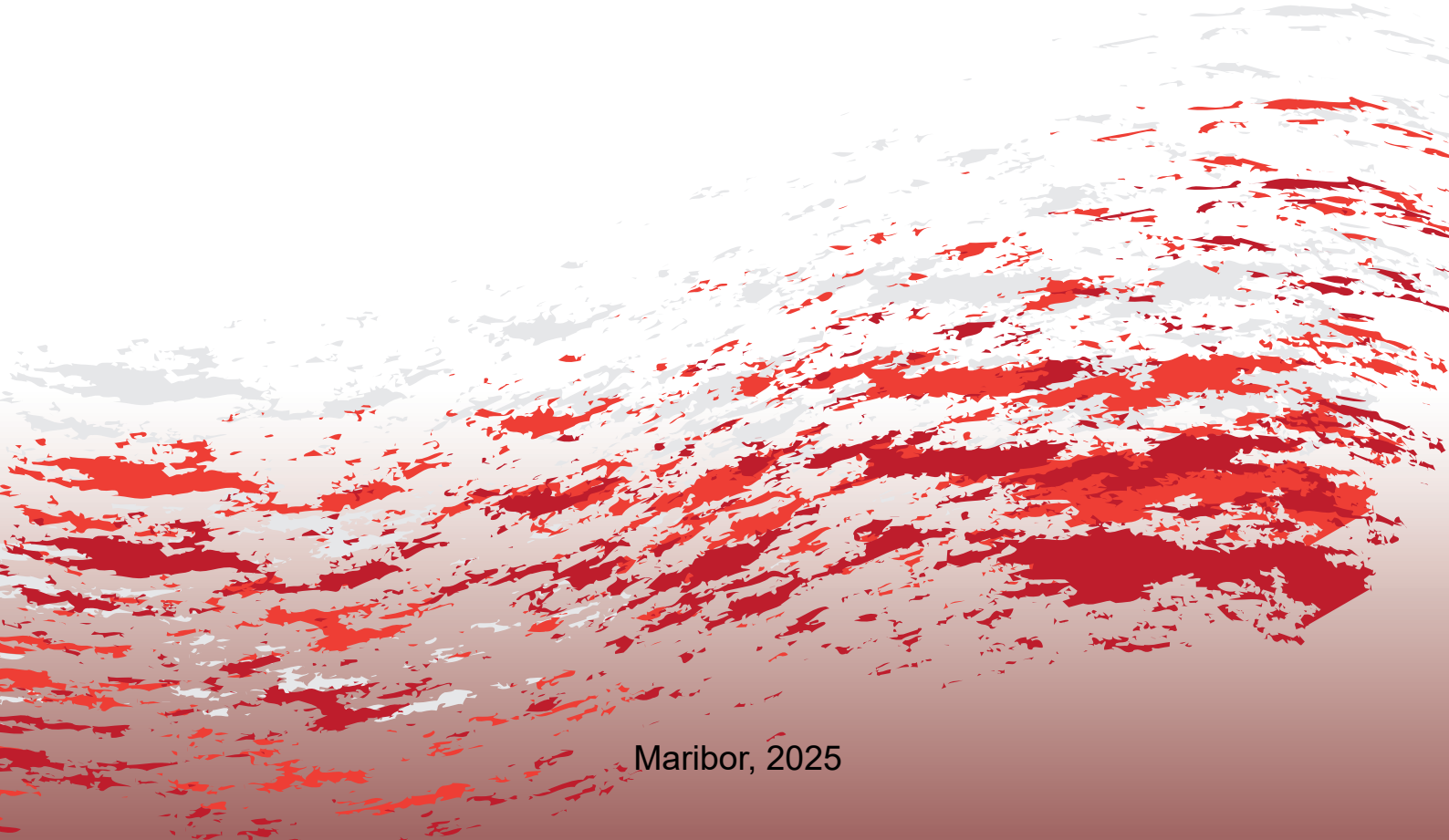
PAM Pokrajinski arhiv Maribor

# Moderna arhivistika

Časopis arhivske teorije in prakse
Journal of Archival Theory and Practice

Letnik 8 (2025), št. 1 / Year 8 (2025), No. 1



Maribor, 2025

**Moderna arhivistika**
*Časopis arhivske teorije in prakse*
*Journal of Archival Theory and Practice*

ISSN 2591-0884 (online)
DOI: https://doi.org/10.54356/MA

Letnik 8 (2025), št. 1 / Year 8 (2025), No. 1
DOI: https://doi.org/10.54356/MA/2025/1

