International Journal of Basic and Applied Sciences, 14 (2) (2025) 281-287

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/bh5z5x68
Research paper

Opportunities for Applying Artificial Intelligence by Commercial Organizations in Data Security and Cyber Threat Monitoring

Anna Poluyan [1]*, Olga Purchina [2], Dmitry Fugarov [2]

[1] Department of Computer Systems and Information Security, Faculty of Computer Science and Computer Engineering, Don State Technical University, 1 Gagarin Square, Rostov-on-Don, 344003, Russia
[2] Department of Automation and Mathematical Modeling in the Oil and Gas Industry, Energy and Oil and Gas Industry Faculty, Don State Technical University, 1 Gagarin Square, Rostov-on-Don, 344003, Russia
**Corresponding author E-mail: AnnaPoluyan1@mymail.academy*

Received: March 18, 2025, Accepted: June 19, 2025, Published: June 21, 2025

Abstract

Intelligent information security methods are approaches based on the use of artificial intelligence and machine learning to increase the level of information protection and combat cyber threats. This is especially important for the financial sector and e-commerce since hackers and fraudsters aim at these companies, and any error by their personnel can lead to large expenses and loss of customer trust. The objective is to determine the opportunities for using AI by commercial organizations in the field of data protection and cyber threat monitoring. To attain this end, the authors conducted an experiment, i.e., they selected 100 companies and divided them into two groups, in each of which they applied AI algorithms to monitor cyber threats, and in one of the groups, they held two online classes on increasing the level of literacy in the field of information security. The study results show that the use of AI algorithms increased protection against cyber threats by 54%, while the efficiency of companies with additional employee training grew by another 27%. The main conclusion is that the use of AI in data security requires substantial data volumes and powerful computing resources. Therefore, a proper plan for the use of AI technologies, combined with personnel training, can significantly increase the protection of information systems and optimize implementation costs.

Keywords: *Information; Machine Learning; Network Traffic; Personnel Training; Protection Systems; Security.*

1. Introduction

Artificial intelligence is a powerful tool for ensuring the security of digital systems [1, 2]. The complexity of information security tasks is growing from year to year [3, 4] as cyber threats are becoming increasingly complex [5]. Among the methods of using AI in information security, first, we would like to mention machine learning [6, 7], deep learning [8], neural networks [9, 10], and data analysis [11].
AI-based methods significantly facilitate the task of protecting against cyberattacks [12] and more efficiently and accurately identify threats [13]. Technologies like Field-programmable gate arrays are gaining popularity due to their low-power requirements, parallelism, and re-configurability.Das and Sandhane [14] also highlighted in their study that field gate arrays rapidly build and adapt neural networks to changes in risk. AI expert systems such as Darktrace and Cylance incorporate self-learning and deep learning to explore solutions to difficulties posed by a client or a certain technology in a particular technical sector. They may also be utilized primarily for decision-making support. Post-2023 transformer models such as GPT-4, CodeBERT, and APTGuard have been applied in malware and phishing detection. Islam et al. [15] concluded that the CodeBERT model excels at discovering and classifying software vulnerabilities in code, reaching 95% accuracy. Technologies such as 'zero trust architecture (ZTA)' that use zero trust principles to plan industrial and enterprise infrastructure and workflows have also been under study. Rose et al. [16] reiterated that zero trust architecture prioritizes securing resources, such as assets, services, workflows, and network accounts, rather than network segments, as network location is no longer the primary factor in resource security. Although this looks promising, threats such as subversion of ZTA decisions and network disruptions can render this framework vulnerable.
In the field of information security, AI is most often used to monitor threats [17]. Many monitoring systems use machine learning algorithms and neural networks to detect threats and anomalies in network operations. This allows for preventing complex cyber-attacks before they can cause serious damage [18]. Such systems use machine learning algorithms to build models of attacker behavior, which more effectively block suspicious traffic and separate it from normal traffic [19]. Recent studies have shown that apart from monitoring threats and anomaly detection, machine learning can also be applied in behavioural analytics by creating baselines of regular user activities within an organization and identifying compromised accounts and potential insider threats. Machine learning can also go beyond detection and

can be applied in automated response systems. AI-ML systems can detect data breaches, isolate vulnerable systems, restrict suspected user accounts, and follow established reaction processes to reduce the effect of attacks [20].
The use of intelligent methods to detect malicious code is also an important task in the field of information security. In this area, AI is used to create more accurate and diverse malware classification models and detect malware signatures [11].
The information contained in logs can also be used to identify threats and determine suspicious activity. The use of machine learning and data analysis methods helps quickly and accurately process large volumes of logs and identify hidden threats. However, AI methods are not universal solutions and require a deep understanding of the problem, as well as the expertise and assessment of information security specialists. For example, AI methods are used for detecting phishing websites. Some of these methods include analyzing web page content, checking the URL, and using blacklists. Proactively tackling AI-based security risks is critical in an industrial context that includes smart factories, autonomous systems, CPS, IoT, cloud computing, and big data. In this way, AI has the potential to automatically give substantial cybersecurity insights without requiring human intervention. AI and machine learning (ML) have the potential to alter cybersecurity and information sharing in cyberspace [21].

