УДК 004.056.5:004.7 DOI: 10.31673/2412-9070.2026.049412

G. GRYNKEVYCH[1], PhD, Associate Professor;
ORCID: 0000-0003-1922-5165
V. VASYLENKO[1], PhD, Associate Professor;
ORCID: 0000-0001-8465-6178
D. RUDIN[2], Independent researcher, IEEE Senior member, Platform Engineer;
ORCID: 0009-0007-4171-4973
O. PLIEKHOV[3], Independent researcher, IEEE Senior member,
ORCID: 0009-0000-1343-4308
[1]State University of Information and Communication Technologies, Kyiv
[2]Capital One, Plano, Texas, USA
[3]Mercury Intermedia, Inc., Brentwood, TN, USA

DESIGN AND IMPLEMENTATION OF AUTOMATED FIREWALL POLICY MANAGEMENT IN ENTERPRISE TELECOMMUNICATION SYSTEMS USING INFRASTRUCTURE-AS-CODE

The paper presents an approach to automating firewall policy management in enterprise telecommunication systems using Infrastructure-as-Code and Security-as-Code practices. The relevance of the study is driven by the increasing complexity of network infrastructures, the growing number of interconnected services, and the need to ensure a high level of cybersecurity while reducing operational costs. Traditional approaches to managing firewall access rules, which rely on manual configuration, are associated with a high probability of errors, slow deployment of changes, and limited process transparency, which negatively affects both security and operational efficiency.

The study analyzes existing approaches to network security automation, including policy-as-code practices, integration with change management systems, and pipeline-based request processing. A model of an automated firewall policy management system is proposed, which includes the use of a centralized configuration repository, automated validation of access requests, network path analysis, and generation of implementation plans.

Special attention is given to the integration with telecommunication infrastructure, including analysis of network zones, traffic flows, and service dependencies. The proposed approach ensures consistency of access policies, improves control over configuration changes, and reduces risks associated with misconfigurations. A modular system design is considered, enabling adaptability to evolving technological environments.

Additionally, the system incorporates a two-stage risk classification model for automated request evaluation and a priority-aware concurrent processing mechanism that ensures preemption of time-sensitive security operations.

The results demonstrate that automation significantly reduces manual effort, improves processing speed of access requests, and enhances service delivery quality. The approach also increases transparency and repeatability of changes while minimizing human-related errors.

Keywords: firewall policy automation, network security, infrastructure as code, security as code, telecommunication systems, access control, cybersecurity.

Introduction

Modern enterprise telecommunication systems operate in conditions of rapidly increasing complexity, driven by the expansion of distributed infrastructures, cloud services, and interconnected applications. The number of endpoints, services, and network interactions continues to grow, resulting in a significant increase in the volume of traffic and security-related events. In such environments, ensuring secure and controlled access between network segments becomes a critical requirement for maintaining both system reliability and cybersecurity [5], [10], [13].

At the same time, the global threat landscape is evolving, with cyberattacks becoming more sophisticated and automated. Recent industry reports indicate a steady growth in both the number and complexity of attacks, including lateral movement within networks and exploitation of misconfigured access controls. In enterprise infrastructures, firewall policies play a key role in controlling traffic flows, enforcing segmentation, and limiting unauthorized access. However, the effectiveness of these mechanisms depends on the correctness, consistency, and timely update of policy rules.

Traditional approaches to firewall policy management are largely based on manual configuration and fragmented workflows. Such processes are time-consuming, error-prone, and difficult to scale in large environments. Misconfigurations, delays in implementing access changes, and lack of transparency in decision-making processes can lead to security vulnerabilities and operational inefficiencies. As infrastructures grow, these limitations become increasingly critical, especially in organizations with complex telecommunication architectures.

In recent years, Infrastructure-as-Code has emerged as a promising approach for managing infrastructure and network configurations in a structured and automated manner. By representing configuration states as code stored in version-controlled repositories, IaC enables repeatability, traceability, and consistency of changes across systems [6]. This approach shifts operational processes from manual execution to controlled and auditable workflows, improving both efficiency and security.

The concept of Security-as-Code extends these principles by integrating security policies directly into automated pipelines. This allows validation of access rules, enforcement of compliance requirements, and early detection of configuration issues before deployment. The integration of IaC and Security-as-Code creates a foundation for automated policy management systems that can significantly improve the quality and reliability of firewall configurations.