Izdaja / Published by:
*Pokrajinski arhiv Maribor / Regional Archives Maribor*



Recenziranje / Peer review process:
*Prispevki so recenzirani. Za objavo je potrebna pozitivna recenzija. Proces recenziranja je anonimen. / All articles for publication in the conference proceedings are peer-reviewed. A positive review is needed for publication. The review process is anonymous.*

Lektoriranje / Proof-reading:
*mag. Boštjan Zajšek, mag. Nina Gostenčnik*

Prevajanje:
*mag. Boštjan Zajšek (slovenščina), mag. Nina Gostenčnik (slovenščina, angleščina)*

Oblikovanje in prelom / Design and typesetting: *mag. Nina Gostenčnik*

*Prejeto / Received: 1. 4. 2025*

*1.04 Strokovni članek* *1.04 Professional article*

https://doi.org/10.54356/MA/2025/HAZD7569

# *CYBER SECURITY AND DATA PROTECTION*

**Saša ĐUKIĆ**
Head of the IT and Digitalization Department, Archives of the Republic of Srpska, Banja Luka, Bosnia and Herzegovina
djusasa@gmail.com

***Abstract:***

*In an era dominated by digital transformation, cybersecurity and data protection have become critical to safeguarding sensitive information and ensuring the integrity of online systems. Cybersecurity focuses on protecting networks, systems, and data from malicious attacks, including phishing, ransomware, and advanced persistent threats. Meanwhile, data protection emphasizes the ethical and legal handling of personal and corporate information, ensuring compliance with regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).*

*As cyber threats continue to evolve, organizations must adopt proactive security measures, such as Zero Trust Architecture (ZTA), artificial intelligence-driven threat detection, and encryption technologies. Additionally, privacy-enhancing technologies (PETs) and post-quantum cryptographic solutions are emerging as key tools in data security. To mitigate risks effectively, companies should implement multi-factor authentication (MFA), conduct regular risk assessments, train employees on security awareness, and establish comprehensive incident response plans.*

*This paper explores the significance of cybersecurity and data protection, the latest trends in security technologies, and best practices for mitigating cyber threats. By adopting a strategic approach to cybersecurity and compliance, organizations can enhance their resilience against cyber risks while fostering trust in the digital landscape.*

***Key words:***

*Cybersecurity, Data Protection, Digital Ecosystem, Cyber Threats, Data Breaches, Risk Assessment, Artificial Intelligence, Machine Learning, Phishing, Ransomware, Accountability*

***Izvleček:***

**Kibernetska varnost in varstvo podatkov**

*V dobi digitalne preobrazbe sta postala kibernetska varnost in varstvo podatkov ključnega pomena za varovanje občutljivih informacij in zagotavljanje celovitosti spletnih sistemov. Kibernetska varnost se osredotoča na zaščito omrežij, sistemov in podatkov pred zlonamernimi napadi, vključno z ribarjenjem, izsiljevalsko programsko opremo in naprednimi trajnimi grožnjami. Zaščita podatkov pa poudarja etično in zakonito ravnanje z osebnimi in poslovnimi podatki ter zagotavlja skladnost s predpisi, kot sta Splošna uredba o varstvu podatkov (GDPR) in Kalifornijski zakon o zasebnosti potrošnikov (CCPA).*

*Ker se kibernetske grožnje še naprej razvijajo, morajo organizacije sprejeti proaktivne varnostne ukrepe, kot so arhitektura ničelnega zaupanja (Zero Trust Architecture - ZTA), odkrivanje groženj na podlagi umetne inteligence in tehnologije šifriranja. Poleg tega se kot ključna orodja za varnost*

*podatkov pojavljajo tehnologije za krepitev zasebnosti (PET) in postkvantne kriptografske rešitve. Za učinkovito zmanjševanje tveganj morajo podjetja uvesti večfaktorsko avtentikacijo (MFA), izvajati redne ocene tveganj, usposabljati zaposlene za varnostno ozaveščanje in vzpostaviti celovite načrte odzivanja na incidente.*

*Ta prispevek obravnava pomen kibernetske varnosti in zaščite podatkov, najnovejše trende na področju varnostnih tehnologij in najboljše prakse za zmanjševanje kibernetskih groženj. S strateškim pristopom h kibernetski varnosti in skladnosti lahko organizacije povečajo svojo odpornost proti kibernetskim tveganjem, hkrati pa krepijo zaupanje v digitalni proctor.*

