

JOURNAL OF DIGITAL LAW AND INNOVATION (JDLI)

LAW • TECHNOLOGY • INNOVATION • JUSTICE

 OPEN
ACCESS

ISSN
3093-9364



OUR FIELDS

- Digital law
- Cybersecurity law
- Artificial intelligence and robotics law
- Intellectual property law
- LegalTech and legal innovations
- E-government and digital public services
- Legal aspects of AgroTech and GreenTech
- Smart city and digital governance



OUR INDEXING



Google Scholar

zenodo

Zenodo



DOI



OpenAIRE



Open Access



AI



UNAUTHORIZED
ACCESS

SYSTEM
BREACH



CYBER ATTACK



<https://unireview.uz/index.php/jdli>



Published by
UniLex Global



VOLUME 2

ISSUE 1



AUGUST 2026



“UNILEX GLOBAL” LLC

**Raqamli huquq va innovatsiya
jurnali
Journal of Digital Law and
Innovation**

**August, 2026
VOLUME 2, ISSUE 1**



EDITORIAL TEAM

Editor-in-Chief, Tukhtashev Hikmatilla Ismatillaevich - Head of the Department of Legal Sciences, Doctor of Philosophy in Legal Sciences (PhD), TIAME National Research University, Tashkent, Republic of Uzbekistan.

1. **Editorial Board Member Borotov Mirodiljon Xomudjonovich** — Doctor of Legal Sciences, Professor, Head of the Department of Civil Law, International Law and International Organizations, Institute of State and Law of the Academy of Sciences of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
2. **Editorial Board Member Maripova Sevarxon Aribjanovna** — Doctor of Philosophy in Legal Sciences (PhD), Associate Professor, Department of Social Sciences, Cyber University State University, Tashkent, Republic of Uzbekistan.
3. **Editorial Board Member Kaharova Munira Maxamajanovna** — Doctor of Political Sciences (DSc), Researcher, Institute of Criminology of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
4. **Editorial Board Member Yuldashev Mutalib Ibrohimovich** — Doctor of Economic Sciences, Professor, Department of Economics, Tashkent University of Science and Technology, Tashkent, Republic of Uzbekistan.
5. **Editorial Board Member Bafaev Shukhrat Gafurovich** — Doctor of Legal Sciences, Head of the Tashkent City Branch, Center for the Analysis of Democratic Processes, Tashkent, Republic of Uzbekistan.
6. **Editorial Board Member Khodjaeva Aziza Bakhtiyarovna** — Doctor of Philosophy in Legal Sciences (PhD), “Academy of Labor and Social Relations” under the Federation of Trade Unions of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
7. **Editorial Board Member Khudoyberdieva Viloyat Jabbrovanovna** — Candidate of Legal Sciences (PhD), Olmazor District Department of Public Education, Tashkent City, Republic of Uzbekistan.
8. **Editorial Board Member Boboumarova Munira Kurbonovna** — Doctor of Philosophy in Legal Sciences (PhD), Department for Organization of Investigative Activities, Investigation Division, Tashkent City Internal Affairs Department, Tashkent, Republic of Uzbekistan.
9. **Editorial Board Member Usmonov Vosid Muhammadievich** — Doctor of Philosophy in Legal Sciences (PhD), Diplomatic University, Tashkent, Republic of Uzbekistan.
10. **Editorial Board Member Mirzayeva Malika Baxadirovna** — Doctoral Researcher, PhD, Associate Professor, Department of Digital Technologies and Artificial Intelligence, Tashkent Institute of Irrigation and Agricultural Mechanization Engineers – National Research University, Tashkent, Republic of Uzbekistan.
11. **Editorial Board Member Allayorov Tulqin Ruziqulovich** — Doctor of Philosophy in Philology (PhD), Associate Professor, Nizami Named Tashkent State Pedagogical University, Tashkent, Republic of Uzbekistan.
12. **Editorial Board Member Tosheva Maftuna Anvar kizi** — Doctor of Philosophy in Legal Sciences (PhD), Tashkent Institute of Irrigation and Agricultural Mechanization Engineers – National Research University, Tashkent, Republic of Uzbekistan.
13. **Editorial Board Member Askarov Jaloliddin Toychievich** — Doctor of Philosophy in Legal Sciences (PhD), Deputy Head, Department of Business Law, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
14. **Editorial Board Member Abdixakimov Islombek Bahodir o'g'li** — Master of Law (LL.M), Head of the Artificial Intelligence and Legal Tech Laboratory, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
15. **Editorial Board Member Kalandarov Aminjon Amondullayevich** — Doctor of Philosophy in Legal Sciences (PhD), Acting Associate Professor, Department of Business Law, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
16. **Editorial Board Member Hakimov Komil Bakhtiyarovich** — Doctor of Legal Sciences (DSc), Professor, Head of the Department of Criminal Law, Criminology and Anti-Corruption, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.

