BULLETIN of Cherkasy State Technological University

Journal homepage: https://bulletin-chstu.com.ua/en

Vol. 31 No. 3. 2026

UDC 004.056:004.85
DOI: 10.62660/bcstu/3.2026.92

ISSN: 2306-4412
E-ISSN: 2708-6070

Information technologies for critical-infrastructure cybersecurity based on machine learning methods

Anatolii Benzar*

Associate Professor
Zakhidnodonbaskyi Institute of the Private Joint Stock Company "Higher Education Institution "The Interregional Academy of Personnel Management"
51408, 400/1 Dniprovska Str., Pavlohrad, Ukraine
https://orcid.org/0000-0002-0943-0109

Abstract. The relevance of the study is determined by the growing number of multi-stages cyberattacks on industrial and corporate networks, which requires a shift from signature-based protection mechanisms to adaptive intelligent systems for threat analysis and forecasting. The purpose of the study was to assess the effectiveness of machine learning for detecting and forecasting cyber threats in the critical infrastructure of the energy sector and to develop an automated cybersecurity architecture. The study analysed cyber threats to energy infrastructure using cyber-event data, prepared the data, trained and compared machine learning models, and then selected the most effective models for implementing the protection system. The study established that cyber threats to critical energy infrastructure have become more complex because information networks are integrated with process control systems. Analysis of incidents in 2022-2025 indicated an increase in the number and complexity of attacks, with control systems, industrial controllers, and server infrastructure being the most vulnerable infrastructure components. A cybersecurity system based on machine learning was developed; it provides event analysis, anomaly detection, and threat forecasting. The gradient boosting model demonstrated the highest effectiveness, with classification accuracy of 96.4%, detection recall of 94.9%, and an F1-score of 95.3%. The time-series analysis model showed a strong capacity to forecast complex attacks with an accuracy of 95.2%. The integration of machine learning models reduced incident detection time to 11 minutes, response time to 39 minutes, and the false-positive rate to 6.8%. The results confirm the effectiveness of machine learning in improving the accuracy, speed, and adaptability of cybersecurity systems for critical infrastructure. The results of the study can be used by cybersecurity specialists, protection-system developers, and critical-infrastructure operators in the energy sector to improve cyber-threat detection and response

Keywords: energy sector; Supervisory Control and Data Acquisition system; industrial control systems; Security Information and Event Management system; anomaly detection; attack forecasting; artificial intelligence

INTRODUCTION

The relevance of the study is determined by the increasing number and complexity of cyber risks to the critical infrastructure of the energy sector, where traditional signature-based protection mechanisms no longer ensure an adequate level of adaptability and speed of response. The increase in attacks on Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS), corporate networks and industrial infrastructure segments necessitates the development of intelligent methods for cyber event analysis that are capable of detecting anomalies, predicting multi-stage attacks and automating response procedures. Therefore, the implementation of machine learning (ML) methods is getting importance for the improvement of

Article's History: Received: 10.04.2026; Revised: 12.08.2026; Accepted: 21.09.2026; Published: 07.10.2026

Suggested Citation:
Benzar, A. (2026). Information technologies for critical-infrastructure cybersecurity based on machine learning methods. *Bulletin of Cherkasy State Technological University*, 31(3), 92-104. doi: 10.62660/bcstu/3.2026.92.

*Corresponding author (benzaranatolii@outlook.com)

Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/)

the efficiency of the monitoring, classification and prediction of cyber risks in critical infrastructure systems of the energy sector.

In the Ukrainian academic discourse, the research in critical-infrastructure cybersecurity is increasingly focused on the assessment of cyber-risks, the improvement of cyber-resilience, and the use of artificial intelligence (AI) methods for detecting and forecasting attacks. R.K. Murasov *et al.* (2025) investigated approaches to assessing and managing risks of cyberattacks on critical infrastructure systems. The researchers found multi-stage attacks were becoming so complex that traditional signature-based mechanisms were no longer enough and they needed to move to adaptive monitoring and analytics models that could quickly detect anomalous activity. They also talked about integrating tools for analysing network events and automating incident response processes. The research of I.V. Stotskyi *et al.* (2025) was devoted to the use of standard AI algorithms to detect and block cyberattacks in military information systems. The researchers have shown that using standard AI algorithms speeds up the detection of threats and reduces the load on the operators of cybersecurity systems. The results confirmed the effectiveness of the ML models in high network-event intensity and the importance of quick response to cyber incidents.

A.A. Mishok *et al.* (2026) presented a different perspective by examining strategies for ensuring the cyber resilience of critical information infrastructure under conditions of hybrid warfare and global technological challenges. The researchers justified the need to develop multi-level cybersecurity systems combining monitoring, analytics, forecasting, and automated incident-response mechanisms. The study showed that the integration of ML-oriented approaches with Security Information and Event Management (SIEM) and Intrusion Detection System/Intrusion Prevention System (IDS/IPS) systems improved the adaptability of cybersecurity and supported more effective detection of complex attacks on critical infrastructure. A. Abisoye *et al.* (2025) analysed the capabilities of AI and ML models in forecasting cyber risks in critical infrastructure. The researchers indicated that the use of ensemble algorithms and neural networks increased the accuracy of anomaly detection and reduced incident response time under conditions of high network-event intensity. A. Uzzaman & M.A. Rony (2023) considered the application of ML models for protecting industrial automation systems and critical infrastructure. The researchers demonstrated that ML algorithms provided more effective detection of anomalous activity in SCADA/ICS systems than conventional rule-based approaches, especially in cases of multi-stage and hidden attacks.

