https://doi.org/10.33271/nvngu/2026-4/156

O. V. Lebid[1],
orcid.org/0000-0003-4253-8696,
I. A. Chikov[*1],
orcid.org/0000-0002-2128-5506,
S. V. Khrushchak[1],
orcid.org/0009-0007-9452-4372,
S. V. Strikha[2],
orcid.org/0000-0002-5937-7748,
O. B. Piven[3],
orcid.org/0000-0001-5601-8304,
M. S. Kovalenko[4,5],
orcid.org/0009-0008-0577-3148

1 – Vinnytsia National Agrarian University, Vinnytsia, Ukraine
2 – State Research Institute for Testing and Certification of Weapons and Military Equipment, Cherkasy, Ukraine
3 – Cherkasy State Technological University, Cherkasy, Ukraine
4 – SCIRE Foundation, Warsaw, Poland
5 – Interregional Academy of Personnel Management, Kyiv, Ukraine
* Corresponding author e-mail: ilya95chikov@gmail.com

DETECTION OF ANOMALIES IN LOCAL TRAFFIC USING SECURE GATING NETWORKS

Purpose. To develop and evaluate a method for detecting anomalies in local network traffic based on the FCRNN-GRU architecture in order to improve classification accuracy and reduce the rate of false positive alerts.

Methodology. In the study, network interactions are represented as normalized time series, which makes it possible to capture the dynamics of traffic changes. The baseline model is a fully connected recurrent neural network capable of identifying complex nonlinear and long-term dependencies due to its densely connected recurrent structure. To improve training efficiency and avoid the vanishing gradient problem, mini-batch stochastic gradient descent is used. The additional integration of GRU (Gated Recurrent Unit) enables optimization of the trade-off between model accuracy and computational complexity. Experimental evaluation was conducted on a dataset of 52,000 network flows, including 32,000 normal traffic instances and 20,000 anomalous ones covering various types of cyber threats. The network environment was simulated on a Linux platform using Mininet and Wireshark, while algorithm implementation was carried out in Python.

Findings. The FCRNN-GRU model demonstrates high performance: detection rate – 98.59 %, false alarm rate – 5.29 %, and classification accuracy – 99.21 %. Compared to traditional and clustering-based methods, the proposed approach provides a significant improvement and confirms its effectiveness.

Originality. The scientific novelty of the study lies in the adaptation of a fully connected recurrent neural network with the integration of gated recurrent units for network traffic analysis tasks. The combination of dense recurrent connections with GRU mechanisms enables more accurate modeling of temporal patterns in traffic behavior, while simultaneously reducing computational costs and improving model efficiency when processing large volumes of data.

Practical value. The proposed approach has practical significance and can be integrated into modern monitoring and cybersecurity systems. Its application contributes to the timely detection of anomalous events in the network, enhances the level of information infrastructure security, and reduces risks associated with cyber threats.

Keywords: *network anomalies, traffic flow, cybersecurity analytics, neural networks, information security*

Received: 16 February 2026
Accepted: 02 June 2026
Available online: 27 August 2026

Introduction. As of 2025, protecting computer networks from unauthorized access and anomalous activities remains a strategic priority at all levels-from the private sector to state institutions. Rapid digitalization of services, widespread deployment of IoT devices, and the transition to cloud infrastructures have significantly expanded the potential threat landscape. Under these conditions, ensuring cyber resilience has become a critical necessity, driving continuous growth in investment in the development of intelligent and more adaptive information security systems [1, 2]. Since they rely on predefined patterns of known threats and are unable to detect new or evolving attack vectors, traditional intrusion detection systems (IDS) based on signatures face difficulties in identifying sophisticated attackers and zero-day exploits [3]. This makes the development of more intelligent and adaptive detection methods essential.

Key factors that exacerbate these challenges in 2025 include:

- the enormous scale of interconnected ecosystems with billions of IoT endpoints lacking robust built-in security services, making them vulnerable to brute-force attacks, botnet encryption techniques, and device compromise [1, 2];
- cloud environments introducing additional complexity through misconfigurations, unsecured APIs, and distributed workloads, enabling easier lateral movement and data exfiltration [3, 4];
- attackers increasingly leveraging artificial intelligence to automate vulnerability discovery, develop polymorphic malware, accelerate exploit development, and evade traditional defensive mechanisms [4, 5].

Literature review. The growing complexity of cyber threats has stimulated extensive research into intelligent methods for identifying anomalous network activity.

© Lebid O. V., Chikov I. A., Khrushchak S. V., Strikha S. V., Piven O. B., Kovalenko M. S., 2026

Traditional signature-based intrusion detection systems (IDS) are unable to cope with emerging zero-day attacks, which has driven a shift toward anomaly-based strategies that employ statistical models, machine learning, and especially deep learning methods [1, 2]. Early efforts relied on statistical and clustering algorithms to detect traffic deviations; however, these approaches were often insufficient for modeling evolving and complex temporal behavior [3, 6].

Recurrent neural architectures, particularly LSTM and GRU, are now at the forefront of effectively capturing sequential dependencies in network traffic flows due to advances in deep learning. Several studies have shown that, compared to traditional methods, hybrid neural structures provide significantly better detection performance and substantially reduce false positive rates [7, 8]. By leveraging advanced feature engineering, integrated neural design, and fine-grained flow-based traffic analysis, Ukrainian researchers have achieved a significantly advanced level of anomaly detection in this field. To reduce computational costs while preserving long-range contextual information, modern solutions often combine gated recurrent units with attention mechanisms [9, 10]. This makes them well-suited for real-time analysis in high-performance network environments. However, handling class imbalance in training data, adapting to continuously evolving traffic profiles, and ensuring seamless integration into real operational environments remain ongoing challenges [4, 11].