ARTIFICIAL INTELLIGENCE AND CYBERSECURITY: THREATS OF A NEW ERA AND PROTECTION STRATEGIES

Turaeva Dilafruz

1st year student of “Cybersecurity Management”
at Cyber University State University
dilafruztorayeva08@gmail.com

ARTICLE INFO

Keywords:

information security,
artificial intelligence (AI),
cybersecurity,
machine learning,
proactive defence,
cyberattacks, anomaly
detection, automated response
(SOAR), security architecture,
system performance.

ABSTRACT

This article systematically examines current information-security challenges arising from the rapid development of digital technologies, with particular emphasis on the role and significance of artificial intelligence (AI) in cybersecurity. The study analyses the impact of machine-learning models on cyber-defence systems, including the operating principles and distinguishing characteristics of anomaly-detection algorithms and automated cyberattacks. Drawing on an applied analysis of contemporary security platforms, the article proposes scientifically grounded approaches to rapid threat processing, the optimal use of AI tools in protection systems, and the implementation of modern proactive defence architectures.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И КИБЕРБЕЗОПАСНОСТЬ: УГРОЗЫ НОВОЙ ЭПОХИ И СТРАТЕГИИ ЗАЩИТЫ

ИНФОРМАЦИЯ СТАТЬИ

Ключевые слова:

Информационная
безопасность,
искусственный интеллект
(ИИ), кибербезопасность,
машинное обучение
(Machine Learning),
проактивная защита,
кибератаки, обнаружение
аномалий,
автоматизированная
реакция (SOAR),
архитектура безопасности,
эффективность системы.

АННОТАЦИЯ

В данной статье систематически анализируются актуальные проблемы информационной безопасности в условиях стремительного развития цифровых технологий, в частности, роль и значение технологий искусственного интеллекта (ИИ) в кибербезопасности. В исследовании рассматривается влияние моделей машинного обучения на системы киберзащиты, в частности, принципы работы и отличительные особенности алгоритмов обнаружения аномалий и автоматизированных кибератак. На основе практического анализа современных платформ безопасности автором выдвинуты научно обоснованные предложения по оперативной обработке угроз, оптимальному использованию средств искусственного интеллекта в системах защиты и внедрению современных архитектур проактивной защиты.

SUN'IY INTELLEKT VA KIBERXAVFSIZLIK: YANGI DAVR TAHDIDLARI VA HIMOYA STRATEGIYALARI

MAQOLA MA'LUMOTI

Kalit so'zlar:

Axborot xavfsizligi, sun'iy intellekt (AI), kiberxavfsizlik, mashinali o'qitish (Machine Learning), proaktiv himoya, kiberhujumlar, anomaliyalarni aniqlash, avtomatlashtirilgan reaksiya (SOAR), xavfsizlik arxitekturasini, tizim samaradorligi.