S. Otoum *et al.* (2021) presented a comprehensive analysis of ML-based intrusion detection systems. The study established that integrating ML algorithms with IDS/IPS systems improved cyber-threat classification accuracy, reduced the false-positive rate, and increased the adaptability of cybersecurity systems to new types of attacks. A. Idowu *et al.* (2025) reported similar results in a study of ML-oriented solutions for protecting smart grids and critical infrastructure. The researchers noted that the use of ML models increased the resilience of energy systems to cyber threats through automated analysis of telemetry data, behavioural analytics, and forecasting of potential incidents. Further research on ML-oriented cybersecurity of critical infrastructure focused on the development of adaptive monitoring systems and automated response to cyber threats. A. Kalnawat *et al.* (2024) examined the role of ML algorithms in protecting critical infrastructure. The researchers indicated that the use of ML models increased the speed of cyber-threat detection, improved analysis of behavioural anomalies, and ensured the adaptation of security systems to a dynamic attack environment. Similarly, K.J. Raval *et al.* (2024) argued for integrating ML with network monitoring and cyber-event analysis systems. The researchers reported that the combination of behavioural analytics, attack forecasting, and automated response improved the cyber resilience of energy and industrial systems. The study by A. Kumar & J.A. Gutierrez (2025) analysed the impact of ML on the effectiveness of intrusion detection systems for critical-infrastructure protection. The researchers demonstrated that ML-oriented IDS provided higher attack-classification accuracy, better detection of hidden anomalies, and a substantial reduction in false positives compared with conventional signature-based mechanisms.

Despite the considerable number of studies devoted to the use of ML methods in cybersecurity, academic literature has paid insufficient attention to the comprehensive integration of ML models with SIEM, IDS/IPS, and SCADA/ICS systems specifically in the context of critical energy infrastructure. Most existing studies focused either on general tasks of detecting network attacks or on individual aspects of intrusion detection systems without considering the specific interaction between Information Technology (IT) and Operational Technology (OT) segments. Issues of the adaptability of ML-oriented systems to high-load event flows, forecasting of Advanced Persistent Threat (APT) multi-stage attacks, and automated response to cyber incidents in the real operating environment of energy enterprises remain insufficiently studied. The purpose of the study was to assess the effectiveness of information technologies for ensuring cybersecurity of critical infrastructure in the energy sector based on ML methods and to develop an ML-oriented architecture for detecting, forecasting, and automatically responding to cyber threats. The study set the following tasks: to analyse existing cyber threats to critical energy infrastructure and determine the features of using ML methods for their detection and classification; to conduct a comparative assessment of the effectiveness of ML models in

analysing network events, forecasting attacks, and automatically responding to cyber incidents.

MATERIALS AND METHODS

The study had a combined theoretical and empirical design and was conducted in 2022-2025 in Dnipropetrovsk Oblast. The sectoral context covered energy-sector enterprises of the DTEK Group, particularly DTEK Pavlohradvuhillia, as an example of complex cyber-physical infrastructure. The empirical data of the study were formed by adapting open datasets on critical-infrastructure cybersecurity and configuring them according to the characteristics of corporate and industrial environments in the energy sector, with reference to the specific features of the infrastructure of DTEK Pavlohradvuhillia. Open scientific datasets of cyber incidents and attacks on industrial systems were also used to align the structure, typology, and scenarios of cyber events, including global cyber-incident datasets from the European Repository of Cyber Incidents, EuRepoC; industrial incidents and attacks on critical infrastructure (RISI dataset); and open data on incidents affecting critical infrastructure of Ukraine. The internal dataset was based on network-traffic logs containing parameters of Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) connections, Internet Protocol (IP) interaction, the volume and frequency of transmitted data, and temporal characteristics of network activity.

The empirical basis of the study was formed from aggregated cyber-monitoring data on critical infrastructure, including network traffic, Security Information and Event Management logs, Intrusion Detection and Prevention System alerts, user authentication events, and telemetry data from industrial control systems. The datasets used contained information on normal network activity, anomalous events, and cyber-threat scenarios, including availability attacks, unauthorised-access attempts, and atypical node behaviour. After pre-processing, cleaning, and anonymisation, a unified dataset was formed and used to train, validate, and test ML models.

The study used systematic analysis of academic publications and a comparative-generalising method to identify current approaches to applying ML algorithms in cybersecurity, assess their effectiveness, and determine prospects for integration into critical-infrastructure protection systems. Experimental testing and comparative analysis of ML models on cyber-event data from critical infrastructure were used to assess the effectiveness of Random Forest, XGBoost, Artificial Neural Network (ANN), Long Short-Term Memory (LSTM), and Isolation Forest algorithms. Comparative analysis was applied to assess the effectiveness of conventional signature-based approaches (SIEM, IDS/IPS) in comparison with ML-oriented methods. Systems analysis of information flows was used to examine the interaction between IT and OT components of the infrastructure of DTEK Group enterprises, particularly DTEK Pavlohradvuhillia. Network flows, server interaction, SCADA/ICS components, Programmable Logic Controller (PLC), Remote Terminal Unit (RTU) controllers, and monitoring systems were analysed, which supported the identification of critical vulnerability points and the structuring of data sources for further modelling. Response time to cyber incidents was defined as the time interval between the initial recording of an anomalous event by monitoring systems and the first response action, such as node isolation, blocking of suspicious activity, or transfer of the incident for processing. For each year, the mean value was calculated from registered events, and changes in response speed were then compared.

An experiment involving noise modelling in the feature set was conducted to assess the resistance of ML models to input-data distortion. Noise was generated by artificially introducing random changes into numerical parameters of network traffic and event logs, including the number of connections, data-transmission frequency, traffic volumes, and temporal characteristics of node activity. For 15% of randomly selected records, feature values were changed by adding Gaussian noise while preserving the initial class structure. Cyber-threat labels were not changed, which supported assessment of the effect of input-data quality degradation specifically on model classification accuracy.

The cyber-threat classification method was used to systematise incidents by attack type and the nature of their impact on infrastructure. An architecture of an ML-oriented cybersecurity system for critical infrastructure was developed, integrating event collection and correlation modules, an ML analytics block, automated response mechanisms, and a security-process management layer. The study applied a set of ML models for detecting, classifying, and forecasting cyber threats in critical energy infrastructure. Random Forest and XGBoost algorithms were used to classify network events and determine attack types; ANN was used to analyse complex nonlinear dependencies; LSTM was used to process temporal sequences of cyber events and detect multi-stage attacks; and Isolation Forest was used to detect unknown anomalies. Model training was conducted using features derived from network traffic, event logs, authentication data, and attack indicators. Before modelling, the data were normalised, balanced, and divided into training and test samples using cross-validation to check the stability of results. Models were implemented and tested in Python using the Scikit-learn and TensorFlow libraries. Wireshark was used for network-traffic collection and analysis, while Splunk Enterprise Security and Elastic Stack SIEM solutions were used for aggregating and correlating security events. Data storage and processing were carried out using SQL- and NoSQL-based solutions, which supported work with structured event logs and large telemetry datasets.

