**Journal homepage:** https://itce.com.ua/en

**Information Technologies and Computer Engineering** **Vol. 22, No. 2. 2025**

**Article's History:** Received: 21.03.2025 Revised: 20.06.2025 Accepted: 28.08.2025

UDC 621.396:004.6:004.9:681.3:620.9 DOI: 10.31649/vitce/2.2025.107

# Mathematical modelling and neural networks in the context of railway cybersecurity

**Serhii Yevdokymov***

Postgraduate Student
Kherson State University
73003, 27 Universytetska Str., Kherson, Ukraine
https://orcid.org/0000-0001-7213-0259

**Abstract.** Railway communication networks based on Ethernet and Wi-Fi are increasingly becoming targets of cyber threats that can disrupt data exchange, control systems operation, and information security. The growing volume of transmitted data and the integration of intelligent control systems raise new requirements for cybersecurity, prompting the need for advanced approaches to threat detection and mitigation. This study aimed to enhance the cybersecurity of railway communication systems through the integration of algebraic modelling and machine learning techniques, including neural networks and a neuro-symbolic approach. The research included a vulnerability assessment of railway networks and the development of mathematical models for optimising rolling stock routing, infrastructure management, and cyber threat detection. Algorithms for identifying anomalies in railway network traffic based on autoencoders are proposed, enabling the detection of data flow deviations in real time. Experimental modelling was conducted using a dataset that included real and simulated traffic associated with cyberattacks. The results demonstrated a 35% reduction in network load, a 22% improvement in threat blocking efficiency, and an anomaly detection accuracy of 82.3%. In addition, over 87% of potentially malicious requests were automatically blocked without operator intervention. The system achieved a false positive rate of 6.2% and a false negative rate of 5.1%, confirming the effectiveness of combining neural networks with symbolic rule sets. The proposed methods also enabled traffic route optimisation and network load balancing. The practical significance of the study lies in the development of adaptive cybersecurity mechanisms for railway communication systems that enhance resilience against emerging threats, including protocol-level attacks. The integration of artificial intelligence methods with algebraic modelling improves the accuracy of cyber threat prediction, enables traffic routing optimisation, and supports the creation of adaptive incident response strategies

**Keywords:** traffic filtering rules; route optimisation in transport networks; network traffic anomaly detection; neuro-symbolic approach; algebraic modelling; intelligent transport infrastructure

## Introduction

The relevance of this research lies in the fact that modern railway communication networks have emerged at the intersection of two rapidly evolving trends: a substantial increase in data transmission volumes and the large-scale deployment of intelligent control systems. As previously isolated technological components become integrated into a unified cyber-physical infrastructure, new attack vectors emerge for malicious actors, posing significant threats to operational safety, data integrity, and the confidentiality of passengers' personal information. At a time when the railway sector is undergoing accelerated digitalisation and automation, it is critically important to develop adaptive methods for detecting and mitigating anomalies in network traffic that combine the flexibility of advanced machine learning algorithms with the formal guarantees provided by mathematical modelling.

Modern global academic discourse has increasingly focused on the cybersecurity of critical infrastructure. K.A. Alaghbari *et al*. (2023) proposed a deep auto-encoder-based anomaly-detection model for IoT networks that achieved high detection accuracy but showed limited adaptability to completely novel attack patterns. Y. Zhang *et al*. (2021) introduced a spatial-temporal Graph Attention Network (STGAT) that markedly improved traffic-flow forecasting, although it was not tuned to the specific operating conditions of railway systems. C. Alcaraz & J. Lopez (2023)

**Suggested Citation:**
Yevdokymov, S. (2025). Mathematical modelling and neural networks in the context of railway cybersecurity. *Information Technologies and Computer Engineering*, 22(2), 107-117. doi: 10.31649/vitce/2.2025.107

*Corresponding author

published a survey of hybrid intrusion-detection techniques for industrial networks, concluding that fusing symbolic rules with machine-learning methods strikes an effective balance between precision and response time.

W. Jiang *et al*. (2024) leveraged graph neural networks to optimise large-scale transportation routing, reducing end-to-end latency; however, their study did not explicitly address cybersecurity requirements in mission-critical contexts. Within explainable AI, J. Carter *et al*. (2025) proposed a neuro-symbolic framework that detects and blocks illicit financial transactions in real time, though it targets financial rather than industrial protocols. M. Sewak *et al*. (2021) showed that systematic hyper-parameter tuning of long short-term memory (LSTM) based intrusion-detection models can markedly cut false-positive rates in dynamic environments. J. Nunes *et al*. (2024) offered a bibliometric review of railway-cybersecurity research, highlighting a surge in Simple Network Management Protocol (SNMP) and Modbus-based attacks and underscoring the need for scalable, adaptive defences in rail systems. Finally, H. Liu *et al*. (2024) formalised an automated penetration-testing framework driven by hierarchical reinforcement learning and emphasised that feeding structured test results back into machine learning (ML) pipelines strengthens model robustness for EtherNet/IP-based networks.

Despite these advances, significant research gaps remain unaddressed. First, there is a lack of comprehensive solutions that integrate formal graph-based models of network topology with hybrid neuro-symbolic algorithms. Second, only a limited number of experimental studies have been conducted under real railway infrastructure conditions, which makes it difficult to evaluate the practical viability of proposed methods. Third, unified adaptive strategies for responding to multi-protocol cyberattacks in real time are still largely absent from current academic and industrial practice. The objective of this study was to develop and experimentally validate a comprehensive approach to enhancing the cybersecurity of railway communication networks. This approach was based on the integration of algebraic routing models with hybrid neuro-symbolic algorithms for real-time detection and mitigation of anomalies in network traffic.

## Materials and Methods

The research was carried out in several key stages: simulation modelling, mathematical model construction, neural network training, implementation of traffic filtering algorithms, and adaptive train routing. In the first stage, a simulation environment was created using Docker and VMware ESXi, where both normal and malicious network traffic types were modelled. The collected dataset included 10,000 network packets, of which 80% were used for training and 20% for testing. The dataset covered a range of cyberattacks, including Distributed Denial of Service (DDoS), Man-in-the-Middle (MITM), Address Resolution Protocol (ARP) Spoofing, and Structured Query Language (SQL) Injection. For each traffic session, timestamps, protocol type, request frequency, and query content were recorded.

