Journal of Mechatronics, Automation and Identification Technology
Vol. 11, No. 1, pp. 6–11, 2026.

# AI-Driven Cyber Risk Assessment in Modern Business Information Systems

Alen Kamis[1], Jelena Ružić[2], Aleksandra Markovic[3], Nemanja Deretic[4], Sasa Kukolj[5]

[1]The College of Service Business, Sokolac - East Sarajevo, Bosnia and Herzegovina
[2]Faculty of Project and Innovation Management, Belgrade, Republic of Serbia
[3] Toplicka Academy of Applied Studies - Department of Business Studies, Blace, Republic of Serbia
[4] Belgrade Business and Arts Academy of Applied Studies, Belgrade, Republic of Serbia
[5]Faculty of Management, Sremski Karlovci, Republic of Serbia
alen@vub.edu.ba, jruzic45@gmail.com aleksandra.markovic@vpskp.edu.rs ,
nemanja.deretic@bpa.edu.rs , sasa.kukolj@famns.edu.rs
Corresponding Author: Alen Kamis

***Abstract*— This paper presents and provides a detailed explanation of a new type of methodology, AI-Driven Cyber Risk Assessment, applied through a case study involving four companies from Bosnia and Herzegovina. Contemporary approaches to information security are increasingly based on dynamic and adaptive risk assessment models, which go beyond static, periodic evaluations and enable continuous monitoring of system security posture. AI-Driven Cyber Risk Assessment represents one of the emerging methodologies in information security, focusing on the analysis and mitigation of cyber risks.**

***Keywords - information security; dynamic threat assessment; AI-Driven Cyber Risk Assessment; case study;***

## I. INTRODUCTION

AI-Driven Cyber Risk Assessment represents a paradigmatic shift in this context, as it uses machine learning models to process large volumes of data from various sources and make decisions in real time [1]. Such an approach is not limited to detecting existing threats but is capable of predicting potential vulnerabilities based on activity patterns and anomalies. This provides organizations with the opportunity to respond preventively rather than reactively, thereby reducing the likelihood of harmful consequences. Within national frameworks, the protection of information systems has become a priority of state security policy due to threats arising from organized cybercrime, industrial espionage, and geopolitically motivated attacks [4]. Industrial sectors that manage critical infrastructure or economic data are particularly targeted by sophisticated attack methods. In this context, the integration of artificial intelligence with control processes can significantly reduce the time required for incident detection, which directly impacts the ability to respond adequately. Through the analysis of four case studies from Bosnia and Herzegovina, the application of the new methodology will be presented across different industrial sectors. Although risk profiles vary depending on the number of employees, the type of workstations, the structure of the server environment, and data backup solutions, the results show a consistent trend of increased resilience to cyber threats across all entities after the implementation of these approaches [2]. It is particularly important to emphasize that companies with formalized information security management procedures were more prepared to incorporate these methods into their business processes. It is interesting to observe how traditional tools function in synergy with AI-driven risk analysis.

## II. DEFINITION AND IMPORTANCE OF INFORMATION SECURITY

Information security, in its broadest sense, is defined as a set of technical, administrative, and legal measures used to protect data and information systems from unauthorized access, modification, destruction, or disruption of operations. It encompasses the protection of the integrity, confidentiality, and availability of information, which is recognized as the foundation of the normal functioning of modern organizations [3]. Its importance stems from the fact that digital systems represent the central nervous system of business operations, infrastructure, and state institutions. Any misuse or disruption in their operation can have a domino effect on the wider environment. Modern concepts of information security go beyond the traditional understanding of data protection through static mechanisms. Instead of periodic evaluation, continuous monitoring and risk assessment are introduced. AI-Driven Cyber Risk Assessment operates by using machine learning algorithms to analyze patterns of system usage and detect anomalies that may indicate emerging threats [1]. In this way, it is possible to respond even before an incident occurs, whereas traditional methods are often limited to post-incident analysis. Alongside the technical



* This paper is a revised and expanded version of the paper presented at the XXV International Symposium INFOTEH-JAHORINA 2026

verification of implemented security controls, special emphasis is placed on procedures related to the management of digital certificates and encryption keys in order to ensure the authentication of all participants in communication. From the perspective of technical implementation, information security includes a multi-layered protection approach (defense in depth) for information systems. In IoT environments, mechanisms such as system login monitoring, antivirus solutions, intrusion detection and prevention systems, and software network traffic analyzers are applied [1]. Data from these sources are automatically processed through SIEM platforms that correlate events in a way that facilitates the detection of complex attack scenarios that might otherwise go unnoticed. The importance of information security grows proportionally with the dependence of business operations on network and server infrastructure [6]. Today, even small business sectors use service models that connect local resources with external cloud platforms, which further expands the potential attack surface. Therefore, the synergy between technologies such as AI-driven analytics and the continuous improvement of employee awareness of cyber risks has become one of the main prerequisites for a resilient information environment.

