000.
23. Elahresh M., Tomašević M., Đorđević J., "A Simulator for a Fault-Tolerant Computing Node", *XLIV Konferencija za ETRAN*, Sokobanja, Jun 2000.
24. Elahresh M., Đorđević J., Tomašević M., "DASS – An Improved Monitoring Technique", *XLIII Konferencija za ETRAN*, Zlatibor, Septembar 1999.
25. Elahresh M., Tomašević M., Đorđević J., "The On-line Error Detection Using the Monitoring Technique", *Informacione tehnologije*, Žabljak, Mart 1998.
26. Tončev M., Tomašević M., Đorđević J., "Višekontekstni komunikacioni kontroler za efikasni DSM multiprocesor", *XLII Konferencija za ETRAN*, Vrnjačka Banja, Jun 1998.
27. Tončev M., Tomašević M., Đorđević J., "Dinamička simulacija multiprocesora sa distribuiranom zajedničkom memorijom", *XLI Konferencija za ETRAN*, Zlatibor, Jun 1997.
28. Jovanović M., Tomašević M., "Analiza složenosti osnovnog i poboljšanog sistema sa reflektivnom memorijom", *XL Konferencija ETRAN-a*, Budva, Jun 1996.
29. Protić J., Tartalja I., Tomašević M., "Prilog razumevanju memorijskih modela konzistencije", *YU INFO96*, Brezovica, April 1996.
30. Tončev M., Tomašević M., Đorđević J. Milutinović V., "Statistička analiza korišćenja primitiva protokola za održavanje keš koherencije kod DSM multiprocesora", *YU INFO96*, Brezovica, April 1996.
31. Protić J., Tomašević M., Milutinović V., "Pregled DSM procesiranja: sistemi", *XXXIX Konferencija ETAN-a*, Zlatibor, Jun 1995.
32. Jovanović M., Tomašević M., "Analitičko modeliranje performansi RM/MC sistema", *XXXIX Konferencija ETAN-a*, Zlatibor, Jun 1995.
33. Jovanović M., Tomašević M., "Simulaciono poređenje dva pristupa sistema sa reflektivnom memorijom", *YU INFO95*, Brezovica, 1995.
34. Protić J., Tomašević M., Milutinović V., "Pregled DSM procesiranja: koncepti", *YU INFO95*, Brezovica, Mart 1995.
35. Tomašević M., Benčik R., Graovac S., "Računarska podrška trenažera za obuku mašinovođa", *JUŽEL94*, Vrnjačka Banja, Oktobar 1994.

36. Savić S., Tomašević M., Milutinović V., "Simulacija i implementacija jednog koncepta distribuirane deljene memorije", *XXXVIII Konferencija ETAN-a*, Niš, Jun 1994.

37. Grujić A., Tomašević M., Milutinović V., "Simulaciona analiza tri DSM pristupa", *XXXVIII Konferencija ETAN-a*, Niš, Jun 1994.

38. Tomašević M., Milutinović V., "Analitička evaluacija decentralizovanih protokola za koherenciju keš memorija", *XXXVII Konferencija ETAN-a*, Beograd, Jun 1993.

39. Tomašević M., Gobović A., Milutinović V., "Simulator multiprocesorskog sistema sa zajedničkom memorijom i zajedničkom magistralom", *XXXVI Konferencija ETAN-a*, Kopaonik, Jun 1992.

40. Tomašević M., Milutinović V., "Dvonivoska hijerarhija keš memorija u multiprocesorskim sistemima sa zajedničkom memorijom i zajedničkom magistralom", *XXXV Konferencija ETAN-a*, Ohrid, Jun 1991.

41. Tomašević M., Džigurski O., Petronijević D., "Simulacija grafičkog prikazivanja podataka u avionskim računarskim sistemima", *XXXIV Konferencija ETAN-a*, Zagreb, Jun 1990.

42. Tomašević M., Džigurski O., Vojvodić I., Petronijević D., "Distribuirani računarski sistem za simulaciju dinamičkih sistema u realnom vremenu", *XXXIII Konferencija ETAN-a*, Novi Sad, Jun 1989.

43. Tomašević M., Đorđević J., Potić V., "Razmatranje arhitekture procesora multiprocesne obrade", *XXX Konferencija ETAN-a*, Herceg Novi, Jun 1986.

44. Đorđević J., Potić V., Ranđić S., Tomašević M., Bojović M., "Analiza preklapanja mikroinstrukcija procesora multiprocesne obrade", *XXVIII Konferencija ETAN-a*, Split, Jun 1984.

45. Bojović M., Đorđević J., Tomašević M., Potić V., Ranđić S., "Komandni jezik za upravljanje procesorom multiprocesne obrade", *XXVIII Konferencija ETAN-a*, Split, Jun 1984.

46. Đorđević J., Tomašević M., "Simulator procesora multiprocesne obrade", *XXVIII Konferencija ETAN-a*, Struga, Jun 1983.

47. Đorđević J., Ranđić S., Tomašević M., "Mikroasembler procesora multiprocesne obrade", *XXVII Konferencija ETAN-a*, Subotica, Jun 1982.

48. Potić V., Đorđević J., Lazić B., Velašević D., Ranđić S., Tomašević M. "Arhitektura i organizacija procesora multiprocesne obrade", *XXVII Konferencija ETAN-a*, Subotica, Jun 1982.