The effectiveness of ML models was assessed using Accuracy, Precision, Recall, F1-score, and ROC-AUC

metrics, which comprehensively characterised the quality of cyber-threat classification. Accuracy was used to assess the overall correctness of event classification, while Precision and Recall separately characterised the quality of attack detection and the false-positive rate. F1-score was used for a comprehensive assessment of the balance between precision and detection recall, and ROC-AUC was used to compare the capacity of models to distinguish normal from anomalous activity regardless of classification thresholds. The results were used to select the most effective models for further integration into the cybersecurity system. The experimental comparison determined the feasibility of using XGBoost for cyber-event classification tasks and LSTM for analysing temporal sequences and forecasting complex attacks. The integrated ML-oriented system was then assessed using indicators of detection and incident-response time, false-positive rate, and cyber-threat forecasting accuracy.

RESULTS

Analysis of the state of cybersecurity of critical infrastructure. Analysis of the operation of energy-infrastructure facilities showed that cybersecurity has ceased to be an auxiliary means of technical information protection, and has become an important strategic element of the continuity of production processes, energy stability and technological reliability of enterprises. The greatest threat for enterprises in the energy sector is complex multi-level cyberattacks, including attacks targeting the disruption of automated process control systems, gaining control over corporate networks, destabilising telecommunications infrastructure and obtaining unauthorised access to production information. The active introduction of digital technologies and the deepening of the interaction between information networks and operational technologies have increased the potential intrusion paths for attackers, which significantly complicates the use of conventional network-protection models.

Energy companies are susceptible to targeted attacks including a long-term hidden presence in the network environment and slow penetration to critical infrastructure elements. The study proved that such attacks are associated with movement between network segments, obtaining elevated access rights, and exploiting previously unknown software vulnerabilities, making them difficult to detect in a timely manner by conventional monitoring tools. The study also indicated an increase in attacks aimed at exhausting network resources and phishing campaigns to steal employee credentials. The main types of cyber risks to critical energy infrastructure are shown in Table 1.

Table 1. Main types of cyber threats to critical energy infrastructure

Threat type	Main mechanism of impact	Potential consequences
Availability attacks (including DDoS)	Overloading network resources and disrupting service availability	Loss of availability of information and technological systems
Unauthorised access (phishing, vulnerability exploitation)	Compromise of credentials or exploitation of system weaknesses	Access to critical infrastructure components
Atypical node behaviour (anomalous activity, insider threats)	Deviation from normal patterns of network interaction	Violation of system integrity and hidden malicious activity

Source: compiled by the author using analysis of data from DiXi Group (n.d.)

The synthesis of cyber-threat types shows the development of a complex multi-vector risk profile for critical energy infrastructure, where individual attacks combine to form multi-stage compromise scenarios. Critical attacks are a combination of social engineering, exploiting vulnerabilities, and hidden intrusion. It impacts the availability, integrity, and confidentiality of the systems. The evolution of isolated incidents to more complex integrated scenarios require the use of ML techniques for the detection of hidden patterns in cyber dangers. The study of cyber-incident dynamics in 2022-2025 using DTEK infrastructure as an example identifies a stable tendency towards an increasing number of attacks and greater attack complexity. At the initial stage, attacks aimed at disrupting service availability and phishing campaigns predominated, while in 2023-2025 combined scenarios affecting information and operational segments of energy infrastructure became dominant. Analysis of incidents within control systems, network infrastructure, and technological components shows that the greatest increase in cyber threats occurred during periods of higher load on energy facilities and during large-scale crisis events (Table 2). The results confirm the need to apply adaptive threat-detection mechanisms to ensure the resilience of DTEK infrastructure.

Table 2. Dynamics of cyber incidents in DTEK infrastructure (2022-2025)

Year	Number of recorded incidents	Share of critical incidents, %	Mean response time, min
2022	412	18.6	94
2023	587	24.3	81
2024	731	31.8	67
2025	846	36.5	54

Source: compiled by the author

The dynamics of incidents in DTEK infrastructure in 2022-2025 indicate a stable increase in the number and criticality of cyber threats. The increased share of complex attacks points to a transition towards more targeted scenarios of impact on critical infrastructure. The simultaneous reduction in response time reflects increased maturity of cybersecurity processes and the introduction of automated mechanisms for monitoring and event analysis. Some industrial controllers and dispatching systems of energy infrastructure operated using outdated data-exchange protocols, which limited authentication, encryption, and information-integrity control. The analysis identifies human-machine interfaces, programmable logic controllers, remote terminal units, and servers for storing technological data as the most vulnerable elements of the industrial environment. The main causes of risk are identified as outdated software, insufficient network segmentation, weak access control, and the complexity of updating systems without stopping production processes.

Cyber incidents affect not only information resources but also the technological stability of energy processes. The consequences of attacks include disruption of automated control systems, delays in transmitting technological data, loss of control over individual equipment components, and the need to switch to manual control. This causes downtime, extra recovery costs, and a higher workload for cybersecurity units. The results confirm the insufficiency of conventional protection methods for the current threat level and justify the use of ML methods for automated anomaly detection, attack forecasting, and improved adaptability of cybersecurity systems.

Development of the architecture of an ML-oriented cybersecurity system. The analysis demonstrates that conventional approaches to cybersecurity, based mainly on signature-based attack detection and manual incident processing, do not provide an adequate level of adaptation to new cyber threats. Accordingly, a cybersecurity system architecture is proposed, based on the integration of Security Information and Event Management platforms, intrusion detection and prevention systems, behavioural-anomaly analysis tools, and ML modules capable of automated real-time classification of cyber events. The developed architecture is characterised by a multi-level organisation of data collection, processing, and correlation, which integrates telemetry information from corporate networks, server infrastructure, industrial controllers, Supervisory Control and Data Acquisition systems, network monitoring tools, and access-control systems. Unlike conventional centralised protection models, the proposed approach creates a single analytical environment for comprehensive analysis of relationships between security events at different levels of information infrastructure. The general structure of the developed system is presented in Figure 1.