The components of information security are, in practice, observed through three fundamental principles: integrity, confidentiality, and availability of data. Integrity ensures that information is not altered without authorization, preserving the consistency of records from the moment of creation to their final use. Confidentiality prevents unauthorized access to sensitive data, while availability guarantees that authorized users can access information and systems when needed [3]. These principles are interconnected and form the foundation upon which classical and modern methodologies, such as AI-Driven Cyber Risk Assessment, are built. The application of AI-Driven Cyber Risk Assessment adds a layer of proactivity to these components, as machine learning algorithms analyze data flows to detect anomalies that may indicate compromised systems [1]. The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

## III. LEGAL AND REGULATORY FRAMEWORK

The legal and regulatory framework of information security in Bosnia and Herzegovina relies on a mixture of entity-level regulations, national strategies, and international standards, which in practice creates a complex environment for the consistent implementation of security policies. The lack of a unified law at the state level, such as the one that exists in Republika Srpska through the Law on Information Security, leads to inconsistencies in regulations between entities [12]. The existence of such divergence complicates the digital protection of systems operating across the country, especially in sectors whose infrastructure crosses administrative boundaries. The fact that the Government of the Federation of Bosnia and Herzegovina was in the process of drafting a similar legal act, but its outcome remains unknown even two years after the public call for comments was published [3], indicates the slowness of the legislative response in an area that requires agility.

Conducted case studies show that the application of the AI-Driven Cyber Risk Assessment methodology depends on a legal foundation that enables data exchange and uninterrupted monitoring of security parameters. Without a clear legal framework defining the standards for such data processing, there is a risk that procedures will not be equally applied or recognized across different jurisdictions within Bosnia and Herzegovina. The financial sector, due to the nature of its data, is particularly sensitive to regulatory gaps. Laws regulating electronic data processing clearly define penal provisions for unauthorized access to protected systems [4]. However, weaknesses arise in international correspondence or cross-border transactions, as it is not always clear how domestic law protects data outside territorial jurisdiction. The legal basis for such verification derives from contractual obligations and regulations on the protection of intellectual property and confidential business information [3].

If a supplier operates from another jurisdiction within the region or the European Union, domestic law must be complementary with international frameworks such as the GDPR for the evaluation to have legal effect. The institutional dimension also plays a significant role; the existence of relevant bodies responsible for managing cyber incidents depends on the organizational and legal framework that grants them authority to act. Insufficient awareness of threats and vulnerabilities among stakeholders, along with the absence of a state-level CERT (Computer Emergency Response Team), reduces the effectiveness of existing norms [10]. The field of cybersecurity at the state level requires strategic documents that define procedures for the protection of critical infrastructure. Without them, even the most sophisticated AI-Driven systems will not have the full legal support necessary for operational response to threats that extend beyond a single organization.

Existing laws sometimes leave room for different interpretations due to the specific constitutional and political structure of the country, which affects the harmonization of regulations [3]. This can lead to internal divisions between entities in the application of security procedures and even delays in adopting modern protection methods used in other jurisdictions. From a practical perspective, this means that organizations wishing to use advanced methodologies must simultaneously follow different sets of regulatory requirements. Combining technical measures from the previous analysis with the infrastructural support of the legal system appears essential if the integrity, confidentiality, and availability of information described earlier in the paper are to be preserved [9]. Laws themselves create the foundation of accountability, while technology literally measures risk indicators in real time [1]. Only through this synergy is it

possible to effectively respond to increasingly sophisticated threats and attacks.