2. Literature Review

As various studies show, AI-powered applications are used in many areas of information security [22, 23]. One of the most common areas is the protection of personal data. Processing large arrays of personal information requires a high level of confidentiality. For this purpose, AI is used to create algorithms for encrypting and decrypting information, identifying suspicious activity, and preventing data leaks [1, 11]. AI-based encryption techniques create more complex and reliable algorithms that are more difficult to brute force. In addition, AI can be used to monitor network traffic and detect suspicious activity [24]. For example, AI can detect when a user is trying to access restricted data or when an unusual request is sent to the server. If AI detects such suspicious activity, it can automatically block access to data and notify the administrator of an unauthorized access attempt.
The creation of AI-based encryption algorithms and the monitoring of network activity help protect personal data from unauthorized access and leaks [25]. However, the security of information systems often depends not only on technical solutions but also on the company's security culture and the training of its employees [26, 27]. The rapid advancement of AI technologies has created room for data exploitation. Guembe et al. [28] highlighted that malicious actors can utilize AI approaches to improve reconnaissance to investigate typical behavior and operations concerning a cybersecurity defensive mechanism, computer infrastructures, and devices. AI technologies can also be used in target profiling, password cracking, and for forecasting cyber breach outcomes, which is a double-edged sword. One notable example of emerging AI threats is the use of deep-fake technology, which allows attackers to produce realistic audio and video impersonations. This feature has been used for social engineering assaults, such as mimicking executives in phishing scams, considerably increasing the chances of successful deception. Furthermore, AI-powered botnets have emerged as a significant danger, with attackers using machine learning to optimize the operation of widespread networks of hacked devices. These botnets can adapt to defenses, coordinate large-scale attacks, and improve their evasion abilities. These offensive applications show the potential for malevolent use of AI, requiring careful defensive measures to combat cyber adversaries' developing methods [29]. The possibilities of AI-generated cyber threats are as endless as the opportunities it presents by implementing it in cybersecurity. From AI-powered ransomware to AI-robust phishing, the paradox surrounding AI and cybersecurity requires scrutiny to avoid abuse [30].
This research focuses on improving the monitoring of data security. The main objective is to determine the possibilities of using AI in monitoring cyber threats for companies to protect their commercial, financial, and banking information using AI-driven methods and additional training sessions for company employees.

3. Experiment Description

To achieve this objective, an experiment was conducted in 2023, and 100 companies were selected using a non-random (non-probability) quota sampling method. The selection criteria were as follows: a company should work in the financial or e-commerce sphere and employ at least 100 people. The company selection procedure lasted for three months. E-mails were sent to the management of companies from different regions of Russia to participate in an experiment and increase the level of security in protecting personal data and monitoring cyber threats. An important condition for experimenting was to select companies that do not regularly train their employees to improve their literacy in the field of protection against cyber threats. After this selection, the companies were divided into two groups (experimental and control), 50 companies in each of them.
In parallel with the company selection, the dataset for AI training was prepared as follows:
The training dataset used for the AI model consisted of approximately 18,000 records collected from internal user activity logs provided by participating companies. Each record contained 12 key features, including login frequency, session duration, access time, device type, location metadata, access to sensitive files, and action outcome (e.g., read/write/delete), among others. The target variable was labeled as action_type, categorized into normal and potentially anomalous behavior based on rule-based internal logs. To preserve privacy, all user identifiers were anonymized, and the data was preprocessed to ensure uniform formatting and remove noise. The dataset was balanced to ensure equal representation of anomalous and typical user behavior to prevent model bias.
To address potential sampling bias, a non-random quota sampling strategy was employed, stratifying companies by sector (e-commerce vs. financial) and ensuring geographic and organizational diversity (company size, number of employees, and regional representation). This approach ensured that the final group of 100 companies reflected a cross-section of the Russian commercial cybersecurity landscape.
The main difference between the experimental group and the control group was that the experimental group and company employees were given two classes to improve their literacy in the field of saving their personal data and basic knowledge of assessing the possibility of cyber threats during the experiment.
Based on the objective of the experiment, we put forward two hypotheses:
H0 claims that it is enough to introduce AI tools to achieve maximum efficiency in reducing cyber threats.
H1 claims that it is necessary to introduce AI algorithms and train personnel to achieve maximum efficiency in reducing cyber threats.

