AN APPROACH TO ENSURING INFORMATION SECURITY OF AN INTELLIGENT CONTROL SYSTEM FOR THE FUNCTIONING OF TUTORING INTEGRATED EXPERT SYSTEMS: INTEGRATION OF SIMULATION MODELING, TEMPORAL INFERENCE AND COGNITIVE ENGINEERING METHODS

Authors

Galina V. Rybina

Dr. of Tech. Sc., professor,

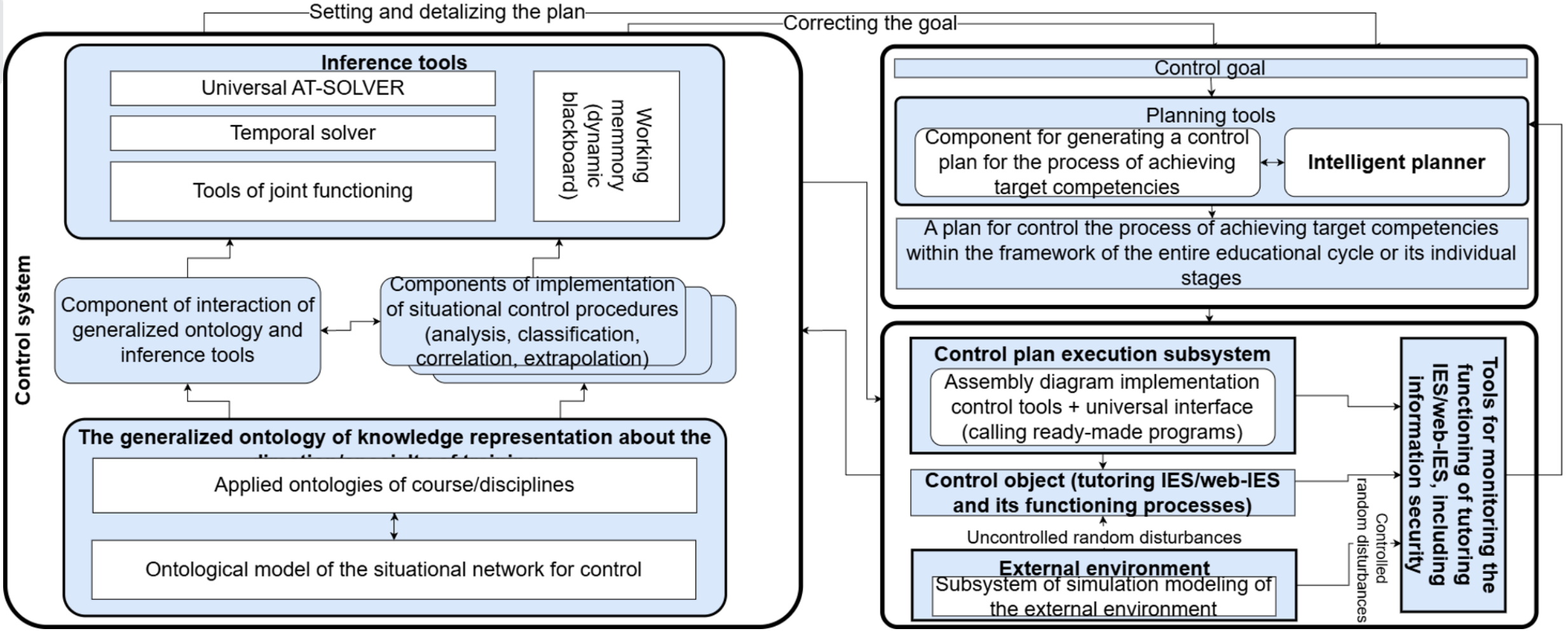
Professor of the Department of Cybernetics, NRNU MEPhI

Andrey A. Grigoryev

PhD

Associate Professor of the Department of Cybernetics, NRNU MEPhI

General architecture of a prototype version of an intelligent control system for control functioning processes of tutoring integrated expert systems



General information about the work

The purpose of this work

To examine the proposed effective approach to addressing the information security (IS) problem associated with the main assets of a complex, multifunctional IS object comprising an intelligent situational control system (ICS) and a system for monitoring the information and software resources of several tutoring integrated expert systems (IES) and web-based IES (hereinafter referred to as IES/web-IES), which are used in the intelligent tutoring process at all stages of the educational cycle.