ANNOTATSIYA

Ushbu maqolada raqamli texnologiyalarning jadal rivojlanishi sharoitida axborot xavfsizligining dolzarb muammolari, xususan, kiberxavfsizlikda sun'iy intellekt (SI) texnologiyalarining o'rni va ahamiyati tizimli tahlil qilinadi. Tadqiqotda mashinali o'qitish modellarining kiberhimoya tizimlariga ta'siri, xususan, anomaliyalarni aniqlash algoritmlari va avtomatlashtirilgan kiberhujumlarning ishlash prinsiplari hamda farqli xususiyatlari ko'rib chiqilgan. Muallif tomonidan zamonaviy xavfsizlik platformalarining amaliy tahlili asosida tahdidlarni tezkor qayta ishlash, himoya tizimlarida sun'iy intellekt vositalaridan optimal foydalanish hamda zamonaviy proaktiv himoya arxitekturalarini joriy etish bo'yicha ilmiy asoslangan takliflar ilgari surilgan.

INTRODUCTION

The first quarter of the twenty-first century has been marked by a profound transformation of information and communication technologies. The rapid development of digital devices, the Internet of Things (IoT), financial systems, and cloud networks has led to an exponential increase in cyberattacks and information-security threats worldwide. Cybersecurity is no longer merely a technological necessity; it has become a key driver determining the secure development of the modern economy, industry, and science. Traditional centralized protection systems and conventional security methods are increasingly losing their ability to respond effectively to the enormous volume and speed of contemporary cyber threats.

At the same time, protecting modern information systems creates serious architectural and security challenges. One of the most pressing issues facing the IT community today is ensuring the rapid, reliable, and continuous detection of threats in information systems. As cyberattacks grow in scale, speed, and diversity, anomaly detection, fault tolerance, and the optimal use of protection resources become increasingly complex. The need to move from traditional signature-based protection against known malware to proactive protection based on artificial intelligence and machine learning is becoming ever more evident.

Within the framework of the Presidential Strategy “Digital Uzbekistan – 2030”, the digitalization of all sectors of the economy, particularly public services and the financial sector, has been identified as a priority. In this process, the introduction of information-security mechanisms, the creation of reliable cyber-protection systems, and the development of architecturally resilient applications occupy a central place in state and corporate policy.

Nevertheless, national practice still lacks sufficient scientific and applied research into the specific characteristics of AI-based protection systems and their adaptation to practical projects, such as high-load networks and real-time countermeasures against cyberattacks.

The purpose of this article is to conduct a systematic comparative analysis of two major contemporary approaches in information security—artificial-intelligence-based and traditional protection systems—to identify their architectural strengths and weaknesses, and to propose effective mechanisms for optimizing the neutralization of cyberattacks under modern conditions. Particular attention is paid to anomaly detection, real-time threat processing, and improving the performance of security systems.

LITERATURE REVIEW

The increasing sophistication of cyberattacks and the growth of network threats in the context of global digitalization require a fundamental transformation of information-security systems. In this regard, the transition from traditional protection methods to artificial intelligence (AI) and machine learning (ML) technologies has been systematically examined by numerous international and domestic researchers. In particular, the role of intelligent systems in proactive cyber defence has been interpreted as follows:

N. Papernot and P. McDaniel (USA, Pennsylvania State University) demonstrated that integrating machine-learning models into security systems can substantially increase the speed of cyber-threat detection. According to their research, AI-based networks can identify zero-day attacks earlier and more accurately than conventional signature-based systems [1].

I. Goodfellow (USA) assessed the practical potential of generative adversarial networks (GANs) for developing self-learning systems in cybersecurity. The research also demonstrated that AI may serve not only as a defensive tool but also as an instrument that cybercriminals can use to automate the generation of malicious code and adversarial attacks [2].

E. Spafford (USA, Purdue University) examined models of interaction between AI and the human factor in cybersecurity risk management. His research emphasizes that, although intelligent systems are effective at filtering large volumes of security logs, complete

automation without human involvement in final strategic decision-making may lead to serious errors [3].

A.A. Ganiyev and M.M. Karimov (Uzbekistan) studied models for developing a national information-security system and protecting critical infrastructure in the digital economy. Their work highlights the importance of modern cryptographic methods and intelligent analytical mechanisms in protecting state secrets and corporate data [4].

D.R. Zaynutdinova and U.T. Aliyev investigated the effectiveness of intelligent systems in countering network attacks. Their research substantiated the scientific significance of using neural networks to predict unauthorized access to information systems through intrusion-detection systems and to support automated blocking mechanisms [5].

