UDC 004.056.55+004.89 DOI https://doi.org/10.35546/kntu2078-4481.2026.1.39

I. O. ROZLOMII
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Information Security
and Computer Engineering
Cherkasy State Technological University
ORCID: 0000-0001-5065-9004

V. H. BABENKO
Doctor of Technical Sciences, Professor,
Professor at the Department of Information Security and Computer Engineering
Cherkasy State Technological University
ORCID: 0000-0003-2039-2841

V. M. ZAZHOMA
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Civil Protection and Information Systems
National University of Civil Protection of Ukraine
ORCID: 0000-0003-2083-2472

ARCHITECTURE OF A MODULAR EXPERT SYSTEM FOR VERIFICATION OF SECURITY POLICIES IN MULTI-TIER INFORMATION ENVIRONMENTS

The article considers the problem of security policy verification in multi-level, distributed and dynamic information environments. The limitations of traditional centralized approaches are shown in the context of the increasing complexity of modern information systems and the number of interconnected policies. The feasibility of using modular expert systems to increase the flexibility, scalability and adaptability of security policy verification processes is substantiated. The emphasis is on the need for formalized policy representation and automated detection of conflicts and gaps in access rules. The proposed approach is focused on use in heterogeneous environments with a multi-level security control structure. The aim of this study is to develop an architecture for a modular expert system for verifying security policies in multi-level information environments. The research is based on the use of methods of formalization of security policies, logical analysis of access rules and modular design of expert systems. Experimental modeling and comparative analysis with existing solutions were used to evaluate the effectiveness of the proposed approach. An architectural model of an expert system with independent verification modules synchronized through a centralized controller is proposed. Experimental results confirm an increase in the speed of policy verification, improved scalability, and reduced knowledge update time compared to traditional approaches. The scientific novelty lies in the combination of a modular approach with a hierarchical model of the information environment for verifying security policies. The proposed architecture provides consistent verification of policies at different levels without interfering with the internal logic of individual modules. The results obtained confirm the effectiveness of the modular expert system for application in complex information environments. The proposed approach can be used as a basis for creating tools for automated control and analysis of security policies in critical information systems.

Key words: *information security, expert system, policy verification, modular architecture, multi-tiered environment, access control.*

І. О. РОЗЛОМІЙ
кандидат технічних наук, доцент,
доцент кафедри інформаційної безпеки та комп'ютерної інженерії
Черкаський державний технологічний університет
ORCID: 0000-0001-5065-9004

В. Г. БАБЕНКО
доктор технічних наук, професор,
професор кафедри інформаційної безпеки та комп'ютерної інженерії
Черкаський державний технологічний університет
ORCID: 0000-0003-2039-2841

В. М. ЗАЖОМА
кандидат технічних наук, доцент,
доцент кафедри цивільного захисту та інформаційних технологій
Національний університет цивільного захисту України
ORCID: 0000-0003-2083-2472