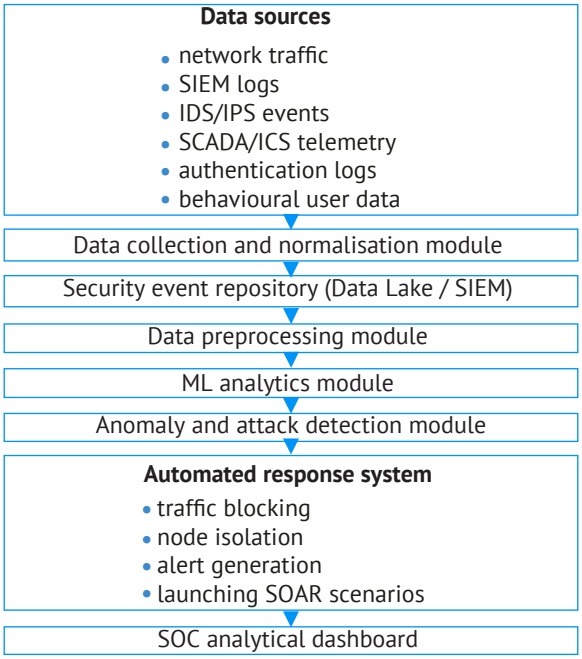


Figure 1. Architecture of an ML-oriented cybersecurity system
Source: developed by the author

The architecture development process indicates that the effectiveness of the cybersecurity system depends on the integration of the security-event management platform and intrusion detection and prevention systems with ML modules. The proposed architecture provides centralised data collection from network, server, and industrial sources, followed by event normalisation and structuring. The combination of

signature-based, behavioural, and temporal analysis improves the accuracy of incident correlation and complex cyber-threat detection. In the system, the security-event management platform functions as an analytical centre for information processing, while intrusion detection systems provide primary detection of suspicious activity. ML integration automates threat classification and shifts cybersecurity from a reactive to a proactive approach.

Results of ML model training. A generalised analysis of ML model assessment results shows their uneven effectiveness depending on algorithmic nature and capacity to adapt to complex characteristics of cyberspatial data (Table 3).

Table 3. Comparative results of ML model effectiveness

Model	Accuracy, %	Precision, %	Recall, %	F1-score, %	ROC-AUC
Random Forest	94.8	93.9	92.7	93.3	0.957
XGBoost	96.4	95.8	94.9	95.3	0.978
ANN	92.6	91.4	89.8	90.6	0.931
LSTM	95.1	94.6	93.8	94.2	0.969
Isolation Forest	88.7	86.9	84.5	85.7	0.882

Source: developed by the author

The results emphasise that the gradient boosting model achieves the highest classification accuracy and stability due to its ability to effectively capture complex nonlinear dependencies among features. The recurrent neural network is the most effective model for analysing temporal sequences and detecting hidden anomalies in dynamic network traffic. The study also confirms the importance of data-processing speed for cybersecurity systems of critical infrastructure because delays in event analysis can contribute to the spread of incidents and negatively affect the stability of production processes. The Random Forest algorithm provides the shortest mean cyber-event processing time, while the recurrent neural network has the highest computational complexity because it must analyse temporal dependencies between events (Fig. 2).

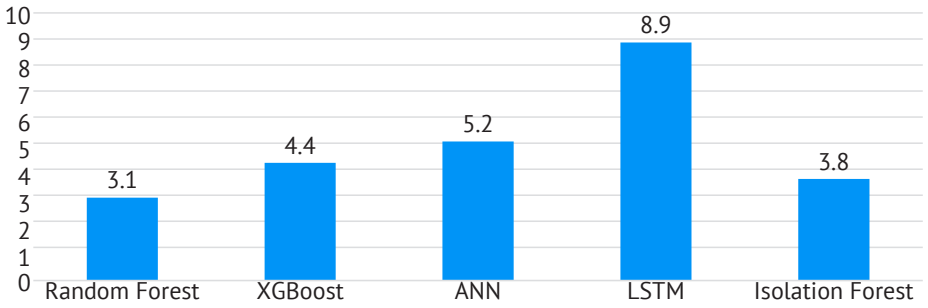


Figure 2. Mean cyber-event processing time for 10,000 events by model, s

Source: developed by the author

Comparison of temporal characteristics identifies a relationship between model complexity and suitability for real-time operation. Ensemble methods provide the highest processing speed, which makes them effective for primary monitoring and filtering of cyber events. Gradient algorithms provide a balance between accuracy and speed, while neural networks have higher computational costs because of the complexity of analysing temporal dependencies. Anomaly detection methods without training on labelled data have medium speed and complement the multi-level protection system because of their capacity to detect unknown threats. The results confirm the feasibility of combining models depending on the stage of cyber-event analysis. The experiment shows that, under conditions of high-load corporate networks, the trade-off between processing speed and classification accuracy is critical. For this reason, the optimal solution is the combined use of fast models for primary event filtering and deep neural networks for detailed analysis of complex anomalies. The analysis also demonstrates that Random Forest and XGBoost have the highest resistance to noise because of the ensemble nature of the algorithms, while ANN models are more sensitive to distortion of data structure (Table 4).

Table 4. Resistance of models to noise in input data

Model	Decrease in accuracy with 15% noise, %
Random Forest	-2.1
XGBoost	-1.8
ANN	-6.5

Continued Table 4.

Model	Decrease in accuracy with 15% noise, %
LSTM	-3.4
Isolation Forest	-4.2

Source: developed by the author

The results confirm that the ensemble models are the most robust to noise in the input data with a degradation of accuracy of only 1.8-2.1%. This means they can maintain classification stability as the data quality degrades. The recurrent neural network is moderately sensitive to noise whereas ANN is the most vulnerable model, losing accuracy up to 6.5%. The anomaly detection method without labelled data is in the middle and provides an acceptable operational performance under unstable conditions. The results suggest that a hybrid approach that uses resistant ensemble models in conjunction with more complex algorithms is capable of analysing cyber events in depth. Independent testing of models for detecting the most widespread cyber risks to critical energy infrastructure shows that their effectiveness depends on the type of attacks and the features of network activity. The Random Forest algorithm and the gradient boosting model have the best results in the detection of distributed denial of service attacks. The gradient boosting model has a precision of 97.3% and a recall of 96.1%, while the Random Forest algorithm has 95.1% and 93.8%, respectively. This demonstrates their high efficiency in detecting anomalous growth of network load and atypical node activity (Table 5).