Milo Tomašević je rođen je 1957. godine u Nikšiću, Crna Gora. Osnovnu školu i gimnaziju završio je u Nikšiću sa diplomom "Luča". Tokom školovanja osvajao je prva mesta na gradskim, republičkim i saveznim (SFRJ) takmičenjima iz matematike, istorije i geografije. Na Elektrotehnički fakultet u Beogradu upisao se 1975. godine i diplomirao 1980. godine kao jedan od najboljih studenata na Smeru za elektroniku. Magistarski rad odbranio je 1984. godine, a doktorsku disertaciju 1992. godine, takođe na Elektrotehničkom fakultetu u Beogradu. Nakon diplomiranja radio je u Institutu Mihajlo Pupin napredujući sve do kategorije savetnika. 1993. godine je postao honorarni docent Elektrotehničkog fakulteta Univerziteta u Beogradu da bi od 1995. potpuno prešao na na Katedru za računarsku tehniku i informatiku Elektrotehničkog fakulteta gde i danas radi kao redovni profesor. Bio je i gostujući istraživač 1990-91. godine na univerzitetu Purdue, West Lafayette, SAD. Na Elektrotehničkom fakultetu je zasnovao I predaje više predmeta iz programiranje, algoritama i multiprocesorskih sistema na sva tri nivoa studija. Predavao je i na više srodnih fakulteta u regionu u periodu od preko dve decenije (državni univerziteti u Podgorici, Banjaluci, Istočnom Sarajevu). Objavio je preko 140 radova u prestižnim međunarodnim i domaćim časopisima i konferencijama, a za neke od njih je dobio nagrade. Odziv na radove iznosi preko 1450 citata (GS, H-index 16). Bio je učesnik više desetina domaćih i međunarodnih projekata koji su kao rezultat imali i inovativne realizacije hardversko-softverskih proizvoda i studije. Bio je recenzent za više renomiranih međunarodnih časopisa, kao i član programskih odbora domaćih i međunarodnih konferencija i časopisa. Održao je, sa koautorima, više predavanja po pozivu kod nas i u inostranstvu (SAD, Nemačka, Italija, Singapur, Južna Koreja, Poljska, Bugarska) i u raznim kompanijama (Encore, NCR, TDT), na univerzitetima i prestižnim međunarodnim konferencijama iz arhitekture računara (ISCA, HPCA, HPC). Koautor je dve knjige iz multiprocesorskih sistema u izdanju IEEE Computer Society Press. Glavne oblasti istraživačkog interesovanja su arhitektura i organizacija računara, paralelni sistemi, algoritmi i strukture podataka, kriptografija, itd. Dobitnik je nagrade "Kapetan Miša Anastasijević". U periodu 2015-17. godine bio je prodekan za saradnju sa privredom, a u periodu 2017-21. godine obavljao je funkciju dekana Elektrotehničkog fakulteta. Oženjen je i otac dvoje dece, Vesne i Vojislava.

Milo Tomašević was born in 1957, Nikšić, Montenegro, where he completed his elementary and high-school education with "Luča" diploma. He held first awards in the state competitions in mathematics, history, and geography. He enrolled in the School of Electrical Engineering, University of Belgrade (UB SEE) in 1975. where he graduated in 1980 as one of the best students in the Department of Electronics. He obtained his MSc degree in 1984. and PhD diploma in 1992. from UB SEE, both in computer engineering. After graduation, he was employed at Mihajlo Pupin Institute, Belgrade, from 1980. to 1995. In 1993. he entered the UB SEE as a part-time assistant professor. In 1995 he became a full-time member of UB SEE where he currently works at the Department of Computer Engineering as a full professor. In the period 1990-91. he was a visiting researcher at Purdue University, West Lafayette, USA. At UB SEE he founded and lectured several courses in programming, algorithms and data structures, and multiprocessor systems at all three levels of studies. For a period of more than two decades, he was a visiting professor at several universities in the region (state universities in Podgorica, Banjaluka and East Sarajevo). He published more than

120 scientific papers in prestigious international and national journals and conferences and obtained awards for some of them. His work is cited more than 1450 times (GS, H-index 16). He participated in more than 30 national and international projects that resulted in innovative software/hardware realizations. He was a reviewer for several renowned international journals and served as a member of the program board of some national and international conferences. He delivered invited talks and tutorials abroad (USA, Germany, Italy, Singapore, South Korea, Poland, Bulgaria) in companies (Encore, NCR, TDT), universities, and conferences (ISCA, HPCA, HPC). He is a co-author of two books published by IEEE Computer Society Press. His main research interests are computer architecture and organization, parallel systems, algorithms and data structures, cryptanalysis, etc. He is the recipient of *Kapetan Miša Anastasijević* award. In the period 2015-17. he was Vice-dean for cooperation with companies, whereas in the period 2017-21. he was Dean of UB SEE. He is married and the father of Vesna and Vojislav.

Univerzitet Crne Gore
adresa / address_Cetinjska br. 2
81000 Podgorica, Crna Gora
telefon / phone_00382 20 414 255
fax_00382 20 414 230
mail_rektorat@ucg.ac.me
web_www.ucg.ac.me
University of Montenegro

Broj / Ref 03 - 1442
Datum / Date 20.07 20 22

Na osnovu člana 72 stav 2 Zakona o visokom obrazovanju („Službeni list Crne Gore", br. 44/14, 47/15, 40/16, 42/17, 71/17, 55/18, 3/19, 17/19, 47/19, 72/19 i 74/20 i 104/21) i člana 32 stav 1 tačka 9 Statuta Univerziteta Crne Gore, Senat Univerziteta Crne Gore, na sjednici održanoj 20.07.2022. godine, donio je

O D L U K U
O IZBORU U ZVANJE

Dr SAVO TOMOVIĆ bira se u akademsko zvanje **redovni profesor Univerziteta Crne Gore za oblast Računarske nauke, na Prirodno-matematičkom fakultetu Univerziteta Crne Gore**, na neodređeno vrijeme.

