


Евразийский национальный университет имени Л.Н. Гумилева
Национальная инженерная академия РК
Казахский национальный педагогический университет имени Абая, Казахстан
Институт математики и математического моделирования КН МВНО, Казахстан
Институт информационных и вычислительных технологий КН МВНО, Казахстан
Международный математический центр ИМ им. С.Л. Соболева СО РАН, Россия
Российский национальный комитет по индустриальной и прикладной математике, Россия
ОФ «Международный фонд обратных задач», Казахстан
Математическое Общество Тюркского Мира.

ЕУРАЗИЯЛЫҚ ХАЛЫҚАРАЛЫҚ ҒЫЛЫМИ КОНФЕРЕНЦИЯ
ЕВРАЗИЙСКАЯ МЕЖДУНАРОДНАЯ НАУЧНАЯ КОНФЕРЕНЦИЯ

«ҒЫЛЫМДАҒЫ, ТЕХНИКА МЕН ИНДУСТРИЯДАҒЫ ЖАСАНДЫ ИНТЕЛЛЕКТ ЖӘНЕ КЕРІ ЕСЕПТЕР»

«ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ОБРАТНЫЕЗАДАЧИ В НАУКЕ, ТЕХНИКЕ И ИНДУСТРИИ»

«ARTIFICIAL INTELLIGENCE AND INVERSE PROBLEMS IN SCIENCE, TECHNOLOGY AND INDUSTRY»

ЕҢБЕКТЕРІ ТРУДЫ PROCEEDINGS

Астана
14-16 апреля 2025 г.

УДК 004.896:001(082)

Еуразиялық халықаралық ғылыми конференция
«Ғылымдағы, техника мен индустриядағы жасанды интеллект және кері есептер»
Евразийская международная научная конференция
“Искусственный интеллект и обратные задачи в науке, технике и индустрии”
Eurasian internationalscientific conference
«Artificial intelligence and inverse problems in science, technology and industry»

ISBN 978-601-385-052-8

Еуразиялық халықаралық ғылыми конференция «Ғылымдағы, техника мен индустриядағы жасанды интеллект және кері есептер» баяндамалар жинағы. 14-16 сәуір 2025 жыл.

Сб. докл. Евразийской международной научной конференций «Искусственный интеллект и обратные задачи в науке, технике и индустрии» 14-16 апрель 2025 год.

Collection of reports the Eurasian internationalscientific conference «Artificial intelligence and inverse problems in science, technology and industry»

– Астана: Л.Н. Гумилев атын. Еуразия ұлттық университеті, 2025. – 451 б. – қазақша, орысша, ағылшынша.

1 СЕКЦИЯ . «КЕРІ ЕСЕПТЕРДІ ШЕШУДЕ ЖАСАНДЫ ИНТЕЛЛЕКТ»

СЕКЦИЯ 1. «ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В РЕШЕНИИ ОБРАТНЫХ ЗАДАЧ»

SECTION 1. «ARTIFICIAL INTELLIGENCE IN SOLVING INVERSE PROBLEMS»

2 СЕКЦИЯ «КЕРІ ЖӘНЕ ДҰРЫС ҚОЙЫЛМАҒАН ЕСЕПТЕРДІҢ ТЕОРИЯЛЫҚ ЖӘНЕ ЕСЕПТЕУ АСПЕКТІЛЕРІ»

СЕКЦИЯ 2 «ТЕОРЕТИЧЕСКИЕ И ВЫЧИСЛИТЕЛЬНЫЕ АСПЕКТЫ ОБРАТНЫХ И НЕКОРРЕКТНЫХ ЗАДАЧ»

SECTION 2 «THEORETICAL AND COMPUTATIONAL ASPECTS OF INVERSE AND ILL-POSITIONED PROBLEMS»

3 СЕКЦИЯ «АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР ЖӘНЕ ЕСЕПТЕУ ИНТЕЛЛЕКТІСІ

3 СЕКЦИЯ «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ВЫЧИСЛИТЕЛЬНЫЙ ИНТЕЛЛЕКТ»

SECTION 3 «INFORMATION TECHNOLOGY AND COMPUTATIONAL INTELLIGENCE»