## IV. AI-DRIVEN CYBER RISK ASSESSMENT – ADVANCED METHODOLOGIES FOR CYBER RISK

The application of the AI-Driven Cyber Risk Assessment methodology across different industrial sectors (case study of this paper) in Bosnia and Herzegovina has proven to be a central tool for advanced assessment and neutralization of cyber threats. Unlike traditional approaches, this methodology is based on automated risk modeling through machine learning algorithms, capable of analyzing vast amounts of operational data from heterogeneous sources in real time [1].

The AI-Driven Cyber Risk Assessment methodology integrates data from various security and infrastructure sources, including SIEM systems, EDR/XDR solutions, network and application logs, vulnerability scanning tools, cloud and identity platforms, which are normalized and correlated to create a unified analytical base. It then uses machine learning techniques to identify known and unknown attack patterns, correlate vulnerabilities with active threats, and model potential attack paths, while AI models analyze historical incidents, current threats, and contextual factors to dynamically assess the probability and impact of threats on systems, applications, users, and business functions. This enables continuous risk ranking and prioritization, predictive analysis, and simulation of "what-if" scenarios for proactive security planning, as well as the generation of automated recommendations and responses for risk mitigation, including patching, policy adjustments, and improvements in access control, all with the aim of increasing organizational resilience and security [8].

Such a system is not limited to passive detection but actively predicts potential vulnerabilities based on anomalies in user and infrastructure behavior. Continuous data collection on network traffic, system access, and configuration changes enables deeper insight into the status of controls that protect the integrity, confidentiality, and availability of information. The technical aspect of this methodology is based on the synergy between public/private key encryption technologies (PKI systems), intelligent monitoring of network traffic through SIEM platforms, and machine learning capable of distinctly identifying incident patterns [5]. When such an ecosystem operates in synchronization, it becomes possible to automatically detect compromised accounts and systems or atypical use of privileged accounts at the very moment a threat emerges. This shortens response time and increases the likelihood of successfully preventing the consequences of high-tech attacks.

Although no security framework guarantees absolute protection against all forms of cyber threats, experience from these case studies confirms that the combination of advanced analytical methods within AI-Driven Cyber Risk Assessment, along with continuous monitoring and evaluation, can drastically reduce organizational exposure to specific attacks such as APT campaigns, MITM interceptions, or internal misuse of privileged accounts [4]. Relying solely on static defense mechanisms becomes inadequate when adversaries use predictive tactics to minimize their footprint while operating within compromised systems [11]. For this reason, this methodology provides additional value by applying the same analytical principles of behavioral prediction—now used for protection rather than exploitation of vulnerabilities [7].

## V. INDUSTRIAL CONTEXT OF METHODOLOGY APPLICATION – CASE STUDY

The case study is based on the example of four companies, which come from different industrial sectors. We were asked not to disclose the names of the companies in the paper. The data were obtained through a survey in the doctoral dissertation of one of the authors.

### *A. Company from the wood industry*

The first company included in the case study operates in the wood industry sector and employs approximately 120 employees. The information technology infrastructure of this company is relatively simple and consists of a total of 25 workstations, including five industrial machines that have embedded personal computers, as well as one central server.

The company does not have an implemented backup solution, which represents a significant risk in terms of data availability and integrity. The IT environment is predominantly oriented toward supporting production processes, with a limited level of automated security controls and without a formalized information security management system. Such an infrastructure makes this company suitable for analyzing the application of modern AI-based methodologies for cyber risk assessment and management in environments with a low level of digital maturity.

### *B. Company from the Leather and Haberdashery* Industry

The second company included in the case study operates in the leather and haberdashery industry and employs around 300 workers. The information infrastructure of the company consists of 20 workstations, two industrial machines with integrated computers, as well as two servers.

Unlike the previous case, the company has a local backup solution, which is implemented through a second server. Although this represents a basic level of data protection, such a solution still carries certain risks in terms of resilience to incidents such as ransomware attacks, hardware failures, or physical threats. The company does not have formally implemented international standards for quality management or information security, which enables the assessment of the effects of applying continuous AI-based risk assessment methodologies in an industrial environment of medium complexity.

### *C. Company from the Automotive Sales and* Maintenance Sector

The third company included in the case study is engaged in the sale and maintenance of new automobiles and employs approximately 75 employees. The IT infrastructure of this company includes around 50 workstations, five industrial computers, as well as four

servers. The company has a local backup solution that is used to protect business-critical data.