SENAT UNIVERZITETA CRNE GORE
PREDSJEDNIK

Prof. dr Vladimir Božović, rektor

doc. dr Savo Tomović

Rođen je u Podgorici 29. 09. 1983. godine. Prirodno-matematički fakultet Univerziteta Crne Gore, Odsjek za matematiku i računarske nauke, smjer računarske nauke upisao je 2002. godine a završio u julu 2006. godine sa prosječnom ocjenom 9,81.

Završio je 2007. godine postdiplomske studije na Prirodno-matematičkom fakultetu Univerziteta Crne Gore, studijski program Računarske nauke, sa prosječnom ocjenom 10,00 i odbranio magistarsku tezu pod nazivom *Data mining tehnike za asocijativna pravila u relacionim bazama podataka*.

Godine 2008. upisao je doktorske studije na Prirodno-matematičkom fakultetu Univerziteta Crne Gore, studijski program Računarske nauke. U redovnim rokovima položio je sve ispite sa ocjenom A i prijavio doktorsku disertaciju pod nazivom *Algoritmi i strukture podataka za identifikovanje asocijativnih pravila u velikim bazama podataka*. Pomenutu doktorsku disertaciju, uspješno je odbranio 22. X 2011. godine i stekao akademski stepen doktora računarskih nauka.

U toku studija bio je dobitnik više nagrada od kojih su najznačajnije: Plaketa Univerziteta Crne Gore za oblast tehničkih nauka za 2006. godinu, Studentska nagrada 19. decembar Skupštine opštine Podgorica za 2005. godinu, Stipendija za talentovane studente Ministarstva prosvjete i nauke za 2003/2004, 2004/2005 i 2005/2006 godinu.

Honorarno je angažovan 2006. godine a od 2007. i zaposlen kao saradnik u nastavi na Prirodno-matematičkom fakultetu Univerziteta Crne Gore. Izvodio je vježbe iz predmeta Operativni sistemi, Programski prevodioci, Vještačka inteligencija i Analitička obrada podataka (data mining) na Prirodno-matematičkom fakultetu, kao i iz informatičkih predmeta na Medicinskom i Građevinskom fakultetu.

U maju 2012. godine izabran je u zvanje docenta za predmete **Principi programiranja** na studijskom programu Računarske nauke, **Analitička obrada podataka - Data Mining** na specijalističkom studijskom programu Računarske nauke na Prirodno-matematičkom fakultetu, **Primjena računara** na studijskom programu Građevinarstvo na Građevinskom fakultetu i **Medicinska informatika** na studijskom programu Stomatologija na Medicinskom fakultetu.

Odlukom Ministarstva nauke Crne Gore proglašen je za najuspješnijeg mladog naučnika do 35 godina života za 2012. godinu.

Od decembra 2013. godine rukovodilac je studijskih programa Računarske nauke i Računarstvo i informacione tehnologije na Prirodno-matematičkom fakultetu.

Izabrane publikacije:

1. Predrag Stanišić, Savo Tomović, "A New Rymon Tree Based Procedure for Mining Statistically Significant Frequent Itemsets", International Journal of Computers Communications & Control, Vol. 5(4), pp. 567-577, 2010 [SCI Expanded]

2. Predrag Stanišić, Savo Tomović, "Apriori Multiple Algorithm for Mining Association Rules", Information Technology and Control, Vol. 37, No. 4, 2008 [SCI Expanded]

3. Predrag Stanišić, Savo Tomović, *Hypothesys Testing Aproach in Mining Statistically Significant Frequent Itemsets*, Mathematica Montisnigri, 2012 [Zentralblatt Math, AMS]

4. Predrag Stanišić, Savo Tomović, "An Efficient Procedure for Mining Statistically Significant Frequent Itemsets", Publications de l'Institut Mathematique, Nouvelle Serie, Vol. 87 (101), 2010 [Zentrallblatt Math, AMS]

5. Predrag Stanišić, Savo Tomović, *An Improvement of Data Mining Apriori Technique*, Mathematica Montisnigri, Vol. 20-21, 2008 [Zentralblatt Math, AMS]

6. Predrag Stanišić, Savo Tomovic, Upper Bounds on the Number of Candidate Itemsets in Apriori Like Algorithms, Proccedings of the 3nd Mediterranean Conference on Embedded Computing , 2014 [IEEE Xplore, digital library]

7. Predrag Stanišić, Savo Tomovic, *Frequent Itemset Mining as Set Interection Problem*, Proccedings of the 2nd Mediterranean Conference on Embedded Computing , 2013 [IEEE Xplore, digital library]

8. Predrag Stanišić, Savo Tomovic, *Frequent Itemset Mining using Two-Fold Cross Validation Model*, Proccedings of the 1st Mediterranean Conference on Embedded Computing , 2012 [IEEE Xplore, digital library]

9. Savo Tomović, Predrag Stanišić, *Cross Validation Method in Frequent Itemset Mining*, Proccedings of the Central European Conference on Information and Intelligent Systems, 2011