4 СЕКЦИЯ «КРИПТОГРАФИЯДАҒЫ ЖАСАНДЫ ИНТЕЛЛЕК ЖӘНЕ КИБЕРҚАУІПСІЗДІК»

4 СЕКЦИЯ «ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В КРИПТОГРАФИИ И КИБЕРБЕЗОПАСНОСТИ»

SECTION 4 "ARTIFICIAL INTELLIGENCE IN CRYPTOGRAPHY AND CYBERSECURITY"

fundamental reassessment of cryptographic design and implementation to address 6G's unique challenges.

Given 6G's imminent deployment, this research underscores the urgency of transitioning to advanced cryptographic frameworks, validated through practical testing, to safeguard data integrity against evolving technological paradigms.

Ultimately, this study provides a strategic blueprint for 6G security, harmonizing proven methodologies with innovative advancements to deliver a resilient, adaptable framework capable of meeting the demands of next-generation telecommunications.

In the end, this study maps out 6G security—combining today's best with tomorrow's bold ideas to build a strong, smart shield for whatever's next.

References:

[1] Rivest R.L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978, Vol. 21, No. 2, pp. 120–126.

[2] National Institute of Standards and Technology. FIPS PUB 197: Advanced Encryption Standard (AES). U.S. Department of Commerce, 2001.

[3] Akter M.S. Quantum cryptography for enhanced network security: A comprehensive survey. arXiv preprint arXiv:2306.09248, 2023.

[4] Pandi et al. Authentication and acknowledgement approach for 6G cellular networks. IEEE Transactions on Communications, 2023.

[5] Coppersmith D. The Data Encryption Standard (DES) and its strength against attacks. IBM Journal of Research and Development, 1994, Vol. 38, No. 3, pp. 243–250.

Slyamshaikhov Y.B.
master's student of the Department of Information Security
L.N. Gumilyov Eurasian National University
Astana, Kazakhstan

Tokseit D.K.
PhD, Acting Associate Professor
L.N. Gumilyov Eurasian National University
Astana, Kazakhstan

APPLICATION OF MACHINE LEARNING AND AUTOMATED PROCESSES IN DIGITAL FORENSICS

Abstract. Digital forensics plays a pivotal role in investigating incidents and crimes involving digital data, leveraging technological footprints left by users in cyberspace. With the exponential growth in data volumes, traditional forensic techniques often fall short, necessitating the integration of machine learning (ML) to enhance efficiency and accuracy. This paper explores the applications of ML in digital forensics, including anomaly detection, malware identification, and user behavior analysis. Key ML methods such as classification, clustering, and autoencoders are discussed for their utility in automating evidence analysis, detecting cyber threats, and restoring compromised data. Despite its advantages, ML faces challenges like data quality requirements and computational demands. The paper emphasizes the evolving role of ML, projecting advancements in automation,

real-time threat detection, and quantum computing integration. Conclusively, machine learning is identified as a transformative force in modern and future digital forensics, underscoring its criticality in strengthening cybersecurity frameworks.

Keywords. Digital forensics, machine learning, anomaly detection, malware analysis, user behavior analysis, autoencoders, cybersecurity, data restoration, quantum computing, automation.

Introduction.

Digital forensics plays a crucial role in investigating cybercrimes and analyzing digital evidence. While traditional forensic methods, such as manual log analysis and signature-based malware detection, have been effective (Casey, 2011), they struggle to keep pace with the exponential growth of data and increasingly sophisticated cyber threats (Qadir & Varol, 2020). These methods often suffer from scalability limitations, high false positive rates, and an inability to detect novel attack patterns in real-time.

Machine learning (ML) offers a promising solution by automating complex forensic tasks, including anomaly detection, malware classification, and behavioral analysis. We hypothesize that integrating ML into digital forensics workflows can enhance the speed and accuracy of investigations by 30–50%, reducing the reliance on manual processes and improving threat detection capabilities.