Background to the problem statement

1. Increasing the level of automation in the control of information and software resources of several tutoring IES/web-IES through the development of an adaptive ontological software environment implemented as an intelligent control system (ICS) architecture that provides situational control and monitoring of the functioning processes of tutoring IES/web-IES, which act as unconventional *intelligent* software-organizational control objects.
2. For the first time, the development of situational control technology is considered in close interrelation with both ICS architectures and the architectures of tutoring IES/web-IES, which represent distinct classes of intelligent systems. Accordingly, the requirements for the reliability and security, specifically, confidentiality of information and software resources used by all tutoring IES/web-IES have increased. The total number of software components involved amounts to 134 components of the AT-TECHNOLOGY workbench. The underlying information support includes several hundred vertices in the ontology system and a unified database containing more than 2,500 learner models.
3. The need to develop a dedicated approach to information security (IS) monitoring of the functioning processes of tutoring IES/web-IES. This approach must provide for the analysis of IS threats and risks affecting the identified IS objects, the modeling of attacks at each level of situational control, and decision support for predicting potential damage resulting from attacks.

Some aspects of addressing information security issues in the educational sector

The widespread development of various e-learning systems and platforms, which address the challenges of ensuring information confidentiality during its collection, storage, and processing.

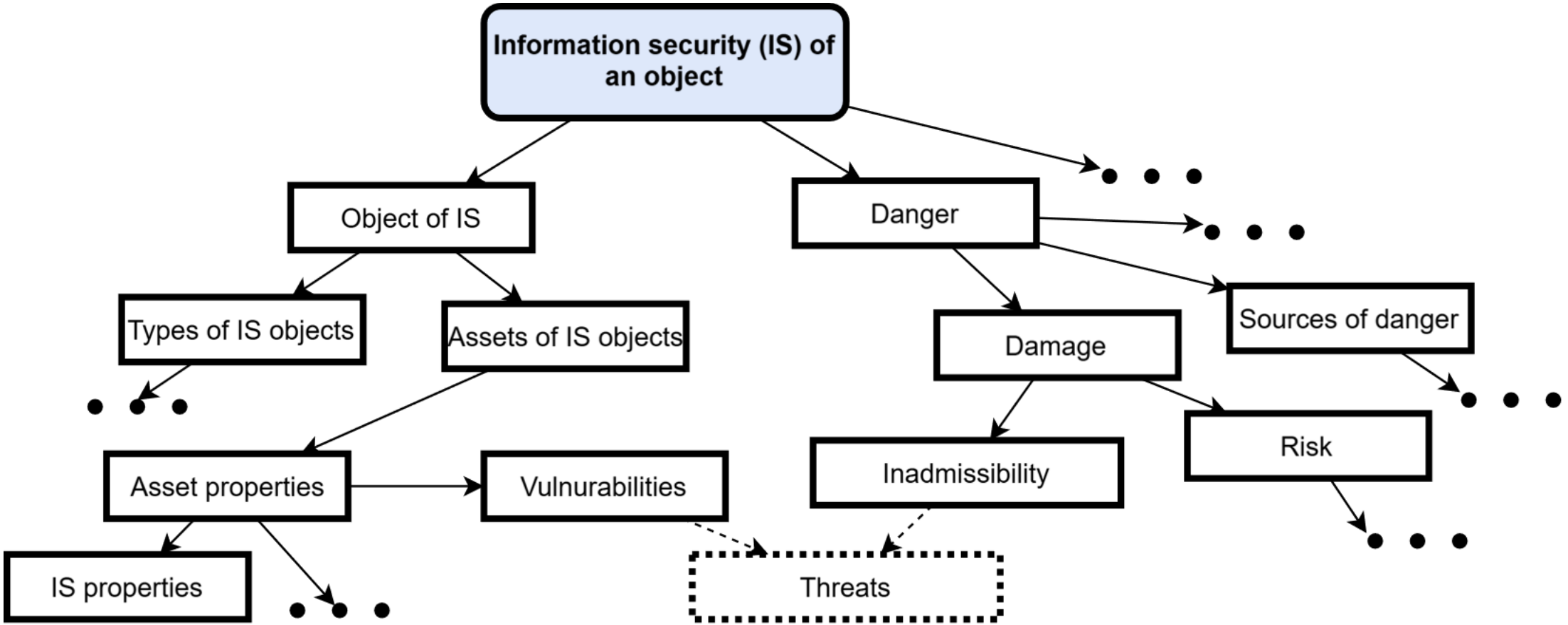
- Moodle
- Chamilo
- Ilias
- ...