АРХІТЕКТУРА МОДУЛЬНОЇ ЕКСПЕРТНОЇ СИСТЕМИ ДЛЯ ВЕРИФІКАЦІЇ ПОЛІТИК БЕЗПЕКИ В БАГАТОРІВНЕВИХ ІНФОРМАЦІЙНИХ СЕРЕДОВИЩАХ

У статті розглянуто проблему верифікації політик безпеки в умовах багаторівневих, розподілених та динамічних інформаційних середовищ. Показано обмеженість традиційних централізованих підходів у контексті зростання складності сучасних інформаційних систем і кількості взаємопов'язаних політик. Обґрунтовано доцільність застосування модульних експертних систем для підвищення гнучкості, масштабованості та адаптивності процесів перевірки політик безпеки. Акцент зроблено на необхідності формалізованого подання політик і автоматизованого виявлення конфліктів та прогалин у правилах доступу. Запропонований підхід орієнтований на використання в гетерогенних середовищах із багаторівневою структурою контролю безпеки. Метою дослідження є розробка архітектури модульної експертної системи для верифікації політик безпеки в багаторівневих інформаційних середовищах. Дослідження базується на використанні методів формалізації політик безпеки, логічного аналізу правил доступу та модульного проєктування експертних систем. Для оцінювання ефективності запропонованого підходу застосовано експериментальне моделювання та порівняльний аналіз із наявними рішеннями. Запропоновано архітектурну модель експертної системи з незалежними модулями верифікації, синхронізованими через централізований контролер. Експериментальні результати підтвердили підвищення швидкості перевірки політик, покращення масштабованості та зменшення часу оновлення знань порівняно з традиційними підходами. Наукова новизна полягає у поєднанні модульного підходу з ієрархічною моделлю інформаційного середовища для верифікації політик безпеки. Запропонована архітектура забезпечує узгоджену перевірку політик на різних рівнях без втручання у внутрішню логіку окремих модулів. Отримані результати підтверджують ефективність модульної експертної системи для застосування в складних інформаційних середовищах. Запропонований підхід може бути використаний як основа для створення інструментів автоматизованого контролю та аналізу політик безпеки в критично важливих інформаційних системах.

Ключові слова: *інформаційна безпека, експертна система, верифікація політик, модульна архітектура, багаторівневе середовище, контроль доступу.*

Introduction

In modern information systems characterized by distribution, multi-level access and dynamically changing security policies, the issue of verifying compliance with these policies is becoming particularly relevant [1]. The growth of data volume, the complexity of interaction between subsystems of different levels of trust and the need to adapt to new threats require not only static, but also dynamic means of monitoring the implementation of security policies [2]. Classical methods that rely on manual verification or hard-coded rules are ineffective in the conditions of high variability and scale of modern information environments. At the same time, in the practical plane, the information security of organizations increasingly depends on the ability to timely detect violations of access policies, conflicts between security rules at different levels and hidden interdependencies that can lead to compromise of the system [3]. In this context, expert systems play a special role – tools that simulate the decision-making processes of a specialist in the field of information security [4]. However, traditional expert systems have limited flexibility, are poorly scalable, and often do not take into account the specifics of modular architectures and the context of multi-level interaction of components [5].

Thus, there is a need to create a new generation modular expert system capable of comprehensive verification of security policies, taking into account both logical dependencies between access rules and the context of decision execution in different information domains [6]. The relevance of the problem is also enhanced by the need to unify approaches to verifying compliance of policies with constantly updated security standards, with the possibility of flexible customization for specific organizational requirements.

Related works

The issue of security policy verification in complex information environments is considered in many scientific studies related to access control, formal policy models, expert systems and means of ensuring compliance with information security standards. Among the common approaches to formalizing security policies, it is worth noting the Bell-LaPadula, Biba, Clark-Wilson models, as well as Role-Based Access Control (RBAC), which laid the foundation for the development of access control mechanisms in systems with multi-level privileges [7–9]. However, these models do not provide sufficient flexibility to adapt to changes in the environment, dynamically redistribute roles and verify the correctness of the implementation of security rules in real time.

In recent years, the emphasis has shifted to dynamic access policies that take into account the context, history of user actions, behavioral patterns and external events. In this context, approaches based on Context-Aware Access

Control (CAAC) and Attribute-Based Access Control (ABAC) are actively developing. Formal methods for checking the consistency of security rules, algorithms for automatically detecting conflicts between policies, and mechanisms for their elimination are being developed. Special attention is paid to the use of logical and ontological models to describe complex dependencies between policies and their elements, as well as the use of fuzzy logic to account for uncertainties.

Expert systems in the field of information security are traditionally focused on incident diagnostics, vulnerability analysis, or recommendation generation [10]. At the same time, architectural aspects of modularity, ensuring scalability, and adapting the expert system to hierarchical levels of the information environment are often ignored. Existing implementations mostly do not allow for effective integration of new knowledge or policies without a complete revision of the rule system. This limits their application in heterogeneous environments with distributed decision-making points and a multitude of autonomous components.