10. Savo Tomović, Predrag Stanišić, *Mining the Most k-Frequent Itemsets with TS-trie*, Proccedings of the IADIS International Conference WWW/Internet 2009, 2009 [DBLP, AMS]

УНИВЕРЗИТЕТ У БЕОГРАДУ

Адреса: Студентски трг 1, 11000 Београд, Република Србија
Тел.: 011 3207400; Факс: 011 2638818; E-mail: kabinet@rect.bg.ac.rs

ВЕЋЕ НАУЧНИХ ОБЛАСТИ
ТЕХНИЧКИХ НАУКА

Београд, 17. јун 2024. год
02 број: 61202-2137/2-24
сћ

На основу члана 75 Закона о високом образовању („Службени гласник РС“, бр. 88/17, 73/18, 67/19 и 67/21), члана 48 став 5 тачка 1 Статута Универзитета у Београду („Гласник Универзитета у Београду”, бр. 201/18, 207/19, 213/20, 214/20, 217/20, 230/21, 232/22, 233/22, 236/22, 241/22, 243/22, 244/23, 245/23, 247/23 и 251/23), члана 13 став 1 Правилника о већима научних области на Универзитету у Београду („Гласник Универзитета у Београду”, бр. 134/07, 150/09, 158/11, 164/11, 165/11, 180/14, 195/16, 197/17, 208/19, 215/20, 239/22 и 245/23), члана 23 став 1 тачка 1 Правилника о начину и поступку стицања звања и заснивања радног односа наставника Универзитета у Београду („Гласник Универзитета у Београду”, бр. 237/22, 240/22 и 242/22) и Правилника о минималним условима за стицање звања наставника на Универзитету у Београду („Гласник Универзитета у Београду“, бр. 192/16, 195/16, 197/17, 199/17, 203/18 и 223/21), а на предлог Изборног већа Електротехничког факултета, број: 920/3 од 14. маја 2024. год. Веће научних области техничких наука, на седници одржаној 17. јуна 2024. године, донело је

О Д Л У К У

БИРА СЕ **др Маја Вукасовић**, у звање доцента на Универзитету у Београду – Електротехнички факултет, за ужу научну област Рачунарска техника и информатика.

О б р а з л о ж е њ е

Универзитет у Београду – Електротехнички факултет („Факултет“) је дана 6. марта 2024. године, у листу „Послови“, објавио конкурс за избор у звање доцента са пуним радним временом, за ужу научну област Рачунарска техника и информатика, због потребе Факултета.

Реферат Комисије за припрему реферата о пријављеним кандидатима стављен је на увид јавности дана 4. априла 2024. године на интернет страни Факултета.

На основу предлога Комисије за припрему реферата о пријављеним кандидатима, Изборно веће Факултета, на седници одржаној 14. маја 2024. године, донело је одлуку о утврђивању предлога да се кандидат др Маја Вукасовић изабере у звање доцента.

Факултет је дана 5. јуна 2024. године доставио Универзитету комплетан захтев за избор у звање на прописаним обрасцима.

Универзитет је комплетну документацију коју је доставио Факултет ставио на web страницу Универзитета, дана 10. јуна 2024. године.

Веће научних области техничких наука, на седници одржаној 17. јуна 2024. године, разматрало је захтев Факултета и утврдило да кандидат испуњава услове прописане чл. 74 и 75 Закона о високом образовању и чланом 135 Статута Универзитета у Београду, као и услове прописане Правилником о минималним условима за стицање звања наставника на Универзитету у Београду, па је донета Одлука као у изреци.

Поука о правном средству:

Против ове Одлуке кандидат пријављен на конкурс може изјавити жалбу Сенату Универзитета, преко Већа научних области техничких наука. Жалба се доставља Већу научних области у року од 8 дана од дана достављања Одлуке.

ПРЕДСЕДНИК ВЕЋА

проф. др Горан Марковић

Доставити:
- Факултету (2),
- Архиви Универзитета (1)

Биографија Маје Вукасовић

Маја Вукасовић је рођена 25.05.1993. године у Београду. Основну школу завршила је у Београду, као ђак генерације и носилац дипломе „Вук Караџић". Након тога завршава Девету гимназију „Михаило Петровић Алас", такође у Београду као носилац дипломе „Вук Караџић". Током школовања, освајала је награде на градским и републичким такмичењима из математике, физике, српског и енглеског језика.

На Електротехнички факултет у Београду уписала се 2012. године на Одсеку за софтверско инжењерство. Дипломирала је 2016. године са просечном оценом 9.98. Дипломски рад под називом „Напредни генератор програмског кода за машине стања на језику UML" одбранила је са оценом 10. Након основних студија уписала је мастер академске студије на Електротехнички факултет у Београду 2016. године. Мастер рад под називом „Симулатор векторског процесора са предикатским извршавањем у више трака" одбранила је 2017. године са оценом 10. Просечна оцена након завршених мастер академских студија је 10.00.

Докторске студије уписала је 2017. године на Електротехничком факултету у Београду на модулу Софтверско инжењерство. Положила је све испите са оценом 10 и остварила 120 ЕСПБ. У истраживачком раду усмерила се ка програмским преводиоцима, са посебним нагласком на оптимизације током превођења програма. Докторску дисертацију под насловом „Побољшање перформанси програма употребом делимично контекстно осетљивих профила" одбранила је 16.01.2024. године.

Објавила је један рад у часопису са SCI листе, 12 радова на страним и домаћим конференцијама као и један рад у домаћем часопису. Учествовала је на међународном пројекту ISSES, четири пројекта Министарства просвете, науке и технолошког развоја, као и пројекту Иновационог фонда „CoCos.ai".