Despite the growing adoption of these approaches, the implementation of automated firewall policy management in enterprise telecommunication environments remains a complex task. Challenges include the need to integrate multiple systems, ensure accurate modeling of network topology and traffic flows, and maintain consistency between intended and actual configurations.

Therefore, there is a need for a structured approach to designing and implementing automated firewall policy management systems that combine principles of Infrastructure-as-Code, Security-as-Code, and modern network architecture. Such an approach should not only improve cybersecurity but also enhance operational efficiency and provide measurable economic benefits in large-scale enterprise environments.

Problem statement

In modern enterprise telecommunication systems, firewall policy management remains a critical component of cybersecurity and network control. Firewalls are responsible for regulating traffic between network segments, enforcing access restrictions, and supporting segmentation strategies that limit the spread of threats. However, as infrastructures grow in scale and complexity, the management of firewall rules becomes increasingly difficult and resource-intensive.

One of the main challenges is the reliance on manual or semi-automated processes for defining, reviewing, and implementing access rules. In large environments, firewall policies may consist of thousands of rules distributed across multiple devices and logical zones. Maintaining consistency across these rules is difficult, especially when changes are requested frequently and must be implemented under time constraints. This often leads to configuration errors, redundant or conflicting rules, and reduced transparency in policy management.

Another significant problem is the lack of integration between network infrastructure, security policies, and operational workflows. In many organizations, firewall changes are initiated through separate systems, such as service management platforms, and then implemented manually by engineers. This separation creates a gap between the intended access requirements and the actual configuration applied to the network. As a result, it becomes difficult to verify whether implemented policies accurately reflect approved requests, which complicates auditing and increases security risks.

From a cybersecurity perspective, misconfigured firewall rules represent a major attack vector. Incorrectly defined access permissions can expose internal services, enable unauthorized communication between network segments, or allow lateral movement within the infrastructure. In addition, the

absence of systematic validation mechanisms makes it difficult to detect such issues before they impact system security.

The problem is further complicated by the dynamic nature of modern telecommunication environments. Changes in application architecture, deployment of new services, and frequent updates in infrastructure require continuous adaptation of firewall policies. Manual processes are not capable of responding to such changes with sufficient speed and reliability, leading to delays in service deployment and increased operational overhead.

At the same time, organizations face the need to optimize operational costs and improve efficiency. Manual policy management requires significant human effort for analysis, implementation, and troubleshooting. This increases the workload on engineering and security teams and limits their ability to focus on higher-level tasks.

Thus, the key problem addressed in this study is the lack of an integrated, scalable, and automated approach to firewall policy management that can ensure consistency, reduce errors, improve security, and decrease operational costs in enterprise telecommunication systems. The solution to this problem requires the development of a unified model that combines network-aware policy analysis, automated validation mechanisms, and Infrastructure-as-Code principles within a single operational framework.

Analysis of recent research and publications

Recent research in the field of cybersecurity and network infrastructure management demonstrates a growing shift toward automation and formalization of security processes. One of the fundamental approaches is based on structured threat modeling frameworks, such as MITRE ATT&CK, which provide a systematic representation of adversarial techniques and are widely used for designing detection and control mechanisms in enterprise environments [13]. In parallel, standardized security controls defined by NIST establish a comprehensive foundation for implementing and managing access policies, including network segmentation and traffic filtering [5].

A significant body of work focuses on the application of Infrastructure-as-Code principles to cybersecurity. These studies highlight the benefits of representing infrastructure configurations, including network and firewall rules, as version-controlled code. Such an approach ensures consistency, traceability, and reproducibility of changes across distributed systems [6]. Furthermore, recent research emphasizes the transition from static configurations to dynamic and automated policy management systems, where infrastructure changes are processed through predefined pipelines [8].

The concept of Security-as-Code extends these ideas by integrating security controls directly into development and operational workflows. In this context, security policies are treated as programmable entities that can be validated, tested, and enforced automatically. Modern approaches also incorporate DevSecOps principles, enabling continuous integration of security mechanisms into system deployment processes [2], [11]. This allows organizations to shift security controls earlier in the lifecycle and reduce the risk of misconfigurations.