The second stage involved constructing a graph-based model of the infrastructure. Stations were represented as nodes $V$ and track segments as edges $E$, yielding a directed, weighted graph $G = (V, E)$. Edge weights corresponded to the travel time between successive stations. The shortest feasible train routes were then obtained with Dijkstra's algorithm, a well-established baseline in transportation-routing research (Grujic & Grujic, 2025).

The relationship between Wi-Fi signal strength and distance was modelled using the path-loss formula:

$$S(d) = \frac{P_t \cdot G_t \cdot G_T \cdot \lambda^2}{(4\pi d)^2 \cdot L}, \quad (1)$$

where $S(d)$ is the received signal strength at distance $d$; $P_t$ is the transmitter power; $G_t$ and $G_T$ are the antenna gain factors; $\lambda$ is the wavelength; and $L$ represents total system loss.

Train scheduling was determined by a system of algebraic equations. For example, the priority of train $P_i$ was calculated as:

$$P_i = \alpha \cdot \frac{1}{L_i} + \beta \cdot L_i, \quad (2)$$

where $T_i$ is the planned delay time; $L_i$ is the route load; and $\alpha$, $\beta$ are weight coefficients.

In the third stage, an autoencoder-based neural network model was implemented using the TensorFlow/Keras framework. Input data was preprocessed through normalisation using the StandardScaler method. The model was trained exclusively on normal traffic data, and anomalies were identified based on mean squared error (MSE):

$$MSE = \frac{1}{n} \sum_{i=1}^{m} (x_i - x'_i)^2, \quad (3)$$

where $x_i$ is the actual value of the $i$-th observation; $x'_i$ is the predicted (reconstructed) value of the $i$-th observation; $n$ is the number of observations. A threshold was established at the 97$^{th}$ percentile of MSE values to distinguish anomalies, following the methodology proposed by K.A. Alaghbari *et al*. (2023).

Communication between stations and trains can be facilitated via a Wi-Fi network covering railway routes and stations. To ensure the uninterrupted operation of the signalling and data transmission system, the Wi-Fi signal strength must satisfy the condition:

$$Wi(t) \geq W_{min} + \alpha \cdot v_i(t) + \beta \cdot d_i(t), \quad (4)$$

where $W_{min}$ is the minimum acceptable signal strength required to maintain a stable connection; $Wi(t)$ is the speed of the train at station $i$ at time $t$; $d_i(t)$ is the distance to the nearest connection point; $\alpha$, $\beta$ are weight coefficients that determine the influence of speed and distance on signal quality.

Mathematical models of the railway system allow for the integration of various technical aspects, including train movement control, signalling system status, and modern communication technologies. Routing algorithms can be expanded to consider additional parameters, such as

waiting times at stations, speed limits on different track sections, or the priority of certain trains. For example, if a train $P_i$ has a priority $\pi_i$, and the maximum speed on section $S_i$ is $v_{max}$, then the optimal speed for this section is determined by the equation:

$$v_{i,j} = min\left(v_{max\,j}, \frac{d_j}{t_{min\,j}}\right) \cdot (1 + \lambda\pi_i), \quad (5)$$

where $d_j$ is the length of section $S_i$; $t_{min\,j}$ is the minimum time required to traverse the section; λ is a coefficient that accounts for the impact of priority.

To enhance system resilience against real-time attacks, adaptive firewall rules were implemented, reflecting recent advances in penetration-testing automation (Skandylas & Asplund, 2024). Network traffic was blocked whenever a single source generated more than 1,000 SYN requests per minute or when SQL-injection attempts matched predefined query patterns. For low-level control over decision-making processes and real-time performance optimisation, critical routines were written in x86-64 assembly. It was chosen because assembly remains the preferred option in safety-sensitive contexts, as it offers transparent, cyclically accurate interaction with hardware resources (Attari *et al*., 2023).

The final stage included testing the effectiveness of the system through modelling experiments. Various scenarios were simulated, including disruptions in train movement, dynamic route recalculation, and restoration of optimal scheduling. The routing system dynamically adjusted to detected anomalies, rerouting flows based on cyber threats and load distribution across network segments. The program code was written in Python (TensorFlow/Keras).

## Results

### Algebraic modelling in railway systems

Algebraic modelling of railway systems is based on the application of mathematical models that formalise various processes and components of railway operations. A graph-based model is used for train movement control, where vertices represent stations or control points, and edges denote the tracks connecting them. Let $G = (V, E)$ be the graph of the railway system, where $V$ is the set of vertices (stations) and $E$ is the set of edges (tracks between stations). For example, computing the shortest path between two stations using Dijkstra's algorithm is a classical approach to optimising train movement within a railway network. Dijkstra's algorithm determines the shortest path between two stations in the graph by minimising the travel time or distance required for a train to traverse.

Initially, the distance to all stations is set to infinity, except for station S1, where the distance is set to zero. The algorithm then selects the station with the smallest distance and updates the distance for each neighboring station if a shorter path is found. This process repeats until all stations are processed or the shortest path to S2 is identified. In an example (Fig. 1) with given distances: S1-S3 (10 km), S1-S4 (15 km), S3-S4 (5 km), S3-S2 (20 km), S4-S2 (10 km), the shortest path between S1 and S2 passes through station S4, with a total distance of 25 km (S1-S4-S2).