4. Monitoring Stages

Standard requirements for protecting an information system include the following security elements that should be implemented:

- Data encryption. Data encryption is the process of converting information into a format that becomes unreadable without the use of an encryption key.
- Access control. Access control is the process of regulating access to confidential information and systems. This can be implemented using passwords, biometric data (e.g., fingerprint scanners), or two-factor authentication.
- Firewalls. Firewalls are network devices that monitor incoming and outgoing network traffic to protect servers from potential threats. They can block malicious traffic and protect the network from DDoS attacks.
- Patches and updates. Software updates are a critical method for ensuring the security of web servers. Such patches address newly discovered vulnerabilities and update the system with the latest libraries and software.
- Security audits. A security audit is the process of examining server security to identify and eliminate vulnerabilities and ensure compliance with regulatory requirements.
- Incoming traffic filtering. Incoming traffic filtering is a method of controlling the flow of network traffic directed at a web server.

All these standard protection methods must be implemented together, forming a system that further enhances security. The decision on which protection method to use depends on the business's capabilities and the criticality level of the data.

It should be noted that all the aforementioned tools have, to some extent, the known drawbacks of signature-based analysis methods: the inability to detect new attacks that have not yet been described in the knowledge base of anomaly detection systems; the possibility of bypassing such systems by altering the attack methodology (e.g., changing the sequence of operations); and a sharp increase in required system resources when expanding the signature database, among others.

This explains the interest in integrating these attack detection methods with other promising approaches, primarily methods for detecting anomalies in network traffic or user actions in computer networks.

The article proposes the integration of standard information security methods and artificial intelligence.

The structural diagram of AI-based security monitoring consisted of the actions described in Table 1.

Table 1: Security Monitoring Algorithm

Step	Title of the step	Explanation
1st	Data Collection	Collect data on user actions, system events, network traffic, and other security-related parameters
2nd	Data Processing	Analyze the collected data using AI technologies like machine learning and neural networks. The analysis can be conducted based on the accumulation of data.
3rd	Threat Detection	Identify potential security threats such as anomalous user behavior and unauthorized access attempts
4th	Threat Reaction	Notify operators about potential threats.

This sequence of actions was implemented using Python, which provides many opportunities for writing AI networks [31].

5. Algorithm Description

Let us look at the steps of the algorithm:

1) Import the necessary libraries for data analysis

: importpandasaspd

importnumpyasnp

2) Load data about user actions in the system. Here, we load data about user actions from a CSV file named user_actions.csv into a DataFrame format. This file implies that it contains records of user actions with various attributes.

data=pd.read_csv('user_actions.csv')

3) Convert the data into a format suitable for analysis by machine learning. At this stage, we split the data into input and output:

X: This is the feature matrix representing all columns except user_id and action_type. user_id is not needed for modeling because a user's ID does not determine their behavior, and action_type is the target variable.

y: This is the target variable containing the values of action_type that we want to predict (i.e., how anomalous the user's actions are).

X=data.drop(columns= ['user_id', 'action_type'])

y=data['action_type']

4) Train the machine learning model on historical data. At this step:

- We import RandomForestClassifier from the sklearn library. This is a powerful machine learning algorithm that uses an ensemble of decision trees for classification.
- We create an instance clf, which will represent our model.
- We train the model using the fit () method, passing the input data X and the target variable y to it.

fromsklearn.ensembleimportRandomForestClassifier

clf=RandomForestClassifier ()

clf.fit (X, y)

5) Get data on current user actions and predict the likelihood of abnormal behavior. We load the current data about user actions from the file current_user_actions.csv. Using the trained model (clf), we obtain the predicted class probabilities for the current data using the predict_proba () method. The input data for this method are the current actions without user_id. The method returns to an array of probabilities, where for each example, the probability of belonging to each class is specified.

current_data=pd.read_csv('current_user_actions.csv')

predictions=clf.predict_proba (current_data. drop(columns=['user_id']))

6) Analysis of the predictions and measures to prevent attacks. A check is performed to determine if there is at least one value for the anomalous class (presumably, the second class) among the predicted probabilities that exceed the threshold of 0.9. If such a value is detected, the functions send_alert_email () and block_user_account () are triggered, sending a notification about anomalous behavior and

blocking the user account, respectively. If no anomalous behavior is detected, the current data is saved to the database using the save_to_database () function.

```
if any (predictions [:1]>0.9):
send_alert_email ('Detected abnormal user behavior')
block_user_account ()
else:
save_to_database(current_data)
```

Load the data about user actions from a file, convert it into a format suitable for machine learning, train the model, and use it to analyze current user actions [24]. If the model detects any abnormal behavior, a notification is sent by email, and the user's account is blocked. During the experiment, e-mail was not blocked, and information was stored in the database.

6. Data Processing

To process the obtained data and select companies for the experiment and further data processing, Yandex. Documents were used. We calculated Student's t-test in Excel.