***Ključne besede:***

*kibernetska varnost, varstvo podatkov, digitalni ekosistem, kibernetske grožnje, kršitev varstva podatkov, ocena tveganja, umetna inteligenca, strojno učenje, ribarjenje, izsiljevalska programska oprema, odgovornost*

## 1 The Importance of Cybersecurity

In the interconnected world of the 21st century, the reliance on digital systems has grown exponentially, transforming how organizations, governments, and individuals operate. This digital evolution, while enabling unprecedented innovation and efficiency, also presents a critical challenge: ensuring cybersecurity and protecting sensitive data. Cybersecurity and data protection have become central to mitigating risks associated with digital operations, safeguarding personal and corporate information, and preserving trust in the digital ecosystem.

Cybersecurity refers to the practice of protecting computer systems, networks, and data from cyber threats such as unauthorized access, theft, or damage. The growing volume and sophistication of cyberattacks necessitate robust strategies and technologies to counteract potential risks. From phishing schemes and ransomware attacks to advanced persistent threats (APTs), the landscape of cybercrime is both complex and dynamic.

Key Elements of Cybersecurity:

- **Confidentiality**: Ensuring that sensitive information is accessible only to authorized individuals or entities.
- **Integrity**: Protecting data from being altered or corrupted, ensuring accuracy and trustworthiness.
- **Availability**: Guaranteeing that systems and data are accessible to authorized users when needed.

## 2 The Role of Data Protection

Data protection complements cybersecurity by focusing on safeguarding personal and sensitive information from misuse or exposure. It involves implementing policies, processes, and technologies that ensure compliance with legal frameworks like the General Data Protection Regulation (GDPR) in the European Union.

## 3 Principles of Data Protection

Data protection focuses on ensuring that archival records remain secure, accessible, and unaltered over time. Legal frameworks such as the **General Data Protection Regulation (GDPR)** and various national **Freedom of Information Acts** require institutions to handle personal and historical records responsibly.

## 4 GDPR and Its Impact on Archival Data Protection

The **General Data Protection Regulation (GDPR)** is a comprehensive data protection law enacted by the European Union (EU) to safeguard individuals' personal data and privacy. It has significant implications for archival institutions that store, process, or share personal data.

### Key Principles of GDPR in Archives

1. **Lawfulness, Fairness, and Transparency** – Archives must ensure that personal data is processed legally and transparently. They should provide clear information about data collection and usage.
2. **Purpose Limitation** – Data collected and stored in archives must only be used for specified, legitimate purposes.
3. **Data Minimization** – Archives should only collect and retain data necessary for archival purposes, avoiding excessive data storage.
4. **Accuracy** – Personal records in archives must be kept accurate and up-to-date, ensuring that incorrect data does not persist over time.
5. **Storage Limitation** – Personal data should not be retained for longer than necessary unless justified by historical, research, or legal requirements.
6. **Integrity and Confidentiality** – Archives must implement security measures to protect personal data against unauthorized access, alteration, or destruction.
7. **Accountability** – Archival institutions must demonstrate compliance with GDPR through documentation, risk assessments, and appropriate safeguards.

### Special Considerations for Archival Institutions under GDPR

**Archival Exemptions** – GDPR allows certain exemptions for archives when processing personal data for historical research or public interest. However, these exemptions require strict security measures.

**Data Subject Rights** – Under GDPR, individuals have rights such as data access, rectification, and erasure. However, in archival contexts, the "right to be forgotten" may not always apply due to historical preservation interests.

**Cross-Border Data Transfers** – If an archive shares or stores data outside the EU, it must comply with GDPR’s international transfer regulations, using mechanisms like **Standard Contractual Clauses (SCCs)** or **Binding Corporate Rules (BCRs)**.

## 5 Key Data Protection Strategies for Archives

1. **Access Control and Authentication** – Implementing multi-factor authentication (MFA) and role-based access controls (RBAC) ensures that only authorized personnel can view or modify archival records.
2. **Data Encryption** – Encrypting archival records protects them from unauthorized access, even if data is intercepted or stolen.
3. **Regular Backups** – Routine backup procedures, including offline and cloud-based backups, ensure that archival materials are not lost due to cyber incidents.
4. **Digital Preservation Techniques** – Utilizing checksum verification, file integrity monitoring, and secure migration strategies helps maintain the long-term accessibility of digital records.
5. **Compliance with Legal Frameworks** – Archives must adhere to national and international data protection laws to ensure ethical handling and storage of records.