Another important direction is the study of automated analysis and validation of network configurations. Research in this area explores methods for evaluating access rules, detecting conflicts, and ensuring compliance with predefined security models. In particular, attention is given to the automation of decision-making processes related to access control, where systems can analyze traffic patterns and determine appropriate firewall rules based on predefined policies [1].

In recent years, artificial intelligence has also been actively integrated into cybersecurity processes. Machine learning techniques are used for anomaly detection, risk assessment, and prediction of potential threats. More advanced approaches involve the use of explainable AI and large language models to support configuration analysis and assist in decision-making processes [4], [9], [12]. These technologies enable more efficient processing of large volumes of data and provide additional insights into complex system behavior.

At the same time, industry reports confirm the increasing importance of automation in response to the growing number of cyber threats and the complexity of enterprise infrastructures. The use of automated security solutions is associated with improved response time, reduced operational overhead, and enhanced system reliability. Recent studies also explore the application of AI-driven approaches to generate and validate Infrastructure-as-Code configurations, further expanding the capabilities of automated systems [3].

Despite these advances, existing research often focuses on individual aspects of the problem, such as infrastructure automation, security policy enforcement, or AI-based analysis. There is a lack of integrated approaches that combine these components into a unified framework specifically tailored for firewall policy management in enterprise telecommunication systems. In particular, insufficient attention is given to the combination of network-aware analysis, automated policy validation, and Infrastructure-as-Code practices within a single operational model.

Therefore, the need remains for a comprehensive approach that integrates automation, cybersecurity, and telecommunication infrastructure management into a unified system capable of ensuring both security and operational efficiency.

Purpose and objectives of the study

The purpose of this study is to develop and justify an approach to automated firewall policy management in enterprise telecommunication systems based on Infrastructure-as-Code and Security-as-Code principles, aimed at improving cybersecurity, increasing operational efficiency, and reducing the risks associated with manual configuration processes.

To achieve this purpose, the following objectives are defined:

1. To analyze existing approaches to firewall policy management in enterprise environments and identify their limitations in terms of scalability, reliability, and security.
2. To examine the applicability of Infrastructure-as-Code and Security-as-Code concepts for managing network access policies in complex telecommunication systems.
3. To develop a conceptual model of an automated firewall policy management system that integrates network analysis, validation mechanisms, and configuration pipelines.
4. To design a risk classification model for automated request evaluation and a concurrency model for priority-aware processing of competing requests.
5. To describe the process of automated request handling, including data collection, traffic path analysis, and generation of implementation plans.
6. To evaluate the impact of automation on operational processes, including reduction of manual effort, improvement of implementation speed, and increase in configuration accuracy.
7. To identify potential limitations and risks associated with the proposed approach, including dependencies on external systems and integration complexity.
8. To outline the practical conditions for implementing the proposed model in real enterprise environments and define directions for further development.

Results of the study

This section presents the main results of the study related to the design and implementation of an automated firewall policy management approach in enterprise telecommunication systems. The focus is placed on the structural organization of the system, the logic of automated processing of access requests, and the evaluation of its operational and security impact.

The proposed solution is analyzed from both technical and practical perspectives, including architectural design, workflow automation, and integration with existing infrastructure. Special attention is given to ensuring consistency of access policies, improving control over network interactions, and reducing the risks associated with manual configuration processes.

Concept of Automated Firewall Policy Management

The proposed approach is based on transforming firewall policy management from a manual, device-oriented process into a structured and automated workflow driven by declarative definitions. In this model, access policies are represented as code and stored in a centralized version-controlled repository. This allows all changes to be tracked, reviewed, and reproduced, ensuring consistency across the entire infrastructure.

The key idea of the approach is to separate the definition of intended access from the execution of configuration changes. Instead of directly modifying firewall rules, users submit structured requests that describe the required access. These requests are processed by the automation system, which performs validation, analysis, and controlled deployment.

Architecture of the Proposed System

The architecture of the automated firewall policy management system is designed as a modular pipeline that integrates multiple components responsible for data processing, validation, and execution.

The system includes the following functional elements:

- a request interface that allows users to submit access requests through structured forms or repository changes;
- a centralized repository that stores policy definitions and access mappings;
- a data collection module that gathers information about network topology, zones, and existing configurations;
- an analysis module that evaluates traffic paths and identifies affected network segments;
- a risk classification module that evaluates requests against a two-stage composite model;
- a validation engine that checks requests against predefined security rules and policies;
- an execution module incorporating a priority-ordered queue that schedules and applies configuration changes based on assigned request priorities;
- integration modules that connect the system with external platforms such as service management and infrastructure tools.