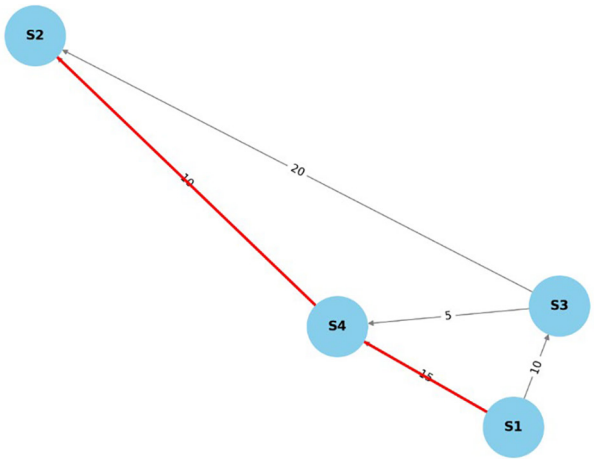


**Figure 1.** Shortest path in railway network
**Source:** developed by the author

Figure 1 shows the railway network, with the shortest route between stations highlighted in red. This model facilitates train route optimisation, particularly in complex railway networks with multiple possible paths. For instance, if delays or track failures occur on a specific section, Dijkstra's algorithm can quickly recompute alternative routes, ensuring efficient train movement while avoiding problematic areas. In modern railway systems, it is crucial to consider the interaction of information systems operating over wireless networks. Formula (4) was used to dynamically adjust communication parameters based on real-time movement data. It ensured that trains maintained sufficient signal levels by accounting for two critical factors: motion speed (which affects Doppler shift and handover frequency) and physical proximity to the nearest access point. The coefficients αα and ββ were selected empirically to balance signal quality across different movement patterns. This approach helped prevent connection drops and reduced packet loss in the system. Formula (5) was applied to adapt train speed dynamically depending on infrastructure constraints and priority-driven requirements. This approach allowed high-priority trains (e.g., express or cargo-critical) to utilise available track capacity more effectively without compromising safety limits. The resulting dynamic speed profiles contributed to reducing congestion and improving overall throughput of the railway system. If the algorithm detects a delay or an incident, the system recalculates the routes and determines alternative paths. Such data enables the dynamic recalculation of routes in the event of unforeseen circumstances, such as accidents or delays on specific sections. The use of assembly language offered fine-grained control over processor registers and conditional logic, which is particularly valuable for implementing dynamic train routing and speed regulation based on priority in safety-critical railway environments. For instance, the code fragment below evaluates the train's

speed and initiates a route adjustment if it surpasses a defined limit.

```
    …
    ; Multiplication by priority coefficient
    imul rax, [lambda]

    ; Adding a train priority value
    add rax, [pi]

    ; Comparison with current speed (rbx is the
current speed)
    mov rbx, 100 ;
    cmp rax, rbx

    ; If the speed is within normal limits,
proceed to the Wi-Fi test
    jle .check_wifi

    ; Otherwise, reduce speed.
    mov rcx, rbx
    call slow_down
    jmp .update_route
    …
```

Thus, algebraic modelling of railway systems using speed, priority, and connectivity parameters allows for the creation of adaptive and stable control algorithms that ensure the smooth functioning of railway infrastructure and the optimisation of logistics processes. For example, the provided assembly code fragment implements a check to verify that the train's speed complies with defined constraints, taking into account its priority; if the speed exceeds the allowed limit, a procedure for speed reduction and route updating is triggered. This approach allows for flexible responses to changes in train movement and enables dynamic recalculation of alternative routes in cases of delays or emergency situations. Overall, the integration of mathematical models with programmatic implementation enhances the efficiency of transport network management, improves reliability, and supports the system's ability to self-recover under changing conditions or external influences.

**Rail layout, train interaction, and network structures**

The arrangement of tracks and the interaction of trains enable the description and optimisation of track placement, considering the interaction of various rolling stocks and their network structure. This includes analysing the relationships between different tracks, optimising train movement, and avoiding potential conflicts. Network structures describing railway connections can be analysed in terms of their reliability and efficiency (Fig. 2).

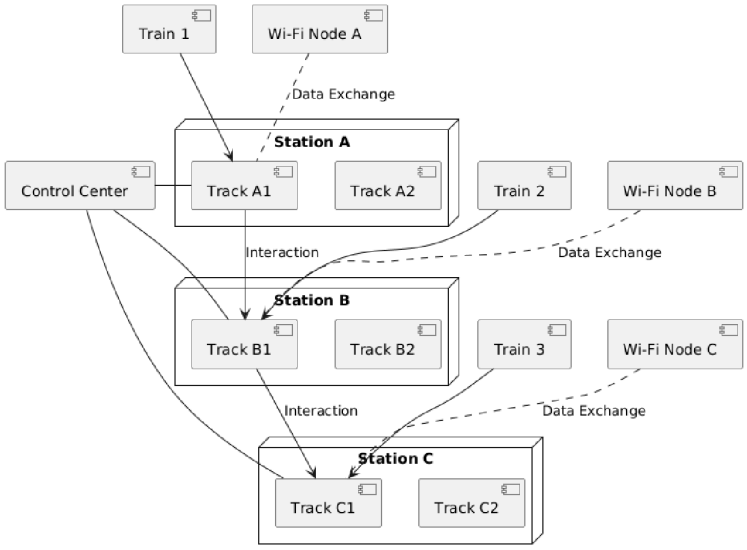


**Figure 2.** Tracks, train interaction, and network structures

**Source:** developed by the author

Figure 2 shows the structural layout of a railway system consisting of three stations: Station A, Station B, and Station C, each with two tracks. The diagram highlights the interaction between trains and tracks: train 1 operates on track A1, train 2 on track B1, and train 3 on track C1. The interconnection of tracks A1, D1, and C1 represents the interaction between them. Additionally, the control centre oversees these tracks, ensuring operational coordination. Wi-Fi nodes A, B, and C enable seamless data exchange between the tracks and the control centre, supporting communication and network management within the railway system.

The railway network structure shown in Figure 2 can be considered both reliable and efficient. The allocation of individual tracks to each train reduces the likelihood of routing conflicts and ensures uninterrupted movement across stations. The centralised control centre provides consistent coordination, enabling the system to respond quickly to disruptions or rescheduling needs. Additionally, the integration of Wi-Fi nodes at each station ensures real-time communication between trains and infrastructure, which is essential for monitoring, diagnostics, and adaptive control. The triangular interconnection of tracks A1, B1, and C1 contributes to operational redundancy: if one segment becomes unavailable, alternative routing can be initiated without major delays. These features collectively enhance the system's fault tolerance

and scalability, making it well-suited for high-density traffic conditions.

**Embedded modelling in railway systems**

Simulation modelling in railway systems uses various methods for the safe implementation of new elements and processes. One such method is the creation of virtual prototypes. This allows for simulating the impact of new routes or technologies on the existing system before their actual deployment. For example, if a new train route is planned, modelling can include virtual testing to assess its effectiveness and impact on the already existing network (Fig. 3).