7. Results

The results of the experiment proved that AI could detect and prevent cyberattacks, as well as analyze the behavior of attackers in secure cloud systems [32], which are becoming popular among users [33]. For example, the companies that participated in the survey use a cloud platform to store and process their data. To protect data from cyberattacks and other threats, we recommend that companies use AI to detect anomalies in network traffic and analyze attacker behavior. AI can monitor incoming and outgoing requests to a server to identify unusual traffic patterns that could indicate an attempted cyber-attack or other suspicious activity [34]. AI can analyze logs to identify patterns of attackers' actions, such as the time of their activity, the use of certain programs, etc. [35]. Based on this analysis, AI can create attacker profiles and use this data to detect suspicious activity and prevent cyberattacks [36].

Assessing data security in a company is critically important for ensuring the security of information systems. There are various intelligent methods used for analyzing and evaluating security. One such method is vulnerability scanning. Automated tools such as Nessus, OpenVAS, and Nikto scan systems to identify known vulnerabilities, using vulnerability databases and performing tests to detect weaknesses. Penetration testing involves simulated attacks on web servers to identify and exploit vulnerabilities, which can be performed manually or using automated tools like Metasploit. The process includes information gathering, vulnerability discovery, vulnerability exploitation, and reporting of results.

To automate the described procedure of risk analysis and management, a software tool called Fuzzy Cognitive Maps (FCM) Builder has been developed. This tool allows for modeling the situation of protecting information resources of a particular department. Factors (target, basic, information resources, destabilizing, and control factors) are added to the model, and cause-and-effect relationships between them are established. The input characteristics for this program are:

a) Factor type.
b) Factor name.
c) factor state variable.
d) initial and limit values of the state variable.

Next, the values of total effects are calculated to assess the impact of destabilizing factors on target factors. After this, both individual components of information risks and the overall risk for the department are calculated. A set of countermeasures—measures aimed at eliminating or reducing the impact of information security threats—is then determined. Based on the identified countermeasures, new values of total effects from the impact of destabilizing factors on target indicators are computed, and information risks are recalculated considering the implemented countermeasures.

The results of the experiment conducted in two groups demonstrate that the use of integrating AI and standard methods has significantly improved the protection of company data against potential threats (Table 2). The effectiveness of the implementation was calculated using the formula:

$$\Delta = \frac{R - R'}{R} * 100\% \quad (1)$$

where:
R is the risk assessment before implementing additional measures, specifically the artificial intelligence algorithm.
R' is the risk assessment after implementing additional measures, specifically the artificial intelligence algorithm.

Table 2: Comparison of Protection Efficiency Between Control and Experimental Groups

Group	AI Implemented	Employee Training	Increase in Protection Efficiency
Control Group	Yes	No	54
Experimental Group	Yes	Yes	81 (including +27% from training)

This table illustrates the comparative efficiency of cybersecurity threat mitigation between two groups of companies. Both groups implemented AI algorithms for monitoring, but only the experimental group received additional employee training. The experimental group showed a total increase in protection efficiency of 81%, including a 27% improvement attributed to staff awareness training.

In the financial sphere, where privacy and transaction security are critical [37], AI should provide an additional layer of protection. Based on the study results, we highlight that AI can be used to identify suspicious transactions and record anomalies in financial transactions [38]. For instance, a bank uses AI algorithms to monitor financial transactions. AI algorithms can analyze ongoing transactions and identify unusual patterns that may indicate fraudulent transactions or other suspicious activity. AI can also automatically analyze customer transactions and identify transfers to unfamiliar countries, unusually large transactions, or multiple transactions from different devices in a short time. If AI detects suspicious activity, it can send a notification to the bank's control center to analyze the transaction in more detail, and either block it or contact the account owner to verify the authenticity of the transaction. During the experiment, we showed that AI can be

used to create fraud prevention algorithms. For example, AI can analyze a customer's data and transaction history to determine which transactions seem to be normal for that customer [39]. If AI detects an unusual operation, it sends a notification to the control center for further verification.

This use of AI increases the level of protection against cyber threats for banks, which helps protect their clients from potential fraudulent transactions and other types of financial crimes. This is especially important for small banks with limited resource capabilities. However, AI should be used in combination with other security methods, such as staff training and two-factor authentication [40].

E-commerce is also becoming popular [41], and its security plays a key role in the effective operation of online stores and other electronic platforms [11, 42]. The results of the study showed that the integration of AI and standard methods increased the level of protection against cyberattacks and data leaks by 57% after the implementation of our algorithm, compared to standard protection measures. Additionally, we confirmed that for Russian e-commerce, the development of AI can significantly enhance effectiveness, several times, in creating personalized offers and recommendations for users based on the analysis of their behavior. AI algorithms can analyze data about customer purchases, preferences, and behavior to create personalized offers and recommendations for each user. AI aims to ensure the security of electronic payments and guarantee protection against cyberattacks [11].