Током студија радила је на праксама у фирмама „SOL" и „Kudos" и била укључена на неколико пројеката компаније „Nordeus". Школске 2013/2014. године прикључила се демонстраторском тиму на Катедри за рачунарску технику и информатику, а нешто касније и на Катедри за примењену математику. На Катедри за рачунарску технику и информатику је запослена од 2016. године, најпре као сарадник у настави, потом као асистент, а од 2024. године као доцент. Трепутно је ангажована на седам предмета који се изводе на студијским програмима Софтверско инжењерство и Рачунарска техника и информатика на основним и мастер академским студијама. Као асистент на Електротехничком факултету била је ангажована на 12 предмета. Учествовала је у изради и спровођењу заједничког студијског програма „Мастер 4.0" са Факултетом организационих наука. Рецензирала је радове на конференцијама ТЕЛФОР и ЕТРАН. Од 2018. године ангажована је као истраживач и сениор програмер у компанији „Oracle Labs". Коаутор је за три наставна материјала из области заштите података.

Библиографија научних и стручних радова

1. Радови у међународним научним часописима са импакт фактором (категорија М20)

1.1. **Maja Vukasovic**, Aleksandar Prokopec, *Exploiting Partially Context-Sensitive Profiles to Improve Performance of Hot Code*, ACM TRANSACTIONS ON PROGRAMMING LANGUAGES AND SYSTEMS, Vol. 45, No. 4, pp. 1-64, Dec 2023, https://doi.org/10.1145/3612937 ISSN 0164-0925, M23

1.2. D. Miladinović, A. Milaković, M. Vukasović, Ž. Stanisavljević, P. Vuletić, **Secure Multiparty Computation Using Secure Virtual Machines**, Electronics , Vol. 13, No. 5, pp. 1-25, 2024. doi:10.3390/electronics13050991, M22

2. Радови на међународним научно-стручним конференцијама (категорија М30)

2.1. Stanisavljević Ž., Walter B., **Vukasović M.**, Todosijevic A., Labedzki M., Wolski M., *GÉANT Software Maturity Model*, TELFOR 2018, Belgrade, Electronic ISBN 978-1-5090-0054-8, pp. 691-694, Nov 2018, DOI: 10.1109/TELFOR.2018.8611887, M33

2.2. **M. Vukasović**, D. Miladinović, A. Milaković, P. Vuletić, Ž. Stanisavljević, *Programming Applications Suitable for Secure Multiparty Computation Based on Trusted Execution Environments*, TELFOR 2022, pp. 1-4, IEEE, Belgrade, Nov, 2022., M33

2.3. P. Đekanović, **M. Vukasović**, D. Bojić, *Model for Evaluating Points-to Analysis in GraalVM Native Image Using Instrumentation-Based Profiling*, Disruptive Information Technologies for a Smart Society. ICIST 2023. Lecture Notes in Networks and Systems, vol 872, pp. 502-512, Springer, Cham, Feb, 2024., M33

2.4. M. Dodović, **M. Vukasović**, D. Drašković, *Comparison of Deep Learning Algorithms for Facial Keypoints Detection*, Disruptive Information Technologies for a Smart Society. ICIST 2023. Lecture Notes in Networks and Systems, vol 872., pp. 117-125, Springer, Cham, Feb, 2024., M33

3. Радови у часописима ван SCI листе (категорија 50)

3.1. **Vukasović M.**, Veselinović B., Stanisavljević Ž., *Design and Implementation of a Configurable System for Managing X509 Certificates*, TELFOR JOURNAL, ISSN 1821-3251, Vol. 10, No. 2, pp. 102-107, Dec 2018, https://doi.org/10.5937/telfor1802102V, M52

4. Радови на домаћим научно-стручним конференцијама (категорија 60)

4.1. Ј. Китановић, Д. Драшковић, **М. Вукасовић**, С. Делчев, *Развој алата за проверу и корекцију текста заснован на графовима и стаблима претраживања*, Зборник радова конференције ЕТРАН 2023, pp. 1-6, Друштво за електронику, телекомуникације, рачунарство, аутоматику и нуклеарну технику - ЕТРАН, Источно Сарајево, Босна и Херцеговина, Jun, 2023., M63

4.2. Т. Шекуларац, Ф. Хаџић, С. Тубић, **М. Вукасовић**, *Софтвер за учење и тестирање SQL језика*, Зборник радова 28. научне конференције "YU INFO 2022", Информационо друштво Србије, Копаоник, Србија, Mar, 2022., M63

4.3. Б. Кнежевић, **М. Вукасовић**, Д. Драшковић, *Решавање проблема проналажења потпуног подграфа*, Зборник радова 27. конференције "YU INFO 2021", pp. 42-47, Информационо друштво Србије, Копаоник, Србија, Mar, 2021., M63

4.4. Д. Драшковић, Ј. Цинцовић, Д. Мијаиловић, **М. Вукасовић**, В. Јоцовић, А. Милаковић, *Предвиђање успеха студената студијског програма Софтверско инжењерство техникама машинског учења*, Зборник радова конференције "ЈУ ИНФО 2020", Информационо друштво Србије, Копаоник, Србија, март 2020, M63

4.5. Вукасовић, М., Веселиновић, Б., Станисављевић, Ж., *Развој конфигурабилног система за рад са X509 сертификатима*, ТЕЛФОР 2017, pp. 876-879, Belgrade, Nov, 2017., M63