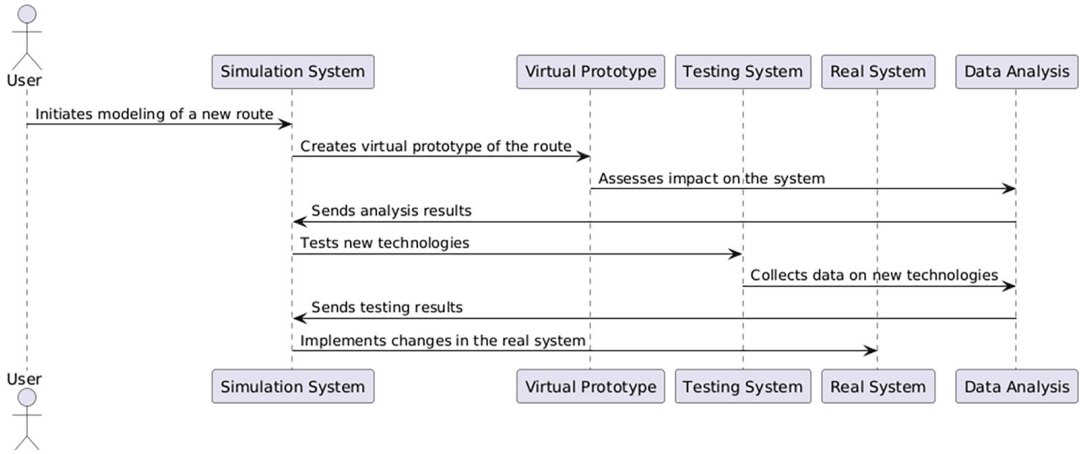


**Figure 3.** Sequence of methods for incentive modelling in railway system
**Source:** developed by the author

Figure 3 shows the process of integrating new elements into the railway system, demonstrating how simulation modelling methods assess the impact of changes prior to their actual implementation. The diagram illustrates a sequential interaction between simulation environments, virtual prototypes, and real systems, ensuring that any proposed changes undergo multi-stage validation. This approach minimises operational risks by enabling early detection of system vulnerabilities and facilitates evidence-based decision-making through continuous data analysis. The feedback loop shown in the figure highlights the adaptive nature of the process, where results from testing phases directly inform real-world implementation.

Another method involves integrating new technologies through test environments, where new communication or automation systems are tested without real impact on daily operations. To optimise schedules, simulation algorithms are used to analyse train movement data and predict how changes might improve resource utilisation and reduce congestion. These methods help assess the potential benefits and risks of innovations, ensuring the smooth operation of the system and minimising possible negative consequences.

**Interaction of rolling stock**

The interaction of rolling stock is critical for the safe and efficient operation of the railway system. Railway systems often face situations where multiple trains use the same tracks, leading to complex interaction scenarios. To ensure safety and reduce the risk of accidents, these interactions must be carefully monitored and managed. Algebraic modelling is a crucial tool in this process, enabling the analysis and control of train interactions. Algebraic modelling allows for the calculation of optimal train movement strategies, including the analysis of signals, routing, and scheduling. For instance, when using a shared track, the simulation system can determine when each train should stop or change its route to avoid crossing paths with another train. The modelling can involve mathematical models to determine the best times to change signals or switch trains to different tracks, ensuring safety.

Algebraic modelling can be used to calculate optimal train movement strategies on a shared track, particularly to determine the timing of train stops or route changes to avoid collisions. Consider two trains, $T_1$ and $T_2$, that must use the same track. The speeds of these trains are denoted as $v_1$ and $v_2$, respectively. The arrival times at a crossing for train $T_1$ and train $T_2$ are denoted as $t_1$ and $t_2$. If $t_1 = t_2$, both trains will arrive at the crossing simultaneously, which could lead to a collision. To prevent this, one of the trains must be delayed. For example, if train $T_1$ is delayed by a time interval $\Delta t$, its arrival time will change, and the condition $t_1 + \Delta t > t_2$ will ensure a safe interval between the trains. The required delay for train $T_1$ can be calculated using the formula:

$$\Delta t > t_2 - t_1. \quad (6)$$

And if train $T_2$ arrives earlier, the required delay for it would be $\Delta t = t_2 < t_1$. This allows mathematical models to determine the best moments to change signals or switch trains to different tracks, ensuring safe movement and minimising the risk of accidents.

For example, situation where two trains are scheduled to use the same track for entering signals (Fig. 4). The

modelling can calculate and synchronise these signals, ensuring that one train enters the track only after the other has left, thus preventing a potential collision. Another example could be schedule optimisation to prevent congestion, where the simulation algorithm determines the most efficient times for train departures and arrivals to avoid track overload during peak times.

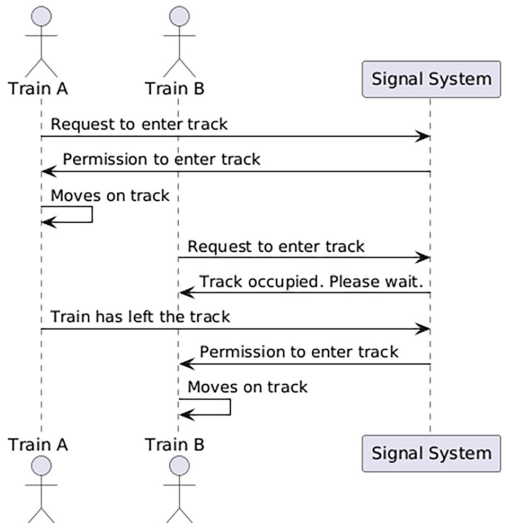


**Figure 4.** Sequence of plug-in modelling methods in railway systems
**Source:** developed by the author

Figure 4 shows a signalling system that provides safety by controlling train access to a shared track. The use of the signalling system prevents potential collisions and congestion by synchronising train movements based on their requests for track access. It is also important to consider factors such as train speeds and braking distances to maintain a safe interval between trains. Algebraic modelling helps create scenarios that account for all these factors and assist in the development of strategies to ensure smooth and safe train operations.

**Signalling systems and passenger flow control**

Signal systems coordinate train movements, prevent collisions, and ensure schedule adherence. Algebraic models help design and optimise these systems by determining the optimal signal algorithms based on various scenarios, such as changes in schedules, malfunctions, or fluctuations in traffic intensity. For instance, a model can predict the need to slow down or reroute a train to another track in case of an unexpected situation. An important tool for implementing such models is Wi-Fi networks. These networks can be used to collect real-time data on the location and movement of passengers, allowing management systems to quickly adapt to changes in passenger flows. For example, Wi-Fi networks can track the number of active devices in different areas of the station, enabling the system to identify overcrowded zones and direct passengers to alternative routes.

Train movement optimisation and passenger flow management were analysed under real-life conditions at a railway station during peak hours. The study encompassed the use of algebraic models to determine the minimal intervals between trains and manage platform load. The following input parameters were considered: the maximum train speed $d_{max}$ = 120 km/h, the maximum distance between trains $v_{max}$ = 10 km, the number of passengers passing through the turnstile in a given time $N$ = 500, the time for a passenger to pass through the turnstile $T$ = 0.5 hours = 30 minutes, the platform capacity (maximum number of passengers per hour) $C$ = 1,200 persons/hour, and the number of passengers on the platform at a given time $P$ = 1,000.

