Ensuring Information Security of the OSTIS Ecosystem

Valery Chertkov
Euphrosyne Polotskaya State University of Polotsk
Polotsk, Belarus
v.chertkov@psu.by

Vladimir Zakharau
Belarusian State University of Informatics and Radioelectronics
Minsk, Belarus
zakharau@bsuir.by

***Abstract*—The development of artificial intelligence systems, associated with the transition to working with knowledge bases instead of data, requires the formation of new approaches to ensuring information security systems. The article is devoted to the review of approaches and principles of ensuring security in intelligent systems of the new generation. The current state of methods and means of ensuring information security in intelligent systems is considered and the main goals and directions for the development of information security ostis-systems are formed. The information security methods presented in the article are extremely important when designing the ostis-systems security system and analyzing their security level.**

***Keywords*—information security, new generation intelligent system, Information security threats**

I. Introduction

A wide variety of information security models, the growing amount of data that needs to be analyzed to detect attacks on information systems, the variability of attack methods and the dynamic change in protected information systems, the need for a rapid response to attacks, the fuzziness of the criteria for detecting attacks and the choice of methods and means of responding to them, the lack of highly qualified security specialists entails the need to use artificial intelligence methods to solve security problems.

II. The specifics of ensuring information security of intelligent systems of a new generation

Information security of intelligent systems should be considered from two points of view:

- application of artificial intelligence in information security;
- organization of information security in intelligent systems.

The use of artificial intelligence in information security

Artificial intelligence is actively used to monitor and analyze security vulnerabilities in information transmission networks [1]. The artificial intelligence system allows machines to perform tasks more efficiently, such as:

- visual perception, speech recognition, decision making and translation from one language to another;
- invasion detection - artificial intelligence can detect network attacks, malware infections and other cyber threats;
- cyber analytics - artificial intelligence is also used to analyze big data in order to identify patterns and anomalies in the organization's cyber security system in order to detect not only known, but also unknown threats;
- secure software development - artificial intelligence can help create more secure software by providing real-time feedback to developers.

Artificial intelligence is used not only for protection, but also for attack, for example, to emulate acoustic, video and other images in order to deceive authentication mechanisms and further impersonation, deceive checking a person or robot capcha, etc.

Currently, it is possible to define the following classes of systems in which artificial intelligence is used [2]:

- UEBA (User and Entity Behavior Analytics) — a system for analyzing the behavior of subjects (users, programs, agents, etc.) in order to detect non-standard behavior and use them to detect potential threats using threat templates (patterns);
- IP (Threat Intelligence Platform) — platforms for early detection of threats based on the collection and analysis of information from indicators of compromise and response to them. The use of machine learning methods increases the efficiency of detecting unknown threats at an early stage;
- EDR (Endpoint Detection and Response) — attack detection systems for rapid response at the end points of a computer network. Can detect malware, automatically classify threats and respond to them independently;
- SIEM (Security Information and EventManagement) — systems for collecting and analyzing information about security events from network devices and applications in real time and alerts;
- NDR (Network Detection and Response) — sys-

tems for detecting attacks at the network level and promptly responding to them. AI uses the accumulated statistics and knowledge base about threats;
- SOAR (Security Orchestration and Automated Response) — systems that allow you to identify information security threats and automate incident response. In solutions of this type, unlike SIEM systems, AI helps not only to analyze, but also automatically respond appropriately to identified threats;
- Application Security — systems that allow you to identify threats to the security of application applications, manage the process of monitoring and eliminating such threats;
- Antifraud — platforms detect threats in business processes and fraudulent transactions in real time. AI is used to identify deviations from identified business processes in order to detect intrusions or process vulnerabilities and increase adaptability to changing business process logic and metrics.

The paper [3] proposes a method for constructing a neuroimmune system for analyzing information security incidents that combines data collection and storage (compression) modules, an information security event analysis and correlation module, and a network attack detection subsystem based on convolutional neural networks. The use of machine learning technologies in information security creates bottlenecks and system vulnerabilities that can be exploited and has the following disadvantages [4]:

- data sets that must be formed from a significant number of input samples, which requires a lot of time and resources;
- requires a huge amount of resources, including memory, data and computing power;
- frequent false positives that disrupt the operation and generally reduce the effectiveness of such systems;
- organized attacks based on artificial intelligence (semantic viruses).

Organization of information security in intelligent systems of a new generation

Let's define the goals of ensuring the information security of new generation systems.