4.6. S. Delčev, **M. Vukasović**, D. Drašković, D. Radojević, M. Janković, M. Bajec, B. Nikolić, *Testing artificial intelligence knowledge with interactive web system*, 24th Telecommunications Forum "TELFOR 2016", IEEE Serbia & Montenegro, Београд, Србија, Nov, 2016., DOI: 10.1109/TELFOR.2016.7818922, M63

4.7. **М. Вукасовић**, М. Мићовић, У. Раденковић, В. Јоцовић, Д. Драшковић, *Примена виртуелне стварности у оквиру медицинских третмана*, 23. конференција "ЈУ ИНФО 2017", pp. 105-110, Информационо друштво Србије, Копаоник, Србија, Mar, 2017., ISBN: 978-86-85525-20-9, M63

4.8. D. Drašković, M. Mićović, U. Radenković, **M. Vukasović**, S. Delčev, V. Jocović, Ž. Šuštran, B. Nikolić, *Реализација веб система за управљање и надгледање софтверских пројеката*, 23. конференција "ЈУ ИНФО 2017", pp. 99-104, Информационо друштво Србије, Копаоник, Србија, Mar, 2017., ISBN: 978-86-85525-20-9, M63

Univerzitet Crne Gore
adresa / address_Cetinjska br. 2
81000 Podgorica, Crna Gora
telefon / phone_00382 20 414 255
fax_00382 20 414 230
mail_rektorat@ucg.ac.me
web_www.ucg.ac.me
University of Montenegro

Broj / Ref 03-9303
Datum / Date 24.12.2019.

Na osnovu člana 72 stav 2 Zakona o visokom obrazovanju („Službeni list Crne Gore" br 44/14, 47/15, 40/16, 42/17, 71/17, 55/18, 3/19, 17/19, 47/19) i člana 32 stav 1 tačka 9 Statuta Univerziteta Crne Gore, Senat Univerziteta Crne Gore na sjednici održanoj 24.12.2019. godine, donio je

O D L U K U
O IZBORU U ZVANJE

Dr Aleksandar Popović bira se u akademsko zvanje vanredni profesor Univerziteta Crne Gore za **oblast Računarstvo,** na Prirodno-matematičkom fakultetu Univerziteta Crne Gore, na period od pet godina.

SENAT UNIVERZITETA CRNE GORE
PREDSJEDNIK

Prof. dr Danilo Nikolić, rektor

Doc. Dr Aleksandar Popović, dipl. mat

BIBLIOGRAFIJA NAUČNIH I STRUČNIH RADOVA

ODBRANJENA MAGISTARSKA TEZA:

1. Popović A., *Specifikacija vizuelnih atributa i struktura poslovnih aplikacija u alatu IIS*Case*, Magistarski rad, Univerzitet u Novom Sadu, Fakultet tehničkih nauka, 2008. Mentor: Prof. Dr Ivan Luković

SPISAK RADOVA:

Radovi objavljeni na konferencijama

1. Stamatović B., Šuković G., Popović A., Bogojević P., Sekulić R., Mostić J., *Frequent Flyer program Montenegro Airlines-a*, XIII naučno-stručna konferencija Industrijski sistemi IS 2005, Herceg Novi, Srbija i Crna Gora, 07-09. 09. 2005, Zbornik radova, Univerzitet u Novom Sadu, Fakultet tehničkih nauka, ISBN: 86-7780-008-5, pp. 369-373.
2. Stamatović B., Šuković G., Popović A., Bogojević P., Sekulić R., Mostić J., *Frequent Flyer program Montenegro Airlines-a*, X naučno-stručni skup - Informacione tehnologije - IT'05, Žabljak, Srbija i Crna Gora, 27.02 - 4.03. 2005, Zbornik radova.
3. Ristić S., Luković I., Aleksić S., Popović A., *An Approach to Building Platform Independent Models*, XIV International Scientific Conference on Industrial Systems IS '08, Novi Sad, Serbia, October 2 – 3, 2008, ISBN 978-86-7892-135-3, Proceedings pp. 201 – 206.
4. Luković I., Ristić S., Aleksić S., Popović A., *An Application of the MDSE Principles in IIS*Case*, III Workshop on Model Driven Software Engineering (MDSE 2008), Berlin, Germany, December 11-12, 2008, Proceedings.
5. Luković I., Popović A., Mostić J., Ristić S., *A Tool for Modeling Form Type Check Constraints*, International Multiconference on Computer Science and Information Technology (IMCSIT), 2nd Workshop on Advances in Programming Languages (WAPL'09), October 12-14, 2009, Mragowo, Poland, Proceedings, Polish Information Processing Society, Poland, ISSN 1896-7094, Vol. 4, pp. 681-688.
6. Đukić V., Luković I., Popović A., *Domain-Specific Modeling in Document Engineering*, Federated Conference on Computer Science and Information Systems (FedCSIS), 3rd Workshop on Advances in Programming Languages (WAPL'11), September 18–21, 2011, Szczecin, Poland, Proceedings, IEEE Computer Society Press, 10662 Los Vaqueros Circle, Los Alamitos, CA 90720, USA, ISBN 978-83-60810-22-4, pp. 817–824.
7. Đukić V., Luković I., Popović A., Ivančević V., *Using Action Reports for Testing Meta-models, Models, Generators and Target Interpreter in Domain-Specific Modeling*, Federated Conference on Computer Science and Information Systems (FedCSIS), 2nd Workshop on Model Driven Approaches in System Development, September 9–12, 2012, Wroclaw, Poland, Proceedings, IEEE Computer Society Press, 10662 Los Vaqueros Circle, Los Alamitos, CA 90720, USA, ISBN 978-83-60810-51-4, pp. 1365–1372.
8. Luković I., Ristić S., Popović A., Mogin P., *An Approach to Platform Independent Specification of a Business Application*, 23rd Central European Conference on Information and Intelligent Systems CECIIS 2012, September 19-21, 2012, Varaždin, Croatia, Proceedings, University of Zagreb, Faculty of Organization and Informatics, ISSN 1847-2001 (Print) ISSN 1848-2295 (Online), pp. 449-456.
9. Đukić V., Luković I., Popović A., Ivančević V., *Domain-Specific Modeling Tools as Client Applications Providing the Production of Documents*, Second Workshop on Industrial Track of Software Language Engineering, September 25, 2012, Dresden, Germany, CEUR Workshop Proceedings, IEEE Computer Society Press, 10662 Los Vaqueros Circle, Los Alamitos, CA 90720, USA, ISSN 1613-0073, pp. 3–14.