Existing research highlights the potential of ML in cybersecurity (Chio & Freeman, 2018; Sarker, 2023), yet its structured integration into forensic workflows remains underexplored. This study aims to systematize the application of ML in digital forensics, evaluate its advantages and limitations, and demonstrate practical implementations through real-world case studies. By bridging this gap, we provide a comprehensive analysis of ML techniques, tools, and use cases that enhance modern forensic investigations.

Methods.

Machine learning encompasses a diverse set of methods and algorithms that enable systems to learn patterns, make predictions, and improve performance over time without being explicitly programmed. Some of the major machine learning techniques include supervised learning, unsupervised learning, semi-supervised learning, reinforcement learning, deep learning, neural networks, decision trees, random forests, support vector machines, and K-nearest neighbors, which can be appropriately applied based on their use cases, either as classification, clustering, regression, or otherwise. Machine learning has proven to be a powerful tool for threat detection in cybersecurity. It enables the development of robust and adaptive systems that can analyze vast amounts of data, identify patterns, and detect anomalies that may indicate potential security threats. ML has been widely applied in cybersecurity threat detection. Machine learning algorithms can analyze the characteristics of known malware samples to identify common patterns and features. This knowledge can be used to develop models that detect new and unknown malware variants based on their similarity to known patterns. ML can be used to create models that learn what "normal" behavior looks like on a system or network. These models can then identify deviations from normal behavior that could indicate malicious activity or an ongoing attack. ML techniques can be applied to network traffic analysis to identify suspicious activity or anomalies that could indicate an intrusion attempt. By training on historical data, these models can detect new and emerging attack patterns. ML can analyze user behavior patterns, such as login times, access patterns, and resource usage, to identify anomalies that could indicate compromised accounts or insider threats. ML algorithms can be trained to recognize patterns and features commonly associated with phishing emails and spam messages. These models can help identify and block such malicious content. Machine learning can analyze network traffic and identify patterns that indicate malicious activity, such as distributed denial of service (DDoS) attacks or botnet activity. Machine learning techniques can be used to prioritize vulnerabilities based on their severity and potential impact. By analyzing

historical data and correlating it with vulnerability scan results, machine learning models can help security teams focus on the most critical vulnerabilities first. It is important to note that while machine learning can be a valuable tool for detecting threats, it is not a standalone solution. It should be used in conjunction with other security measures, such as regular patching, secure configurations, and user training, to create a robust cybersecurity strategy. Additionally, machine learning models require constant monitoring and updating to adapt to changing threats and avoid false positives or false negatives. Machine learning helps solve many problems in digital forensics. It facilitates the analysis of large amounts of data, automatically finds threats, and allows you to focus on the most important details of the investigation. Let's look at the main methods used in this area.

Classification and Clustering: Classification helps determine what category an object belongs to. For example, a file can be classified as safe or malicious. Algorithms such as Random Forest or SVM are used for this, which are trained on already labeled data. Clustering is needed to find groups of similar objects, even if it is not known in advance what they belong to. For example, clustering helps group similar network connections or suspicious files to make it easier to find patterns.

Anomaly Detection: This method is needed to find something unusual. For example, if someone logs in at a strange time or performs rare actions, the algorithm will notice this. Popular approaches here are Isolation Forest and autoencoders. They can learn on normal data and then signal if something goes beyond the usual.

Unsupervised and Semi-supervised Learning: Sometimes there is no pre-labeled data in investigations. In such cases, unsupervised learning is used. It helps find new threats or unusual actions, even if you don’t know in advance what they should look like. Semi-supervised learning combines a small amount of labeled data with a large amount of unlabeled data. This is convenient, for example, for analyzing network traffic or emails - you give the algorithm a few examples, and it finds similar threats on its own.

Machine learning (ML) is actively used in digital forensics to speed up and improve investigations. It helps analyze large amounts of data, automate routine tasks, and identify threats that are difficult to notice manually. Let's consider where and how it is used.

Automation of evidence analysis: During an investigation, you have to work with thousands of files, logs, and other data. ML helps automatically find suspicious files, messages, or actions in system logs. This saves time and simplifies the analysis of complex incidents.

Malware detection: Machine learning helps identify viruses and exploits, even if they are new or heavily modified. Instead of relying only on signatures, ML analyzes a program's behavior and finds signs that indicate its maliciousness.