Fig. 1. Architecture of the automated firewall policy management system

Automated Request Processing Workflow

The automated workflow begins with the submission of an access request. Instead of directly implementing changes, the system performs a sequence of steps to ensure correctness and security.

The workflow includes:

- validation of input data and completeness of the request;
- identification of source and destination zones;
- analysis of the traffic path across the network;
- determination of firewall devices and policy layers involved;
- evaluation of requested access against predefined risk criteria;
- generation of a detailed implementation plan.

The implementation plan contains all necessary configuration changes and is presented for review and approval. This approach reduces the need for manual analysis and ensures that all decisions are based on consistent rules.

The automated processing of firewall policy requests is implemented through a structured workflow that integrates user interaction, validation, approval, and configuration deployment stages. The overall process is illustrated in fig. 2.

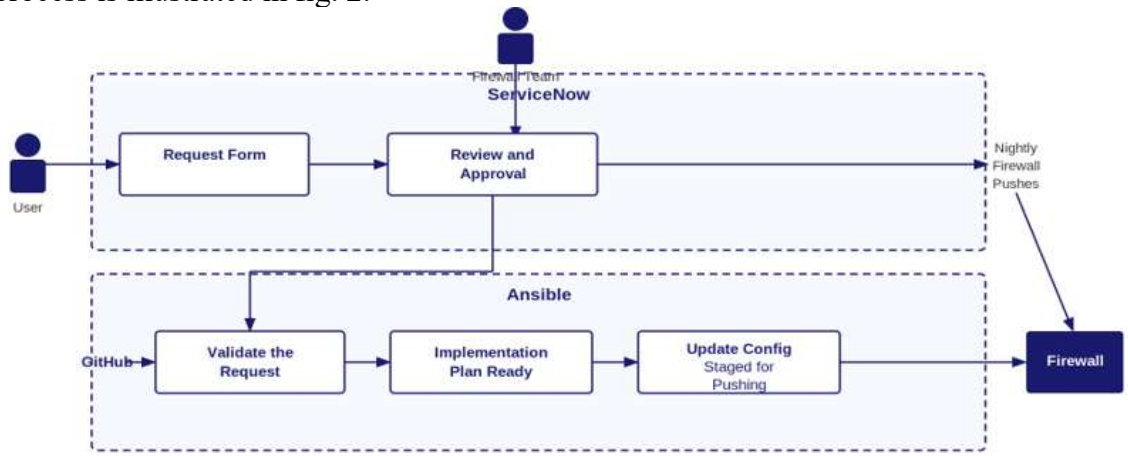

Fig. 2. Automated firewall policy request processing workflow

Network-Aware Policy Analysis

An important feature of the proposed system is its ability to analyze network topology and traffic flows. Instead of applying generic rules, the system evaluates how traffic will traverse the infrastructure and determines the exact points where policies must be enforced.

This includes:

- mapping traffic paths through network zones;
- identifying dependencies between services;
- detecting potential conflicts with existing rules;
- ensuring that access policies align with segmentation strategies.

Such analysis improves the accuracy of policy implementation and reduces the likelihood of unintended access.

Security and Validation Mechanisms

The system incorporates a set of validation mechanisms designed to ensure compliance with security requirements. Access requests are checked against predefined policies, including restrictions on prohibited connections and requirements for additional review in high-risk scenarios.

Risk evaluation is performed using a structured access matrix that classifies requests based on their potential impact. Requests that exceed predefined thresholds are flagged for manual review. This ensures that automation does not compromise security while still reducing the overall workload.

In addition, the system maintains traceability between requested, approved, and implemented changes. This enables effective auditing and simplifies incident investigation.

Two-Stage Risk Classification Model

The risk evaluation mechanism described above is implemented as a two-stage composite classifier inspired by analogous architectures applied to short-text classification under constrained-runtime conditions [7]. The first stage operates over a deterministic rule set encoding regulatory compliance restrictions, prohibited zone pairs, and protocol-level blacklists derived from organizational security policy. Requests matching any rule that mandates manual review or denial are routed to the corresponding workflow without further processing.