From the monograph [5] the objectives of ensuring the information security of traditional intelligent systems are:

- ensuring the confidentiality of information in accordance with the classification;
- ensuring the integrity of information at all stages of related processes (creation, processing, storage, transfer and destruction) in the provision of public services;
- ensuring timely availability of information in the provision of public services;
- ensuring observability aimed at capturing any activity of users and processes;
- ensuring the authenticity and impossibility of refusal of transactions and actions performed by participants in the provision of public services;
- accounting for all processes and events related to the input, processing, storage, provision and destruction of data.

Since intelligent systems of the new generation will interact with similar systems while understanding what the request is about, the goals of the provision will look different. The goals of ensuring the information security of new generation intelligent systems are:

- ensuring the safety of the semantic compatibility of information;
- protection of reliability and integrity of information;
- ensuring the availability of information at different levels of the intellectual system;
- minimization of damage from events that pose a threat to information security.

Currently, classical approaches and principles have been developed to ensure the security of knowledge bases (data), communication interfaces (information exchange) between the components of intelligent systems, such as encryption of transmitted data, filtering of unnecessary (redundant) content, and data access control policy.

The information security system should be created on the following principles:

- the principle of equal strength - means ensuring the protection of equipment, software and control systems from all types of threats;
- the principle of continuity - provides for continuous security of information resources of the system for the continuous provision of public services;
- the principle of reasonable sufficiency - means the application of such measures and means of protection that are reasonable, rational and the costs of which do not exceed the cost of the consequences of information security violations;
- the principle of complexity - to ensure security in all the variety of structural elements, threats and channels of unauthorized access, all types and forms of protection must be applied in full;
- the principle of comprehensive verification - is to conduct special studies and inspections, special engineering analysis of equipment, verification studies of software. Emergency messages and error parameters should be continuously monitored, hardware and software equipment should be constantly tested, as well as software integrity control, both during software loading and during operation;
- the principle of reliability - methods, means and forms of protection must reliably block all penetration routes and possible channels of information

leakage; for this, duplication of means and security measures is allowed;
- the principle of universality - security measures should block the path of threats, regardless of the place of their possible impact;
- the principle of planning – planning should be carried out by developing detailed action plans to ensure the information security of all components of the system for the provision of public services;
- the principle of centralized management – within a certain structure, the organized and functional independence of the process of ensuring security in the provision of public services should be ensured;
- the principle of purposefulness – it is necessary to protect what must be protected in the interests of a specific goal;
- the principle of activity - protective measures to ensure the safety of the service delivery process must be implemented with a sufficient degree of persistence;
- the principle of service personnel qualification – maintenance of equipment should be carried out by employees who are trained not only in the operation of equipment, but also in technical issues of information security;
- the principle of responsibility - the responsibility for ensuring information security must be clearly established, transferred to the appropriate personnel and approved by all participants as part of the information security process.

III. The principles underlying the information security of ostis systems

The OSTIS ecosystem is a collective of interacting:

- ostis-systems;
- users of ostis systems (end users and developers);
- other computer systems that are not ostis-systems, but are additional information resources or services for them.

The core of OSTIS technology includes the following components:

- semantic knowledge base OSTIS, which can describe any kind of knowledge, while it can be easily supplemented with new types of knowledge;
- OSTIS problem solver based on multi-agent approach. This approach makes it easy to integrate and combine any problem solving models;
- ostis-system interface, which is a subsystem with its own knowledge base and problem solver.

The presented architecture of the OSTIS Ecosystem implements:

- all knowledge bases are united into the Global Knowledge Base, the quality of which (logicality, correctness, integrity) is constantly checked by many agents. All problems are described in a single knowledge base, and specialists are involved to eliminate them, if necessary;
- each application associated with the OSTIS Ecosystem has access to the latest version of all major OSTIS components, components are updated automatically;
- each owner of the OSTIS Ecosystem application can share a part of their knowledge for a fee or for free.

It is important to note that information security is closely related to the architecture of the built system: a well-designed and well-managed system is more difficult to hack. Therefore, it is very important to develop an information security system at the stage of designing the architecture and structure of a future next-generation intelligent system.

The OSTIS Ecosystem is a community where ostis systems and users interact, where rules must be established and controlled. Illegal and destabilizing actions by all members of the community should not be allowed. The user cannot directly interact with other ostis systems, but only through a personal agent. This agent stores all personal data of the user and access to them should be limited.

In the OSTIS Ecosystem, all agents must be identified. It should be noted that the personal user agent in the Ecosystem solves the problem of identifying the user himself.