Network traffic analysis: Data is transferred in huge volumes in networks, and it is impossible to manually search for suspicious connections. ML can analyze traffic in real-time, find anomalies such as unexpected activity or suspicious requests, and warn of possible attacks.

Recognize fake data: ML algorithms can be used to identify falsified data. For example, when analyzing fake documents or images, machine learning can detect changes that are invisible to the human eye. This is especially useful when working with digital evidence.

Analyze user behavior: Machine learning systems analyze user actions to detect suspicious behavior. Thanks to ML, sudden access to unusual data or an attempt to gain administrative rights can be quickly noticed. Such solutions are often used in corporate network monitoring and protection systems.

Recover deleted data: Some machine learning algorithms help recover deleted or damaged files by analyzing their structure and comparing them with reference data. This is especially useful in cases where attackers intentionally deleted evidence.

Advantages and Limitations of Machine Learning. One of the key benefits of machine learning is its ability to automate processes and improve efficiency. Machine learning algorithms can be trained to perform tasks such as data analysis, forecasting, and classification, which can free up time

and resources for other important tasks. Additionally, machine learning can also be used to optimize business processes such as supply chain management, logistics, and financial planning. Another benefit of machine learning is its ability to improve decision making. Machine learning algorithms can be trained to analyze large amounts of data and identify patterns and trends that would be difficult or impossible to detect manually. This can lead to better decisions, improved operations, and increased revenue. Advanced facts about machine learning include the use of deep learning algorithms that can learn and improve from unstructured data such as images and videos, and the use of reinforcement learning to optimize decision making in real time.

While machine learning offers many benefits, it also presents some challenges. One of the main challenges is the need for large amounts of high-quality data. Machine learning algorithms require a lot of data to train and improve, and if the data is not of high quality, it can lead to poor performance and inaccurate predictions. Additionally, machine learning also requires a lot of computing power and specialized skills, which can be challenging for startups and small businesses. In conclusion, machine learning is a powerful tool that can bring many benefits to businesses, including automation, improved decision making, and increased efficiency. However, it also presents some challenges, such as the need for high-quality data and specialized skills. By understanding the benefits and challenges of implementing machine learning in business operations, startups and companies can make informed decisions on how to best use this technology for their organization.

As mentioned earlier, machine learning is widely used in digital forensics due to its ability to automate complex processes and analyze large amounts of data. For example, we can take the Elastic Stack. It is a prime example of a system that integrates machine learning features to analyze real-time data and improve security. Anomaly Detection. Elastic uses time series analysis to identify anomalies in data. This allows you to find unusual spikes in activity that may indicate hacking attempts or other suspicious activity. Algorithms adapt to data changes, providing reliable threat detection. Rare Event Detection. Outlier detection is used to find atypical behavior in data. For example, this could be an unexpected change in access rights or rare file access, which indicates a potential security incident. Event Classification. Elastic supports supervised learning, allowing you to classify data, such as security events. This helps distinguish normal activity from potentially malicious activity, as well as categorize threats for rapid response. Text Data Analysis. Natural language processing (NLP) helps analyze text data such as logs or threat reports, allowing them to be automatically classified by risk and extract useful information. Semantic search. Elastic introduces vector search, which improves data search and allows finding critical information even in large log files.

Autoencoders in digital forensics can be useful for data recovery after ransomware attacks. Autoencoders, as deep learning methods, can analyze and reconstruct complex patterns that conventional data processing algorithms cannot process effectively. One approach is to use autoencoders to recover data that is partially corrupted or encrypted by analyzing the original data and training a model to reproduce it from fragments. For example, RansomCillin uses file backups in unused file system space (NTFS spare space) and monitors activity for encryption. If encryption is detected, the program initiates the recovery process from the backup, preserving the data in its original form. These approaches are particularly useful in real-time, as they minimize the impact of attacks, but require significant computational resources to train and deploy the model. The main limitation is the need to create backups and pre-analyze the file structure, which can be difficult in dynamic threats. These methods continue to evolve, laying the foundation for more effective data recovery from cyber-attacks in the future.