In summary, the analysis of global and national scientific literature indicates a persistent trend confirming the effectiveness of deep learning models (particularly recurrent and hybrid architectures) in network anomaly detection tasks. Nevertheless, further research remains necessary. Special attention should be given to model scalability, improved interpretability, and reliable deployment in real-world network systems.

Methodology and data. To address the stated challenges, artificial intelligence and machine learning-based anomaly detection methods are increasingly being applied. In particular, recurrent architectures such as LSTM and GRU demonstrate significant potential for effectively capturing temporal patterns in network traffic.

The use of such models enables the early detection of hidden or previously unknown deviations in time series data-for example, in sequences of network flows or user behavior profiles. This significantly improves the ability of systems to adapt to emerging threats (including zero-day attacks), reduces the need for large volumes of labeled data, and enhances real-time performance compared to classical statistical or rule-based methods [9, 12].

Overall, the cybersecurity landscape of 2025 shows a clear shift toward hybrid, adaptive, and behavior-based defense strategies. Modern solutions integrate deep learning, continuous self-learning mechanisms, Zero Trust concepts, and automated threat analytics, enabling rapid response to the evolving cyber risk environment.

In this context, anomaly detection methods have become an area of intensive scientific development. Unlike traditional signature-based analysis, which relies on fixed attack patterns, anomaly-based approaches model the "normal" behavior of a network. This allows any deviations to be identified as potential threats, providing significantly greater flexibility in detecting previously unknown attacks. Among modern approaches, deep learning methods-particularly recurrent neural networks such as LSTM and GRU-play a key role. Due to their ability to effectively analyze temporal dependencies in network traffic, these architectures enable the detection of complex hidden patterns that are typically missed by traditional analytical methods [7, 9].

On datasets such as NSL-KDD and UNSW-NB15, optimized LSTM-based models have demonstrated strong detection performance with lower false alarm rates. Modern deep learning architectures significantly outperform traditional machine learning classifiers such as SVM, Random Forest, and Naïve Bayes. They are particularly effective at identifying complex, dynamic cyber threats that often bypass conventional algorithmic thresholds, thanks to their ability to model sequential patterns [1].

The accuracy of traffic anomaly analysis is further improved by hybrid architectures combining LSTM and GRU layers, often with additional regularization or structural modifications [2]. On modern datasets such as CSE-CIC-IDS2018, research on hybrid convolutional-recurrent models and multi-scale designs has achieved multi-class attack classification accuracy exceeding 98 % [9].

According to research results from 2024–2025, cybersecurity is experiencing intensive adoption of deep learning technologies, including graph neural networks, autoencoders, and variants of recurrent neural networks. These methods are increasingly integrated with hybrid intrusion detection systems (IDS) and software-defined networking (SDN) solutions [3, 8]. Despite their strong performance, challenges remain in class imbalance handling, real-time processing efficiency, and the development of semi-supervised or unsupervised learning approaches. Overall, these trends indicate a shift toward data-driven adaptive architectures capable of identifying emerging threats in conditions of limited labeled data.

The presented study extends these approaches by focusing on the application of specialized neural networks for accurate anomaly detection in local network traffic flows. Particular attention is given to modeling temporal dependencies and developing robust detection mechanisms, making the proposed solution a practical contribution to the implementation of deep learning methods for traffic analysis in modern high-speed environments.

Results. The study employs sequential pattern analysis for LAN environments with the primary objective of enabling real-time detection of malicious or anomalous behavior.

The proposed anomaly-based framework identifies deviations from pre-established baseline profiles, in contrast to traditional signature-based intrusion detection systems (IDS), which rely on predefined threat signatures. To achieve this, the model captures complex statistical relationships and temporal dependencies present in network traffic.

Traffic is formally represented as a multidimensional time series. Let X_t be a feature vector at a discrete time step t. Each component $x_i \in X_t$ corresponds to specific traffic characteristics, such as temporal features (e.g., time between consecutive packets), connection metadata (e.g., encoded IP addresses, port numbers, and

protocol flags), and volume metrics (e.g., the number of packets per second, total number of transmitted bytes).

Thus, network traffic within a defined time window is represented as a sequence $X = [x_1(t), x_2(t), x_n(t)]$, where T represents the observation interval. This sequential structure facilitates the application of recurrent neural networks (RNNs), which use recurrent state transitions to capture temporal dynamics [11, 13].

The hidden state h_t is computed as a function of the current input vector X_t and the previous hidden state h_{t-1}. At each time step t, the model updates its internal representation, gradually accumulating information about the process evolution.

Due to the recurrent architecture, the network considers the context of the entire sequence, combining short-term variations with long-term dependencies. This enables effective separation of structured deviations indicating anomalous or targeted activity from random fluctuations of legitimate network traffic, while preserving a coherent temporal "memory" of the process.