Some scientific works suggest using a modular approach to building expert systems, where each module is responsible for a separate domain of knowledge or a subset of policies [11]. This approach makes it possible to simplify knowledge updating, localize the analysis logic for individual levels of the information structure, and maintain flexibility when operating conditions change. However, these approaches are mainly focused on single-level environments or do not take into account the context of multi-level interaction between modules, which limits the possibilities of their practical application in complex systems.

Thus, despite a significant number of publications, there are no holistic architectural solutions for building a modular expert system capable of performing security policy verification in a multi-level information environment, taking into account the specifics of its dynamics, hierarchy, and contextual interaction between components. It is this scientific gap that determines the need for further research in this direction.

Formulation of the purpose of the research

The purpose of the study is to develop an architecture of a modular expert system for verifying security policies in multi-level information environments, which provides flexibility, scalability, and adaptability to changing operating conditions.

Materials and methods

Modular expert system architecture. The proposed architecture of a modular expert system for security policy verification is based on the principles of modularity, hierarchy, extensibility, and integrativity. The system consists of independent functional blocks that interact through a common interface for knowledge management and exchange of verification results. Key components include expertise modules, each of which is responsible for a specific subject area or level of the system; a central knowledge base where formalized information about security policies is accumulated; an integration interface that provides data exchange with external sources (information systems, organizational policies, event logs); and a verification subsystem that initiates logical verification of policies according to established criteria.

The architecture provides a centralized controller that coordinates the exchange of information between modules, aggregates results, and is responsible for making agreed decisions in cases of conflicts. This approach provides flexible scaling of the system, localization of changes, independent updating of individual modules, and adaptation to new policy formats without a significant revision of the entire system.

Figure 1 shows a general architecture diagram: the system core, to which the examination modules, knowledge base, verification module and interface for interaction with the information environment are connected. The modules can be activated independently or by event trigger. The system can be expanded by connecting new modules without affecting other components.

The model of a multi-level information environment formalizes it as a structure consisting of logically separated levels: application, system and network. Each of the levels implements its own security policies, has separate access rules, authentication protocols, log storage formats, as well as specific restrictions on the execution of operations. The application level is responsible for user actions in the application software, role management, and permission verification based on business logic. The system level covers operating system policies, process protection, and control over access rights to files and resources. The network level includes mechanisms for firewalling, network segmentation, VPN policies, and inter-segment routing control.

The hierarchical model allows you to clearly delimit the scope of responsibility of each module of the expert system. This makes it possible to avoid duplication of checks, ensure consistency of analysis, and consistency in the application of policies, taking into account the inheritance of restrictions and permissions between levels. Typical scenarios are identified where lower-level rules may conflict with more general higher-level policies. In such cases, modules should use a reverse delegation mechanism to refine decisions.

Figure 2 shows a three-tier environment model with corresponding policy examples and security checkpoints. The hierarchy allows the expert system to implement vertical verification logic: from general organizational policies to specific technical constraints at the device and network levels.

Formalization of policies and logic for their processing. The model of security policy representation and processing within the framework of the proposed expert system is based on a unified representation of policies in the form of logical rules or decision trees, which provides formal processing, comparison and verification. Each rule is described by access