## 6 Advanced Data Protection Measures for Archives

1. **Homomorphic Encryption** – This encryption method allows computations to be performed on encrypted data without decryption, ensuring privacy in data processing.
2. **Redundant Array of Independent Disks (RAID)** – Using RAID configurations (RAID 5, RAID 6, or RAID 10) ensures fault tolerance and data redundancy for archival storage.
3. **Immutable Storage Solutions** – WORM (Write Once, Read Many) storage ensures that archival records cannot be modified or deleted after they are written.
4. **Intrusion Detection and Prevention Systems (IDPS)** – Implementing AI-driven **IDPS solutions** helps monitor network traffic for suspicious activities and mitigates potential cyber threats before they affect archival data.
5. **Data Anonymization and Masking** – Sensitive personal records in archives can be anonymized using techniques such as **differential privacy** to ensure compliance with privacy laws while maintaining data usability.

## 7 Emerging Trends in Cybersecurity and Data Protection

### Zero Trust Architecture (ZTA)

The Zero Trust model assumes that threats can originate both inside and outside an organization’s network. It requires strict identity verification for every individual and device attempting to access resources.

### Blockchain for Data Integrity

Blockchain technology offers a decentralized approach to maintaining archival records, ensuring immutability and verifiability. Implementing blockchain solutions can enhance trust in the authenticity of archived materials.

### Artificial Intelligence for Threat Detection

AI-driven security systems can monitor network traffic and detect anomalies indicative of cyber threats. Machine learning algorithms can identify potential breaches before they compromise archival data.

### Cloud-Based Archiving with Secure Access Controls

Cloud storage solutions provide redundancy and disaster recovery options for digital archives. However, implementing strong access controls and encryption is necessary to prevent unauthorized access.

### Digital Watermarking and Fingerprinting

Embedding digital watermarks or cryptographic fingerprints in archived documents ensures authenticity and traceability. This technique helps verify the integrity of digital records over time.

### Quantum Computing

While quantum computing offers transformative potential, it also poses risks to traditional encryption methods. Preparing for post-quantum cryptography is a growing concern for security professionals.

### Privacy-Enhancing Technologies (PETs)

Techniques such as homomorphic encryption and secure multi-party computation enable data processing while maintaining privacy, aligning with stringent data protection regulations.

## 8 Strategies for Effective Cybersecurity and Data Protection

- **Comprehensive Risk Assessment**: Organizations must identify vulnerabilities, evaluate potential impacts, and prioritize mitigation strategies.
- **Multi-Factor Authentication (MFA)**: Strengthening access controls with MFA adds an extra layer of security.
- **Employee Training and Awareness**: Educating employees on recognizing phishing attempts, using strong passwords, and adhering to security protocols is crucial.
- **Incident Response Plans**: Establishing clear protocols for detecting, responding to, and recovering from security breaches minimizes damage and downtime.
- **Regular Audits and Compliance Checks**: Ensuring that cybersecurity measures and data protection practices align with evolving standards and regulations.

## 9 Conclusion

As archives increasingly transition to digital formats, the relationship between cybersecurity and data protection becomes more critical than ever. Implementing robust security frameworks, adhering to legal regulations, and leveraging emerging technologies can help archival institutions mitigate cyber threats and protect sensitive historical and cultural records. By prioritizing security measures, institutions ensure the long-term preservation, accessibility, and authenticity of digital archives, safeguarding valuable information for future generations.

## 10 Literature overview

**Knibbs, C., Hibberd, G. (2024).** A Practitioner's Guide to Cybersecurity and Data Protection. New York: Routledge.
*This book offers an accessible introduction and practical guidance on cybersecurity, focusing on ensuring client confidentiality and data integrity. It serves as a valuable resource for professionals seeking to understand and implement effective cybersecurity measures.*

**Palmer, W. (2023).** Cybersecurity - Data Protection and Strategies: First Edition. Outskirts Press.
*This publication covers a wide range of topics related to data protection strategies, providing in-depth knowledge on the safe use of technologies concerning networks, hardware, software, and mobile applications. It's particularly useful for IT students, practitioners, and scholars aiming to deepen their understanding of cybersecurity strategies.*

**Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022).** Cyber risk and cybersecurity: a systematic review of data availability. The Geneva Papers on Risk and Insurance - Issues and Practice, 47(3), 698–736. Retrieved from https://doi.org/10.1057/s41288-022-00266-6.