Unlike the previous companies, this organization is certified according to the ISO 9001 standard, which indicates the existence of formalized business processes and a quality management system. However, ISO 9001 does not directly cover information security management, which makes this company interesting for analyzing the integration of new AI-Driven cyber risk assessment methodologies into existing management and operational processes.

*D. Company – System Integrator*

The fourth company included in the case study operates as a system integrator and employs around 90 employees. The IT infrastructure of this company is the most complex among the analyzed cases and includes 120 workstations (90 laptop computers and 30 desktop computers), six physical servers on which approximately 30 virtual servers are implemented, a central storage system, one NAS device, as well as an S3 immutable online storage solution.

The company holds ISO 9000 and ISO/IEC 27001 certificates, which indicates a high level of process formalization and maturity in quality and information security management. Such an environment represents a suitable example for the application of advanced AI-based methodologies such as continuous risk assessment, continuous monitoring of controls, as well as risk management in supply chains and relationships with third parties.

## VI. Analysis and Results

The case study is based on the example of four companies from different industrial sectors. We were asked not to disclose the names of the companies in the paper. The data were obtained through a survey in the doctoral dissertation of one of the authors.

Within the AI-Driven Cyber Risk Assessment methodology, cyber risk is defined as a dynamic function of probability, impact, and contextual exposure, where the values are evaluated using AI models trained on security and operational data.

The basic definition of risk is given by the expression:

$$R = P \times I \quad (1)$$

where is:

- $R$– cyber risk
- $P$ – probability of threat realization (AI-based assessment)
- $I$– impact of the incident on business operations

The probability of threat realization is modeled as a function of multiple variables:

$$P = f(V, T, H) \quad (2)$$

where is:

- $V$– level of technical vulnerabilities (e.g., CVE, configurations)
- $T$– current threat intelligence
- $H$– historical security incidents

The AI model (e.g., logistic regression or a neural network) approximates the probability within the range:

$$P \in [0,1]$$

The modeling of incident impact is defined as a weighted sum of business consequences:

$$I = w_1 I_{fin} + w_2 I_{ops} + w_3 I_{rep} \quad (3)$$

where is:

- $I_{fin}$– financial impact
- $I_{ops}$– operational impact
- $I_{rep}$– reputational impact
- $w_1 + w_2 + w_3 = 1$– weights determined by AI analysis of the business context

The AI-Driven methodology introduces a system exposure factor (Attack Surface Factor):

$$E \in [0,1]$$

which depends on:

- number and type of IT resources
- system connectivity
- internet exposure

The final AI-Driven risk model for an individual threat is defined as:

$$R_{AI} = P \times I \times E \quad (4)$$

For the overall environment, the total risk is:

$$R_{AI}^{total} = \sum_{j=1}^{n} (P_j \times I_j \times E_j) \quad (5)$$

where n is the number of identified threats.

For comparison between different organizations, the risk (risk index) is normalized to a 0–100 scale:

$$R_{index} = \frac{R_{AI}^{total}}{R_{AI}^{max}} \times 100 \quad (6)$$

where is:

$R_{AI}^{max}$– maximum theoretical risk value in the analyzed set

*A. Dataset Preparation and AI Model Training*

AI models used in the research were trained on empirical data collected through a structured survey conducted as part of one of the authors' doctoral dissertation, as well as on additional technical data obtained through the analysis of the IT infrastructure of the involved organizations.

The overall dataset included:

- 4 organizations from different industrial sectors
- 68 identified security controls (technical and organizational)
- 42 types of threats mapped according to MITRE ATT&CK and ENISA classifications
- three years of historical incident data (2023–2025)
- 120+ identified technical vulnerabilities (CVE classification)

The dataset included:

- Vulnerability assessment results (V)
- Recorded security incidents (H)
- A
- Assessment of business impact (financial, operational, and reputational)

- System exposure parameters (number of publicly accessible services, network segmentation, backup architecture, existence of SOC monitoring, etc.)

### *B. Artificial Intelligence (AI) Model*

Two models were used to assess the probability of threat realization:

- Logistic regression (baseline model)
- Multilayer neural network (MLP – Multi-Layer Perceptron with one hidden layer)

The input variables of the model were:

X = {V, T, H, number of endpoints, number of public services, type of backup solution, network segmentation, existence of ISO standards}

The model was trained on 80% of the dataset, while 20% was used for validation. The average accuracy of incident realization classification was 84%, while the AUC (Area Under the Curve) value was 0.87.