Table 5. Effectiveness of DDoS attack detection

Model	Precision, %	Recall, %
Random Forest	95.1	93.8
XGBoost	97.3	96.1
ANN	91.7	89.2
LSTM	94.8	95.4

Source: developed by the author

The results of the analysis of phishing and insider threats indicate that neural models provide higher effectiveness by considering behavioural characteristics of users, temporal dependencies, and atypical activity scenarios. ML models improve the detection of hidden threats compared with conventional signature-based approaches, especially when analysing insider attacks and anomalous network traffic. Comparison of Random Forest and XGBoost demonstrates the advantage of XGBoost in classification accuracy for complex dependencies, while Random Forest is characterised by higher processing speed and suitability for operational monitoring. The LSTM model shows the best results in detecting multi-stage attacks because of its capacity to analyse sequences of events over time.

Synthesis of the ML model assessment results confirms that XGBoost is the most effective model for further integration into the critical-infrastructure cybersecurity system. It demonstrates the highest classification indicators (Accuracy – 96.4%, Precision – 95.8%, Recall – 94.9%) and the best resistance to noise changes in input data, providing an optimal balance between accuracy and event-processing speed. Unlike deep learning models, XGBoost is characterised by lower computational complexity, which makes it suitable for real-time operation. LSTM retains an advantage in detecting complex temporal dependencies and is used as an extra analytical module for deeper analysis of multi-stage attacks. Therefore, within the proposed architecture, XGBoost is selected as the main model for classifying cyber threats; it increases detection accuracy, reduces the number of false positives, and improves the effectiveness of automated response.

Integration of machine learning models into the cybersecurity system and assessment of effectiveness. Experimental testing results show that the implementation of the ML module reduces incident detection and response time compared with conventional approaches (Table 6). Delays are reduced through automated event correlation, fewer manual checks, and the use of behavioural analysis.

Table 6. Comparison of cyber-incident response time

Approach	Mean detection time, min	Mean response time, min
Conventional event-analysis systems	41	94
Rule-automation systems	28	73
ML-oriented system	11	39

Source: developed by the author

The comparative analysis indicates that integration of the ML module substantially improves the speed of response to cyber incidents through automated event correlation, behavioural analysis, and reduced

manual checking. The ML-oriented approach provides faster detection of complex threats and improves the effectiveness of cyber-event flow processing compared with conventional mechanisms. The results confirm the feasibility of shifting from static analysis rules to an adaptive cybersecurity model capable of considering context and relationships between events. The number of false positives was assessed using a test event set with a controlled ratio of normal to anomalous activity. The comparison emphasises that ML models provide better differentiation between legitimate and suspicious behaviour than conventional mechanisms (Table 7). The values presented reflect the results of experimental model comparison rather than the absolute level of false positives in an industrial environment, where mechanisms for context enrichment, prioritisation, and multi-level event filtering are also applied.

Table 7. Results of reducing the false-positive rate

Approach	False-positive rate, %
Conventional event analysis	27.4
Rule-based analysis	18.9
ML-oriented analysis	6.8

Source: developed by the author

The data obtained confirm that the application of ML models improves the quality of event classification by considering behavioural characteristics and the context of network activity. The best results are provided by the ensemble algorithms XGBoost and Random Forest because of their resistance to noise and capacity to work with large data flows. LSTM demonstrates an advantage in detecting attacks that develop gradually and are characterised by temporal dependencies between individual events. A separate test set containing event sequences with multi-stage attack scenarios was used to assess the capacity of the system to forecast threats. The results indicate that ML models outperform rule-based approaches in forecasting accuracy because they consider not only individual events but also their relationships over time (Table 8).

Table 8. Cyber-threat forecasting accuracy

Method	Forecasting accuracy, %	Detection recall, %
Rule-based analysis	71.2	66.4
Random Forest	89.3	87.1
XGBoost	93.6	91.8
LSTM	95.2	94.1

Source: developed by the author

The results emphasise that consideration of temporal dynamics and complex dependencies between events substantially increases the capacity of the system to forecast the development of cyber threats. Models based on sequence analysis are the most effective in that they can detect hidden patterns that are characteristic of multi-stage attacks. A further characteristic of ensemble algorithms is high forecasting stability as they can generalise heterogeneous features and reduce the effect of random deviations in data. Overall, the results confirm that adaptive ML models are better than static rules for early detection and prediction of complex cyber incidents. Results of the integration experiment show that the best model for further implementation in the cybersecurity system is XGBoost that offers the best ratio of accuracy, processing speed and resistance to changes in data structure. Random Forest is to be used as a fast module for initial event filtering, while LSTM can be used for deeper analysis of complex temporal attack scenarios. The selected XGBoost model is the basic building block for the next architecture for detecting and classifying cyber assaults.

DISCUSSION

Analysis of academic publications shows a growing interest in the use of ML methods, behavioural analytics and integrated monitoring platforms for protecting critical infrastructure from complex cyber assaults. The focus in most studies was shifted from conventional signature-based mechanisms to adaptive systems for analysing network events, forecasting attacks and automatically responding to incidents. A. Dalal (2024) examined strategies for developing multi-level cybersecurity for corporate networks and critical infrastructure. The researcher pointed out the need for integrating monitoring systems, network segmentation and incident-response automation. These results are consistent with the current study, which demonstrates that the combination of security-event management systems, intrusion detection systems, and ML modules enhances cybersecurity adaptability and decreases threat response time. However, the researcher focused on the organisational and strategic aspects of cyber security while the present study focuses on a practical assessment of the effectiveness of specific ML models. H.I. Kure *et al.* (2022) proposed an integrated cyber-risk

management system for protecting critical infrastructure using risk forecasting mechanisms. The researchers demonstrated that the application of ML models increased the accuracy of potential-threat assessment and ensured a proactive approach to cybersecurity. These results are consistent with the conclusions obtained regarding the high effectiveness of XGBoost and LSTM models in forecasting multi-stage attacks. L. Maglaras *et al*. (2022) analysed key challenges in critical-infrastructure cybersecurity and current approaches to overcoming them. The researchers noted that conventional signature-based attack detection systems have limited effectiveness in cases of complex and previously unknown threats, while behavioural analysis and AI models offer a promising approach. Their results directly correlate with the present study, which also highlights the advantage of ML models over rule-based approaches in terms of classification accuracy, adaptability, and reduction of false positives. However, the study by L. Maglaras *et al*. was primarily review-based, while the present paper includes empirical testing of models on large datasets from real energy infrastructure. Further research on protecting critical infrastructures examined the durability of interconnected infrastructure systems, prediction of cyber assaults, and the use of proactive attack analysis models. B.A. Alkhaleel (2024) systematically reviewed the application of ML methods to ensure the resilience of interdependent critical infrastructures. The researcher determined the most effective were integrated models that incorporated network-event analysis, behavioural analytics, and risk-forecasting mechanisms. These results are in line with existing research, which also shows that the combination of security-event management systems, industrial-network telemetry and ML models increases cybersecurity adaptability.