The reviewed literature indicates that optimizing strategies for countering cyber threats in the modern information environment is not merely a technological task but a complex intellectual challenge. Changes in the nature and automation of cybercrime require information-security systems to evolve from traditional reactive approaches toward AI architectures capable of anticipating threats and supporting autonomous decision-making [1, 4].

METHODOLOGY

Quantitatively and architecturally assessing the impact of artificial intelligence (AI) and automated security processes on cyber-defence performance is an important methodological direction in contemporary information-technology research. A comprehensive analysis requires the integration of experimental data with statistical and mathematical models, enabling the identification of causal relationships between the volume of network threats and the response speed of protection systems.

Within this study, empirical data are used to analyse the relationship between network-traffic volume in Security Operations Centres (SOCs) and the principal indicators of protection platforms—traditional signature-based and AI-based security—including threat-detection time, the number of protection nodes, and CPU/GPU resource utilization [3].

Dynamic analysis of cyber threats and protection indicators. The rapid growth of malicious code and network attacks in modern cluster systems directly affects structural changes in security architectures. According to the analysed data, the volume of cyber threats recorded in corporate networks increased at an average annual rate of 40–50% between 2020 and 2025 [4]. This process has produced two principal approaches to security: proactive

protection based on AI and neural networks, and reactive protection based on signatures (Table 1).

First, under the proactive AI-based approach, machine-learning models enable real-time detection of network anomalies. Direct intelligent analysis of cyber threats has significantly accelerated iterative prediction and streaming anomaly detection. In particular, the time required to analyse one terabyte of network logs and block a threat has been reduced from several hours in traditional defence systems to several minutes—and in some cases seconds—in AI-based systems. This demonstrates the significant performance potential of AI technologies in cyber defence.

Second, the reactive signature-based approach remains a cost-effective and stable environment for reliably blocking large volumes of known malware and processing threats against established databases. However, because each process requires comparison with and updating of malware-signature databases, delays in responding to zero-day attacks are increasing. This represents a practical manifestation of the bottleneck phenomenon in security architecture.

Table 1. C Comparative dynamics of cyber-threat detection indicators in security clusters (experimental analysis for 2020–2026)

Year	Network Traffic and Threats (TB/day)	Average Response Time of Traditional System (hours)	Average Response Time of AI System (minutes)	Number of Protection Nodes (units)	CPU/GPU Resource Utilization (%)
2020	50	4.5	45.0	15	40
2021	120	6.2	52.0	25	48
2022	250	8.8	65.0	40	58
2023	480	12.5	78.0	65	68
2024	850	16.0	95.0	90	76
2025	1,500	22.4	120.0	120	85
2026 (projected)	2,200	28.5	145.0	150	92

Cyber-defence tools exhibit a dual character: AI enables rapid proactive analysis, while traditional signatures provide high reliability and fault tolerance against known threats. This combination is driving the development of qualitatively new hybrid architectures and SOAR (Security Orchestration, Automation, and Response) solutions.

Analysis of the relationships among the presented indicators reveals the effectiveness of protection platforms in the following areas:

1. Proportionality between response time and threat volume. Between 2020 and 2026, the volume of threats increased from 50 TB to 2,200 TB, directly increasing cluster workload. While the approximately 44-fold increase in attack volume extended processing time in the traditional system by about 6.3 times—from 4.5 hours to 28.5 hours—the increase remained comparatively lower in the AI architecture due to intelligent optimization.

2. Cluster nodes as a driver of parallel protection. A tenfold increase in the number of nodes, from 15 to 150, created horizontal scaling within the security system. These resources supported not only data storage but also distributed processing of complex machine-learning models and real-time attacks such as DDoS.

3. Trade-off between speed and computing resources. The projected increase in CPU/GPU utilization to 92% in 2026 indicates the growing demand for computing resources in intelligent AI platforms. This indicator points to the risk of compute-bound constraints when designing security infrastructure.

4. Protection performance as an indicator of architectural quality. Balancing the capabilities of both technologies increases the adaptability of security resources to modern information-flow requirements. This reduces the risk of sharp performance degradation in traditional firewalls and demonstrates the architecture's resilience under high workloads.