To improve the model's sensitivity to temporal patterns, the FCRNN architecture employs dense interneuronal connections within its hidden layers. The network maintains persistent internal memory by integrating feedback from previous time steps, allowing it to capture long-term dependencies in sequential data. The hidden state of each neuron is updated according to the following transition equation [5]

$$S(t+1) = r \cdot \Phi(t+1)\, S(t) + \Psi(t+1), \qquad (1)$$

where

$$\Phi(t+1) = Wr(t+1)\, W(t+1);$$

$$\Psi(t+1) = Y(t+1) X(t+1).$$

The FCRNN architecture ensures continuity of neuron states, allowing it to capture subtle temporal correlations in network traffic. These interdependencies are often crucial for timely anomaly detection, as they reflect hidden transformations in system behavior. At the same time, the sequential characteristics of network traffic can be reasonably treated as a stochastic process. Within this approach, the output value at time t can be described by an autoregressive model, where the current state is expressed as a linear combination of previous values with an added random component that models the influence of unpredictable factors [14]. Such an interpretation enables an effective combination of classical statistical methods with neural network capabilities for deeper analysis of temporal dependencies.

The autoregressive representation of traffic flow is expressed by the following equation [6]

$$y_t = c + y_{t-1} + e_t. \qquad (2)$$

This structure establishes the basis for describing temporal correlations in network traffic and how they are related to the dynamic nature of traffic. Temporal state-transition patterns are also modeled in recurrent neural networks, and this formulation ensures an appropriate representation of sequential dependencies in real network processes.

Training a fully connected recurrent neural network (RNN) on large-scale intrusion detection datasets often suffers from vanishing or exploding gradients, especially when the network is deep or contains a large number of neurons. To address this issue, the MBGD (Mini-Batch Gradient Descent) algorithm is applied. Mini-batch gradient descent algorithm updates the network weights using small subsets of data rather than the entire dataset, balancing convergence speed and stability [7]

$$\theta_{t+1} = \theta_t - \eta \cdot \nabla_\theta L_B(\theta_t). \qquad (3)$$

The introduction of momentum further stabilizes the optimization process by damping oscillations [9]

$$v_{t+1} = \mu v_t - \eta \cdot \nabla_\theta L_B(\theta_t); \quad \theta_{t+1} = \theta_t + v_{t+1}. \qquad (4)$$

In our opinion, this approach improves convergence, reduces traffic-related issues, and enables online updates as new traffic data continuously arrives.

To reduce computational overhead in an efficient temporal model, the neural architecture incorporates a gated recurrent unit. Compared to the traditional LSTM framework, the gated recurrent unit offers a more compact design by combining the input and forget gates into a single update gate. This structural simplification reduces the overall number of trainable parameters, accelerates convergence, and improves training efficiency while preserving the ability to capture important sequential dependencies [7].

The FCRNN-GRU framework provides a unified solution for real-time anomaly detection in local networks, systematically overcoming the limitations of traditional methods. Unlike statistical models constrained by data dimensionality, clustering methods affected by traffic dynamics, or signature-based intrusion detection systems (IDS) that are blind to zero-day threats, this approach leverages temporal memory to achieve higher accuracy and lower false positive rates.

Through the integration of recurrent mechanisms and gating structures, the model effectively adapts to evolving patterns of network activity. This enables not only the detection of known attack types but also the reliable identification of anomalous deviations indicating hidden malicious activity, ensuring a high level of infrastructure resilience without the need for frequent database updates.

The proposed methodological approach is based on a sequential data processing pipeline, which performs normalization and encoding of input network traffic features during the preprocessing stage. The main computational module of the system is built on a RNN-GRU, which is trained on time-series data to model complex contextual dependencies. The application of gradient-descent-based optimization methods enables effective minimization of classification errors, ensuring accurate tracking of the model's hidden-state dynamics in real time. The final stage involves evaluating model performance using standard classification quality metrics, in particular $F_{1\text{-}score}$ and *ROC-AUC*, providing an objective basis for comparative analysis of different anomaly detection methods.

This integrated workflow ensures robustness and adaptability of the system in complex, large-scale network environments.

The proposed FCRNN-GRU-based anomaly detection system was implemented and evaluated within a representative medium-sized office network. The infrastructure included 150–200 active endpoints, including workstations, servers, VoIP equipment, and IoT devices,

providing a diverse baseline of network traffic. The deployment aimed to assess the model's robustness under realistic variations in daily network activity and heterogeneous protocol patterns [6, 15]. Continuous monitoring was conducted over a 30-day window, capturing standard business operations along with controlled simulations of adversarial conditions. These scenarios included:

- reconnaissance and access attempts – port scanning and brute-force login attempts;
- anomalous dynamics – abnormal traffic spikes and data exfiltration patterns.

The network architecture, as shown in the topology, uses a centralized logging and analysis server for the FCRNN-GRU model. Flow-level data is collected from access and perimeter switches, enabling the system to perform high-precision analysis of both internal and external traffic dynamics (Fig. 1).

The proposed architectural structure demonstrates that the developed solution can be implemented in a typical office network environment without significant modifications to the existing infrastructure. The use of data collection at the network flow level ensures non-intrusive integration into the traffic exchange process and does not disrupt the operation of core services [16]. This approach contributes to simultaneously improving the efficiency of the network management system while maintaining its performance, providing continuous real-time security monitoring.

Fig. 2 illustrates the internal configuration of the FCRNN-GRU model used for anomaly detection. The architecture integrates fully connected recurrent layers with GRU components, including update and reset gates to facilitate efficient modeling of temporal dependencies in network traffic sequences. The hidden state representations encode the evolving behavioral characteristics of users and services, enabling accurate discrimination between legitimate load variations and potentially malicious activity.