Requests not matched by deterministic rules are forwarded to the second stage, which applies a lightweight classification model to the structured request description, source-destination metadata, and free-text justification field. The model assigns each request to one of four risk tiers - CRITICAL, HIGH, NORMAL, and LOW - mirroring the tier structure commonly used in incident management practice.

A minimum confidence threshold τ is applied to all model outputs. Predictions where $\max(p) < \tau$ are downgraded to require manual review regardless of the predicted tier. This design reflects an asymmetric error-cost model: a false negative - inadvertent automatic approval of a risky request - is operationally more costly than a false positive that escalates a benign request for manual review. The threshold value is selected based on the operational tolerance of the security team and may be tuned per deployment environment.

The two-stage design also provides graceful degradation. When the model artifact is unavailable or its preconditions are not met - for example, when a request contains insufficient text for reliable inference - the system falls back to the deterministic rule layer alone, preserving baseline functionality without forcing the request out of the automated pipeline.

Priority-Aware Concurrent Request Processing

In real enterprise deployments, multiple access-change requests arrive concurrently, originating from different teams and targeting different segments of the network. A naive implementation that processes requests in strict first-in-first-out order may delay time-sensitive security operations - such as emergency revocation of compromised credentials or rapid blocking of newly disclosed vulnerable services - behind routine, non-urgent requests already in the pipeline.

To address this, the execution module incorporates a priority-ordered queue protected by a mutex and driven by a single-consumer actor pattern. Each request is assigned a priority value at the valida-

tion stage based on its risk classification (Section 5.5.1) and on contextual flags such as active incident-response operations. The actor dequeues the highest-priority pending request first, ensuring that CRITICAL security operations preempt NORMAL and LOW priority requests regardless of arrival order. Mutex protection guarantees that each firewall device receives one configuration change at a time, eliminating race conditions that would otherwise arise when concurrent requests target overlapping rule sets.

This concurrency model has been previously evaluated in a related on-device messaging context, where replacing FIFO packet ordering with priority-based preemption reduced critical-message scheduling latency by approximately three orders of magnitude under saturated queue load [7]. The same architectural principle applies to the firewall management domain: the cost of delaying a critical security operation behind routine traffic is asymmetric and operationally significant, justifying preemptive scheduling at the execution layer.

Operational and Economic Impact

The implementation of the proposed approach leads to measurable improvements in operational efficiency. Automation reduces the time required to process access requests and minimizes the number of manual steps involved. As a result, engineering teams can focus on more complex tasks instead of routine configuration work.

From an economic perspective, the reduction of manual effort directly decreases operational costs. Faster processing of requests also improves service delivery and reduces delays in deploying new applications. The decrease in configuration errors leads to fewer incidents, which further reduces the cost associated with troubleshooting and service disruptions.

Table 1

Comparison of manual and automated firewall policy management

Parameter	Manual Management	Automated Management
Configuration process	Manual changes by engineers	Pipeline-based automated execution
Error probability	High	Low
Processing time	Slow	Fast
Scalability	Limited	High
Transparency	Low	High
Traceability	Limited	Full version control
Security consistency	Inconsistent	Policy-driven and validated
Operational cost	High	Reduced

Overall, the proposed system provides a balance between security, efficiency, and scalability. It enables organizations to manage firewall policies in a controlled and transparent manner while adapting to the dynamic nature of modern telecommunication environments.

Limitations of the Proposed Approach

Despite its advantages, the approach has several limitations. The system relies on integration with multiple external platforms, and its effectiveness depends on the availability and accuracy of data from these systems. Any inconsistency or failure in dependent systems may affect the automation workflow.

In addition, the implementation of such a system requires initial investment in design and integration. The complexity of the workflow may also require specialized expertise for maintenance and further development.

Nevertheless, these limitations are typical for complex enterprise systems and can be mitigated through proper design, monitoring, and continuous improvement of the platform.

Conclusions and future research

The study presents an approach to automated firewall policy management in enterprise telecommunication systems based on Infrastructure-as-Code and Security-as-Code principles. The proposed

model transforms traditional manual processes into a structured and controlled workflow, enabling consistent, transparent, and reproducible management of network access policies.

The results demonstrate that automation of firewall policy management significantly improves operational efficiency and reduces the risk of configuration errors. The use of centralized repositories and pipeline-based processing ensures traceability of changes and alignment between requested and implemented access. The integration of network-aware analysis allows for more accurate identification of affected segments and supports consistent enforcement of security policies.