This trend can be explained by several engineering factors.

First, the introduction of AI tools and deep-learning abstractions is enabling high-speed decision-making processes with minimal human intervention. In particular, the increasing number of cluster nodes continuously expands the ability to distribute security policies across memory resources and thus acts as an important performance driver.

Second, the expansion of the AI security ecosystem increases network adaptability and facilitates faster integration with large data centres. This contributes to reducing protection disruptions and friction among system components.

Despite these technological capabilities, improvements in threat-detection speed are not uniform across all architectural resources. Analysis of large-scale security workloads indicates that:

- CPU/GPU utilization rises sharply, increasing the likelihood of out-of-memory (OOM) errors and overheating;
- delays occur when AI models synchronize parameters across the network (network weight synchronization);

— consequently, structural imbalances between memory and processor resources become more pronounced in the allocation of protection resources.

This indicates the parallel emergence of resource-starvation and bottleneck phenomena.

Econometric analysis: Regression model. A simple linear regression model was applied to quantitatively assess the impact of distributed security-cluster indicators on threat-detection speed (Figure 1). The system response (latency) time (Y) was selected as the dependent variable, while the volume of processed network threats (X) was used as the principal explanatory variable. The model is expressed as follows [11]:

$$Y = a + bX + \varepsilon$$

where:

- a — is the initial (baseline) latency, including the initialization costs of the AI system;
- b — is the regression coefficient reflecting the effect of threat volume on latency;
- ε — is the random error capturing factors not included in the model, such as network disruptions and the complexity of zero-day attacks.

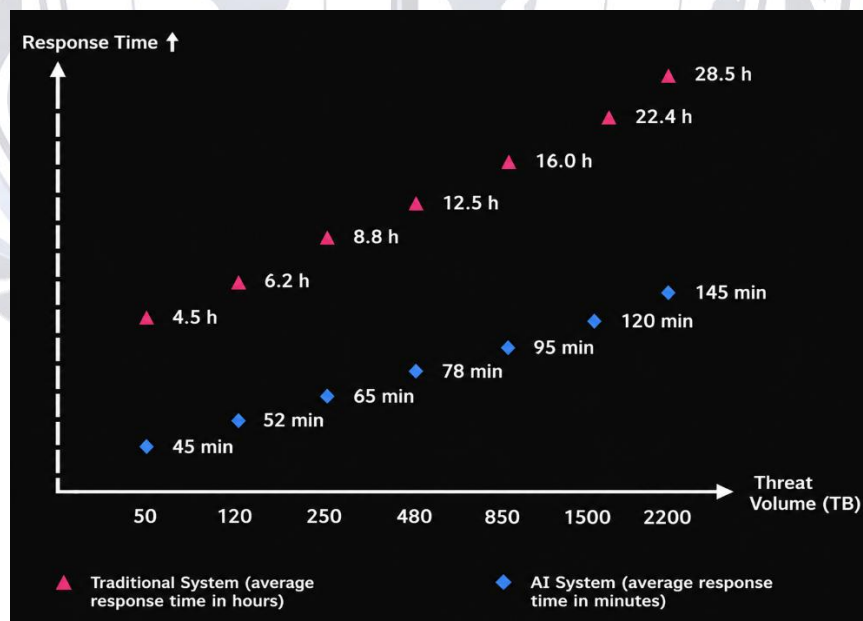


Figure 1. Linear (quantitative) relationship between cyber-threat volume and response time in AI-based and traditional security clusters.

The regression model, grounded in mathematical methodology, makes it possible to identify the functional relationship between cybersecurity-system indicators (attack volume) and defence performance.

DISCUSSION AND RESULTS

Under conditions of increasing cyberattacks and digital threats, corporate security infrastructure must evolve from the traditional function of network monitoring toward active intelligent threat analysis and automated neutralization (“insights and response”). In this process, cyber-defence architecture should function not merely as a mechanism for recording attacks but as an active defence regulator of the digital ecosystem and a driver of security decision-making. The study identifies the following priority directions and expected outcomes for improving security policy in high-load networks.