Hidden state representations encode the temporal dynamics of network packet sequences, integrating the context of previous observation steps through the mathematical apparatus of gated GRU units. The operation of the GRU block at each time step t is described by the following system of equations

$$z_t = \sigma(W_z x_t + U_z h_{t-1} + b_z; \quad (5)$$

$$r_t = \sigma(W_r x_t + U_r h_{t-1} + b_r; \quad (6)$$

$$\tilde{h}_t = \tanh(W_h x_t + U_h(r_t \odot h_{t-1}) + b_h); \quad (7)$$

$$h_t = (1 - z_t) \odot h_{t-1} + z_t \odot \tilde{h}_t, \quad (8)$$

where z_t is the update gate vector, which determines how much information from the previous hidden state should be retained; r_t is the reset gate vector that controls the degree of forgetting of the previous state; $\tilde{h}_t$ is the candidate hidden state; h_t is the current hidden state; σ is the sigmoid activation function; $\odot$ denotes the element-wise Hadamard product; W and b are weight matrices and bias vectors, respectively.

The resulting hidden state vector h_T at the final step of the time window is passed to a fully connected output layer with a Sigmoid activation function, which scales the output into the range [0, 1], producing a probabilistic estimate of whether the analyzed time interval belongs to the class of anomalous activity. If the output value exceeds the predefined classification threshold (by default $\theta = 0.5$), an anomaly or potential cybersecurity threat is flagged.

State management mechanisms and the recurrent structure of the model make it possible to preserve long-term contextual information while simultaneously adapting to short-term fluctuations in network traffic. In turn, this improves the precision of anomaly detection, reduces the number of false positive alerts, and enhances the system's robustness against unknown threats, including zero-day scenarios, compared to classical statistical and signature-based methods.

In summary, the conducted study demonstrates that the proposed FCRNN-GRU-based approach can be effectively applied in real office network environments. The model has shown scalability, adaptability to dynamic traffic conditions, and consistently high detection accuracy under varying load levels.

Fig. 3 presents the structural configuration of the FCRNN. In this architecture, intermediate computational states are denoted as S_0, S_1 and S, corresponding to successive transformations between hidden layers during temporal data processing. The fully connected recurrent architecture enables a bidirectional flow of information between temporal states, allowing more effective consideration of both past context and current sequence characteristics. Let the input vector at step ttt be defined as [7, 8, 13]

$$X_t = \left\{ x_t^{(1)}, x_t^{(2)}, \ldots, x_t^{(m)} \right\}. \quad (9)$$

To ensure full inter-layer connectivity in the current architecture, the number of neurons in the first and last hidden layers is uniformly set to n. This configuration

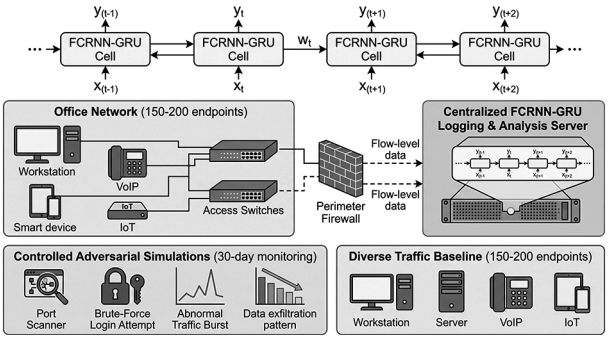

Fig. 1. Architecture and operational flow of the FCRNN model for network traffic analysis

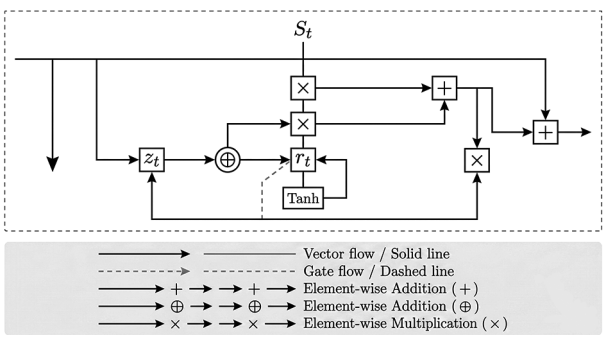

Fig. 2. The main architecture of the FCRNN-GRU model for sequential anomaly detection

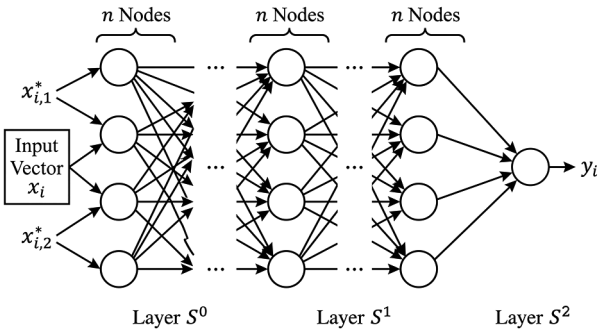

Fig. 3. Proposed structural topology of the dense hidden layer FCRNN model

guarantees that each neuron in the preceding layer is connected to all neurons in the subsequent layer, forming a fully dense matrix. Such a design promotes comprehensive interaction between extracted features and enhances the overall representational capacity of the network [10, 17].

The proposed architectural solution for the simultaneous modeling of spatial and temporal dependencies in network traffic is based on the integration of a specialized recurrent layer with dense connectivity (FCRNN – Fully Connected Recurrent Neural Network). Traditional recurrent neural networks often face limitations in representational capacity when processing multidimensional feature vectors, since relationships between individual components at the current time step are modeled separately from historical context.

To overcome this limitation and improve the accuracy of hidden threat identification, a densely fully connected design is implemented within the hidden layer structure. This means that each neuron in the hidden layer dynamically interacts not only with its own previous state and the corresponding element of the input sequence, but also maintains direct recurrent connections with all other neurons in this layer at the previous time step. Such a topology significantly expands the information capacity of the network and enables the detection of complex nonlinear patterns of anomalous activity without a critical increase in model depth. The detailed structural topology of the proposed dense hidden FCRNN layer is shown in Fig. 3.