AI-powered e-commerce personalization ensures the security of online stores. It also helps attract customers and protect their data from potential threats [44, 44]. In our opinion, effectiveness can be achieved when AI is used in combination with other security methods, such as SSL encryption and two-factor authentication, to ensure the maximum protection of user data.

Thus, we proved that AI-based security systems have many advantages, such as increasing efficiency, automating processes, reducing costs, and increasing the speed of response to threats [45].

One of the main advantages is the ability to increase the efficiency of data protection and quickly respond to threats [46]. AI functions, such as machine learning and analysis of large arrays of data, can quickly identify vulnerabilities in systems and prevent cyberattacks [47, 48]. Automating processes and using AI can also reduce information security costs. Most security tasks can be performed by AI algorithms without the need to hire additional employees [49]. AI systems can quickly respond to a changing threat and prevent potential attacks before they cause serious damage [50, 51].

According to some scientists, their use can have several serious disadvantages and risks [52].

One of the main risks is a potential threat to confidentiality. AI algorithms can process large amounts of data, including personal information, which can lead to data leaks and privacy violations [53]. In addition, errors in AI algorithms are a serious disadvantage of this technology in the sphere of information security [54]. Erroneous data analysis or incorrect threat identification can lead to false positives and failures in security systems [55]. The potential abuse of AI is also a security risk. Hackers can use AI to create more complex and sophisticated cyberattacks, making them more difficult to detect and prevent [56].

Thus, the use of AI in information security has both advantages and disadvantages and requires a comprehensive understanding of technology and the expertise of information security specialists. With the right approach, AI can significantly improve data security and ensure network efficiency. The observed improvements in security efficiency were interpreted considering established best practices, such as the NIST SP 800-53 framework, which outlines control baselines for anomaly detection, access management, and incident response.

The main conclusion is that the possibility of using AI by commercial organizations in the field of data protection and monitoring cyber threats will be effective if they have specific strategies for using AI in information security. Such strategies should be developed based on performance assessment. The strategy should define the goals, objectives, and expected results, as well as the methods and technologies used to achieve these goals. Machine learning can be quickly set up to process new data, but it requires substantial data volumes to be trained on. Neural networks can create more accurate models of attacker behavior but setting them up can be a complex and compute-intensive process. Data analysis allows creating detailed data sets but involves qualified specialists and personnel who are familiar with the basics of information security. Thus, the H1 hypothesis was confirmed, i.e., to achieve maximum efficiency in reducing cyber threats, it is necessary to introduce AI algorithms and train personnel.

8. Conclusion

AI methods in information security can be used to prevent cyberattacks, protect personal data, analyze user activity, and fulfill other tasks. We need to consider both the advantages and disadvantages of these technologies and find solutions that will provide high security with minimum interference in the privacy of users. An important advantage of using AI in information security is the ability to automate processes to quickly respond to threats and protect digital systems. Therefore, it is necessary to constantly improve AI and find a balance between security and the protection of personal data, as well as train company employees in the basics of information security. Beyond immediate benefits, there are significant theoretical ramifications to the incorporation of AI in cybersecurity that demand attention. The inability of machine learning to adjust to adversarial intelligence is one such implication. AI is excellent at finding patterns in large datasets, but because it is based on historical data, it is susceptible to new or zero-day threats that are designed to avoid detection. A basic asymmetry in cyber defense is brought to light by these learning constraints: defenders must foresee every potential attack vector, while attackers must identify just one vulnerability. Furthermore, bias and over-fitting risks are introduced by AI's reliance on training data, which could result in missed threats or false positives.

Furthermore, concerns about transparency, accountability, and ethical governance surface as AI systems increasingly make security decisions on their own. This emphasizes the necessity of human-in-the-loop designs that strike a balance between supervision and automation.Given these theoretical ramifications, enhancing AI technologies is insufficient. Strong frameworks for AI auditability, adversarial resilience, and ethical deployment must also be established by researchers and practitioners. A multidisciplinary strategy that combines computer science, cognitive theory, and cyber law will be essential to ensure AI's safe and long-term deployment as it continues to transform cybersecurity.

References

[1] Kaur R, Gabrijelčič D & Klobučar T (2023), Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804

[2] Kirillova EA, Zulfugarzade TE, Blinkov OE, Serova OA & Mikhaylova IA (2021), Prospects for developing the legal regulation of digital platforms. Jurídicas CUC 18(1), 35-52. https://doi.org/10.17981/juridcuc.18.1.2022.02

[3] Eskerkhanova LT, Beloglazova LB, Masyutina NM, Romanishina TS & Turishcheva TB (2023), Increasing the competitiveness of future economists for work in Industry 4.0. Perspectives on Science and Education 2, 158-173. https://doi.org/10.32744/pse.2023.2.9

[4] Bayazitova R, Kaishatayeva A & Vasilyev A (2023), Working from home, telework, equality and the right to privacy: A study in Kazakhstan. Social Sciences 12(1), 42. http://dx.doi.org/10.3390/socsci12010042

[5] Vasyukov VF, Bocharov AV, Kashina E & Singilevich DA (2021), Cyberstalking as a type of cybercrime: Counteraction opportunities in Russian and international legislation. Revista Relações Internacionais do Mundo Atual 2(35), 1-16.