The first direction is to modernize Security Operations Centres (SOCs) on the basis of a hybrid SOAR (Security Orchestration, Automation, and Response) architecture integrating traditional signature-based protection with artificial-intelligence technologies. Under conditions of digital competition, protection systems should move beyond traditional monolithic firewalls toward data-driven, horizontally scalable defence systems capable of predicting attacks. Existing systems often rely on retrospective log files, human-dependent delays, and slow analytical mechanisms, reducing protection effectiveness and increasing the risk that zero-day attacks will remain undetected.

Accordingly, this article proposes the creation of an integrated “Intelligent Cyber Defense Platform”. The platform would combine the reliable blocking of known malware by traditional systems with deep-learning-based rapid analysis of complex anomalies, integrating security actors and tools within a unified digital-defence ecosystem.

The proposed intelligent platform would perform the following core functions:

- automatic analysis of network traffic, including real-time assessment of suspicious activity in continuous streaming data;
- processing of historical cyberattack databases, including secure analysis of large malicious-code archives using SIEM (Security Information and Event Management);
- optimization of defence algorithms, including automated recommendations to redirect threats to secure sandbox environments when available protection resources are insufficient;
- real-time SOC monitoring of CPU/GPU utilization and attack intensity across

protection nodes;

- proactive detection through machine learning to predict anomalous users or transactions.

The platform's operational algorithm consists of the following stages:

1. Data ingestion – receiving streams of logs and transactions from various sources, including servers, applications, and network devices;
2. Storage – securely storing raw security logs in an encrypted, closed file system;
3. Processing – loading network data into memory and using AI-powered parallel-search algorithms to detect anomalies;
4. Serving and response – automatically blocking analysed threats through firewall APIs and presenting them interactively to security personnel;
5. Outcome monitoring – tracking and analysing the state of the defence cluster and statistics on neutralized threats.

The proposed system is expected to produce the following outcomes:

- a 30–40% reduction in the average time required to detect and neutralize cyber threats;
- more efficient use of defence-cluster CPU/GPU resources;
- a reduction in false-positive findings and verification delays;
- improved fault tolerance and a lower risk of network failure during DDoS attacks;
- expanded capabilities for real-time threat hunting and streaming-anomaly detection.

The second direction is to introduce distributed Zero Trust and Kubernetes-based approaches to protection-resource management. To maintain stable protection performance during large-scale cyberattacks, architectural policy should move from static firewall models toward dynamic isolation and load-balancing mechanisms. Accordingly, this article proposes a cluster-based model for developing security nodes.

The proposed cluster approach is based on integrating the following elements into the defence infrastructure:

- central nodes that manage security policies (Security Managers / Master Nodes);
- local nodes that block attacks at the edge (Worker / Edge Nodes);
- distributed security logs and threat-intelligence cache areas;
- network segmentation and strict Zero Trust authentication mechanisms.

The following technological measures are proposed for practical implementation:

- infrastructure development: neutralizing malicious traffic at the nearest edge-security node before it reaches the system core;
- resource isolation: allocating precisely defined network and memory limits to suspicious programs and computing tasks through containerization in a sandbox environment;
- attack-flow management: buffering and filtering large traffic flows, such as DDoS attacks, through dedicated message brokers or filtering centres;
- scaling: automatically adding new inspection nodes to the protection cluster according to the level of risk through auto-scaling mechanisms.

As a result, the economics of security shifts away from maintaining idle reserve hardware toward a model in which resources are activated in response to actual demand during cyberattacks.

The third direction is the dynamic alignment of AI computing parameters with attack workload. Ensuring resilient defence under high-volume cyber threats requires close integration between AI algorithms and cluster configuration. At present, discrepancies between these two factors in terms of computing resources may lead to system overheating or intensify the problem of compute exhaustion.

The central element of the proposed approach is the introduction of dynamic AI model management (model tuning), regularly adjusting models to the requirements of incoming attack flows. This mechanism includes:

- excluding ordinary high-volume but safe traffic, such as video streams, from deep inspection in order to conserve resources;
- predicting data skew, where attack traffic is distributed disproportionately across protection nodes, and redistributing the workload;
- optimizing garbage collection to remove obsolete threat signatures from cache;
- integrating next-generation cyber-threat analysis formats capable of processing unstructured data.