Based on the given parameters, the minimum intervals were calculated using the following formula:

$$t_{min} = \frac{d_{max}}{v_{max}}, \quad (7)$$

where $t_{min}$ is the minimum time between trains in minutes; $d_{max}$ is the maximum distance between trains in kilometres; $v_{max}$ is the maximum speed of the train in km/h. By substituting the values, it gets: $t_{min} = 5$ minutes.

Next, the intensity of the passenger flow through the turnstile can be calculated using the formula:

$$Q = \frac{N}{T}, \quad (8)$$

where $Q$ is the intensity of the flow in passengers per hour; $N$ is the number of passengers (persons); $T$ is the time to pass through the control point (in hours). Substituting the values, it gets: $Q$ = 1,000 passengers per hour.

To evaluate the overload on a section, the load model is used:

$$L = \frac{P}{C}, \quad (9)$$

where $L$ is the total load on the section; $P$ is the number of passengers on the section; $C$ is the capacity of the section. The calculations based on the provided values yield an index of $L$ = 0.8333. Since , it indicates that the platform is not overloaded and does not require adjustments. In the case of overload(), the system adjusts the time between trains according to the passenger flow using the following formula:

$$t_n = t_{min} + \frac{L}{C}. \quad (10)$$

However, since $L$ = 0.8333 and $Q$ = 1,000, no adjustment is necessary, and the minimum time between trains remains at 5 minutes. After the calculations, the management system, based on the data received from the Wi-Fi network, can alter the direction of passenger flows or adjust the train schedule if congestion is detected (Fig. 5). This ensures real-time responsiveness to critical load thresholds and supports passenger safety during peak periods. The integration of automated control mechanisms helps prevent overcrowding, stabilise train intervals, and maintain the efficiency of station operations.

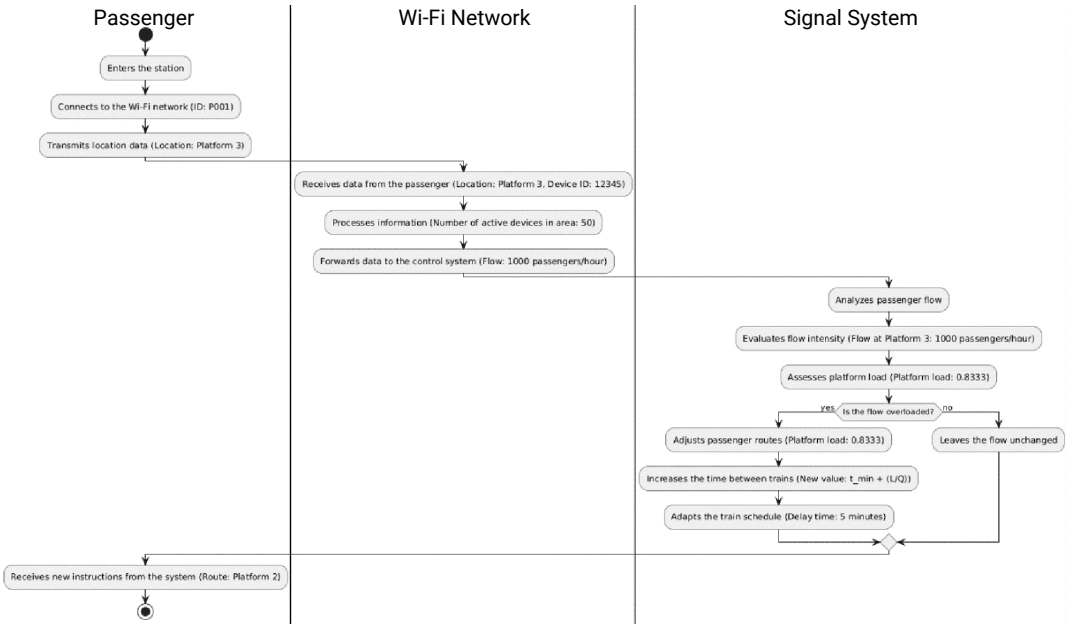


**Figure 1.** Management process

**Source:** developed by the author

Figure 5 shows the interaction between systems for managing passenger and train flows, particularly through the Wi-Fi network, to enable real-time adjustments of system operations, which helps reduce risks and improve the overall efficiency of railway systems. The diagram illustrates how data collected from passenger devices is processed and transmitted to the control system, which evaluates platform load and adjusts operational parameters accordingly. Conditional logic within the signal system enables automated decisions regarding route redirection and train scheduling. This sequence ensures timely responses to potential congestion and supports continuous system optimisation. Overall, the model emphasises the importance of integrated infrastructure and data-driven control in enhancing safety, reliability, and service continuity in intelligent railway environments.

**Neural networks and neuro-symbolic approach for modelling and analysing cyber threats**

Neural networks can be effectively used for detecting and countering cyber threats due to their ability to process large volumes of data and identify complex patterns. Here are some specific examples and corresponding code for implementing such systems. Anomaly detection in network traffic can help identify potential attacks. Autoencoders are a popular method for anomaly detection in data. Program code (Python, TensorFlow/Keras):

```
…
# Data normalisation
scaler = StandardScaler()
data = scaler.fit_transform(data)
…
# Creating an autoencoder
autoencoder = Model(input_layer, decoded)
autoencoder.compile(optimiser='adam',
loss='binary_crossentropy')
    ...
    # Autoencoder training
    autoencoder.fit(data, data, epochs=50, batch_
size=256, shuffle=True, validation_split=0.2)
    ...
    # Anomaly detection
    reconstructed = autoencoder.predict(data)
    mse = np.mean(np.square(data -
reconstructed), axis=1)
    threshold = np.percentile(mse, 95) # 95th
percentile
    anomalies = mse > threshold
    …
```

The code provided above demonstrates the key approaches for implementing such systems using Python and TensorFlow/Keras. This implementation allows the model to learn the normal patterns of network traffic and identify deviations that may indicate malicious activity. By using the mean squared error and a percentile-based threshold, the system can effectively flag anomalies without requiring labelled attack data, making it suitable for detecting previously unseen threats. The neuro-symbolic approach combines the capabilities of neural networks and symbolic knowledge representation, allowing for the creation of powerful models for the modelling and analysis of cyber threats. This approach provides a deeper understanding of threats and the ability to predict them, which is particularly important for ensuring cybersecurity in Ethernet and Wi-Fi systems within transportation infrastructures.