[6] Akhmetshin E, Fayzullaev N, Klochko E, Shakhov D & Lobanova V (2024), Intelligent data analytics using hybrid gradient optimization algorithm with machine learning model for customer churn prediction. Fusion: Practice and Applications 14(2), 159-171. http://dx.doi.org/10.54216/FPA.140213

[7] Abdullaev I, Prodanova N, Ahmed MA, Lydia EL, Shrestha B, Joshi GP & Cho W (2023), Leveraging metaheuristics with artificial intelligence for customer churn prediction in telecom industries. Electronic Research Archive 31(8), 4443-4458. http://dx.doi.org/10.3934/era.2023227

[8] Akhmetshin E, Nemtsev A, Shichiyakh R, Shakhov D & Dedkova I (2024), Evolutionary algorithm with deep learning based fall detection on Internet of things environment. Fusion: Practice and Applications 14(2), 132-145. http://dx.doi.org/10.54216/FPA.140211

[9] Kazakov O, Azarenko N & Kozlova I (2024), Developing a method for building business process models based on graph neural networks in the absence of task identifier data. Qubahan Academic Journal 4(1), 19-25. https://doi.org/10.58429/qaj.v4n1a333

[10] Chumakova EV, Korneev DG, Gasparian MS, Ponomarev AA & Makhov IS (2023), Building a neural network to assess the level of operational risks of a credit institution. Journal of Theoretical and Applied Information Technology 101(11), 4205-4213, available online: http://www.jatit.org/volumes/Vol101No11/8Vol101No11.pdf

[11] Angin P, Bhargava B & Ranchal R (2019), Big data analytics for cyber security. Security and Communication Networks 2019, 4109836. https://doi.org/10.1155/2019/4109836

[12] Dokholyan S, Ermolaeva EO, Verkhovod AS, Dupliy EV, Gorokhova AE, Ivanov VA & Sekerin VD (2022), Influence of management automation on managerial decision-making in the agro-industrial complex. International Journal of Advanced Computer Science and Applications 13(6), 597-603. http://dx.doi.org/10.14569/IJACSA.2022.0130672

[13] Iskajyan SO, Kiseleva IA, Tramova AM, Timofeev AG, Mambetova FA & Mustaev MM (2022), Importance of the information environment factor in assessing a country's economic security in the digital economy. International Journal of Safety and Security Engineering 12(6), 691-697. https://doi.org/10.18280/ijsse.120604

[14] Das R & Sandhane R (2021), Artificial intelligence in cyber security. Journal of Physics Conference Series, 1964(4), 042072. https://doi.org/10.1088/1742-6596/1964/4/042072

[15] Islam MA, Islam R, Chowdhury SA, Nur AH, Sufian MA & Hasan M. (2024), Assessing Cybersecurity Threats: The application of NLP in advanced threat intelligence systems. In Lecture notes in networks and systems (pp. 1–14). https://doi.org/10.1007/978-3-031-70924-1_1

[16] Rose S, Borchert O, Mitchell S & Connelly S (2020), Zero trust architecture. Stafford, VA, Cybersecurity & Infrastructure Security Agency Department of Homeland Security. https://doi.org/10.6028/nist.sp.800-207

[17] Purchina O, Poluyan A & Fugarov D (2021), Hybrid immune algorithms application for solving unclear optimization problems. In Parinov IA, Chang SH, Kim YH & Noda NA (eds) Physics and mechanics of new materials and their applications. PHENMA 2021. Springer, Cham, pp. 591-596. https://doi.org/10.1007/978-3-030-76481-4_50

[18] Fugarov DD, Gerasimenko EY & Gerasimenko AN (2021), Modeling of electric mass transfer process in controlled electrochemical resistance. Journal of Physics: Conference Series 2131, 042050. https://doi.org/10.1088/1742-6596/2131/4/042050

[19] Purchina O, Poluyan A & Fugarov D (2023), An algorithm based on artificial intelligence for solving information security tasks. E3S Web of Conferences 371, 03066. http://dx.doi.org/10.1051/e3sconf/202337103066

[20] Khan MI, Arif A & Khan ARA (2024), The most recent advances and uses of AI in cybersecurity. BULLET: Jurnal Multidisiplin Ilmu, 3–3(04), 566–578.