The weights $w_1$, $w_2$, and $w_3$ in expression (3) were determined by optimizing the model loss function, enabling the adjustment of weighting factors to the specific business context of the organization.

### *C. Definition of scenarios before and after the application of the AI methodology*

The risk index values before and after do not represent a change in the model itself, but rather a change in the state of security controls within the organization.

#### *1) Before the application of the AI methodology*

The initial value refers to the organization's baseline state, characterized by:

- lack of a formalized risk assessment
- absence of continuous threat monitoring
- limited or non-existent backup solutions
- weak network segmentation
- absence of centralized log management
- a reactive approach to incident handling

The risk was calculated based on the actual state of the infrastructure at the time of the initial analysis.

#### *2) After the application of the AI-driven methodology*

The post-implementation value represents the simulated state of the organization after implementing the recommendations generated by the AI model, which included:

- introduction of a structured risk assessment
- implementation of the 3-2-1 backup strategy
- network segmentation and isolation of critical systems
- implementation of MFA authentication
- deployment of EDR monitoring
- continuous threat monitoring
- establishment of a formal incident response process

The post-implementation risk index was calculated using the same mathematical model (4) and (5), but with updated parameters P, I, and E reflecting the improved state of security controls..

#### *3) Results of the application of the AI methodology*

Based on the application of the aforementioned model, the following risk indices were obtained, as shown in Table I.

TABLE I – Presentation of AI-Driven Risk Model Results

| Company | IRisk index before the application of the AI methodology | Risk index after the application of the AI methodology |
|---|---|---|
| Wood industry | 85 | 45 |
| Leather and leather goods industry | 70 | 40 |
| Automotive sales and maintenance | 60 | 30 |
| System integrator | 45 | 20 |

The results are graphically presented in Figure 1, before and after the application of the AI-driven methodology.:

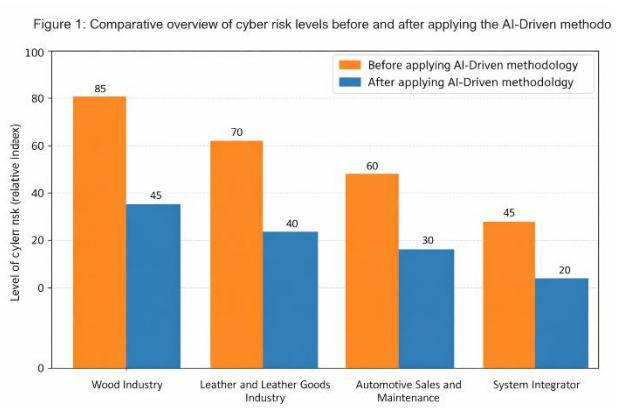


Figure 1 – Presentation of results before and after the application of the AI-driven risk assessment methodology

The application of the AI-Driven Cyber Risk Assessment methodology showed a significant impact on the reduction of cyber risk across different industrial sectors. Based on the comparative values before and after implementation, it is evident that a significant reduction in risk occurred in all observed categories.

The wood industry records a decrease from 85 to 45, representing an absolute reduction of 40 index points, i.e., a relative decrease in the risk index of approximately 47.1%. This result indicates an almost halved level of risk, which is indicative of the high effectiveness of the applied methodology in a sector with traditional processes.

The leather and leather goods industry achieved a reduction from 70 to 40, which represents a decrease of 30 points or approximately 42.9%. Although the percentage reduction is slightly lower compared to the wood industry, the result still confirms significant progress in mitigating cyber threats.

The company engaged in automotive sales and maintenance shows a decrease from 60 to 30, representing an absolute reduction of 30 points, i.e., 50%. This result suggests that the automotive sector is particularly responsive to optimization through AI-driven approaches, likely due to the complexity of digital services and interconnected systems.

The system integrator company records the highest relative improvement, with a decrease from 45 to 20, representing a reduction of 25 points or approximately

55.6%. This result indicates exceptional effectiveness of the methodology in an environment focused on integrating various technological solutions, where risk control is critical.