Later studies showed that there was a general preference for shifting from reactive signature-based mechanisms to adaptive cyber security systems based on ML, predictive analytics and response automation. S.B. Shah (2025) pointed out that ensemble algorithms yield higher classification accuracy and faster incident response compared to traditional rule-based approaches. The present study reports similar results, with Random Forest and XGBoost models exhibiting the greatest effectiveness under conditions of high load and noisy data. This confirms the strong suitability of ensemble methods for processing large event flows in critical infrastructure. A. Alqudhaibi *et al*. (2023) expanded the approach to cyber-threat forecasting by analysing the motivations and behavioural scenarios of attackers. By contrast, the present study is based mainly on analysis of telemetry, network, and SIEM data, which supports assessment of the actual behaviour of infrastructure in real time. The variation in the results can be explained by differences in the input data. A.O. Adewusi *et al*. (2024) focused on the automation of monitoring and response processes as a basis for improving the resilience of critical infrastructure. These conclusions are consistent with the present study, in which integration of automated response scenarios reduces incident-localisation time and the workload on SOC analysts. Collectively, the results of these studies indicate that the most effective systems for modern critical infrastructure are comprehensive ML-oriented systems that combine threat forecasting, behavioural analytics, event correlation, and automated response within a single analytical environment.

Taken together, the studies confirmed the tendency to move from isolated signature-based protection mechanisms to integrated adaptive cybersecurity systems oriented towards automated event analysis, behavioural analytics, and threat forecasting. The studies by O.O. Ajayi *et al*. (2025) and H. Singh (2025) addressed the need for network segmentation, centralised monitoring, and adaptive attack-detection mechanisms in critical infrastructure. The results of these researchers are consistent with the present study, which also shows that integration of security-event management systems, intrusion detection tools, and ML models increases the resilience of infrastructure to complex multi-stage attacks. The studies by H. Alkahtani & T.H.H. Aldhyani (2022) and A. Yaseen (2024) emphasised the high effectiveness of deep learning algorithms and automated response in industrial environments. Their results correlate with the present study, where LSTM models and automated security orchestration mechanisms also provide effective detection of behavioural anomalies and reduce incident-localisation time. However, differences in accuracy and performance indicators may have resulted from differences in data characteristics.

Subsequent studies confirmed the high effectiveness of ML and deep learning methods for anomaly detection, attack forecasting, and automation of cybersecurity for critical infrastructure. The studies by A. Pinto *et al*. (2024) and F. Al-Quayed *et al*. (2024) demonstrated the effectiveness of behavioural analysis, neural networks, and unsupervised learning methods under conditions of dynamic industrial environments; this is consistent with the present study, where Isolation Forest, LSTM, and ANN models also provide effective detection of complex anomalies and hidden attack patterns. Differences in the results are explained by the fact that previous studies mainly focused on individual network types or algorithms, while the present study covers the comprehensive corporate and industrial infrastructure of the energy sector with large-scale flows of real telemetry and network data. N. Mohamed (2025) further confirmed the promise of integrating forecasting models with security orchestration systems and real-time stream event processing. These conclusions fully correlate with the present study, in which the combination of ML models,

security-event management systems, and automated response increases the adaptability and operational speed of critical-infrastructure cybersecurity.

S.R.P. Dandamudi *et al*. (2025) examined the capabilities of predictive ML models for network-infrastructure protection and cyber-threat analysis. The researchers established that ensemble algorithms provided the best balance between processing speed and incident-classification accuracy in high-load networks. These results are consistent with the present study, in which Random Forest and XGBoost models also demonstrate the highest performance, resistance to noise, and effectiveness under conditions of large event flows. J. Govea *et al*. (2024) analysed the effectiveness of using AI to ensure cybersecurity of critical energy infrastructure. The researchers indicated that the application of ML models substantially increased cyber-threat detection accuracy and the adaptability of monitoring systems to changes in network activity. The results correspond to the present study, which also confirms the advantage of XGBoost, Random Forest, and LSTM algorithms in attack classification and anomaly forecasting tasks.

D.R. Chirra (2024) proposed the use of federated ML to build systems for detecting and responding to threats in critical infrastructure. The researcher demonstrated that distributed model training increased the level of data confidentiality and ensured the scalability of cybersecurity systems. The results partially correlate with the present study because both cases point to the need for distributed processing of security events and response automation. The monograph by S. Yevseiev *et al*. (2022) examined approaches to modelling security systems for critical-infrastructure facilities with consideration of multi-level protection architecture and interaction between information and technological components. The researchers noted the importance of comprehensive risk analysis, network segmentation, and development of integrated monitoring systems. These conclusions are fully consistent with the present study, which also emphasises the critical importance of centralised event correlation, protection of SCADA/ICS segments, and multi-level cybersecurity architecture for ensuring the resilience of energy infrastructure to current cyber threats. Synthesis of the results indicates that the studies mostly confirm the effectiveness of ML methods for cybersecurity of critical infrastructure, but most of them focused either on individual algorithms or on isolated components of security systems. By contrast, the present study covers comprehensive integration of monitoring, analysis, forecasting, and automated response within a single protection architecture for energy infrastructure.