[21] De Azambuja AJG, Plesker C, Schützer K, Anderl R, Schleich B & Almeida VR (2023), Artificial Intelligence-Based Cyber Security in the context of Industry 4.0 – A survey. Electronics, 12(8), 1920. https://doi.org/10.3390/electronics12081920

[22] Vaslavskaya I, Aboimova I, Aleksandrova I, Nekrasov K & Karshalova A (2023), Achieving the principles of sustainable development: Implementation of smart solutions in the infrastructure of modern megacities. E3S Web of Conferences 449, 05001. https://doi.org/10.1051/e3sconf/202344905001

[23] Rakhimgalieva P, Serikbayeva N, Seiitkazy P, Kaishatayeva A & Suleimenova Z (2021), Adaptation of students to professional activity through innovative technologies. World Journal on Educational Technology: Current Issues 13(4), 1102-1123. http://dx.doi.org/10.18844/wjet.v13i4.6312

[24] Auganbai A, Kalymbek B, Shulanbekova GK, Urisbaeva AA & Yerezhepkyzy R (2020), Protection of objects of historical and cultural heritage: Legal problems and the application of information technologies. Environmental Policy and Law 49(6), 379-388. https://doi.org/10.3233/epl-190191

[25] Ydyrys S, Ibrayeva N, Abugaliyeva F, Zhaskairat M & Uvaliyeva A (2023), Regulatory and legal support for the development of digital infrastructure in rural areas as a factor in improving the level of sustainable development and quality of life of the rural population. Journal of Environmental Management and Tourism 14(5), 2271-2280. https://doi.org/10.14505/jemt.v14.5(69).08

[26] Bezpalov V, Goncharenko L, Fedyunin D, Lochan S & Avtonomova S (2023), Developing a model of work duration under the influence of risk events in the implementation of life cycle contracts for large energy construction projects. Journal of Infrastructure, Policy and Development 7(3), 1946. http://dx.doi.org/10.24294/jipd.v7i3.1946

[27] Borodina M, Idrisov H, Kapustina DA, Zhildikbayeva A, Fedorov D, Gerasimova E & Solovyanenko N (2023), State regulation of digital technologies for sustainable development and territorial planning. International Journal of Sustainable Development and Planning 18(5), 1615-1624. http://dx.doi.org/10.18280/ijsdp.180533

[28] Guembe B, Azeta A, Misra S, Osamor VC, Fernandez-Sanz L & Pospelova V (2022), The emerging threat of AI-driven cyber-attacks: a review. Applied Artificial Intelligence, 36(1). https://doi.org/10.1080/08839514.2022.2037254

[29] Mohammed A (2023), AI and Machine Learning in Cybersecurity: Strategies, Threats, and Exploits. Innovative Computer Science Journal, 9(1), 1–4. https://innovatesci-publishers.com/index.php/ICSJ

[30] Syed SA (2025), Adversarial AI and Cybersecurity: Defending Against AI-Powered Cyber Threats. IRE Journals, 8(9), 1030–1031. https://www.researchgate.net/publication/390555579

[31] Deitel P & Deitel H (2019), Python for artificial intelligence, big data, and cloud computing. Pearson, 600 p.

[32] Burkov A (2018), The hundred-page machine learning book. MIT Press, London, 500 p.

[33] Purchina O, Poluyan A & Fugarov D (2022), Securing an information system via the SSL protocol. International Journal of Safety and Security Engineering 12(5), 563-568. https://doi.org/10.18280/ijsse.120503

[34] Poluyan AYu, Fugarov DD, Purchina OA, Nesterchuk VV, Smirnova OV & Petrenkova SB (2018), Adaptive algorithm of selecting optimal variant of errors detection system for digital means of automation facility of oil and gas complex. Journal of Physics: Conference Series 1015, 022013. http://dx.doi.org/10.1088/1742-6596/1015/2/022013

[35] Kirillova EA, Zenin SS, Parshin IA, Predbannikova OI & Rubakova II (2022), Cyberbullying among students in an educational institution: Opportunities for counteraction. International Journal of Computer Science and Network Security 22(5), 602–606. https://doi.org/10.22937/IJCSNS.2022.22.5.83

[36] Purchina O, Poluyan A & Fugarov D (2021), The algorithm development based on the immune search for solving unclear problems to detect the optical flow with minimal cost. E3S Web of Conferences 258, 06052. https://doi.org/10.1051/e3sconf/202125806052

[37] Kirillova E (2023), Developing methods for assessing the introduction of smart technologies into the socio-economic sphere within the framework of open innovation. International Journal of Sustainable Development and Planning 18(3), 693-702. https://doi.org/10.18280/ijsdp.180305

[38] Francois C (2017), Deep learning with Python. Manning Publications, New York, NY, 384 p.