Active interest in the relationship between information security and AI, including within the educational sphere

Lack of comprehensive, systemic research in the field of information security as applied to the architectures of intelligent tutoring systems (ITS) of various typologies

Key research in the field of information security that served as reference points for developing and refining the conceptual framework as applied to ICS and tutoring IES/web-IES.

Tolstoy A.I. Systematics of concepts in the field of information security // Information Technology Security. 2023. Vol. 30. № 1. P. 130-148. DOI: https://dx.doi.org/10.26583/bit.2023.1.10



Continuation of slide no. 5

Kotenko I. V., Saenko I. B., Mityakov E. S., Kochin V. P. **Methodology for Analyzing Information Security Threats Using Digital Twins** // Journal of the Belarusian State University. Mathematics and Informatics. 2025. Issue 3. P. 76–91.

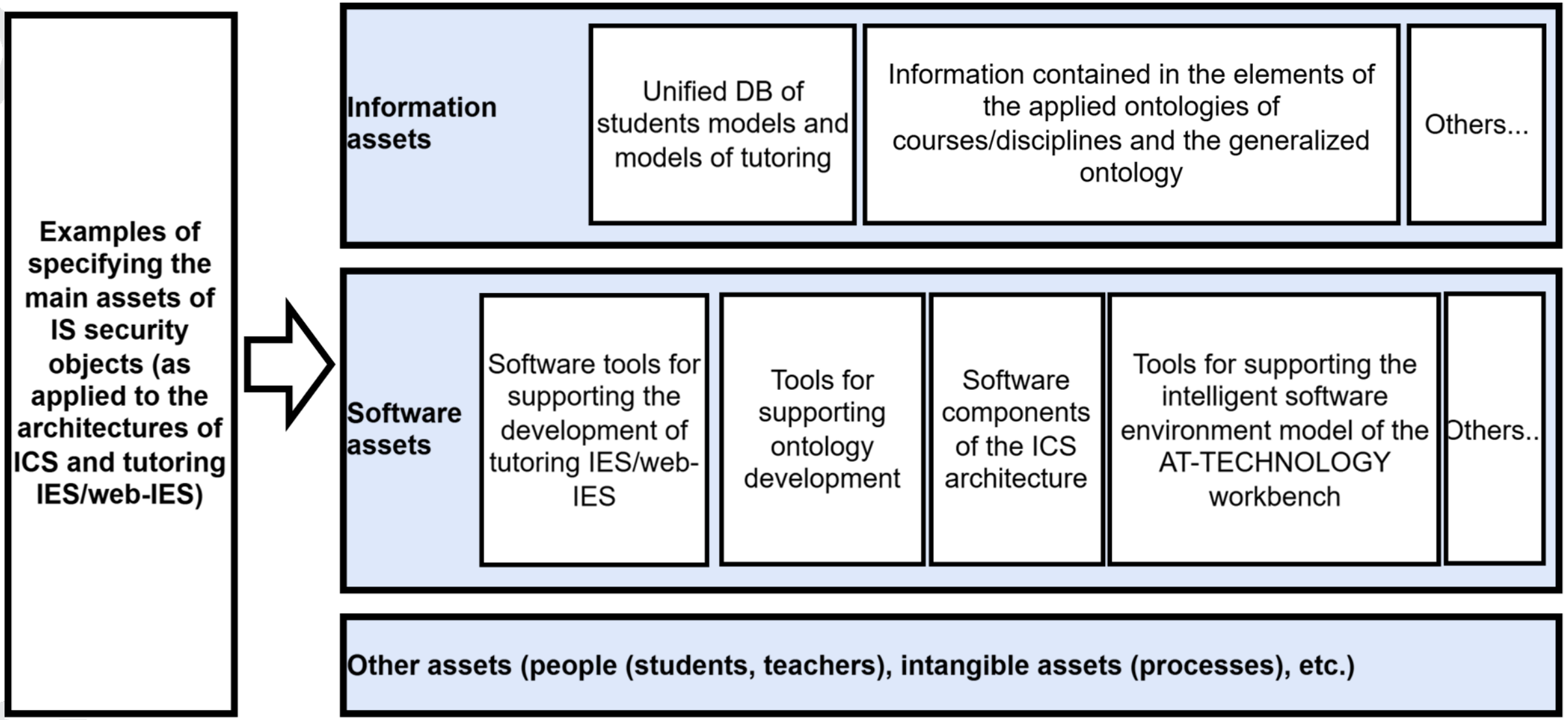
Rudakova T. A., Rudakova O. Yu. **Enterprise Information Security Strategy: Monitoring and Management** // Strategic Decisions and Risk Management. 2026. Vol. 17, No. 1. P. 73–83. DOI: 10.17747/2618-947X-2026-1-73-83.