By tuning the FCRNN, it became easier to model complex nonlinear relationships between different network signals through coordinated layer-wise interactions. The internal structural components of the architecture enable smooth temporal information propagation and more effective utilization of time-related context, improving the distinction between normal and anomalous network patterns even under unpredictable conditions [5, 18]. In addition, the proposed structural scheme provided a foundation for integrating GRU mechanisms. The resulting hybrid FCRNN-GRU architecture ensured more stable temporal training while simultaneously reducing the computational cost required for real-time data analysis.

In contrast to classical recurrent networks with feedback connections, the FCRNN employs an explicit temporal feedback mechanism, enabling more natural modeling of sequential dependencies. At each time step, the network simultaneously processes the current input vector and the hidden state from the previous step. This dual-input structure supports sequential feature extraction and adaptive representation of dynamically changing network behavior.

As the volume of input data increases, the FCRNN unfolds along the temporal axis, allowing consistent sequence processing and efficient computation. However, in deeper configurations, the problem of vanishing gradients may arise during backpropagation, which negatively affects learning [4, 19]. To address this issue, GRU modules were integrated into the hidden layers, simplifying the network structure, stabilizing the training process, and preserving the model's ability to capture important temporal patterns.

For a comprehensive understanding of the practical implementation of the proposed method, a structural-functional scheme of the security system was developed. It clearly illustrates the architecture of information flows and the interaction between key computational modules – from the moment raw packet traffic is captured in local communication channels to the generation of alerts about cyber threats. Such an organization of the workflow enables an effective separation between passive data collection and intelligent analytical processing, thereby minimizing additional overhead on the network infrastructure and ensuring the scalability of the solution. The detailed interconnection of system components and the processing logic are presented in Fig. 4.

The operational logic of the system corresponds to a structured pipeline designed for high-precision analysis of internal and external traffic dynamics. As shown in Fig. 4, the workflow integrates adaptive gradient optimization and sliding window control into a unified detection system.

Step 1: Initialization and resource management. The scale of the intermediate hidden layer is predefined based on historical empirical data to prevent excessive use of hardware resources.

Step 2: Gradient optimization. According to input data standardization, the MBGD (Mini-Batch Gradient Descent) algorithm is used to adjust the model loss and the convergence direction.

Step 3: Structural adaptation. At this stage, depending on the complexity and scale of the input data, GRU units are integrated into the model, gradually replacing standard neurons in the recurrent layer. This substitution reduces the risk of the vanishing gradient problem during training and improves the stability and accuracy of the model during parameter optimization.

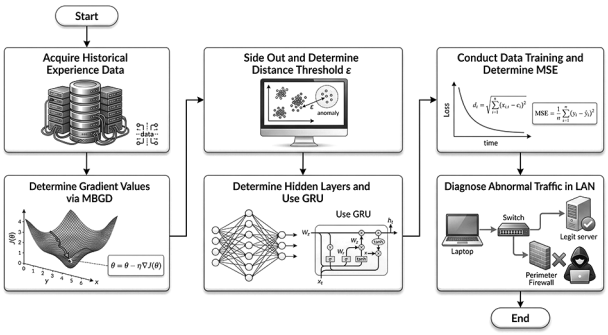

Fig. 4. Work flow of anomaly detection in a local network based on the FCRNN-GRU model

Step 4: Threshold setting and training. A control distance threshold ε is defined. The training process continues until the mean squared error (MSE) stabilizes, ensuring that the loss function remains within a low-fluctuation range.

Step 5: Detection and evaluation. At this stage, the obtained prediction results are compared with reference (target) values. Deviations exceeding the defined threshold are classified as anomalous events. Such events may include port scanning, brute-force password attacks, or unauthorized data deletion.

The overall workflow combines adaptive gradient optimization, a sliding window mechanism, and controlled recurrent learning into a unified anomaly detection system. The proposed algorithm ensures stable convergence under large-scale network traffic processing conditions, reduces the risk of gradient vanishing, efficiently utilizes computational resources, and supports continuous real-time anomaly detection.

The combination of MBGD optimization and the GRU-enhanced FCRNN architecture significantly improves detection robustness in a dynamic local network environment.

The study used the open network dataset DBLP Datasets, which contains three types of HTTP traffic: PUT, POST (P5SO), and GET requests [6, 16].

The structure of the dataset allows for a comprehensive evaluation of the model's ability to detect both large-scale network attacks, such as DDoS, and more complex targeted application-layer attacks, including logical injections. A balanced ratio of normal and anomalous samples provides a more objective assessment of detection effectiveness and reduces the risk of bias toward the dominant class.

The experimental study of the anomaly detection task was conducted using the Mininet emulation platform, which enables the reproduction of computer network topologies and the simulation of various network interaction scenarios with a level of detail close to real-world conditions.

The FCRNN-GRU model was implemented in Python 3.5. Experiments and result evaluation were performed using specialized Python scripts in a Linux operating system environment. This approach ensured controlled generation of network traffic, stability and reproducibility of experimental results, scalability of input data volumes, and precise measurement of performance metrics for further analysis.