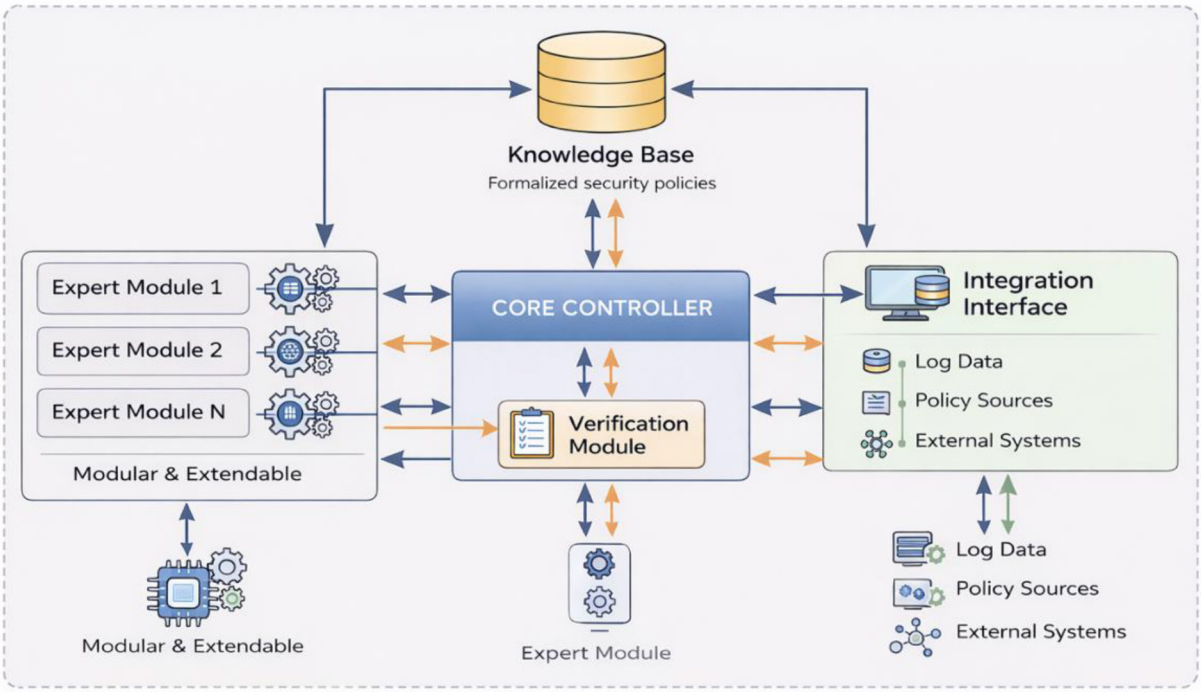

Fig. 1. General architecture of the expert system

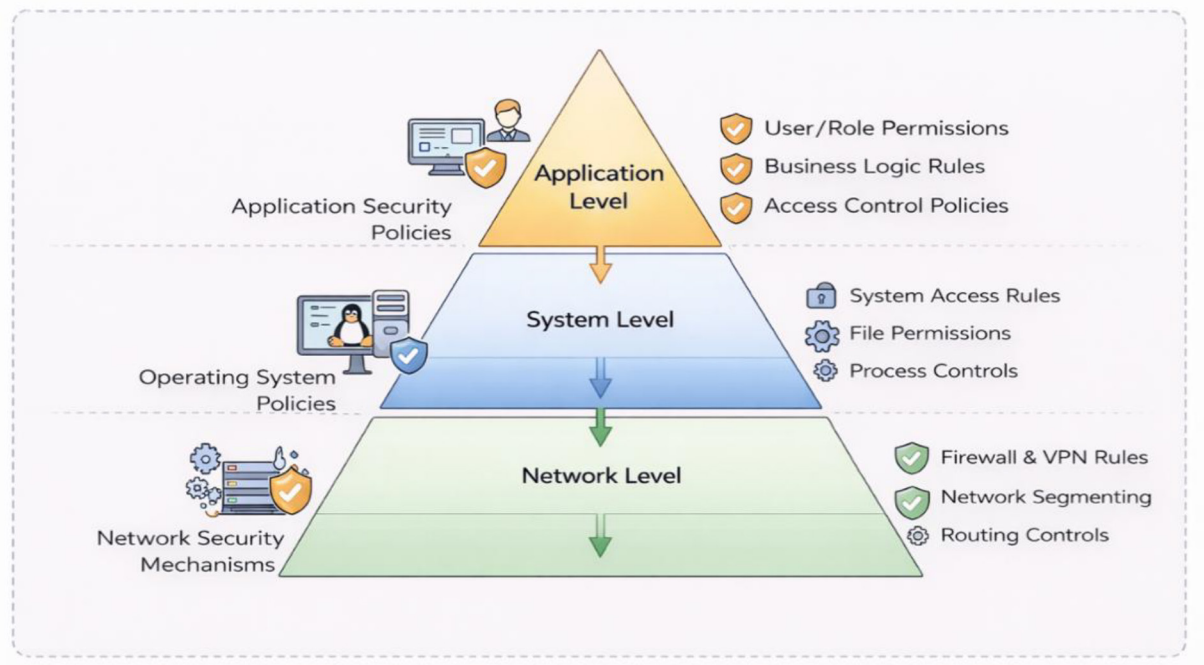

Fig. 2. Hierarchy of levels of the information environment

conditions and corresponding actions, which allows you to automate the verification of the legality of operations in the system. Formalization is carried out in the form of logical expressions, where each atomic element describes an attribute of the subject, object or access context.

For the formal representation of access policies in the form of logical constructs, the following generalized representation is used – IF (Subject.Role = ‘Admin’) ∧ (Object.Type = ‘Confidential’) ∧ (Time ∈ WorkingHours) THEN Access = ALLOW.

This expression reflects a typical policy that allows only administrators to access sensitive objects during specified time intervals. This approach allows for a clear formalization of decision-making conditions and the application of logical methods for subsequent verification.

Table 1

Example of formalized policies

Policy ID	Subject.Role	Object.Type	Context (Time)	Access
P1	Admin	Confidential	WorkingHours	ALLOW
P2	User	Public	Any	ALLOW
P3	Guest	Confidential	Any	DENY
P4	Admin	SystemConfig	OffHours	DENY

This structure provides machine readability, facilitates the search for conflicts (for example, between policies P1 and P4) and supports automated processing by the verification module.

The policy verification mechanism in a modular environment is implemented as a set of independent modules, each of which is responsible for checking policies of its own level (network, system, application) or a specific category (access, authentication, confidentiality). These modules operate autonomously, but are synchronized via a central controller or data exchange bus. The modules receive policy fragments from the knowledge base, check their compliance with consistency rules and return the results in the form of a status: valid, conflict, lack of coverage.

In the event of conflicts between modules, a weighted consensus or priority mechanism is used, which determines which module is given priority. For example, network-level rules may have priority over application-level rules in the event of conflicts regarding access routing.

The diagram (Fig. 3) shows the logic of interaction between modules: each module receives a verification request from the controller, performs analysis, returns a result, which is aggregated and used to form a conclusion about the policy as a whole. Communication between modules is provided via an event-driven bus or API.

Prototyping of the basic configuration of the expert system was implemented using the Drools rule engine, which allows processing logic in the form of declarative rules. Knowledge is stored in the format of DRL files that support consistency checking and launching simulation scenarios. Each module is implemented as a separate service that interacts with the controller via REST API.