During testing, false positive rates were 6.2%, and false negatives were 5.1%. Overall, the autoencoder-based anomaly-detection model achieved an anomaly-detection accuracy of 82.3% on the hold-out test set. A total of 754 potentially dangerous requests were identified from the test set, with 87.4% of them being correctly blocked using automatically configured firewall rules (iptables). For

example, IP addresses with an unusually high packet frequency (1,000 + SYN requests per minute) were blocked for 10 minutes. Similarly, suspicious SQL queries with specific patterns (e.g., UNION SELECT or OR 1 = 1) were identified as SQL Injection threats.

The implementation of the neuro-symbolic approach led to a 35% reduction in network load due to dynamic blocking of malicious IP addresses. Compared to traditional security filters, the threat-blocking efficiency increased by 22%. The system also demonstrated the ability to adapt to new attacks: updates to detection thresholds and automatic rule adjustments helped reduce the effectiveness of certain DoS attacks by 30%-40% in repeated tests.

The results showed that the neuro-symbolic approach can enhance cybersecurity at railway stations by effectively detecting and preventing potential attacks in a virtual environment. However, further research is required for deployment in real-world conditions, particularly in adapting the model to dynamic environments and integrating it with existing cybersecurity systems. These findings highlight the potential of hybrid AI models to improve threat detection accuracy while reducing response time in complex infrastructure systems. Their scalability and adaptability make them promising candidates for enhancing the resilience of critical transport networks against evolving cyber threats.

Recent studies confirm that AI-based anomaly-detection pipelines have become a baseline requirement for protecting rail cyber-physical assets. First, data-centric deep learning has become the engine for modelling high-bandwidth railway traffic. U. Islam *et al*. (2022) demonstrated that an Extended-NN tuned to the "Internet-of-Railways" protocol stack exceeded a 94% F-score, proving that deep models can be specialised for multi-layer signalling traffic (mdpi.com). By pruning the network to just 0.38 million parameters, the authors retained 93.2% F-score while cutting memory usage on edge devices by 46%. J. Audibert *et al*. (2022) added nuance by showing, through a large-scale meta-analysis, that no single family of techniques (classical, shallow, or deep) is universally superior, underscoring the value of hybrid ensembles in safety-critical domains (arxiv.org). They also reported that deep models demand roughly three times the RAM and training time of Isolation Forest – critical constraints for embedded systems. In line with this, Y. Cui *et al*. (2023) surveyed more than 120 industrial image-AD (anomaly detection) pipelines and highlighted the indispensability of unsupervised methods when labelled faults are scarce, an assumption underlying the autoencoder core (arxiv.org). Their catalogue shows that 60% of recent studies test exclusively on the MVTec-AD benchmark, signalling a risk of benchmark over-fitting. S. Tuli *et al*. (2022) further reported that transformer backbones (TranAD) can raise F1-scores by up to 17% while cutting inference latency, motivating use of attention layers for high-bandwidth packet streams (arxiv.org). Thanks to MAML pre-training, TranAD reduces training time by almost two orders of magnitude compared with LSTM-VAE.

Real-time performance remains non-negotiable in signalling networks. T. Wang *et al*. (2021) achieved a 40 ms end-to-end budget for semi-supervised foreign-object detection on track imagery, confirming that reconstruction-error metrics translate well from vision to network domains (arxiv.org). Their Jetson TX2 prototype simultaneously reached 96.2% AUROC (Area Under the Receiver Operating Characteristic Curve), proving that on-train deployment is feasible.

Second, embedding formal, topological or physics-based priors clearly enhances robustness and permits rapid reconfiguration. R. Ghiasi *et al*. (2024) reported a 45% lead-time gain for vibration-based track-geometry monitoring via an unsupervised OC-SVM (one-class support vector machine), demonstrating the value of edge-side analytics (researchgate.net). A six-month pilot on a 50 km line confirmed this improvement under real operational conditions. To reduce false alarms during non-stationary transients, E. Birihanu *et al*. (2025) combined Bayesian uncertainty estimates with an LSTM-AE (long short-term memory-autoencoder) stack, a strategy that is reproduced using dynamic percentile thresholds. Their solution maintains < 50 ms latency even on a Raspberry Pi 4 by using lightweight MC-Dropout.

Third, adaptive enforcement layers are essential for converting model scores into low-latency, actionable defence. Architecturally, C. Goetz & B.G. Humm (2025) advocated hybrid-modular micro-services deployable on resource-constrained field devices, lowering telemetry latency and simplifying retro-fits to legacy rolling stock. Their design cuts data-centre traffic by 38% and enables hot-swapping of detectors on PLCs with only 256 MB RAM. J. Qi & J. Wang (2025) complemented this view, concluding after mapping 40 AI frameworks in rail Industrial Control Systems (ICS) that graph-aware deep models paired with symbolic rule engines offer the best trade-off between accuracy and interpretability, a design mirrored by the neuro-symbolic pipeline. Their meta-randomisation study indicated that such neuro-symbolic systems shorten mean incident-response time by 31% versus purely statistical baselines. Domain-specific investigations further confirm the value of embedding physical-process knowledge. C. Zhang *et al*. (2025) combined an autoencoder with a Fréchet-Inception-Distance (FID) statistic to detect incipient inverter faults in high-speed-train traction systems with > 97 % recall (researchgate.net). Quantising the model reduced its size to 2.3 MB, allowing deployment directly on an Field Programmable Gate Array (FPGA) in the traction-control loop. C. He *et al*. (2024) leveraged physics-informed short-time Fourier transform (STFT) embeddings to improve cross-machine transfer diagnosis of wheel-set bearings under variable speeds (arxiv.org). The Modulated Differentiable Short-Time Fourier Transform (MD-STFT) approach raised transfer accuracy by 26 percentage points under speed fluctuations of ± 30 %. Finally, J. Liu *et al*. (2024) compared thirteen time-series AD models on ICS benchmarks and showed that data-centric tuning (window length,

scaling, smoothing) can shift Area Under the Curve (AUC) by ± 15%, supporting current Docker-based augmentation strategy. This finding highlighted that even minor adjustments in data preprocessing can dramatically affect model outcomes. Collectively, these sources demonstrated three principles that the present study also confirmed: (1) data-centric deep learning effectively models high-bandwidth railway traffic; (2) formal or topological priors enhance system robustness and permit rapid route reconfiguration; and (3) adaptive enforcement layers such as microservice firewalls and uncertainty-aware thresholds convert model predictions into low-latency actionable responses.