*This research article analyzes existing academic and industry literature on cybersecurity and cyber risk management, focusing on data availability. It highlights the challenges posed by the lack of accessible data on cyber risks, which is crucial for stakeholders aiming to address cybersecurity issues effectively*.

**Raul, A. C. ed. (2014).** The Privacy, Data Protection and Cybersecurity Law Review. London: Law Business Research.
*Edited by Alan Charles Raul, this review provides a comprehensive overview of the evolving global privacy, data protection, and cybersecurity landscape. It includes contributions from legal experts worldwide, offering insights into various legal frameworks and practices.*

**Febriyani, W., Kusumasari, T. F., & Lubis, M. (2023).** Data Security: A Systematic Literature Review and Critical Analysis. In 2023 International Conference on Advancement in Data Science, E-learning and Information System (ICADEIS) (pp. 1–6). 2023 International Conference on Advancement in Data Science, E-learning and Information System (ICADEIS). IEEE. Retrieved from https://doi.org/10.1109/icadeis58666.2023.10270832.

*This paper systematically reviews existing literature on data security, identifying current research directions, main challenges, and suggesting future research avenues. It's a valuable resource for understanding the complexities and evolving nature of data security.*

**Oluwatoyin Ajoke Fayayola, Oluwabukunmi Latifat Olorunfemi, & Philip Olaseni Shoetan. (2024).** DATA PRIVACY AND SECURITY IN IT: A REVIEW OF TECHNIQUES AND CHALLENGES. Computer Science & IT Research Journal, 5(3), 606–615. Retrieved from https://doi.org/10.51594/csitrj.v5i3.909.

*This literature review provides an overview of techniques and challenges associated with ensuring data privacy and security in information technology. It discusses various methods and their effectiveness in protecting data within IT systems.*

**Gupta, I., & Singh, A. K. (2022**). A Holistic View on Data Protection for Sharing, Communicating, and Computing Environments: Taxonomy and Future Directions (Version 1). arXiv. Retrieved from https://doi.org/10.48550/ARXIV.2202.11965.

*This paper presents a comprehensive view of data protection in various environments, discussing data leakage protection systems, challenges, and future research directions. It's particularly useful for understanding data protection in the context of data sharing and communication.*

## POVZETEK

# KIBERNETSKA VARNOST IN VARSTVO PODATKOV

**Saša ĐUKIĆ**
Vodja oddelka za IT in digitalizacijo, Arhiv Republike Srbske,
Banja Luka, Bosna in Hercegovina
djusasa@gmail.com

V današnjem digitalno zaznamovanem svetu je zaščita podatkov bistvenega pomena za varovanje občutljivih informacij, zagotavljanje neprekinjenega delovanja in ohranjanje zaupanja v digitalni ekosistem. Zaščita digitalnih vsebin, ki vključujejo vse digitalne informacije, od besedila in slik do glasbe in videoposnetkov, je v sodobni dobi digitalne tehnologije zelo pomembna tema. Tovrstne vsebine je mogoče zlahka deliti in širiti po spletu, kar povzroča številne izzive na področju varstva intelektualne lastnine in zasebnosti. Kibernetska varnost se osredotoča na zaščito sistemov, omrežij in podatkov pred grožnjami, kot so nepooblaščen dostop, zlonamerna programska oprema in napredni trajni napadi. Temeljna načela kibernetske varnosti – zaupnost, celovitost in razpoložljivost – dajejo smernice za preprečevanje razvijajočih se tveganj v vse bolj povezanem okolju.

Za zaščito digitalne vsebine je mogoče uporabiti številne tehnike in ukrepe, vključno s kriptografskimi tehnikami, upravljanjem pravic, digitalnimi podpisi in digitalnimi vodnimi žigi. Te tehnike lahko pomagajo zaščititi digitalno vsebino in zmanjšajo tveganje kraje ter zlorabe.

Varstvo podatkov dopolnjuje kibernetsko varnost, saj poudarja varovanje osebnih in občutljivih podatkov. S strogimi predpisi, kot je Splošna uredba o varstvu podatkov (GDPR), morajo organizacije sprejeti prakse, ki zagotavljajo preglednost, odgovornost in zmanjšanje količine podatkov. Upoštevanje teh okvirov ne preprečuje le kršitve varnosti podatkov, temveč tudi krepi zaupanje javnosti in skladnost s predpisi.