By linking task ranking with security-resource policy:

- a threat score is assigned to each suspicious transaction or IP address;
- the priority of inspection tasks is clearly determined, distinguishing serious attacks from routine scanning;

- the system's GPUs and processing cores are allocated to the most significant risks on the basis of these indicators.

The proposed system is expected to:

- improve attack-detection quality and defence reliability;
- reduce the likelihood of system failure during high-intensity attacks such as DDoS;
- strengthen the competitiveness and resilience of corporate security architecture against contemporary hacking techniques;
- eliminate imbalances between AI protection algorithms and allocated computing resources.

CONCLUSION

Implementation of the proposed mechanisms would create a qualitatively new proactive protection model for corporate security infrastructures—one characterized by high performance and resilience to cyber threats. The model would increase the adaptability of security systems, sustainably reduce delays in threat detection and neutralization, and significantly strengthen the resilience of defence architectures against large-scale cyberattacks.

1. The exponential growth of cyberattack traffic and the limitations of traditional signature-based security systems increase the risk of network failure and intrusion. At the same time, these developments are driving the emergence of a new AI-based protection standard that requires cybersecurity engineers to possess advanced architectural and algorithmic skills.

2. The experimental analysis indicates that, to prevent bottlenecks and resource starvation caused by complex and high-intensity attacks, security clusters should continuously apply dynamic allocation of protection resources and ongoing optimization of AI models through model tuning.

3. Establishing hybrid defence architectures in Security Operations Centres—integrating traditional protection with artificial intelligence through SOAR—can reduce technological dependence on a single point of failure (SPOF) and improve the resilience of information infrastructure to unexpected high-traffic attacks such as DDoS.

REFERENCES

1. Papernot N., McDaniel P., Jha S., Fredrikson M., Celik Z.B. The Limitations of Deep Learning in Adversarial Settings. – IEEE ESSoB, 2016. – 16 p.
2. Goodfellow I., Pouget-Abadie J., Mirza M., Xu B., Warde-Farley D. Generative Adversarial Nets in Cybersecurity. – NIPS, 2014. – 13 p.
3. Spafford E.H., Schudel G. Cyber Security and Threat Intelligence. 4th Edition. – O'Reilly Media, 2019. – 756 p.
4. G'aniyev A.A., Karimov M.M. Axborot xavfsizligi tizimlari va intellektual himoya texnologiyalari. O'quv qo'llanma. – T.: "Aloqachi", 2021. – 245 b.
5. Chio C., Freeman D. Machine Learning and Security: Protecting Systems with Data and Algorithms. – O'Reilly Media, 2018. – 616 p.
6. Zaynutdinova D.R., Aliyev U.T. Tarmoq xurujlariga qarshi kurashishda intellektual tizimlar va neyron tarmoqlar. Monografiya. – T.: "Fan va texnologiya", 2022. – 180 b.
7. Liao H. Artificial Intelligence for Cybersecurity: A Survey. – Springer, 2019. – 120 p.
8. Gulyamov S.S., Ayupov R.H. Raqamli iqtisodiyotda axborot xavfsizligi va proaktiv mudofaa modellari. Darslik. – T.: TMI, 2022. – 310 b.
9. Haluska T., Haluska M. Artificial Intelligence in Cyber Security: Lightning-Fast Threat Analysis. – O'Reilly Media, 2020. – 276 p.
10. Karimov M.M. Zamonaviy kiberxavfsizlik infratuzilmasi va intellektual tahlil. O'quv qo'llanma. – T.: TATU, 2021. – 210 b.
11. Mukkamala S., Sung A.H. Cyber Security and AI: Principles and best practices of scalable realtime threat systems. – Manning Publications, 2018. – 328 p.
12. Buczak A.L., Guven E. Comparative Analysis of Machine Learning Methods for Cyber Security Intrusion Detection. – IEEE Communications Surveys & Tutorials, 2016. – 18 p.