In the considered OSTIS Ecosystem, it is required to organize information security at each of the levels of interaction: data exchange, data access rights, authentication of Ecosystem clients, data encryption, obtaining data from open sources, ensuring the reliability and integrity of stored and transmitted data, monitoring the violation of communications in knowledge base, tracking vulnerabilities in the system.

threat in ostis-system

⊃ *threat. breach of confidentiality of information*
⇒ *explanation**:
[unauthorized access to read information]

⊃ *threat. violation of the integrity of information*
⇒ *explanation**:
[unauthorized or erroneous change, distortion or destruction of information, as well as unauthorized impact on technical and software information processing tools]

⊃ *threat. accessibility violation*
⇒ *explanation**:
[blocking access to the system, its individual components, functions or information, as well as the impossibility of obtaining information in a timely manner (unacceptable delays in obtaining information)]

⊃ *threat. violation of semantic compatibility*
⇒ *explanation**:

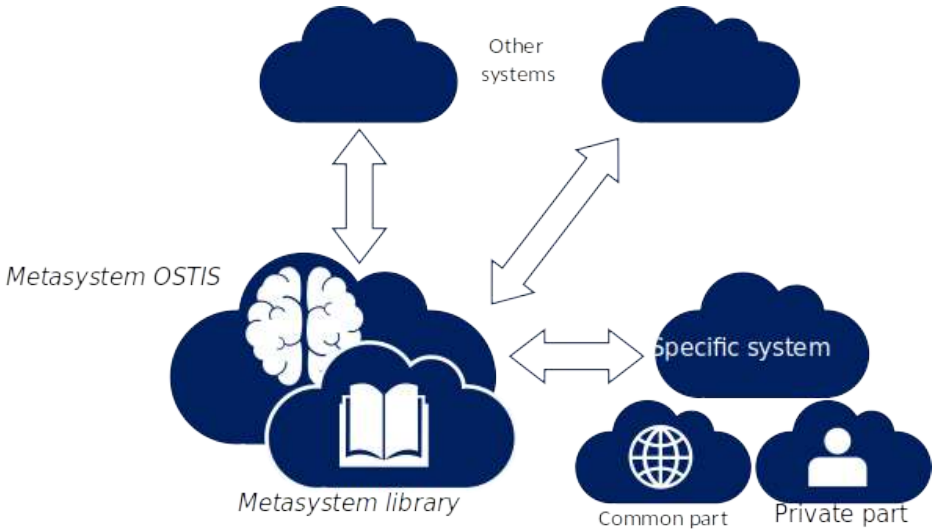

Figure 1. OSTIS Ecosystem Architecture

[violation of the generality of concepts and in the generality of basic knowledge]

⊃ *threat. destruction of knowledge base semantics (semantic viruses)*

⇒ *explanation**:
[substitution or removal of nodes and links between them in the knowledge base]

⊃ *threat. excessive amount of incoming information*

⊃ *threat. breach of non-repudiation*

⇒ *explanation**:
[issuance of unauthorized actions as legal, as well as concealment or substitution of information about the actions of subjects]

⊃ *threat. breach of accountability*

⇒ *explanation**:
[unauthorized or erroneous change, distortion or destruction of information about the performance of actions by the subject]

⊃ *threat. violation of authenticity (authenticity)*

⇒ *explanation**:
[performing actions in the system on behalf of another person or issuing unreliable resources (including data) as genuine]

⊃ *threat. breach of credibility*

⇒ *explanation**:
[intentional or unintentional provision and use of erroneous (incorrect) or irrelevant (at a specific point in time) information, as well as the implementation of procedures in violation of the regulations (protocol)]

Let's present the main directions of ensuring the information security of ostis-systems to prevent emerging threats:

- limitation of information traffic analyzed by the intelligent system;
- policy of differentiation of access to the knowledge base;
- connectivity;
- introduction of semantic metrics;
- semantic compatibility;
- activity.

It should be noted that at the design stage of the OSTIS technology itself, the basic principles of ensuring information security were already laid down as part of the design of individual components of the system. So already initially, support for semantic compatibility and cohesion is provided in ostis systems due to the system's ability to detect malicious processes in the knowledge base.

Restriction of information traffic analyzed by the intelligent system

The exponential growth of the volume of information circulating in information flows and resources under the conditions of well-defined quantitative restrictions on the capabilities of the means of its perception, storage, transmission and transformation forms a new class of information security threats characterized by the redundancy of the total incoming information traffic of intelligent systems.