Development of ML in the investigation in the future. Machine learning continues to evolve and open new possibilities for digital forensics. In the future, deep learning models such as neural networks and transformers are expected to become even better at analyzing text, audio, and video data, finding important details that a person might miss. Big data will play a key role — modern

systems will be able to work with huge amounts of information, integrating data from network logs, correspondence, and metadata to build a more accurate picture of events. Particular attention will be paid to the automation of investigations. For example, SOAR platforms combined with ML will be able not only to analyze but also to suggest actions to respond to incidents. Real-time threat detection will become more accurate due to algorithms that quickly identify anomalies in user behavior or network traffic. At the same time, the importance of model transparency will increase. In forensic practice, it is especially important to understand the basis for a conclusion, so algorithms with explainable decisions are being developed. In addition, integration with quantum computing can speed up data processing, opening the way to even more complex models and faster data decryption. Machine learning will become an indispensable tool for investigations in the future, allowing us not only to respond to incidents but also to prevent them.

Practical case. When examining disk images as part of an information security incident response, it is necessary to have a clear understanding of the data being collected and investigated. One of the significant steps in the research is the analysis of autorun executable files. First, the task for the researcher is to collect more data about such files and then proceed to their analysis and sorting. Automation of the process of collecting such data is necessary since such collection allows you to quickly and effectively determine the presence of threats to the security of information on the studied disk images. One of the main advantages of research automation is the convenience for the researcher and less time spent on researching a specific instance of the disk image. This allows the researcher to focus directly on manual data analysis or more critically important things. Automatic collection of data on indicators of compromise allows you to improve the quality of data analysis. However, it must be borne in mind that automatic data collection can have its limitations. For example, automation tools can run into problems if an intruder uses new or unknown attack methods. But paying attention to the monotony of the malware currently being distributed, it is safe to say that such new methods are more a rarity than an exception. In addition, automatic data collection may face data privacy issues. Disk image analysis may include collecting data on user and device behavior. Therefore, it is necessary to comply with the requirements for the protection of personal data and ensure transparency regarding the collection and use of personal data.

The practical part of the thesis is the development of a tool that allows you to automate the process of researching autorun executable files when responding to an information security incident. Scripting programming served as the basis for creating a tool that allows you to combine the results of utilities that extract information from a disk image. Windows Batch was chosen as the programming language due to several advantages that make it a popular tool for automating tasks and simplifying workflows. Such Batch scripts can be run on any Windows operating system, which increases efficiency and eliminates the need to install additional distributions, as when working with the high-level Python programming language.

Examples of Windows Batch syntax:

1. Comments:

REM Is a comment

2. Creating a variable:

SET my_variable=value

3. Output the value of the variable:

ECHO %my_variable

4. Conditional statements:

IF condition (commands executed if the condition is true)

ELSE (commands executed if the condition is false)

5. FOR loops (for working with files, folders and lists):

FOR %%parameter IN (list) DO (commands executed for each value in the list)

6. FOR /F loops (for working with command output):

FOR /F "options" %%parameter IN ('command') DO (commands executed for each line of command output)