Additionally, the system incorporates a two-stage risk classification model for automated request evaluation and a priority-aware concurrent processing mechanism based on an actor-mutex queue, ensuring that time-sensitive security operations preempt routine traffic in saturated request pipelines.

From a cybersecurity perspective, the proposed approach enhances control over network interactions and reduces the likelihood of misconfigurations that may lead to unauthorized access or lateral movement within the infrastructure. The inclusion of validation mechanisms and risk assessment improves the reliability of decision-making and supports compliance with predefined security requirements.

In addition, the study confirms the economic benefits of automation. The reduction of manual effort, acceleration of request processing, and decrease in the number of incidents contribute to lowering operational costs and improving overall service quality. The approach also supports scalability, making it applicable to large and dynamically evolving telecommunication environments.

At the same time, several limitations have been identified. The effectiveness of the system depends on the integration of multiple external platforms and the availability of accurate data. The initial implementation requires careful system design and configuration, as well as ongoing maintenance and adaptation to changes in infrastructure and technologies.

Future research may focus on further development of automated decision-making mechanisms, including the use of artificial intelligence for advanced policy analysis and optimization. Additional studies are required to evaluate system performance in real-world environments using quantitative metrics such as processing time, error rates, and resource utilization. Further work may also explore the integration of automated firewall policy management into broader cybersecurity frameworks and orchestration platforms.

Author Contributions

Ganna GRYNKEVYCH – conceptualization, methodology, development of the research framework, formulation of theoretical foundations, analysis of scientific sources, preparation of the literature review, definition of research objectives, supervision and coordination of the study, writing and editing of the manuscript; Volodymyr VASYLENKO – cybersecurity analysis, definition of security requirements, development of firewall policy management concepts, analysis of network security mechanisms, validation of the proposed approach from a cybersecurity perspective, contribution to risk assessment and policy validation logic; Dmytro RUDIN – system design and practical implementation aspects, development of the automated workflow model, analysis of infrastructure components and integration mechanisms, evaluation of performance and operational efficiency, contribution to architecture design and technical validation of the proposed solution; Oleksandr PLIEKHOV – design of the two-stage composite risk classification model for access request evaluation, design of the priority-aware concurrent request processing model based on actor-mutex serialization, integration of asymmetric error-cost reasoning into the validation pipeline.

Declaration on Artificial Intelligence

During the preparation of the article, artificial intelligence tools were used to a limited extent for auxiliary tasks, in particular for checking grammar, stylistic design and improving the quality of formulations. All main ideas, approaches, research results and conclusions were formulated by the authors independently.

Conflict of interest

The authors declare that there is no conflict of interest and confirm that during the preparation of this work there were no commercial, financial or other relationships that could be considered as being capable of influencing the results of the study or their interpretation. The work was carried out in accordance with the principles of academic integrity, ethical standards of scientific research and the requirements of the editorial policy on preventing conflicts of interest.

References

1. Callegati, F., Cerroni, W., & Ramilli, M. (2025). Investigating operational technology attacks as code. Empirical Software Engineering. https://doi.org/10.1007/s10664-025-10713-2

2. Coston, I. (2025). Enhancing secure software development with DevSecOps and Zero Trust integration. Applied Sciences, 15(3), 1234. https://doi.org/10.3390/app15031234

3. Li, Y., Zhang, H., & Chen, X. (2025). Security-aware infrastructure-as-code generation using large language models. arXiv. https://doi.org/10.48550/arXiv.2511.12385

4. Mohamed, N., & Altrjman, C. (2025). Advances in artificial intelligence and machine learning for cybersecurity. Cogent Engineering, 12(1). https://doi.org/10.1080/23311975.2025.2518496

5. National Institute of Standards and Technology. (2022). Security and privacy controls for information systems and organizations (SP 800-53 Rev. 5). https://doi.org/10.6028/NIST.SP.800-53r5

6. Pinto, R. (2023). Infrastructure as code for cybersecurity training. Journal of Cybersecurity Education, Research and Practice, 2023(1). https://doi.org/10.32727/8.2023.30

7. Pliekhov, O. (2026). AI-driven message prioritization for offline BLE mesh networks in disaster response scenarios. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.6428398

8. Rahman, A., & Williams, L. (2020). Software security in DevOps: Synthesizing practitioners' perceptions and practices. Proceedings of the IEEE/ACM International Conference on Software Engineering. https://doi.org/10.1145/3377811.3380366