As a result, the overflow of information resources of an intelligent system with redundant information can provoke the spread of distorted (destructive semantic) information. The general methodology for protecting intelligent systems from excessive information traffic is carried out through the use of axiological filters that implement the functions of numerical assessment of the value of incoming information, selection of the most valuable and screening (filtering) of less valuable (useless or harmful) using well-defined criteria.

Active means of destroying the semantics of knowledge bases (semantic viruses) should also be singled out as a separate category of information security threats [6].

Knowledge base access control policy

Mandatory access control (MAC) is based on mandatory (forced) access control, which is determined by four conditions: all subjects and objects of the system are identified; a lattice of information security levels is specified; each object of the system is assigned a security level that determines the importance of the information contained in it; each subject of the system is assigned an access level that determines the level of trust in him in the intellectual system. In addition, the mandate policy has a higher degree of reliability. The implementation of this policy is based on the developed algorithm for determining the agreed security levels for all elements of the ontology.

Since semantic knowledge bases, unlike a relational database, allow executing rules for obtaining logical conclusions, it is relevant to ensure data security by developing algorithms and methods that can only receive data that have security levels less than the access levels of the subjects who requested them [7].

Connectivity

All information stored in the semantic memory of the intelligent system is systematized in the form of a single knowledge base. Such information includes directly processed knowledge, interpreted programs, formulations of tasks to be solved, plans and protocols for solving problems, information about users, a description of the syntax and semantics of external languages, a description of the user interface, and much more [8]. In the information knowledge base between fragments of information (units of information), the possibility of establishing links of various types should be provided. First of all, these links can characterize the relationship between information units. Violation of connections leads to an incorrect logical conclusion, or to obtaining false knowledge, or to incompatibility of knowledge in the base.

Introduction of semantic metric

On a set of information units, in some cases it is useful to set a relation that characterizes the semantic proximity of information units, i.e. the force of the associative connection between information units [9]. It could be called the relevance relation for information units. This attitude makes it possible to single out some typical situations in the knowledge base. The relevance relation when working with information units allows you to find knowledge that is close to what has already been found.

Semantic Compatibility

Internal semantic compatibility between the components of an intelligent computer system (i.e., the maximum possible introduction of common, coinciding concepts for various fragments of a stored knowledge base), which is a form of convergence and deep integration within an intelligent computer system for various types of knowledge and various problem solving models, which ensures effective implementation of the multimodality of an intelligent computer system. External semantic compatibility between various intelligent computer systems, which is expressed not only in the commonality of the concepts used, but also in the commonality of basic knowledge and is a necessary condition for ensuring a high level of socialization of intelligent computer systems [10].

Activity

In an intellectual system, the knowledge available in this system contributes to the actualization of certain actions. Thus, the execution of activities in an intelligent system should be initiated by the current state of the knowledge base. The appearance in the database of facts or descriptions of events, the establishment of links can become a source of system activity [11]. Including deliberate distortion of information and connections can become a source of deliberate distortion of information.

For new generation intelligent systems, there are a number of aspects that require the development of new algorithms and methods for ensuring information security in addition to existing mechanisms:

- multi-level access to individual parts of the knowledge base, as information can be public, personal, confidential;
- monitoring of changes in the meanings of words over time, as well as the meanings of translation from a foreign language that may influence decisions;
- protection against unauthorized use by using cryptosemantic ciphers;
- constant monitoring of vulnerabilities in the system;
- logging of actions (interactions) of the system.

To solve the tasks set, an expert ostis system can be used, which is capable of detecting abuses and anomalies in the behavior of all participants in the OSTIS Ecosystem based on continuous monitoring and the introduction of protocols for the interactions of participants.

The creation and application of expert systems is one of the important stages in the development of information technology and information security [12]. Accordingly, the solution to the problems of ensuring information security can be obtained based on the use of expert systems:

- it becomes possible to solve complex problems with the involvement of a new mathematical apparatus specially developed for these purposes (semantic networks, frames, fuzzy logic);
- the use of expert systems can significantly improve the efficiency, quality and efficiency of decisions through the accumulation of knowledge.

IV. Conclusion

For effective information protection of the system at the present stage, a symbiosis of traditional technologies

and technologies implemented within the framework of OSTIS is required. It should also be noted that ensuring information security based on OSTIS technology is much easier, because many aspects have already been implemented at the design stage of the technology itself. It is important to note that a new generation intelligent information system is an independent entity that can consciously, purposefully and constantly take care of itself, including its own security.