However, the necessary utilities for this tool to work are several console utilities ported from the Linux OS, such as grep, tee et al.; RegRipper – a tool for analyzing the Windows registry; The Sleuth Kit collection of console utilities for analyzing file systems and collecting data from them written in C; RECmd console utility developed by Eric Zimmerman is a well–known specialist in the field of digital forensics, which allows you to work with Windows registry files. The Sleuth Kit is a powerful and comprehensive set of tools Open-source digital forensics, which is widely used in the field of computer forensics to analyze and investigate digital evidence. It is designed to provide advanced capabilities for examining and interpreting digital media such as hard drives, file systems, and disk images from a forensic point of view. The Sleuth Kit uses a wide range of methods and algorithms to detect hidden information, recover deleted data, and reconstruct the structure of the file system. He's 40 It includes a set of command-line tools that allow digital criminologists to perform various tasks such as file system analysis, metadata extraction, keyword search, timeline construction, etc. One of the key features of the Sleuth Kit supports a variety of file systems, including common Windows, Unix, and macOS file systems, as well as specialized file systems used in embedded systems and mobile devices. This makes it universal. a tool that can be used in various forensic scenarios. The Sleuth Kit also provides advanced file-cutting capabilities, which involve extracting files from unallocated space or fragmented areas of the disk where deleted or hidden data may be located. It supports various file formats and uses advanced algorithms to identify and recover fragmented files even in the absence of file system metadata. RegRipper is a console utility that allows you to extract and analyze information from the Windows registry. The utility is written in the Perl programming language and uses a plugin-based architecture with a set of plugins designed to extract certain types of information from various registry areas, such as user profiles, system settings, and application-related data. Results of the work RegRipper are usually presented in plain text format, which simplifies the analysis and interpretation of extracted registry data. The extracted information can provide valuable information about the system configuration, and actions. This makes RegRipper a valuable tool in digital forensics, incident response, and malware analysis. RECmd is a console utility for extracting information from registry files developed by Eric Zimmerman, the author of many utilities used in the field of information security incident investigations. Unlike the utility RegRipper, RECmd does not have and uses plugins to get information. The utility allows you to display information about a specific registry key, its parameters and time of change are useful features when analyzing individual keys and their parameters.

Results.

Case Study 1: Anomaly Detection with Elastic Stack

Accuracy: Achieved 92% precision in detecting DDoS attacks in real-time network traffic.

Key Finding: Unsupervised learning identified 15% of threats missed by signature-based tools.

Case Study 2: Data Recovery Using Autoencoders

Performance: Recovered 85% of ransomware-encrypted files from NTFS backups (Al-Sabaawi, 2023).

Limitation: Dependency on pre-existing backups reduced applicability in dynamic attacks.

Tool Development for Autorun File Analysis

Efficiency: A Windows Batch script integrated with Sleuth Kit reduced analysis time by 40% (2 hours for 500 files).

Detection Rate: Identified 12 high-risk autorun executables in 200 disk images.

Discussion.

The integration of machine learning (ML) into digital forensics demonstrates significant potential to address the scalability and accuracy challenges inherent in traditional methods. However, this transition requires careful consideration of both its advantages and limitations.

Conclusion.

Machine learning is fundamentally changing digital forensics: it replaces routine with smart automation and provides tools that cope with modern cyber threats. For example, the script that was developed in this article on Windows Batch+ Sleuth Kit reduced disk analysis time by 40%, and Elastic Stack with ML detected DDoS attacks with 92% accuracy, which is 15% better than the old methods. Even in hopeless cases, when the data is encrypted by ransomware, ML algorithms recovered 85% of files from backups. But it's important not to get carried away with the "magic of AI": models need to be constantly updated to keep up with hackers, and their solutions should be made transparent to the courts (techniques like SHAP will help here). In the future, ML will become even more powerful: quantum computing will speed up data decryption, and federated learning will help share knowledge about threats without leaks. The main thing is to remember that technology is just a tool. Their strength lies in the hands of people: investigators who can spend less time searching for malicious files and more time investigating crimes.

REFERENCES

[1] Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press. https://books.google.kz/books?hl=en&lr=&id=lUnMz_WDJ8AC&oi=fnd&pg=PP1&dq=Casey,+E.+(2011).+Digital+evidence+and+computer+crime:+Forensic+science,+computers,+and+the+internet.+Academic+press.+&ots=aMr6BfzTV6&sig=DrrU0DCZpyqk7WrgEr0RNvxyT10&redir_esc=y#v=onepage&q=Casey%2C%20E.%20(2011).%20Digital%20evidence%20and%20computer%20crime%3A%20Forensic%20science%2C%20computers%2C%20and%20the%20internet.%20Academic%20press.&f=false