10. Tolvanen J.P., Djukic V., Popović A., *Metamodeling for Medical Devices: Code Generation, Model-debugging and Run-time Synchronization*, Procedia Computer Science, Elsevier, DOI: 10.1016/j.procs.2015.08.382, ISSN: 1877-0509, Vol. 63, 2015, pp. 539-544.
11. Djukić V., Popović A., Tolvanen J.P., *Domain-Specific Modeling for Robotics – from language construction to ready-made controllers and end-user applications*, MORSE '16 Proceedings of the 3rd Workshop on Model-Driven Robot Software Engineering, ACM Digital Libraries, New York, NY, USA, ISBN: 978-1-4503-4259-9 DOI: 10.1145/3022099.3022106, Leipzig, Germany, July 1, 2016, pp. 47-54.
12. Djukić V., Popović A., Lu Z., *Run-time Code Generators for Model-level Debugging in Domain-specific Modeling*, Proceedings of the International Workshop on Domain-Specific Modeling (DSM 2016), ACM Digital Libraries, New York, NY, USA, ISBN: 978-1-4503-4894-2 DOI: 10.1145/3023147.3023148, Amsterdam, Netherlands, October, 2016, pp. 1-7

Radovi objavljeni u časopisima

1. Popović A., Luković I., Ristić S., *A Specification of the Structures of Business Applications in the IIS*Case Tool*, Info M – Journal of Information Technology and Multimedia Systems, Belgrade, Serbia, ISSN: 1451-4397, No. 25, 2008, pp. 17-24.
2. Luković I., Popović A, Mostić J., Ristić S., *A Tool for Modeling Form Type Check Constraints and Complex Functionalities of Business Applications*, Computer Science and Information Systems (ComSIS), Consortium of Faculties of Serbia and Montenegro, Belgrade, Serbia and Montenegro, ISSN: 1820-0214, Vol. 7, No. 2, 2010, pp. 359-385.
3. Luković I., Ristić S., Aleksić S., Banović J., Popović A., *A Chain of Model Transformations in IIS*Case*, Scripta Scientiarum Naturalium, University of Montenegro, Faculty of Natural Sciences and Mathematics, Podgorica, Montenegro, ISSN: 1880-8356, Vol. 1, No. 1, 2010, pp. 59-76.
4. Obrenović N., Popović A., Aleksić S., Luković I., *Transformations of check constraint PIM specifications*, Computing and Informatics (CAI), Slovak Academy of Sciences, Institute of Informatics, Bratislava, Slovakia, ISSN 1335-9150, Vol. 31, No. 5, 2012, pp. 1045-1079.
5. Đukić V., Luković I., Popović A., Ivančević V., *Model Execution: An Approach based on extending Domain-Specific Modeling with Action Reports*, Computer Science and Information Systems (ComSIS), Consortium of Faculties of Serbia and Montenegro, Belgrade, Serbia, DOI: 10.2298/CSIS121228059D, ISSN: 1820-0214, Vol. 10, No. 4, 2013, pp. 1585-1620.
6. Popović A., Dimitrieski V., Luković I., Đukić V., *A DSL for modeling application-specific functionalities of business applications*, Computer Languages, Systems & Structures (COMLAN), Elsevier Science Publishers B. V., DOI: 10.1016/j.cl.2015.03.003, 2015.
7. Djukić V., Popović A., *Handling complex representations in visual modeling tools for MDSD/DSM by means of code generator languages*, Journal of Computer Languages, Elsevier Science Publishers, Volume 75, 2023, ISSN 2590-1184, https://doi.org/10.1016/j.cola.2023.101208.
8. Popović A., Ivković V., Trajković N., Luković I., *A domain-specific language for managing ETL processes*, PeerJ Computer Science, https://doi.org/10.7717/peerj-cs.
9.