CONCLUSIONS

The study established that cyber threats to critical infrastructure in the energy sector have become complex and multi-stage, moving beyond conventional attacks on information systems. Integration of corporate networks with industrial control systems expanded the attack surface and reduced the effectiveness of classical protection models oriented mainly towards perimeter security and signature-based detection. Analysis of cyber incidents in 2022-2025 indicated an increase in the number and complexity of attacks that began to affect not only information resources but also technological processes of energy enterprises. Process control systems, industrial controllers, remote devices, and server infrastructure remain the most vulnerable. Outdated technologies, insufficient network segmentation, and limited access-control mechanisms were identified as the main risk factors.

The analysis contributed to the design of an ML-oriented cybersecurity architecture combining event collection, data correlation, behavioural analysis and automated threat detection. The proposed approach allows moving from reactive response to known attacks to proactive anomaly detection and cyber-incident forecasting. The experimental evaluation of ML models showed that the XGBoost model exhibited the best performance with a classification accuracy of 96.4%, a detection recall of 94.9%, an F1-score of 95.3%, and a ROC-AUC of 0.978. The LSTM model demonstrated high effectiveness in the analysis of temporal dependencies and the forecasting of complex attacks with 95.2% accuracy, but required greater computational resources. XGBoost showed the best performance in detecting distributed denial-of-service attacks with a precision of 97.3% and recall of 96.1%. The results show that the integration of the models into the cybersecurity system reduced the mean incident detection time, response time, and false-positive rate to 11 min, 39 min, and 6.8%, respectively. This verified that the use of ML enhances the accuracy of cyber-event analysis by automated correlation, considering behavioural characteristics and context of network activity. The synthesis of the results highlighted the feasibility of applying a hybrid cybersecurity architecture, with XGBoost for threat classification, Random Forest for quick primary event filtering, and LSTM for the analysis of temporal attack scenarios. This method guarantees a balance between the accuracy, speed and adaptability of the protection system of critical energy infrastructure. The study is limited in that the results were obtained through modelling and a limited set of cyber-threat scenarios, which does not fully reflect the diversity of real attacks in different types of infrastructure. Future work includes extending the datasets, adding more deep learning models, and adapting the system to real distributed cyber-physical environments.

ACKNOWLEDGEMENTS

None.

FUNDING
None.

CONFLICT OF INTEREST
None

REFERENCES

[1] Abisoye, A., Akerele, J., Odio, P.E., Collins, A., Babatunde, G., & Mustapha, S.D. (2025). Using AI and machine learning to predict and mitigate cybersecurity risks in critical infrastructure. *International Journal of Engineering Research and Development*, 21(2), 205-224.
[2] Adewusi, A.O., Okoli, U.I., Olorunsogo, T., Adaga, E., Daraojimba, D.O., & Obi, O.C. (2024). Artificial intelligence in cybersecurity: Protecting national infrastructure: A USA review. *World Journal of Advanced Research and Reviews*, 21(1), 2263-2275. doi: 10.30574/wjarr.2024.21.1.0313.
[3] Ajayi, O.O., Alozie, C.E., & Abieba, O.A. (2025). Enhancing cybersecurity in energy infrastructure: Strategies for safeguarding critical systems in the digital age. *Trends in Renewable Energy*, 11(2), 201-212. doi: 10.17737/tre.2025.11.2.00192.
[4] Alkahtani, H., & Aldhyani, T.H.H. (2022). Developing cybersecurity systems based on machine learning and deep learning algorithms for protecting food security systems: Industrial control systems. *Electronics*, 11(11), article number 1717. doi: 10.3390/electronics11111717.
[5] Alkhaleel, B.A. (2024). Machine learning applications in the resilience of interdependent critical infrastructure systems – a systematic literature review. *International Journal of Critical Infrastructure Protection*, 44, article number 100646. doi: 10.1016/j.ijcip.2023.100646.
[6] Al-Quayed, F., Ahmad, Z., & Humayun, M. (2024). A situation based predictive approach for cybersecurity intrusion detection and prevention using machine learning and deep learning algorithms in wireless sensor networks of industry 4.0. *IEEE Access*, 12, 34800-34819. doi: 10.1109/ACCESS.2024.3372187.
[7] Alqudhaibi, A., Albarrak, M., Aloseel, A., Jagtap, S., & Salonitis, K. (2023). Predicting cybersecurity threats in critical infrastructure for industry 4.0: A proactive approach based on attacker motivations. *Sensors*, 23(9), article number 4539. doi: 10.3390/s23094539.
[8] Chirra, D.R. (2024). Advanced threat detection and response systems using federated machine learning in critical infrastructure. *International Journal of Advanced Engineering Technologies and Innovations*, 2(1), 61-81.
[9] Dalal, A. (2024). Implementing robust cybersecurity strategies for safeguarding critical infrastructure and enterprise networks. *International Journal of Management, Technology and Engineering*, 14(2), 90-111. doi: 10.2139/ssrn.5268076.
[10] Dandamudi, S.R.P., Sajja, J., & Khanna, A. (2025). Advancing cybersecurity and data networking through machine learning-driven prediction models. *International Journal of Innovative Research in Computer Science and Technology*, 13(1), 26-33. doi: 10.55524/IJIRCST.2025.13.1.4.
[11] DiXi Group. (n.d.). *Information on massive strikes on Ukraine's critical infrastructure*. Retrieved from https://map.ua-energy.org.
[12] Govea, J., Gaibor-Naranjo, W., & Villegas-Ch, W. (2024). Transforming cybersecurity into critical energy infrastructure: A study on the effectiveness of artificial intelligence. *Systems*, 12(5), article number 165. doi: 10.3390/systems12050165.
[13] Idowu, A., Ismaila, I., & Ojeniyi, J.A. (2025). Machine learning-driven cybersecurity solutions for enhanced smart grids and critical infrastructure: A review. *NIPES – Journal of Science and Technology Research*, 7(3), 159-184. doi: 10.37933/nipes/7.3.2025.11.
[14] Kalnawat, A., Dhabliya, D., Vydehi, K., Dhablia, A., & Kumar, S.D. (2024). Safeguarding critical infrastructures: Machine learning in cybersecurity. In G. Li, U. Subramaniam & M. Sekar (Eds.), *International conference on environmental development using computer science (ICECS'24)* (Vol. 491; article number 02025). Sivakasi: AAA College of Engineering and Technology. doi: 10.1051/e3sconf/202449102025.
[15] Kumar, A., & Gutierrez, J.A. (2025). Impact of machine learning on intrusion detection systems for the protection of critical infrastructure. *Information*, 16(7), article number 515. doi: 10.3390/info16070515.
[16] Kure, H.I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Computing and Applications*, 34(18), 15241-15271. doi: 10.1007/s00521-022-06959-2.
[17] Maglaras, L., Janicke, H., & Ferrag, M.A. (2022). Cybersecurity of critical infrastructures: Challenges and solutions. *Sensors*, 22(14), article number 5105. doi: 10.3390/s22145105.
[18] Mishok, A.A., Lyashenko, V.A., Dyrman, Yu.V., & Ilchyshyn, V.V. (2026). Strategies for ensuring the cyber resilience of a country's critical information infrastructure in the context of hybrid warfare and global technological challenges. In O. Iohov, V. Maliuk & O. Novykova (Eds.), *The application of information technologies in the training and operations of security and defence forces* (pp. 98-99). Kharkiv: National Academy of the National Guard of Ukraine.