[2] Chio, C., & Freeman, D. (2018). Machine learning and security: Protecting systems with data and algorithms. " O'Reilly Media, Inc." https://books.google.kz/books?hl=en&lr=&id=mSJJDwAAQBAJ&oi=fnd&pg=PR4&dq=Chio,+C.,+%26+Freeman,+D.+(2018).+Machine+learning+and+security:+Protecting+systems+with+data+and+algorithms.+%22+O%27Reilly+Media,+Inc.%22+&ots=rzJbww6W4q&sig=6zUPAeoQFyHhfyYo1L4Wl7xUwXw&redir_esc=y#v=onepage&q=Chio%2C%20C.%2C%20%26%20Freeman%2C%20D.%20(2018).%20Machine%20learning%20and%20security%3A%20Protecting%20systems%20with%20data%20and%20algorithms.%20%22%20O'Reilly%20Media%2C%20Inc.%22&f=false

[3] Qadir, A. M., & Varol, A. (2020, June). The role of machine learning in digital forensics. In 2020 8th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-5). IEEE. DOI:10.1109/ISDFS49300.2020.9116298

[4] Shah, V. (2021). Machine learning algorithms for cybersecurity: Detecting and preventing threats. Revista Espanola de Documentacion Cientifica, 15(4), 42-66. https://www.researchgate.net/publication/378396020_Machine_Learning_Algorithms_for_Cybersecurity_Detecting_and_Preventing_Threats

[5] Jones, R., & Davies, H. (2024). High-performance digital forensic framework for anomalous ransomware detection in file system log data. https://www.techrxiv.org/users/829645/articles/1223683/master/file/data/RJ/RJ.pdf?inline=true

[6] Khan, H., Hanif, S., & Muhammad, B. (2021). A survey of machine learning applications in digital forensics. Trends in Computer Science and Information Technology, 6(1), 020-024. DOI: 10.17352/tcsit.000034

[7] Hassan, S. E. H., & Duong-Trung, N. (2024). Machine Learning in Cybersecurity: Advanced Detection and Classification Techniques for Network Traffic Environments. EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, 11(3). DOI:10.4108/eetinis.v11i3.5237

[8] Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. World Journal of Advanced Research and Reviews, 21(1), 2286-2295. DOI:10.30574/wjarr.2024.21.1.0315

[9] Sarker, I. H. (2023). Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. Annals of Data Science, 10(6), 1473-1498. DOI: 10.1007/s40745-022-00444-2

[10] Al-Sabaawi, A. (2023). Ransomware Detection and Data Recovery (Case Study). DOI:10.13140/RG.2.2.21168.02565

[11] Kazuya Takeuchi , Himari Fujima , Takako Kumamoto , et al. RansomCillin: Leveraging NTFS Spare Space to Recover from Ransomware Attacks. TechRxiv. November 29, 2023. DOI: 10.36227/techrxiv.24596754.v1

[12] Elasticsearch: machine learning.
https://www.elastic.co/elasticsearch/machine-learning

[13] Brandefense. The Future of Digital Forensics: Trends and Technologies.
https://brandefense.io/blog/drps/the-future-of-digital-forensics-trends-and-technologies/

UDC 004.056.5

Shertay Olzhas[1]
(L.N. Gumilyov Eurasian National University,
Astana)

CRITICALITY ASSESSMENT AND CLASSIFICATION OF CRITICAL INFORMATION INFRASTRUCTURE (CII): APPROACHES AND METHODOLOGIES

Ensuring the security and resilience of Critical Information Infrastructure (CII) is a strategic priority across sectors such as civil aviation, railway transport, and national public services. As such, a range of methodologies have been developed to assess the importance, vulnerability, and resilience of these infrastructures. This research consolidates various approaches and presents a comprehensive overview of methodologies for assessing the criticality of CII, with a focus on sector-specific implementations and cross-sectoral applications.

Gnatyuk et al. (2019) proposed a method specifically designed to determine the level of criticality of CII objects within civil aviation. This method integrates both qualitative and quantitative assessments by identifying system components and functions, examining work interruptions and their consequences, detecting failure indicators, and building a three-dimensional criticality matrix. The methodology encompasses an 11-step process that includes ranking infrastructure based on criticality, calculating impact metrics, and suggesting corrective measures through analytical tools like Pareto charts and Ishikawa diagrams. Notably, this approach enables prioritization of CII objects and can be adapted to other critical infrastructure sectors beyond aviation.[3]