## VII. Conclusion

Within this research, the application of the AI-Driven Cyber Risk Assessment methodology was analyzed through a case study of four companies from different industrial sectors in Bosnia and Herzegovina. The methodology proved to be an effective tool for a quantitative and more objective assessment of cyber risk, based on the analysis of large volumes of data, predictive threat modeling, and contextual evaluation of information system exposure. Unlike traditional approaches, the AI-Driven Cyber Risk Assessment methodology enables dynamic risk assessment and faster identification of critical points in the IT environment.

The results obtained through the application of the proposed model indicate that all analyzed companies achieve a significant reduction in the level of cyber risk after the introduction of AI-Driven assessment. A decrease in the cyber risk index was observed in the range of approximately 42.9% to 55.6%, which clearly confirms the high potential of this methodology in improving cybersecurity. The highest relative effect was recorded in the company operating as a system integrator, which can be associated with the existing level of digital maturity and the ability to more effectively integrate AI-based security mechanisms. At the same time, companies from the wood industry and the automotive sales and maintenance sector also show significant improvements, despite a lower initial level of security maturity.

The obtained findings indicate that the integration of advanced artificial intelligence techniques into cyber risk management processes is strategically justified and brings measurable and comparable benefits across different industrial domains. Based on the research results, it can be concluded that AI-Driven Cyber Risk Assessment represents a sustainable and scalable approach that can significantly contribute to improving the resilience of information systems and the overall level of cybersecurity in modern business environments.

## References


[1] M. Stojanović, J. Marković-Petović, Dinamička procena bezbednosnog rizika u industrijskim IoT sistemima, Novembar 2021. https://doi.org/10.37528/ftte/9788673954455/postel.2021.020.

[2] O. Matthew Ijiga, I. Peter Idoko, G. Isenyo Ebiega, F. Itunu Olajide, T. Isaiah Olatunde, and C. Ukaegbu, Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention, Open Access Research Journal of Science and Technology, vol. 11, no. 1, pp. 001–004, May 2024, https://doi.org/10.53022/oarjst.2024.11.1.0060.

[3] P. Ukić, Pravni okvir zaštite od visokotehnološkog kriminala u Bosni i Hercegovini – analiza strateških ciljeva i mogućnost usklaivanja sa evropskom strategijom sajber bezbednosti, 45RKKP, tom 61, izd. 2, str. 45–67, August. 2023, https://doi.org/10.47152/rkkp.61.2.3.

[4] К. Јонев, Х. Бериша, А. Ћираковић, Информациона безбедност Руске федерације, str. 100, 2018, https://doi.org/10.5937/vojdelo1802100J.

[5] Z. Vujić, V. Rajs, Sajber bezbednost u automobilskoj industriji, Zbornik radova Fakulteta tehničkih nauka, Novi Sad, Februar 2019., https://doi.org/10.24867/29IH02Vujic

[6] Ž. Milojević, L. Dulović, Velike baze podataka – Big Data, primena u vojno-bezbednosnom sistemu, str. 236, Mart 2018, https://doi.org/ 10.5937/vojdelo1803236M.

[7] C. Ratnawat and C. Prakash, Sarcouncil Journal of Multidisciplinary under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 (CC BY-NC- ND 4.0) International License Revolutionizing Cyber Insurance: AI-Driven Risk Scorecards for SMEs, July 2025, https://doi.org/10.5281/zenodo.15793533.

[8] Y. Agzayal and M. Bouhorma, AI-Driven Cyber Risk Management Framework, , pp. 571–584, Jan. 2024, https://doi.org/10.1007/978-3-031-53824-7_51.

[9] W. Stallings, Cryptography and network security : principles and practice. Hoboken, New Jersey: Pearson Education, Inc, 2020.

[10] M. Nikolić, M. Petrović, Analiza konteksta, rizika i prilika u procesu upravljanja medicinskim otpadom na teritoriji Autonomne pokrajine Vojvodine, Zbornik radova Fakulteta tehničkih nauka, Novi Sad, Mart 2024. https://doi.org/10.24867/24HZ03Nikolic.

[11] G. Sam, E. R Kaburuan, AI-Driven Cyber Risk Assessment: Protecting against Cyberthreats Determined with Machine Learning." Journal of Wireless Networks and Communication Systems, 2025, https://jwncs.melangepublications.com/index.php/jwncs/article/view/9

[12] Уредба-о-мјерама-информационе-безбједности-РС, https://cert.aikt.rs/ova_doc/uredba-o-mjerama-informacione-bezbjednosti-rs/.