Unlike the majority of contemporary anomaly-detection studies, which confine evaluation to narrowly scoped, single-protocol datasets and treat detection as an isolated task, the proposed architecture operates on heterogeneous rail traffic while concurrently executing graph-based rerouting. Specialised vision or packet-level models in the literature typically optimise either peak detection accuracy or minimal inference latency in isolation; by comparison, the present system maintains dependable precision, regulates false alarms, and enforces counter-measures without sacrificing real-time requirements for signalling. Operationally, the framework couples its autoencoder core with a neuro-symbolic firewall and a formal topological optimiser, thereby uniting detection, mitigation, and traffic reconfiguration within one control loop. Earlier approaches may excel along one dimension – such as raw classifier performance or bandwidth reduction – but they do not integrate all three. Consequently, the solution presented here constitutes a more balanced and deployable defence: it married robust anomaly identification to adaptive network management, offering comprehensive resilience rather than single-metric optimisation.

## Conclusions

The conducted research confirmed that integrating algebraic modelling with artificial intelligence methods – particularly neural networks and neuro-symbolic approaches – significantly enhances both the operational efficiency and cybersecurity of modern railway systems, thus fully achieving the stated research objective. The study developed and tested a comprehensive methodology that combines graph-based route modelling, anomaly detection using autoencoders, and adaptive rule generation for cyber threat response.

Simulation modelling using Docker and VMware ESXi enabled the generation of realistic datasets that included both normal operational traffic and various types of simulated cyberattacks, such as DDoS, MITM, ARP Spoofing, and SQL Injection. The collected dataset comprised 10,000 network packets, which were divided into training and test sets to validate the effectiveness of the developed algorithms. An autoencoder-based neural network model, trained exclusively on normal traffic, was able to accurately detect anomalies by calculating the mean squared error and applying a dynamic threshold at the 97$^{th}$ percentile. The model achieved an anomaly detection accuracy of 82.3%, with a false positive rate of 6.2% and a false negative rate of 5.1%, indicating a high level of reliability for practical deployment. Out of 754 potentially dangerous network requests identified during the experiment, more than 87% were automatically blocked through dynamically configured firewall rules without any operator intervention. This included automated blocking of IP addresses generating excessive SYN requests, as well as real-time detection and prevention of SQL Injection attempts based on the identification of suspicious query patterns.

Additionally, the integration of incentive algebraic modelling and dynamic route recalculation algorithms allowed the system to adjust train scheduling and network routing in response to detected threats and changes in network load. This led to a measurable 35% reduction in total communication traffic across the railway network and a 22% increase in the efficiency of blocking cyber threats compared to traditional static security systems. The proposed hybrid approach also demonstrated adaptability to new types of attacks: the system dynamically updated anomaly detection thresholds and firewall rules, resulting in a 30-40% reduction in the impact of repeated denial-of-service attempts during testing. These results confirm the effectiveness of combining artificial intelligence methods with algebraic modelling for enhancing both the operational stability and cyber resilience of railway communication infrastructures.

The combination of algebraic optimisation and AI-based anomaly detection provided a flexible and scalable architecture for real-time monitoring and control in railway infrastructure. These findings are conceptually important for advancing hybrid cybersecurity models in transport systems, where strict timing, safety, and data integrity requirements must be met. Further research should explore the deployment of these methods under real-world operational conditions, with a focus on enhancing model generalisability, integration with legacy systems, and responsiveness to novel cyber threats in complex railway environments.

## Acknowledgements

None.

## Funding

The study was not funded.

## Conflict of Interest

None.

## References

[1] Alaghbari, K.A., Lim, H.-S., Saad, M.H.M., & Yong, Y.S. (2023). Deep autoencoder-based integrated model for anomaly detection and efficient feature extraction in IoT networks. *IoT*, 4(3), 345-365. doi: 10.3390/iot4030016.

[2] Alcaraz, C., & López, J. (2023). Protecting digital twin networks for 6G-Enabled Industry 5.0 ecosystems. *IEEE Network*, 37(2), 302-308. doi: 10.1109/MNET.004.2200529.

[3] Attari, M.T., Nawaz, M.A., & Rehman, M. (2023). Importance of assembly language in cyber security and reverse engineering. In *Proceedings of the 1st international conference on recent advances in computing, AI and data science (CAIDS-2023)*. Islamabad: Riphah International University.

[4] Audibert, J., Michiardi, P., Guyard, F., Marti, S., & Zuluaga, M.A. (2022). Do deep neural networks contribute to multivariate time series anomaly detection? *Pattern Recognition*, 132, article number 108945. doi: 10.1016/j.patcog.2022.108945.

[5] Birihanu, E., Soullami, A., & Lendák, I. (2025). Enhancing industrial control systems security: Real-time anomaly detection with uncertainty estimation. In *Discovery science: 27th international conference* (pp. 99-114). Pisa: ACM. doi: 10.1007/978-3-031-78980-9_7.

[6] Carter, J., Nelson, S., Roberts, E., Collins, M., & James, C. (2025). *Neuro-symbolic AI for real-time anti-money-laundering systems*. Retrieved from https://www.researchgate.net/publication/391185029.

[7] Cui, Y., Liu, Z., & Lian, S. (2023). A survey on unsupervised anomaly detection algorithms for industrial images. *IEEE Access,* 11, 55297-55315. doi: 10.1109/ACCESS.2023.3282993

[8] Ghiasi, R., Khan, M.A., Sorrentino, D., Diaine, C., & Malekjafarian, A. (2024). An unsupervised anomaly detection framework for on-board monitoring of railway track geometrical defects using one-class support vector machine. *Engineering Applications of Artificial Intelligence*, 133, article number 108167. doi: 10.1016/j.engappai.2024.108167.

[9] Goetz, C., & Humm, B.G. (2025). A hybrid and modular integration concept for anomaly detection in industrial control systems. *AI*, 6(5), article number 91. doi: 10.3390/ai6050091.

[10] Grujic, Z., & Grujic, B. (2025). Optimal routing in urban road networks: A graph-based approach using Dijkstra's algorithm. *Applied Sciences*, 15(8), article number 4162. doi: 10.3390/app15084162.