PROJEKTI:

1. "Frequent Flyer – informacioni sistem za praćenje učestalosti avionskih letova i putnika na tim letovima", "Montenegro Airlines d.o.o", Univerzitet Crne Gore, Prirodno-matematički fakultet, Podgorica, Crna Gora, 2004-2005, saradnik na projektu, programer
2. "DVDocParser - softverski paket za evaluaciju, parsiranje i leksičku analizu programskih sktruktura specijalizovanog jezika DVDocLang", "Djukić softver solušns", Nirnberg, 2005-2006, spoljni saradnik, samostalni programer

3. "DVQL – prevodilac i interpreter za programe pisane u domenski specifičanom jeziku DVQueryLang", "Djukić softver solušns", Nirnberg, 2007-2008, spoljni saradnik, samostalni programer

4. "MEIS – Montenigrin education information system", Ministrarstvo prosvjete i nauke Republike Crne Gore, Prirodno-matematički fakultet, , Podgorica, Crna Gora, 2006, saradnik na projektu, programer

NASTAVA:

Izvođenje vježbi – redovna nastava

1. Programiranje I, Prirodno-matematički fakultet, Podgorica, 2 + 2, III semestar, 2006/07–2012/13
2. Programiranje II, Prirodno-matematički fakultet, Podgorica, 2 + 2, IV semestar, 2006/07–2012/13
3. Baze podataka, Prirodno-matematički fakultet, Podgorica, 3 + 3, V, 2006/07–2007/08
4. Napredne baze podataka, Prirodno-matematički fakultet, Podgorica, 3 + 3, VI, 2006/07–2007/08
5. Baze podataka, Prirodno-matematički fakultet, Podgorica, 3 + 2, V semestar, 2008/09-2012/13
6. Napredne baze podataka, Prirodno-matematički fakultet, Podgorica, 3 + 2, VI, 2008/09–2012/13
7. Softversko inženjerstvo, Prirodno-matematički fakultet, Podgorica, 3 + 2, VIII semestar, 2005/06–2008/09
8. Geografski informacioni sistemi, Prirodno-matematički fakultet, Podgorica, 3 + 1, VII semestar, 2010/11-2012/13

KURSEVI I SEMINARI:

Autorski kursevi

1. Šuković G., Popović A., *Algoritmi i strukture podataka u programskom jeziku JAVA*, Ministrarstvo prosvjete i nauke Republike Crne Gore, Tivat, 2008

2. Šuković G., Popović A., *Ljetnja škola programiranja*, Prirodno-matematički fakultet, Ispitni centar Crne Gore, "doMEn d.o.o", Cetinje, 2009

3. Šuković G., Popović A., Tomović S., *Ljetnja škola programiranja*, Prirodno-matematički fakultet, Ispitni centar Crne Gore, "doMEn d.o.o", Kolašin, 2010

4. Šuković G., Popović A., Tomović S., *Ljetnja škola programiranja*, Prirodno-matematički fakultet, Ispitni centar Crne Gore, "doMEn d.o.o", Nikšić, 2011

5. Šuković G., Popović A., Tomović S., *Ljetnja škola programiranja*, Prirodno-matematički fakultet, "doMEn d.o.o", Cetinje, 2012

Prof. dr Aleksandar Popović, dipl. mat.,

BIOGRAFSKI PODACI

Aleksandar Popović rođen je Podgorici 28.06.1982. U Podgorici 2001. godine završio je Matematičku gimnaziju "Slobodan Škerović". Dobitnik je diplome "Luča". Iste godine upisuje se na Prirodno-matematički fakultet u Podgorici, odsjek za matematiku i računarske nauke, smjer računarske nauke. U toku studija dobitnik je više nagrada od kojih su najznačajnije: Studentska nagrada "19. decembar" koju dodjeljuje Skupština opštine Podgorica za 2003. godinu, "Stipendija za talentovane studente" koju dodjeljuje Ministarstvo prosvjete i nauke za 2002/2003 i 2003/2004 školsku godinu. Diplomirao je 2005. godine s prosječnom ocjenom u toku studija 9.90(9 i 90/100). Iste godine upisuje se na poslijediplomske studije na Fakultetu tehničkih nauka, odsjek računarstvo i automatika, smjer računarske nauke. Sve ispite predviđene planom i programom položio je s prosječnom ocenom 10. U Novom Sadu 2008. godine uspješno je odbranio magistarsku tezu pod nazivom "Specifikacija vizuelnih atributa i struktura poslovnih aplikacija u alatu IIS*Case". Ista godine upisuje doktorke studije na Prirodno-matematičkom fakultetu u Podgorici, smjer računarske nauke. Uspješno je odbranio polazna istraživanja i prijavio doktorsku tezu pod nazivom "Jedan pristup specificiranju izvršnih modela aplikacija informacionog sistema". Pomenutu doktorsku tezu uspješno je odbranio 07.09.2013. godine i stekao akademski stepen doktora računarskih nauka.

Od 2006. godine radio je kao saradnik u nastavi na Prirodno-matematičkom fakultetu u Podgorici gdje učestvuje u nastavi, pripremi i izvođenju vježbi iz većeg broja predmeta. Za docenta je izabran 2014. godine za predmete Objektno-orijentisano programiranje, Uvod u informacione sisteme, Geografski informacioni sistemi i Matematički softverski paketi. U zvanje vanrednog profesora izabran je 2019. godine.

Aleksandar Popović je rezultate svog naučno-istraživačkog rada publikovao u većem broju međunarodnih časopisa koji se nalaze u referentnim bazama podataka. Pored toga, izlagao je rezultate istraživanja na međunarodnim konferencijama, gdje su njegovi radovi štampani u cjelini u zbornicima.

Učestvovao je u realizaciji značajnog broja projekata u kojima su u državnu upravu i privredu prenešena znanja iz raznih disciplina računarskih nauka: baza podataka, programiranja, operativnih sistema, informacionih sistema, i internet tehnologija.