Vasilyev V. I., Vulfin A. M., Gerasimova I. B., Kartak V. M. **Cybersecurity Risk Analysis Using Fuzzy Cognitive Maps** // Cybersecurity Issues. 2020. No. 2 (36). P. 11–21. DOI: 10.21681/2311-3456-2020-2-11-21

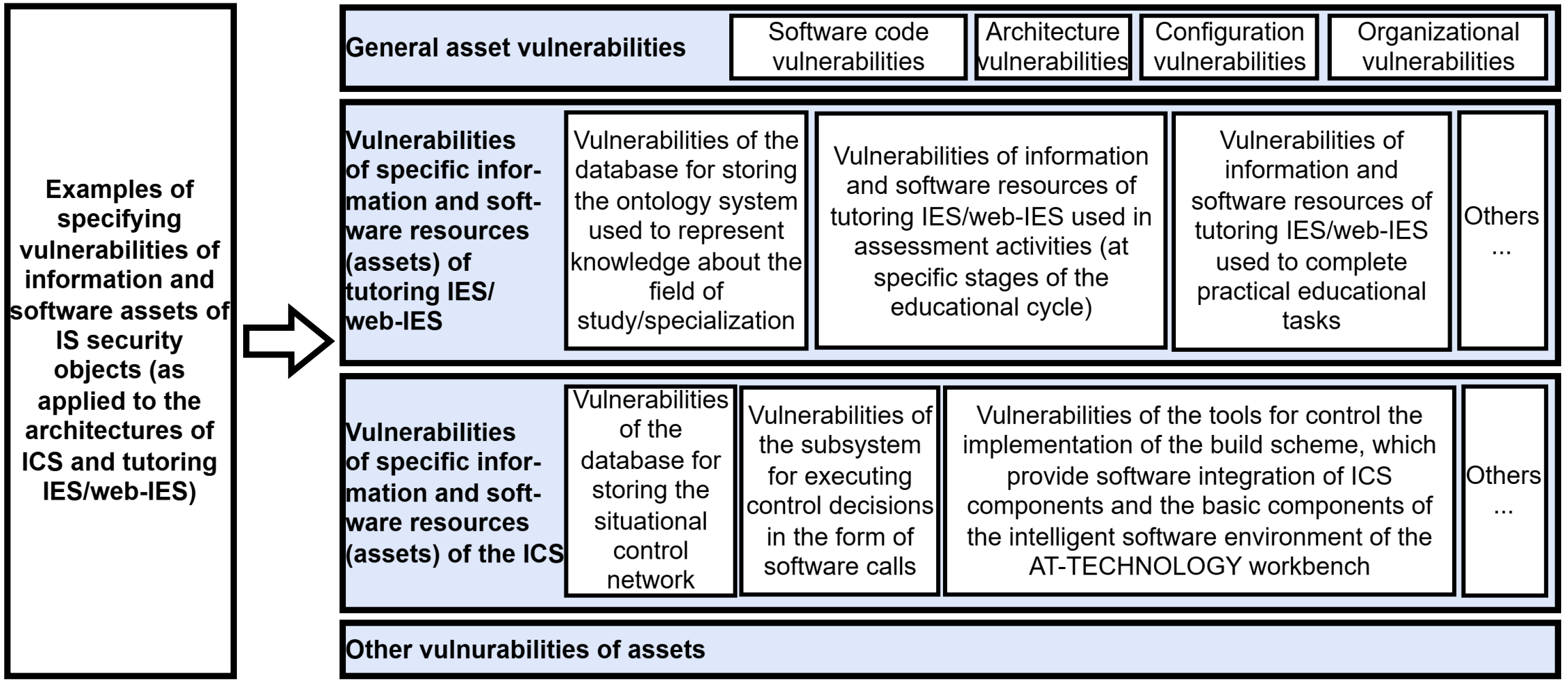
Shamsutdinov R. R., Vasilyev V. I., Vulfin A. M. **Intelligent System for Monitoring Information Security of the Industrial Internet of Things Using Artificial Immune Systems Mechanisms** // Systems Engineering and Information Technology. 2024. Vol. 6, No. 4 (19). P. 14–31. DOI: 10.54708/2658-5014-SIIT-2024-no4-p14

Others…

Specification of the conceptual framework based on the systemology of concepts in the field of IS, as applied to the architectures of ICS and tutoring IES/web-IES



Specification of the conceptual framework based on the systemology of concepts in the field of IS, as applied to the architectures of ICS and tutoring IES/web-IES



Specification of the conceptual framework based on the systemology of concepts in the field of IS, as applied to the architectures of ICS and tutoring IES/web-IES