[39] Fugarov D (2023), Technological control of the granulometric composition of active materials of chemical current sources. In Guda A (ed) Networked control systems for connected and automated vehicles. NN 2022. Springer, Cham, pp. 1417-1423. https://doi.org/10.1007/978-3-031-11051-1_145

[40] Poluyan AYu, Purchina OA, Fugarov DD, Golovanov AA & Smirnova OV (2019), Solution of task on the minimum cost data flow based on bionic algorithm. Journal of Physics: Conference Series 1333(3), 032056. http://dx.doi.org/10.1088/1742-6596/1333/3/032056
[41] Khlynin E, Korovkina N, Zhukov R, Kozlova N & Myasnikova E (2023), Effect of information and communications technology on the efficient operation of the organizational and economic mechanism of enterprise fixed assets management. Relações Internacionais do Mundo Atual 2(4), e-0630766 available online: https://revista.unicuritiba.edu.br/index.php/RIMA/article/view/6376
[42] Bagratuni K, Kashina E, Kletskova E, Kapustina D, Ivashkin M, Sinyukov V, Karshalova A, Hajiyev H & Hajiyev E (2023), Impact of socially responsible business behavior on implementing the principles of sustainable development (experience of large business). International Journal of Sustainable Development and Planning 18(8), 2481-2488. https://doi.org/10.18280/ijsdp.180819
[43] Kozinkina AI (2020), A magneto dielectric AC measuring transducer for refinery automation systems. Journal of Machinery Manufacture and Reliability 49(11), 963-970.
[44] Fugarov DD, Purchina OA, Poluyan AYu, Gerasimenko AN & Rasteryaev NV (2019), Magnetodielectric AC measuring transducer for automation systems in oil refineries. Journal of Physics: Conference Series 1333(6), 062020. http://dx.doi.org/10.1088/1742-6596/1333/6/062020
[45] Cherckesova L, Revyakina E, Safaryan O, Porksheyan V & Kazaryan M (2024), Analysis of the possibilities of carrying out attacks on the functions of transferring control to operating system console using active intelligence methods. International Research Journal of Multidisciplinary Scope 5(2), 516-534. http://dx.doi.org/10.47857/irjms.2024.v05i02.0558
[46] Gerasimenko Y, Gerasimenko A, Gerasimenko Y, Fugarov D, Purchina O & Poluyan A (2021), Mathematical modeling and synthesis of an electrical equivalent circuit of an electrochemical device. In Murgul V & Pukhkal V (eds) International scientific conference energy management of municipal facilities and sustainable energy technologies EMMFT 2019. Springer, Cham, pp. 471-480. http://dx.doi.org/10.1007/978-3-030-57453-6_45
[47] Goodfellow I, Bengio Y & Courville A (2016), Deep Learning Network. MIT Press, London, 800 p.m.
[48] Aggarwal C (2018), Neural networks and deep learning. Springer, Cham, 360 p.
[49] Fugarov DD, Gerasimenko YY, Nesterchuk VV, Gerasimenko AN & Onyshko DA (2018), Methods for revealing hidden failures of automation system for technological processes in the oil and gas sector. Journal of Physics: Conference Series 1118, 012055. http://dx.doi.org/10.1088/1742-6596/1118/1/012055
[50] Purchina O, Poluyan A & Fugarov D (2023), Improving the security level of the information system using the SSL protocol. E3S Web of Conferences 371, 30-67. http://dx.doi.org/10.1051/e3sconf/202337103067
[51] Akhmetshin E, Kirillova E, Abdullayev I, Fedorov A, Tretyak E & Kochetkov E (2024), Legal status and the issues of legal personhood of artificial intelligence. Relacoes Internacionais no Mundo Atual 1(43), 356-366, available online: https://revista.unicuritiba.edu.br/index.php/RIMA/article/view/6722
[52] Fugarov D (2022), Development and mathematical modeling of the AC sensor for refinery automation systems smart innovation. Systems and Technologies 247, 271-281.
[53] Geron A (2018), Hands-on machine learning with Scikit-Learn, Keras, and TensorFlow. O'Reilly Media, Incorporated, Sebastopol, CA, 800 p.
[54] Purchina O, Poluyan A & Fugarov D (2023), Building algorithms based on artificial intelligence for solving problems to ensure information security. In Parinov IA, Chang SH & Soloviev AN (eds) Physics and mechanics of new materials and their applications. Springer, Cham, pp. 568-573. https://doi.org/10.1007/978-3-031-21572-8_50
[55] Fugarov D & Gerasimenko Y (2023), Mathematical modeling of electrolyte concentration field in the controlled electrochemical resistance. In Beskopylny A, Shamtsyan M & Artiukh V (eds) XV International scientific conference “INTERAGROMASH 2022”. Springer, Cham, pp. 1688-1695. https://doi.org/10.1007/978-3-031-21432-5_181
[56] Sutton RS & Barto AG (2018), Reinforcement learning: An introduction. 2nd ed. MIT Press, London, 552 p.