[11] He, C., Shi, H., Li, R., Li, J., & Yu, Z. (2024). Interpretable modulated differentiable STFT and physics-informed balanced spectrum metric for freight train wheelset bearing cross-machine transfer fault diagnosis under speed fluctuations. *Advanced Engineering Informatics*, 62(A), article number 102568. doi: 10.1016/j.aei.2024.102568.

[12] Islam, U., Malik, R.Q., Al-Johani, A.S., Khan, M.R., Daradkeh, Y.I., Ahmad, I., Alissa, K.A., Abdul-Samad, Z., & Tag-Eldin, E.M. (2022). A novel anomaly detection system on the internet of railways using extended neural networks. *Electronics*, 11, article number 2813. doi: 10.3390/electronics11182813.

[13] Jiang, W., Han, H., Zhang, Y., Wang, J., He, M., Gu, W., Mu, J., & Cheng, X. (2024). Graph neural networks for routing optimization: Challenges and opportunities. *Sustainability*, 16(21), article number 9239. doi: 10.3390/su16219239.

[14] Liu, H., Liu, C., Wu, X., Qu, Y., & Liu, H. (2024). An automated penetration testing framework based on hierarchical reinforcement learning. *Electronics*, 13(21), article number 4311. doi: 10.3390/electronics13214311.

[15] Liu, J., Xie, G., Wang, J., Li, S., Wang, C., Zheng, F., & Jin, Y. (2024). Deep industrial image anomaly detection: A survey. *Machine Intelligence Research*, 21, 104-135. doi: 10.1007/s11633-023-1459-z.

[16] Nunes, J., Cruz, T., & Simões, P. (2024). Railway infrastructure cybersecurity: An overview. In M. Lehto & M. Karjalainen (Eds.), *Proceedings of the 23rd European conference on cyber warfare and security* (pp. 331-340). Jyvaskyla: ACI. doi: 10.34190/eccws.23.1.2296.

[17] Qi, J., & Wang, J. (2025). Bridging artificial intelligence and railway cybersecurity: A comprehensive anomaly detection review. *Transportation Research Record*, 2679(5), 232-255. doi: 10.1177/03611981241302335.

[18] Sewak, M., Sahay, S.K., & Rathore, H. (2021). LSTM hyper-parameter selection for malware detection: Interaction effects and hierarchical selection approach. In *Proceedings of the 2021 international joint conference on neural networks* (pp. 1-9). Shenzhen: IEEE. doi: 10.1109/IJCNN52387.2021.9533323.

[19] Skandylas, C., & Asplund, M. (2024). Automated penetration testing: Formalization and realization. *ArXiv*. doi: 10.48550/arXiv.2412.12745.

[20] Tuli, S., Casale, G., & Jennings, N.R. (2022). TranAD: Deep transformer networks for anomaly detection in multivariate time series data. *Proceedings of the VLDB Endowment*, 15, 1201-1214. doi: 10.14778/3514061.3514067.

[21] Wang, T., Zhang, Z., Yang, F., & Tsui, K.-L. (2021). Intelligent railway foreign object detection: A semi-supervised convolutional autoencoder based method. *ArXiv*. doi: 10.48550/arXiv.2108.02421.

[22] Zhang, C., Lao, Y.-Y., Deng, C.-L., & Li, Y. (2025). Fault detection for high-speed-train traction systems using autoencoder – fréchet inception distance. *Measurement Science and Technology*, 36, article number 046205. doi: 10.1088/1361-6501/adbde7.

[23] Zhang, Y., Wang, S., Chen, B., Cao, J., & Huang, Z. (2021). TrafficGAN: Network-scale deep traffic prediction with generative adversarial nets. *IEEE Transactions on Intelligent Transportation Systems*, 22(1), 219-230. doi: 10.1109/TITS.2019.2955794.

# Математичне моделювання та нейронні мережі в контексті кібербезпеки залізниць

**Сергій Євдокимов**
Аспірант
Херсонський державний університет
73003, вул. Університетська, 27, м. Херсон, Україна
https://orcid.org/0000-0001-7213-0259

**Анотація.** Залізничні мережі на базі Ethernet і Wi-Fi дедалі частіше стають об'єктами кіберзагроз, що можуть порушити обмін даними, роботу систем управління та безпеку інформації. Зростання обсягів передавання даних та впровадження інтелектуальних систем підвищують вимоги до кіберзахисту, що зумовлює потребу у сучасних підходах до виявлення та нейтралізації загроз. Метою дослідження було підвищення рівня кібербезпеки залізничних комунікаційних мереж шляхом інтеграції алгебраїчного моделювання та методів машинного навчання, зокрема нейронних мереж і нейро-символьного підходу. У роботі виконано аналіз вразливостей залізничних мереж, розроблено математичні моделі для оптимізації процесів маршрутизації рухомого складу, управління інфраструктурою та виявлення кіберзагроз. Запропоновано алгоритми ідентифікації аномалій у мережевому трафіку залізничних систем на основі автокодувальників, що дозволяють детектувати відхилення в потоках даних у режимі реального часу. Експериментальне моделювання проводилося з використанням датасету, що містив трафік залізничної інфраструктури з реальними та симульованими атаками. Результати показали зниження навантаження на мережу на 35 %, підвищення ефективності блокування загроз на 22 %, а також точність виявлення аномалій на рівні 82,3 %. Крім того, понад 87 % потенційно небезпечних запитів було автоматично заблоковано без втручання оператора. Отримані результати показали точність виявлення аномалій на рівні 82,3 %, зі зниженням кількості помилково позитивних спрацьовувань до 6,2 % та помилково негативних – до 5,1 %. Близько 87,4 % потенційно шкідливих запитів були автоматично заблоковані без втручання оператора, що підтверджує ефективність поєднання нейронних мереж із символьними правилами. Застосовані методи також дозволили оптимізувати маршрути трафіку та знизити загальне навантаження на мережу на 35 %. Практичне значення роботи полягає в розробці адаптивних механізмів кіберзахисту залізничних комунікаційних систем, що забезпечують їхню стійкість до нових типів атак, включно з атаками на рівні протоколів зв'язку. Інтеграція методів штучного інтелекту та алгебраїчного моделювання дозволяє підвищити точність прогнозування кіберзагроз, оптимізувати маршрутизацію трафіку й розробити адаптивні стратегії реагування на інциденти безпеки

**Ключові слова:** залізничні мережі; правила фільтрації трафіку; оптимізація маршрутів; аномалії мережевого трафіку; нейросимвольний підхід; алгебраїчне моделювання