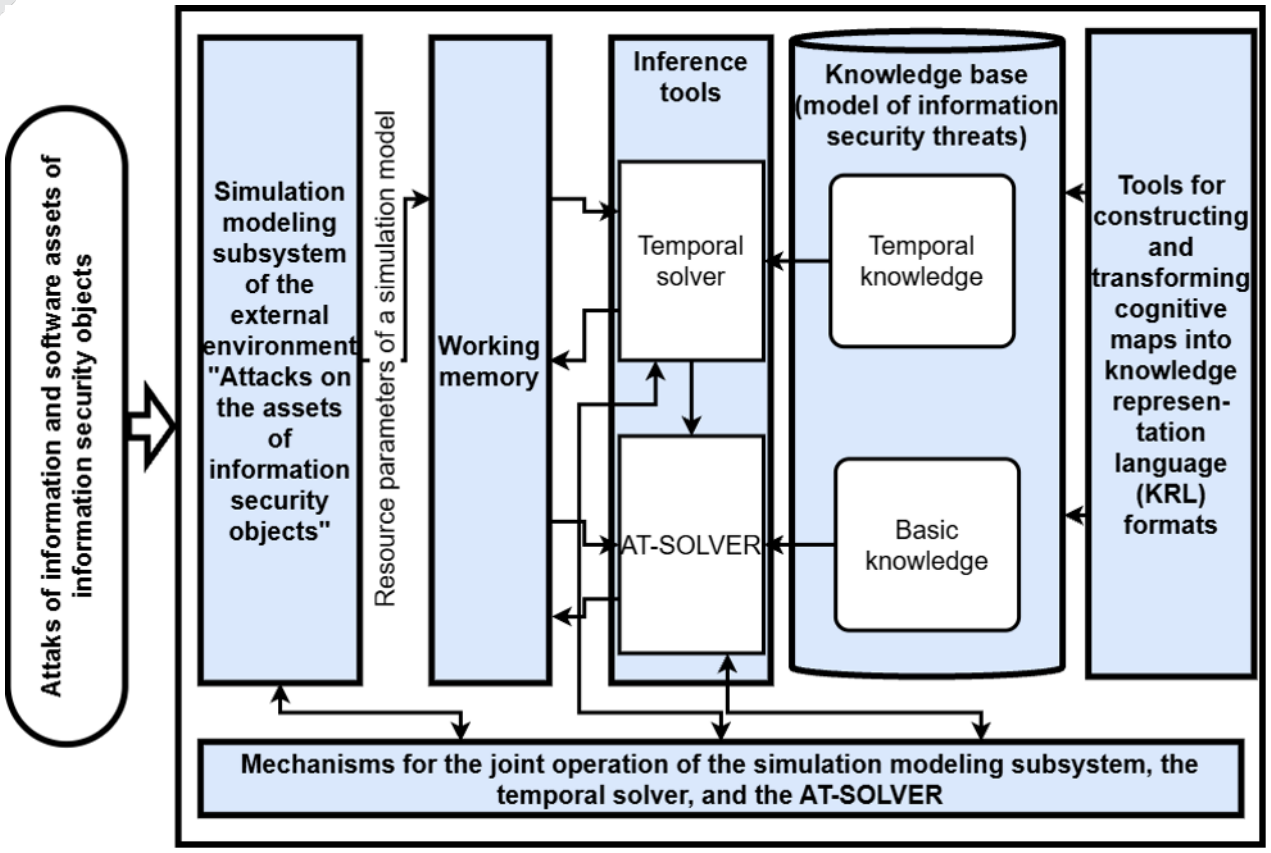
Examples of specifying security threats to objects (as applied to the architectures of ICS and tutoring IES/web-IES)



General types of security threats to objects	Threats from various sources (internal/external attackers, etc.)	Threats to various security properties of assets of IS security objects (confidentiality, integrity, availability, etc.)	Threats exploiting various types of vulnerabilities in the assets of IS security objects	Others ...
Security threats to the functioning processes of tutoring IES/web-IES	Security threats to the unified database of students and tutoring models	Security threats to the general database for storing the ontology system	Threats of unauthorized access to the methodological support for assessment activities at the stages of the educational cycle	Threats of damage to information and software resources during the completion of practical educational tasks	Другие ...
Security threats to the functioning processes of the ICS	Threats of unauthorized modification of the database for storing the ontological model of the situational control network	Threats of incorrect execution of control decisions (in the form of software calls) at different levels of the situational control network	Threats of violations in the use of contracts of documented ICS software components	Others ,,,
Other threats				

Development of a prototype of a dynamic IES 'Monitoring information security in the operational processes of tutoring IES/web-IES'

Architecture of the prototype of a dynamic IES 'Monitoring information security in the operational processes of tutoring IES/web-IES'



A total of **26** cognitive maps have been constructed, collectively incorporating the following concepts:

- approximately **120** critical software code vulnerabilities
- **34** configuration vulnerabilities
- **7** architectural vulnerabilities
- **11** organizational vulnerabilities

The current version of the knowledge base contains **124** temporal rules and **72** basic rules.

The simulation model "Attacks on assets of information security objects" developed in the RAO^{AT} language, comprises **35** resources and 154 operations.

Specifics of an IS threat model described using an extended knowledge representation language

Based on fundamental rules, the interrelationships between identified vulnerabilities in key information and software assets are described—vulnerabilities whose existence determines the presence of specific IS threats.