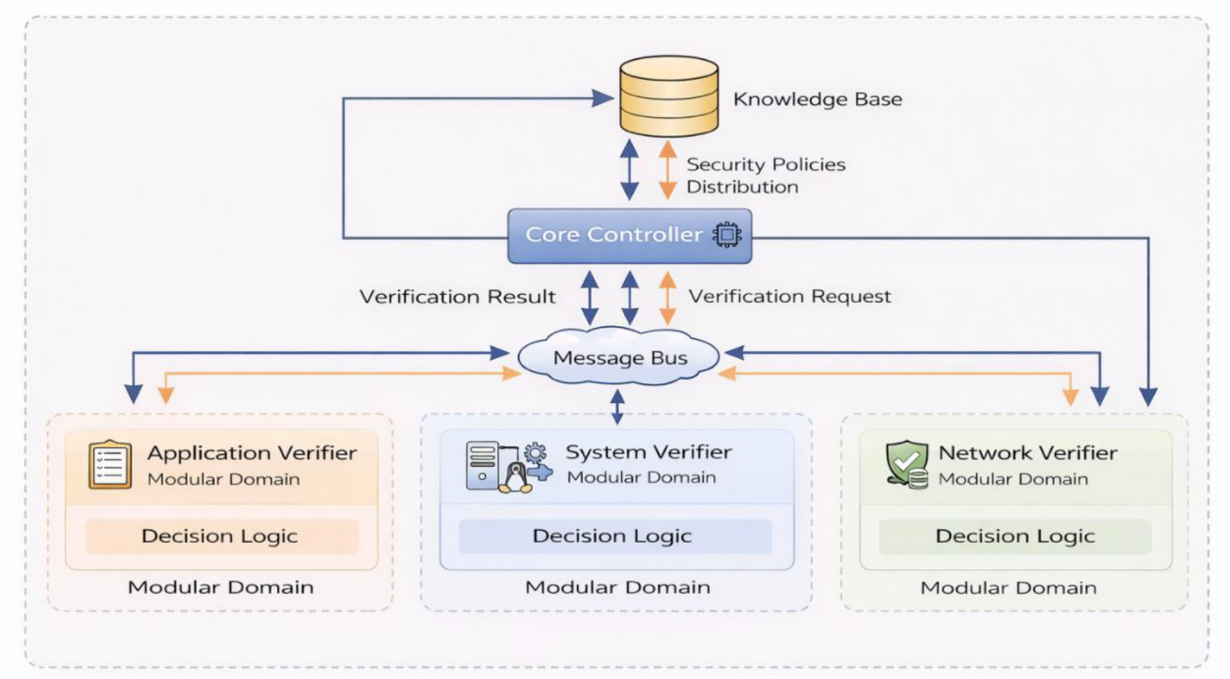

Fig. 3. Verification module interaction model

Within the framework of the application scenario, an information system with three access levels was considered: administrator, employee, and guest. For each of the levels, access policies to certain system objects were formed. A test simulation of requests to objects in different time and role contexts was conducted. The system successfully detected conflicting policies, as well as cases when some objects were not covered by any policy, which demonstrated the effectiveness of the verification mechanism and confirmed the operability of the proposed model.

The results of the experimental study confirmed the effectiveness of the proposed modular expert system for verifying security policies in a multi-level information environment. During the testing process, the system verified a set of policies

of varying complexity (from simple attribute-based to context-dependent), simulating work in a distributed environment with a large number of requests and conflicts. The analysis was carried out in comparison with two existing approaches: a centralized monolithic verification system and a hybrid system with partial modularity.

The evaluation was carried out according to the following key metrics:

– average verification time of one policy (ms);
– maximum number of simultaneously processed policies;
– knowledge update time after adding a new policy;
– flexibility of configuring modules for the domain (adaptability index);
– scalability during expansion (number of added modules without performance degradation).

Table 2

Comparative evaluation of systems

System	Verification time (ms)	Max politician	Update time (ms)	Adaptability	Scalability
Monolithic centralized	95	1 000	500	Low	Limited
Partially modular	60	2 500	240	Medium	Moderate
Proposed modular system	28	5 000	85	High	High

The proposed system showed the best results by all criteria. Its ability to adapt is especially noticeable: connecting a new module did not affect other parts of the system, and knowledge updating occurred with minimal delay. All components functioned independently, which allowed parallelizing the processes of policy analysis and increasing the overall speed.

The generalization of the results provides grounds for substantiating the scientific novelty and practical value of the study. The innovativeness of the architecture lies in the combination of full modularity with a centralized coordination core that does not interfere with the internal logic of the modules, but only synchronizes the results and conflicts. This approach allows you to scale the system while maintaining the integrity of the logic, and effectively adapt it to new policies and domains without violating the already implemented functions.

The advantages of the model are manifested in high flexibility, speed of adaptation to security changes, the ability to localize errors within a separate module, as well as the convenience of expanding knowledge without reviewing the entire database. Thanks to this approach, the tasks related to:

– policy verification in dynamic, heterogeneous environments;
– updating and merging policies from different sources;
– consistency control when changing the environment structure are more effectively solved.