References

[1] S. Isoboev, D. Vezarko, and A. Chechel'nitskii, "Intellektual'naya sistema monitoringa bezopasnosti seti besprovodnoi svyazi na osnove mashinnogo obucheniya [intelligent system for monitoring the security of a wireless communication network based on machine learning]," *Ekonomika i kachestvo sistem svyazi*, no. 1(23), pp. 44–48, 2022.

[2] A. Skrypnikov, V. Denisenko, E. Khitrov, I. Savchenko, and K. Evteeva, "Reshenie zadach informatsionnoi bezopasnosti s ispol'zovaniem iskusstvennogo intellekta [solving information security problems using artificial intelligence]," *Sovremennye naukoemkie tekhnologii*, no. 6, pp. 277–281, 7 2021.

[3] V. Chastikova and A. Mityugov, "Metodika postroeniya sistemy analiza intsidentov informatsionnoi bezopasnosti na osnove neiroimmunnogo podkhoda [methodology for building an information security incident analysis system based on the neuroimmune approach]," *Elektronnyi Setevoi Politematicheskii Zhurnal «Nauchnye Trudy Kubgtu»*, no. 1, pp. 98–105, 2022.

[4] D. D. Abdurakhman, "Iskusstvennyi intellekt i mashinnoe obuchenie v kiberbezopasnosti [artificial intelligence and machine learning in cybersecurity]," *Sovremennye problemy lingvistiki i metodiki prepodavaniya russkogo yazyka v vuze i shkole*, no. 34, pp. 916–921, 2022.

[5] A. Ostroukh, *Intellektual'nye sistemy: monografiya*. Krasnoyarsk: Nauchno-innovatsionnyi tsentr, 2020.

[6] A. Baranovich, "Semanticheskie aspekty informatsionnoi bezopasnosti: kontsentratsiya znanii," *Istoriya i arkhivy*, no. 13(75), pp. 38–58, 2011.

[7] V. Khoang and A. Tuzovskii, "Resheniya osnovnykh zadach v razrabotke programmy podderzhki bezopasnosti raboty s semanticheskimi bazami dannykh [solving the main tasks in the development of a security support program for working with semantic databases]," *Doklady TUSURa*, no. 2(28), pp. 121–125, 2013.

[8] V. Glenkov, N. Guliakina, I. Davydenko, and D. Shunkevich, "Semanticheskaya model' predstavleniya i obrabotki baz znanii [semantic model for representation and processing of knowledge bases]," L. Kalinichenko, Y. Manolopulos, N. Skvortsova, and V. Sukhomlina, Eds. FIC IU RAN, 10 2017, pp. 412–419.

[9] A. Dement'ev, "Metriki semanticheskikh dannykh [semantic data metrics]," *Molodoi uchenyi*, no. 24(419), pp. 48–51, 6 2022.

[10] V. Golenkov, N. Guliakina, I. Davydenko, and A. Eremeev, "Methods and tools for ensuring compatibility of computer systems," in *Open semantic technologies for intelligent systems*, ser. 4, V. Golenkov, Ed. BSUIR, Minsk, 2019, pp. 25–52.

[11] V. Druzhinin and D. Ushakov, *Kognitivnaya psikhologiya. Uchebnik dlya vuzov [Cognitive psychology. Textbook for universities]*. M.: PER SE, 2002.

[12] E. Sozinova, "Primenenie ekspertnykh sistem dlya analiza i otsenki informatsionnoi bezopasnosti [the use of expert systems for the analysis and evaluation of information security]," *Molodoi uchenyi*, no. 10(33), pp. 64–66, 10 2011. [Online]. Available: https://moluch.ru/archive/33/3766/

Обеспечение информационной безопасности Экосистемы OSTIS

Чертков В. М., Захаров В. В.

Большое разнообразие моделей обеспечения информационной безопасности, всё возрастающий объем данных, которые необходимо анализировать для обнаружения атак на информационные системы, изменчивость методов атак и динамическое изменение защищаемых информационных систем, необходимость оперативного реагирования на атаки, нечеткость критериев обнаружения атак и выбора методов и средств реагирования на них, нехватка высококвалифицированных специалистов по защите влечет за собой потребность в использовании методов искусственного интеллекта для решения задач безопасности.

В статье рассмотрены подходы к использованию искусственного интеллекта для обеспечения безопасности традиционных информационных систем, особенности обеспечения информационной безопасности интеллектуальных систем нового поколения и основные угрозы и принципы, лежащие в основе обеспечения информационной безопасности ostis-систем.

Received 13.03.2023