Using temporal objects (intervals and events), the various stages of the development of threats manifested through specific attacks originating from the external environment are described.

Temporal rules—which define temporal relationships between intervals and/or events—were used to describe the processes by which threats manifest and evolve at various control levels.

Initially, based on the processing of system analysis results, **16** cognitive maps were constructed, which served as the foundation for building a knowledge base (KB) that contains an information security threat model

In total, the current version of the dynamic IES prototype contains:

- **43** temporal objects (intervals and events)
- **124** temporal rules
- **72** basic rules

Specifics of a simulation model for attacks on key assets, described using the RAO^{AT} language

Simulation model (SM) of a complex technical system based on the RAO method

SM_{CTS} = <Res, E, IE, C, A, OprE, OprIE, G>

Res
A set of CTS resources

E
A set of regular events triggered by the standard operation of resources

IE
A set of irregular events that occur either due to abnormal resource operation or for reasons external to the CTS

C
The set of all possible states of the CTS

A
A set of specific actions, with which the events marking the beginning and end of actions are associated

OprE
A set of operations that provide the generation of regular events E

OprIE
A set of operations that facilitate the generation of irregular events (IE)

G
Algorithms for transforming the values of parameters that describe the states of CTS resources

Examples of specifying elements of the SM for attacks against key assets of information security objects

A set of resources $Res = \{Res_i\}$

$Res = \{Res_i\}$ – a set of resources describing key information and software assets

Resource parameters – describe the state of assets, as well as vulnerabilities within those assets that could be exploited

A set of regular events $E = \{E_i\}$

$E = \{E_i\}$ – a set of regular events modeling the standard operation of assets

A set of irregular events $IE = \{IE_i\}$

$IE = \{IE_i\}$ – a set of irregular events that model the progression of attacks, each corresponding to a specific threat

Currently, the description of the SM in the RAO^{AT} language includes:

- **35** resources, for which more than **330** parameters defining their state have been specified;
- **154** operations that model the standard functioning of the system as well as potential impacts on assets during the execution of attacks—including those involving the exploitation of vulnerabilities.

Experimental study of the capabilities of a dynamic IES prototype, focusing on the simulation of attacks on assets

Identifying the type of threat actor, their capabilities, and the target assets for attacks

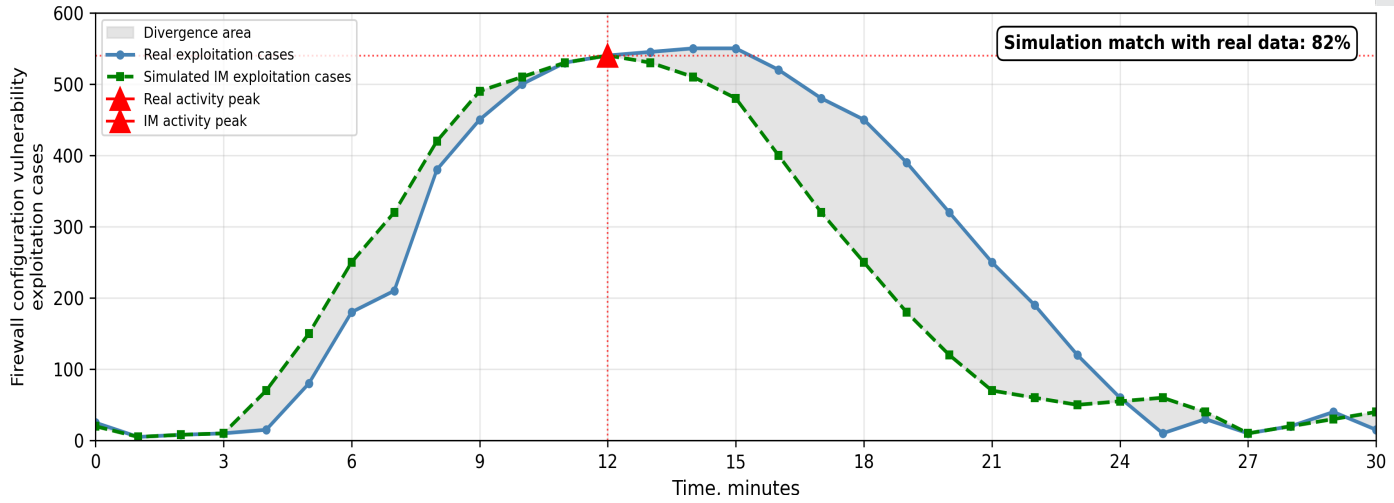
Selection of asset vulnerabilities most relevant to the execution of attacks