The proposed architecture is suitable for implementation in complex information security systems operating at the organizational, state or critical level. It is especially appropriate in cases where high speed, reliability and scalability of security policy verification are priorities.

Conclusions

The study proposed an architectural approach to building a modular expert system focused on verifying security policies in multi-level information environments. Unlike traditional centralized or partially modular solutions, the developed system combines the independence of policy processing at each level with centralized coordination of results, which provides high flexibility, scalability and adaptability to changes.

The built model allows to distinguish policies by levels and domains, to detect conflicts and gaps in coverage, and to automatically reconcile verification results. Experimental testing has shown that the proposed system outperforms existing analogues in key performance metrics, including verification speed, adaptability to policy changes, and support for a large number of simultaneous checks. The results confirm the practical suitability of the system for use in heterogeneous distributed environments, where timely and reliable verification of security policy compliance is critical. The developed architecture can be the basis of a new generation of tools for automated analysis and management of security policies in complex IT infrastructures.

Bibliography

1. Burke, Q., Mehmeti, F., George, R. at al. Enforcing multilevel security policies in unstable networks. *IEEE Transactions on Network and Service Management*. 2022. Vol. 19. No. 3. P. 2349–2365. DOI: https://doi.org/10.1109/TNSM.2022.3176820

2. Rozlomii, I. O., Naumenko, S. V. Architecture and functional features of secured next-generation database management systems with serverless and edge computing support. *Systems and Technologies*. 2025. Vol. 69. No. 1. P. 130–137. DOI: https://doi.org/10.32782/2521-6643-2025-1-69.16

3. Akello, B. O. Organizational information security threats: Status and challenges. *World Journal of Advanced Engineering Technology and Sciences*. 2024. Vol. 11. No. 1. P. 148-162. DOI: https://doi.org/10.30574/wjaets.2024.11.1.0152

4. Sikman, L., Sarajlic, N. Modelling of fuzzy expert system for an assessment of security information management system uis (university information system). *Tehnički vjesnik*. 2022. Vol. 29. No. 1. P. 60–65. DOI: https://doi.org/10.17559/TV-20200721154801

5. Panzer, M., Gronau, N. Designing an adaptive and deep learning based control framework for modular production systems. *Journal of Intelligent Manufacturing*. 2024. Vol. 35. No. 8. P. 4113–4136. DOI: https://doi.org/10.1007/s10845-023-02249-3

6. Розломій, І., Фауре, Е., Науменко, С. Методи аутентифікації у вбудованих системах з обмеженими обчислювальними ресурсами. *Measuring and Computing Devices in Technological Processes*. 2025. Vol. 1. P. 29–35. DOI: https://doi.org/10.31891/2219-9365-2025-81-4

7. Babak, V., Babak, S., Eremenko, V., Kuts, Y., & Zaporozhets, A. Protection of Measurement Information from Unauthorized Access. In *Information-Measuring Systems: Theory and Application*, 2025, Cham: Springer Nature Switzerland, pp. 409–458. DOI: https://doi.org/10.1007/978-3-031-89406-0

8. Forsyth, E., Horne, R. Clark-Wilson policies in ACP: controlling information flow between solid apps. In *CEUR Workshop Proceedings*, Leuven, Belgium, May 2–3, 2024. Vol. 3947, pp. 100–108. URL: https://ceur-ws.org/Vol-3947/short14.pdf

9. Singh, M. P., Sural, S., Vaidya, J., Atluri, V. A role-based administrative model for administration of heterogeneous access control policies and its security analysis. *Information Systems Frontiers*. 2024. Vol. 26. No. 6. P. 2255–2272. DOI: https://doi.org/10.1007/s10796-021-10167-z