The effectiveness of the proposed FCRNN-GRU model was evaluated using three key parameters specifically selected to measure the accuracy and reliability of anomaly detection in network traffic [20, 21]

$$DR = \frac{TP}{TP + FN} \cdot 100\ \%; \tag{10}$$

$$FAR = \frac{FP}{FP + TN} \cdot 100\ \%; \tag{11}$$

$$ACC = \frac{TP + TN}{TP + TN + FP + N} \cdot 100\ \%, \tag{12}$$

where TP denotes the number of cases in which the model correctly identified an anomaly; TN denotes the number of cases in which the model correctly classified normal traffic as normal; FP denotes the number of cases in which normal traffic was incorrectly classified as anomalous (false alarm); FN denotes the number of cases in which the model failed to detect a real anomaly, incorrectly classifying it as normal traffic.

DR, also known as detection rate (or sensitivity), reflects the model's ability to identify real threats. It represents the proportion of correctly detected anomalies relative to the total number of actual anomalies in the dataset. A high DR value is critical for security systems, as it minimizes the likelihood of missing an attack.

FAR represents the false alarm rate of the model. It indicates the proportion of normal traffic that is incorrectly classified as anomalous. An excessively high FAR is undesirable, as it increases the workload of network administrators and may lead to ignoring real threats due to the large number of false alerts.

ACC indicates the overall proportion of correct classifications (both anomalous and normal packets) relative to the total number of samples in the dataset. This metric provides a general view of model performance; however, in conditions of class imbalance (when normal traffic significantly exceeds anomalous traffic), it should be interpreted only together with DR and FAR to obtain an objective assessment. For high-performance operation of the FCRNN-GRU model in real-world conditions, it is necessary to maximize DR (approaching 100 %) and minimize FAR (approaching 0 %). The combination of these metrics enables a comprehensive evaluation of the model's ability to distinguish critical threats in a dynamic network environment.

The overall dataset of 52,000 requests was randomly divided into 10 test groups. For each group, DR, FAR, and ACC values were calculated separately (Tables 1–3).

The FCRNN-GRU model demonstrates consistently high anomaly detection performance across all test sets. On average, the detection rate exceeds 98 %, indicating its ability to correctly identify the majority of malicious or atypical network events. At the same time, the false alarm rate is maintained at approximately 5 %, which reflects sufficient robustness of the model against incorrect classification of legitimate traffic.

The overall accuracy, exceeding 99 %, further confirms the stability and reliability of the proposed architecture under various network load scenarios and changing traffic structures.

Statistical detection methods demonstrate a moderate level of effectiveness, achieving an average attack de-

Table 1

Indicators of the FCRNN-GRU model

Test group	DR, %	FAR, %	ACC, %
1	98.12	5.84	99.03
2	98.67	5.21	99.26
3	97.94	6.02	98.88
4	99.08	4.76	99.41
5	98.53	5.33	99.17
6	99.21	4.69	99.46
7	98.05	5.97	98.94
8	98.74	5.08	99.28
9	98.36	5.44	99.12
10	99.15	4.58	99.52
Average value	98.59	5.29	99.21

Table 2

Statistical anomaly detection algorithms

Test group	DR, %	FAR, %	ACC, %
1	87.42	9.88	89.74
2	86.95	10.36	88.91
3	88.13	9.64	90.12
4	89.54	8.97	91.03
5	87.86	9.45	89.67
6	90.12	8.74	92.18
7	86.73	10.21	88.54
8	88.47	9.32	90.41
9	87.69	9.87	89.96
10	89.98	8.69	91.84
Average value	88.29	9.51	90.24

Table 3

Anomaly detection algorithm based on clustering and indicators

Test group	DR, %	FAR, %	ACC, %
1	89.31	10.74	90.63
2	88.64	11.08	89.97
3	87.92	11.56	89.14
4	90.48	9.83	91.76
5	89.75	10.27	90.85
6	91.06	9.54	92.34
7	88.53	10.92	89.72
8	89.68	10.15	90.93
9	88.97	10.61	90.18
10	91.34	9.27	92.58
Average value	89.57	10.40	90.81

tection rate (DR) of approximately 88 %. At the same time, a relatively high false alarm rate of around 10 % is observed, indicating certain limitations of these approaches when dealing with complex and dynamic network traffic patterns. In particular, methods based on fixed threshold values are not sufficiently adaptive to changes in traffic structure and behavior.

Although in some experimental runs the overall accuracy exceeds 90 %, the variability of results across different test sets indicates insufficient stability and limited generalization capability of the method.

Clustering-based approaches show some improvement in detection speed compared to traditional statistical methods. However, this improvement is accompanied by an increase in the number of false positives, which negatively affects their practical applicability in real-world network environments. As a result, despite higher operational efficiency, the overall detection quality remains insufficiently stable for reliable deployment without additional false-positive filtering mechanisms.

An elevated FAR indicates the model's sensitivity to natural variability in network traffic, which sometimes leads to the incorrect classification of legitimate activity as anomalous. Although the overall accuracy remains high (above 90 %), this approach is inferior to the FCRNN-GRU model in terms of stability, consistency of results, and the ability to provide timely and preventive threat detection.

Conclusions. The presented study introduces an approach to detecting anomalous network traffic in local networks based on the FCRNN-GRU architecture. The experimental results confirm the high effectiveness of the proposed method: the average detection rate reaches 98.59 %, the false alarm rate is 5.29 %, and the overall accuracy achieves 99.21 %. These results outperform traditional statistical and clustering-based methods.

Thanks to the combination of a fully connected recurrent architecture with GRU modules, the model effectively captures temporal dependencies in the data, ensures stable training through mini-batch gradient optimization, and demonstrates high adaptability to dynamic changes in network traffic. The proposed approach is suitable for real-time deployment in local networks and provides scalable, accurate, and reliable anomaly detection for modern cybersecurity tasks.