Novi trendi na področju kibernetske varnosti poudarjajo potrebo po inovativnih rešitvah. Arhitektura ničelnega zaupanja (*zero trust architecture*) na primer predpisuje strogo preverjanje identitete za vse uporabnike in naprave, ne glede na njihovo lokacijo. Umetna inteligenca in strojno učenje se vse pogosteje uporabljata za prepoznavanje groženj in avtomatizacijo odzivov, čeprav te tehnologije prinašajo tudi nove ranljivosti, če jih zlonamerni akterji izkoristijo. Varnost v oblaku je še eno ključno področje, saj podjetja svoje dejavnosti selijo na splet, za zaščito podatkov pa je potrebno robustno šifriranje in stalno spremljanje. Prihod kvantnega računalništva predstavlja izziv za tradicionalne metode šifriranja, zato so potrebne postkvantne kriptografske rešitve. Tehnologije za povečanje zasebnosti (PET), kot je homomorfno šifriranje, še bolj uravnotežijo uporabnost podatkov in skladnost z zasebnostjo.

Za obvladovanje teh izzivov morajo organizacije sprejeti učinkovite strategije za kibernetsko varnost in zaščito podatkov. Bistveni ukrepi so celovita ocena tveganja, večfaktorska avtentikacija (*multi-factor authentication*), usposabljanje zaposlenih, načrti odzivanja na incidente in redne revizije skladnosti. S spodbujanjem kulture varnostne ozaveščenosti in uporabo naprednih tehnologij lahko subjekti učinkovito zmanjšajo tveganja.

Navsezadnje sta kibernetska varnost in varstvo podatkov sestavni del obvladovanja zapletenosti digitalne dobe. S pravimi okviri in proaktivnimi pristopi lahko organizacije zavarujejo svoje sisteme, zaščitijo osebne podatke in zagotovijo odpornost proti razvijajočim se kibernetskim grožnjam.

**O avtorju:**

**Saša Đukić** se je rodil 22. februarja 1986 v Banjaluki, kjer je končal osnovno in srednjo računalniško šolo. Leta 2015 je diplomiral na Pravni fakulteti v Banjaluki. Je ustanovitelj Društva anonimnih umetnikov UAA!, ki je organiziralo in izvedlo številne projekte v Banjaluki. Od leta 2016 je zaposlen v Arhivu Republike Srbske v Banjaluki kot vodja Oddelka za informacijsko tehnologijo in digitizacijo. Večinoma uporablja znanje za oblikovanje in optimizacijo spletnih strani ter pozna osnove programskih jezikov html, css, javascript, php, sql. Za Arhiv Republike Srbske je oblikoval in vzdržuje spletno mesto arhiva, namestil je odprtokodno spletno programsko opremo Atom (Access to memory), vzdržuje strežnik Linux za potrebe programa Atom pa tudi njegovo migracijo na splet na domeni arhipedija.com. Opravil je usposabljanje za razvoj podatkovnih baz MCSA SQL 2016 in za razvoj spletnih aplikacij v programskem jeziku Php. Je tajnik Arhivskega društva Bosne in Hercegovine, član Komisije za strokovne izpite za delavce pri ustvarjalcih arhivskega gradiva in član Komisije za opravljanje strokovnega arhivskega izpita ter priznavanje strokovnih arhivskih nazivov. Je tudi avtor razstave »Potres v Banjaluki 1969: solidarnost, obnova in gradnja« iz leta 2019.

**About the author:**

**Saša Đukić** was born on February 22, 1986, in Banja Luka, where he completed the primary and secondary IT school. He graduated at the Faculty of Law in Banja Luka in 2015. He is the founder of the Association of anonymous artists UAA! that has organized and implemented many projects in Banja Luka. Since 2016, he has been employed at the Archives of the Republika Srpska in Banja Luka, as Head of the IT and Digitization Department, mostly using knowledge of creating and optimizing web sites, knowing the basics of html, css, javascript, php, sql languages. In the Archives of the Republic of Srpska he created and maintains the website of the Archives , installation of Atom and maintenance of the Linux server for the needs of Atom (Access to memory) Open-source web-based software, as well as its migration to the web at the domain arhipedija.com . He got training in: MCSA SQL 2016 Database Development; Php Web development. He is the secretary of the Archivist Association of Bosnia and Herzegovina. He is the member of the Commission for the professional exams for workers in the protection of public records outside the archives and a member of the Commission for taking the professional archival exam and recognizing professional archival titles. He is the author of the exhibition “Earthquake in Banja Luka 1969: solidarity, reconstruction and construction” from 2019.