9. Rudin, D., Vasylenko, V., & Grynkevych, G. (2025). AI agents for automated network incident detection and misconfiguration identification. Internauka. https://doi.org/10.25313/2520-2057-2025-12-12019

10. Rudin, D., Vasylenko, V., & Grynkevych, G. (2025). Data protection in Wi-Fi networks of financial institutions: WEP to WPA3 evolution and economic impact. Internauka. https://doi.org/10.25313/2520-2057-2025-8-12018

11. Rudin, D., Vasylenko, V., & Grynkevych, G. (2026). Adaptive network security automation: DevSecOps, ML detection, and policy-as-code. Internauka. https://doi.org/10.25313/2520-2057-2026-1-12020

12. Sharma, A. (2025). Explainable artificial intelligence in cybersecurity: A comprehensive review. ICT Express. https://doi.org/10.1016/j.icte.2025.10.004

13. Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). MITRE ATT&CK: Design and philosophy. MITRE Corporation. https://doi.org/10.13140/RG.2.2.31085.77280

Г. О. Гринкевич, В. В. Василенко, Д. Г. Рудін, О. В. Плєхов

ПРОЄКТУВАННЯ ТА ВПРОВАДЖЕННЯ АВТОМАТИЗОВАНОГО УПРАВЛІННЯ ПОЛІТИКАМИ МІЖМЕРЕЖЕВИХ ЕКРАНІВ У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ПІДПРИЄМСТВА НА ОСНОВІ ПІДХОДІВ INFRASTRUCTURE-AS-CODE

У роботі розглянуто підхід до автоматизації управління політиками міжмережевих екранів у корпоративних телекомунікаційних системах із використанням сучасних практик Infrastructure-as-Code та Security-as-Code. Актуальність дослідження зумовлена зростанням складності мережевих інфраструктур, збільшенням кількості взаємодіючих сервісів та необхідністю забезпечення високого рівня кібербезпеки при одночасному зниженні операційних витрат. Традиційні підходи до управління правилами доступу, що базуються на ручній конфігурації, характеризуються високою ймовірністю помилок, низькою швидкістю впровадження

змін та обмеженою прозорістю процесів, що негативно впливає на безпеку та ефективність функціонування системи.

У дослідженні проаналізовано існуючі підходи до автоматизації мережевої безпеки, зокрема використання політик доступу як коду, інтеграцію з системами керування змінами та застосування пайплайнів обробки запитів. Запропоновано архітектуру автоматизованої системи управління політиками міжмережевих екранів, яка включає використання централізованого репозиторію конфігурацій, механізмів перевірки запитів на відповідність політикам безпеки, автоматизованого аналізу мережевих маршрутів та формування планів впровадження змін.

Особливу увагу приділено інтеграції з телекомунікаційною інфраструктурою, включаючи аналіз мережевих зон, маршрутів трафіку та залежностей між сервісами. Запропонований підхід дозволяє забезпечити узгодженість політик доступу, підвищити рівень контролю та зменшити ризики, пов'язані з неправильною конфігурацією. Окремо розглянуто використання модульної архітектури, що забезпечує можливість адаптації системи до змін технологічного середовища.

Додатково запропоновано двостадійну модель класифікації ризику запитів для автоматизованої оцінки та механізм пріоритетної паралельної обробки, що забезпечує витіснення критичних операцій безпеки серед конкуруючих запитів.

У роботі також наведено оцінку ефективності запропонованого підходу з точки зору зниження трудовитрат, підвищення швидкості обробки запитів та покращення якості надання доступу. Визначено, що автоматизація дозволяє мінімізувати людський фактор, підвищити прозорість процесів та забезпечити відтворюваність змін у системі.

Отримані результати можуть бути використані для побудови сучасних систем управління мережевою безпекою в організаціях з розвиненою телекомунікаційною інфраструктурою, а також для подальшого розвитку підходів до автоматизації процесів кіберзахисту.

Ключові слова: автоматизація мережевої безпеки, міжмережеві екрани, Infrastructure-as-Code, Security-as-Code, телекомунікаційні системи, управління доступом, кібербезпека.

Надійшла до редакції: 15.06.2026
Прийнята до друку: 20.07.2026
Опубліковано: 17.08.2026