Future research directions include optimizing the computational complexity of the FCRNN-GRU model for integration into resource-constrained hardware solutions (e.g., routers or IoT devices), as well as testing its robustness under extreme peak loads of real network traffic.

Discussion. Previous studies on statistical and clustering-based anomaly detection have reported moderate performance, with a detection rate (DR) of around 88–90 % and a false alarm rate (FAR) of approximately 10 %, often under conditions of high intra-class variability [4, 11]. Deep learning models, such as LSTM- and GRU-based architectures, have improved temporal modeling and reduced FAR; however, they still face challenges related to computational complexity and adaptation to dynamic local network environments [4–8, 11].

The proposed FCRNN-GRU model outperforms these methods, achieving an average DR of 98.59 %, FAR of 5.29 %, and ACC of 99.21 %. Fully connected recurrent layers with gated units effectively capture sequential traffic patterns, while mini-batch gradient optimization ensures stable and efficient training. The model demonstrates reliable generalization across different network conditions and is capable of detecting both known and previously unseen anomalies in real time, making it well-suited for operational deployment in local networks.

However, several limitations of the proposed approach should be highlighted. First, the model requires prior accumulation of data within a time window of size T before initiating the classification process, which introduces a minimal delay at the initial stage of session monitoring. Second, anomaly detection performance may degrade in scenarios where attackers use advanced obfuscation techniques or payload encryption (e.g., HTTPS/TLS v1.3). In such cases, classification must rely solely on flow metadata and statistical temporal packet distribution features, which requires further investigation.

References.

1. Haidur, H. I., Gakhov, S. O., & Bryhynets, A. A. (2023). Detection of network anomalies using neural network algorithms. *Telecommunication and Information Technologies, 1*, 016173. https://doi.org/10.31673/2412-4338.2023.016173

2. Ilyenko, A., Ilyenko, S., Kravchuk, I., & Herasymenko, M. (2022). Prospective directions for traffic analysis and intrusion detection based on neural networks. *Cybersecurity: Education, Science, Technique, 1*(17), 46-56. https://doi.org/10.28925/2663-4023.2022.17.4656

3. Marchenko, R., Kovalenko, A., & Znaidiuk, V. (2024). Analysis of methods for detecting anomalous traffic in Internet of Things (IoT)

networks. *Systems of Control, Navigation and Communication, 1*(1), 133-147. https://doi.org/10.26906/SUNZ.2024.1.133
4. Al-Ghuwairi, A. R., Sharrab, Y., Al-Fraihat, D., Al-Ghazi, M., & Khatatneh, M. (2023). Intrusion detection in cloud computing based on time series anomalies utilizing machine learning. *Journal of Cloud Computing, 12*, 127. https://doi.org/10.1186/s13677-023-00491-x
5. Almuhanna, R., & Dardouri, S. (2025). A deep learning/machine learning approach for anomaly based network intrusion detection. *Frontiers in Artificial Intelligence, 8*, 1625891. https://doi.org/10.3389/frai.2025.1625891
6. Alsyaibani, O. M. A., Utami, E., Raharjo, S., & Hartanto, A. D. (2022). Stacked LSTM-GRU model for traffic anomalies detection. *Telematika, 15*(2), 81-91. https://doi.org/10.35671/telematika.v15i2.1855
7. Oğuz, H. T., & Kalaycıoğlu, A. (2022). Anomaly detection in multi-tiered cellular networks using LSTM and 1D CNN. *Journal on Wireless Communications and Networking, 101*. https://doi.org/10.1186/s13638-022-02183-7
8. Wang, Y.-C., Houng, Y.-C., Chen, H.-X., & Tseng, S.-M. (2023). Network anomaly intrusion detection based on deep learning approach. *Sensors, 23*(4), 2171. https://doi.org/10.3390/s23042171
9. Lebid, O. V., Kiporenko, S. S., & Vovk, V. Y. (2023). Cyberattack detection and information security enhancement based on neural network technology in the conditions of cyberwar. *Science and Technology Today, 1*(15), 238-256. https://doi.org/10.52058/2786-6025-2023-1(15)-238-256
10. Lebid, O. V., & Kiporenko, S. S. (2024). Integration of fractal analysis and machine learning for anomaly and cyberattack detection. *Science and Technology Today, 12*(40), 1294-1313. https://doi.org/10.52058/2786-6025-2024-12(40)-1294-1313
11. Sisoienko, S., Babenko, V., & Zazhoma, V. (2025). Local area network traffic monitoring system with anomaly detection functionality. *Science and Technology Today*, *6*(47), 1608-1619. https://doi.org/10.52058/2786-6025-2025-6(47)-1608-1619
12. Chikov, I., Khaietska, O., Okhota, Yu., Titov, D., Prygotsky, V., & Nitsenko, V. (2023). Modeling of the synthetic indicator of competitiveness of agricultural enterprises: a methodological approach to the use of neural network tools. *Financial and Credit Activity: Problems of Theory and Practice*, *5*(52), 222-242. https://doi.org/10.55643/fcaptp.5.52.2023.4149
13. Bieliatynskyi, A., Bakulich, O., Bokyi, A., Kis, I., & Piven, O. (2024). Conceptual Model of Digital Transformation of Enterprise Management Processes. In E. Faure, Yu. Tryus, T. Vartiainen, O. Danchenko, M. Bondarenko, C. Bazilo, & G. Zaspa (Eds.). *Information Technology for Education, Science, and Technics. ITEST 2024. Lecture Notes on Data Engineering and Communications Technologies, 222*. Springer, Cham. https://doi.org/10.1007/978-3-031-71804-5_4
14. Jain, G., Sharma, M., & Agarwal, B. (2019). Optimizing semantic LSTM for spam detection. *International Journal of Information Technology, 11*(2), 239-250. https://doi.org/10.1007/s41870-018-0157-5
15. Yu, Y., Si, X., Hu, C., & Zhang, J. (2019). A review of recurrent neural networks: LSTM cells and network architectures. *Neural Computation, 31*, 1235-1270. https://doi.org/10.1162/neco_a_01199
16. Khoroshko, V. A., Tkach, Yu. N., & Shelest, M. E. (2021). Multialternative detection of cyberatacs in information networks. *Ukrainian Scientific Journal of Information Security, 26*(3), 136-141. https://doi.org/10.18372/2225-5036.27.16001
17. Mahbub, M. (2020). Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics. *Journal of Network and Computer Applications, 168*. https://doi.org/10.1016/j.jnca.2020.102761
18. Valackienė, A., & Odejayi, R. O. (2024). The impact of cyber security management on the digital economy: multiple case study analysis. *Intellectual Economics, 18*(2), 261-283. https://doi.org/10.13165/IE-24-18-2-02
19. Ślesicka, A., & Ślesicki, B. (2025). The use of deep learning for military vehicle identification in SAR imagery. *Scientific Journal of Silesian University of Technology. Series Transport, 128*, 251-268. https://doi.org/10.20858/sjsutst.2025.128.14
20. Ingram, K., Diachenko, O., Halytskyi, O., Nitsenko, V., Romaniuk, M., & Zhumbei, M. (2022). Formalization of the Optimal Choice of the Activities of Agricultural Enterprises for the Implementation of Information and Communication Technologies. *Financial and Credit Activity: Problems of Theory and Practice, 3*(44), 141-149. https://doi.org/10.55643/fcaptp.3.44.2022.3758
21. Kobets, D., Kasmin, D., Khruschak, S., Ziyautdinov, J., & Vodolazhska, T. (2025). Using artificial intelligence to optimize human resource management processes. *Periodicals of Engineering and Natural Sciences, 13*(3), 541-550. https://doi.org/10.21533/pen.v13.i3.504