10. Ferreira, L., Silva, D. C., Itzazelaia, M. U. Recommender systems in cybersecurity. *Knowledge and Information Systems*. 2023. Vol. 65. No. 12. P. 5523–5559. DOI: https://doi.org/10.1007/s10115-023-01906-6

11. Iatrellis, O., Stamatiadis, E., Samaras, N., at al. An intelligent expert system for academic advising utilizing fuzzy logic and semantic web technologies for smart cities education. *Journal of Computers in Education*. 2023. Vol. 10. No. 2. P. 293–323. DOI: https://doi.org/10.1007/s40692-022-00232-0

References

1. Burke, Q., Mehmeti, F., George, R., Ostrowski, K., Jaeger, T., La Porta, T. F., & McDaniel, P. (2022). Enforcing multilevel security policies in unstable networks. *IEEE Transactions on Network and Service Management*, 19(3), pp. 2349–2365. DOI: https://doi.org/10.1109/TNSM.2022.3176820

2. Rozlomii, I. O., & Naumenko, S. V. (2025). Architecture and functional features of secured next-generation database management systems with serverless and edge computing support. *Systems and Technologies*, 69(1), pp. 130–137. DOI: https://doi.org/10.32782/2521-6643-2025-1-69.16

3. Akello, B. O. (2024). Organizational information security threats: Status and challenges. *World Journal of Advanced Engineering Technology and Sciences*, 11(1), pp. 148–162. DOI: https://doi.org/10.30574/wjaets.2024.11.1.0152

4. Sikman, L., & Sarajlic, N. (2022). Modelling of fuzzy expert system for an assessment of security information management system uis (university information system). *Tehnički Vjesnik*, 29(1), pp. 60–65. DOI: https://doi.org/10.17559/TV-20200721154801

5. Panzer, M., & Gronau, N. (2024). Designing an adaptive and deep learning based control framework for modular production systems. *Journal of Intelligent Manufacturing*, 35(8), pp. 4113–4136. DOI: https://doi.org/10.1007/s10845-023-02249-3

6. Rozlomii, I. O., Faure, E. V., & Naumenko, S. V. (2025). Authentication methods in embedded systems with limited computing resources. *Measuring and Computing Devices in Technological Processes*, no. 1, pp. 29–35. DOI: https://doi.org/10.31891/2219-9365-2025-81-4

7. Babak, V., Babak, S., Eremenko, V., Kuts, Y., & Zaporozhets, A. (2025). Protection of Measurement Information from Unauthorized Access. In *Information-Measuring Systems: Theory and Application*, pp. 409–458. Cham: Springer Nature Switzerland. DOI: https://doi.org/10.1007/978-3-031-89406-0

8. Forsyth, E., & Horne, R. (2024, May). Clark-Wilson policies in ACP: controlling information flow between solid apps. In *CEUR Workshop Proceedings*, Vol. 3947, pp. 100–108. URL: https://ceur-ws.org/Vol-3947/short14.pdf

9. Singh, M. P., Sural, S., Vaidya, J., & Atluri, V. (2024). A role-based administrative model for administration of heterogeneous access control policies and its security analysis. *Information Systems Frontiers*, *26*(6), pp. 2255–2272. DOI: https://doi.org/10.1007/s10796-021-10167-z

10. Ferreira, L., Silva, D. C., & Itzazelaia, M. U. (2023). Recommender systems in cybersecurity. *Knowledge and Information Systems*, *65*(12), pp. 5523–5559. DOI: https://doi.org/10.1007/s10115-023-01906-6

11. Iatrellis, O., Stamatiadis, E., Samaras, N., Panagiotakopoulos, T., & Fitsilis, P. (2023). An intelligent expert system for academic advising utilizing fuzzy logic and semantic web technologies for smart cities education. *Journal of Computers in Education*, *10*(2), pp. 293–323. DOI: https://doi.org/10.1007/s40692-022-00232-0

Дата першого надходження статті до видання: 11.01.2026
Дата прийняття статті до друку після рецензування: 13.02.2026
Дата публікації (оприлюднення) статті: 30.04.2026