[19] Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems*, 67, 6969-7055. doi: 10.1007/s10115-025-02429-y.
[20] Murasov, R.K., Pharaon, S.I., & Huk, O.M. (2025). Critical infrastructure cybersecurity: assessment and management of cyberattack risks. *Modern Information Technologies in the Sphere of Security and Defence*, 54(3), 75-83. doi: 10.33099/2311-7249/2025-54-3-75-83.
[21] Otoum, S., Kantarci, B., & Mouftah, H. (2021). A comparative study of AI-based intrusion detection techniques in critical infrastructures. *ACM Transactions on Internet Technology*, 21(4), article number 81. doi: 10.1145/3406093.
[22] Pinto, A., Herrera, L.C., Donoso, Y., & Gutierrez, J.A. (2024). Enhancing critical infrastructure security: Unsupervised learning approaches for anomaly detection. *International Journal of Computational Intelligence Systems*, 17, article number 236. doi: 10.1007/s44196-024-00644-z.
[23] Raval, K.J., Jadav, N.K., Rathod, T., Tanwar, S., Vimal, V., & Yamsani, N. (2024). A survey on safeguarding critical infrastructures: Attacks, AI security, and future directions. *International Journal of Critical Infrastructure Protection*, 44, article number 100647. doi: 10.1016/j.ijcip.2023.100647.
[24] Shah, S.B. (2025). Machine learning for cyber threat detection and prevention in critical infrastructure. *Journal of Global Research in Electronics and Communications*, 2(2), 1-7. doi: 10.5281/zenodo.14955016.
[25] Singh, H. (2025). Advanced cybersecurity techniques for safeguarding critical infrastructure against modern threats. *Science, Technology and Development*, 14(3), 161-179. doi: 10.2139/ssrn.5267496.
[26] Stotskyi, I.V., Kostenko, V.P., Nalisnyi, G.I., & Sharnin, S.A. (2025). Use of AI algorithms for detection and blocking of cyberattacks on military information systems. *Bulletin of Kherson National Technical University*, 2(3), 443-447. doi: 10.35546/kntu2078-4481.2025.3.2.56.
[27] Uzzaman, A., & Rony, M.A. (2023). Machine learning-based cybersecurity models for safeguarding industrial automation and critical infrastructure systems. *International Journal of Scientific Interdisciplinary Research*, 4(4), 224-264. doi: 10.63125/2mp2qy62.
[28] Yaseen, A. (2024). Enhancing cybersecurity through automated infrastructure management: A comprehensive study on optimizing security measures. *Journal of Computational Social Dynamics*, 38-60.
[29] Yevseiev, S., *et al.* (2022). *Modeling of security systems for critical infrastructure facilities*. Kharkiv: PC Technology Center. doi: 10.15587/978-617-7319-57-2.

Інформаційні технології забезпечення кібербезпеки критичної інфраструктури на основі методів машинного навчання

Анатолій Бензарь
Доцент
Західнодонбаський інститут Приватного акціонерного товариства «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом»
51408, вул. Дніпровська, 400/1, м. Павлоград, Україна
https://orcid.org/0000-0002-0943-0109

Анотація. Актуальність дослідження зумовлена зростанням кількості багатостадійних кібератак на промислові та корпоративні мережі, що потребує переходу від сигнатурних механізмів захисту до адаптивних інтелектуальних систем аналізу та прогнозування загроз. Метою дослідження було оцінювання ефективності застосування машинного навчання для виявлення та прогнозування кіберзагроз у критичній інфраструктурі енергетичного сектору з розробленням архітектури автоматизованого кіберзахисту. У дослідженні було проаналізовано кіберзагрози енергетичної інфраструктури на основі даних кіберподій, проведено підготовку даних, навчання та порівняння моделей машинного навчання, після чого обрано найефективніші моделі для впровадження системи захисту. У результаті дослідження встановлено, що кіберзагрози для критичної енергетичної інфраструктури стали складнішими через об'єднання інформаційних мереж із системами керування технологічними процесами. Аналіз інцидентів у 2022-2025 роках показав зростання кількості та складності атак, найбільш уразливими компонентами яких були системи керування, промислові контролери та серверна інфраструктура. Розроблено систему кіберзахисту на основі машинного навчання, яка забезпечує аналіз подій, виявлення аномалій і прогнозування загроз. Найвищу ефективність продемонструвала модель градієнтного підсилення, яка забезпечила точність класифікації 96,4 %, повноту виявлення 94,9 % та F1-score 95,3 %. Модель аналізу часових послідовностей показала високу здатність до прогнозування складних атак із точністю 95,2 %. Інтеграція моделей машинного навчання дозволила скоротити час виявлення інцидентів до 11 хвилин, час реагування до 39 хвилин і знизити частку хибних спрацювань до 6,8 %. Отримані результати підтвердили ефективність застосування машинного навчання для підвищення точності, швидкості та адаптивності систем кіберзахисту критичної інфраструктури. Результати дослідження можуть бути використані фахівцями з кібербезпеки, розробниками систем захисту та операторами критичної інфраструктури в енергетичному секторі для підвищення ефективності виявлення та реагування на кіберзагрози

Ключові слова: енергетичний сектор; система диспетчерського контролю та збору даних; промислові системи керування; система управління подіями та інформацією безпеки; виявлення аномалій; прогнозування атак; штучний інтелект