Executing a simulation model run and recording the statistical characteristics of the simulated attacks

Analysis of results

A comparison was made with data derived from an analysis of **16** incidents recorded during the **2025–2026** academic year. The research focused on specific types of documented attacks that involved the exploitation of particular vulnerabilities.

The best simulation model run, in which an attack involving the exploitation of various network vulnerabilities was modeled.



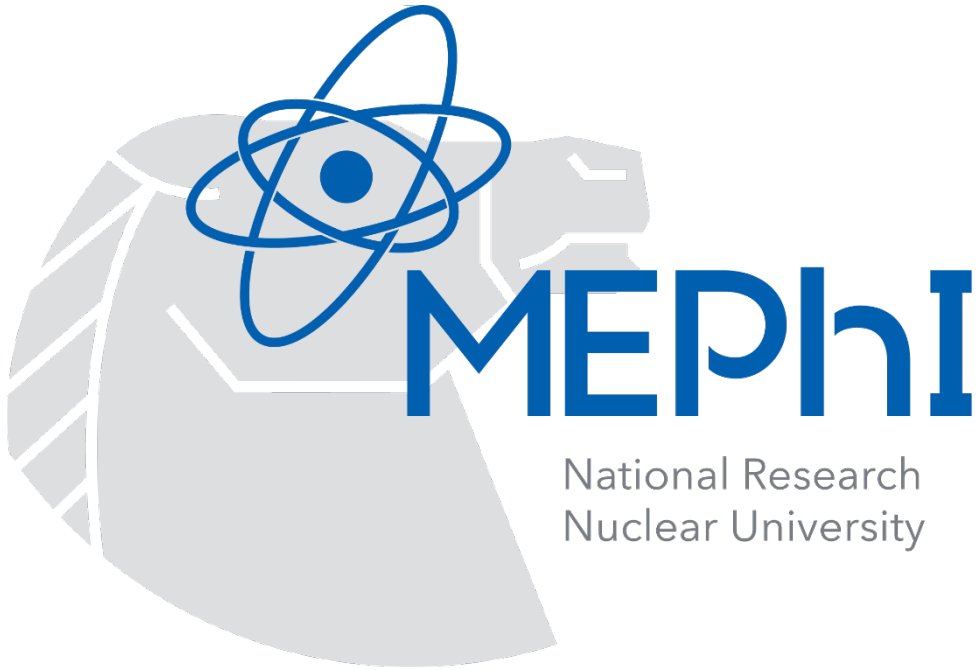
Conclusion

The experience of applying intelligent tutoring technology based on tutoring IES/web-IES has demonstrated the need to develop new monitoring tools to ensure the information security of such objects as the ICS and a set of several tutoring IES/web-IES.

At this stage of the research, an approach to information security monitoring has been proposed based on the joint use of knowledge engineering and cognitive modeling methods (using a knowledge representation model in the form of cognitive maps) and simulation modeling methods. The approach is based on a systems analysis of the main assets of information security objects and potential information security threats.

To monitor the information security of the functioning processes of tutoring IES/web-IES, a prototype of a dynamic IES has been developed and experimentally investigated. Its implementation is based on the integration of simulation modeling and temporal inference methods, which jointly determine the logic of real-time decision-making.

Experimental studies are currently being conducted to investigate the capabilities of the dynamic IES prototype in detecting attacks and predicting potential damage to the assets of information security objects.



Thank you for attention