Виявлення аномалій у локальному трафіку за допомогою безпечних гейтінг-мереж

О. В. Лебідь[1], *І. А. Чіков*[*1], *С. В. Хрущак*[1], *С. В. Стріха*[2], *О. Б. Півень*[3], *М. С. Коваленко*[4,5]

1 – Вінницький національний аграрний університет, м. Вінниця, Україна
2 – Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, м. Черкаси, Україна
3 – Черкаський державний технологічний університет, м. Черкаси, Україна
4 – Фонд SCIRE, м. Варшава, Польща
5 – Міжрегіональна академія управління персоналом, м. Київ, Україна
[*] Автор-кореспондент e-mail: ilya95chikov@gmail.com

Мета. Розроблення й оцінка методики виявлення аномалій у локальному мережевому трафіку на основі архітектури FCRNN-GRU для підвищення точності класифікації та зниження рівня хибнопозитивних спрацювань.

Методика. У межах дослідження мережеві взаємодії подано як нормовані часові послідовності, що дає змогу ураховувати динаміку змін трафіку. Базовою моделлю виступає повнозв'язана рекурентна нейронна мережа, здатна виявляти складні нелінійні й довготривалі залежності завдяки щільній структурі рекурентних зв'язків. Для підвищення ефективності навчання й уникнення проблеми зникнення градієнтів використано міні-пакетний стохастичний градієнтний спуск. Додаткова інтеграція GRU (Gated Recurrent Unit – керований рекурентний модуль) дозволяє оптимізувати співвідношення між точністю моделі та її обчислювальною складністю. Експериментальна перевірка проведена на вибірці з 52 000 мережевих потоків, серед яких 32 000 відповідають нормальному трафіку, а 20 000 – аномальному, що охоплює різні типи кіберзагроз. Моделювання мережевого середовища здійснювалося на платформі Linux із використанням інструментів Mininet і Wireshark, тоді як програмна реалізація алгоритмів виконувалася мовою Python.

Результати. Модель FCRNN-GRU демонструє високі показники: коефіцієнт виявлення – 98,59 %, рівень хибних тривог – 5,29 %, точність класифікації – 99,21 %. Порівняно із традиційними та кластерними методами, запропонований підхід забезпечує суттєве покращення результатів і підтверджує свою ефективність.

Наукова новизна. Полягає в адаптації повнозв'язаної рекурентної нейронної мережі з інтеграцією керованих рекурентних одиниць для задач аналізу мережевого трафіку. Поєднання щільних рекурентних зв'язків із механізмами GRU дає змогу більш точно відтворювати часові закономірності поведінки трафіку, водночас зменшуючи обчислювальні витрати й підвищуючи ефективність моделі в умовах обробки великих обсягів даних.

Практична значимість. Запропонований підхід має прикладне значення й може бути інтегрований у сучасні системи моніторингу й забезпечення кібербезпеки. Його використання сприяє своєчасному виявленню аномальних подій у мережі, підвищенню рівня захищеності інформаційної інфраструктури та зниженню ризиків, пов'язаних із кіберзагрозами.

Ключові слова: *мережеві аномалій, потік трафіку, аналітика кібербезпеки, нейронні мережі, інформаційна безпека*