Information security in intelligent semantic systems

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

***Abstract*—The development of artificial intelligence causes the transition to semantic information processing technologies, which require the formation of new approaches to ensuring the 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 ensuring information security in intelligent systems is given and the formed main goals and directions for the development of information security are presented. The methods of ensuring information security considered in the article are extremely important when analyzing the level of security of new generation intelligent systems.**

***Keywords*—information security, intelligent systems, semantic systems**

I. Introduction

One of the modern directions in the development of information technologies is the transition to working with the semantics of information and the creation of intelligent systems of a new generation [1]. The main advantage of which is the organized work with the semantic knowledge base. A feature of such a knowledge base is that the intelligent system is able to obtain new knowledge that is not directly contained in the database.

Since the design, construction and use of intelligent systems based on semantic knowledge bases began relatively recently, the issue of ensuring their security has not yet been fully resolved. In this regard, it is relevant to develop methods and algorithms that allow maintaining the safety of the functioning of such intelligent systems.

Currently, many methods have been developed to ensure information security in intelligent systems based on storing information in relational databases. But these methods cannot be used to ensure the security of semantic intelligent systems. Because such systems use semantic databases. Semantic databases are characterized by a strong hierarchical relationship between elements. Also, in semantic databases, it is possible to obtain new knowledge by using certain logical rules. Separate methods and algorithms have already been developed to solve the problems of ensuring the security of semantic databases: user access control based on named RDF graphs, user access control at the triplet level in the RDF storage. But the developed methods and algorithms have a number of shortcomings that do not allow to effectively ensure the comprehensive security of semantic databases.

II. Artificial intelligence and information security

Based on the analysis of literary sources, the information security of intelligent systems is considered from two aspects: 1) the use of artificial intelligence in information security; 2) organization of information security in intelligent systems.

A. Applications of artificial intelligence in information security

It should be noted that artificial intelligence (machine learning) is actively used to monitor and analyze security vulnerabilities in information transmission networks [2]. An 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.

– intrusion 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;

– secure software development: native intelligence can help create more secure software by providing developers with real-time feedback.

In [3], a method for constructing a neuroimmune system for analyzing information security incidents is proposed, which combines modules for collecting and storing (compressing) data, a module for analyzing and correlating information security events, and a subsystem for detecting network attacks based on convolutional neural networks. The use of machine learning technologies in information security creates bottlenecks and system vulnerabilities that can be exploited and have 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).

B. Organization of information security in intelligent systems

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

From the monograph by A.V. Ostroukh [5], the goals of ensuring the information security of traditional intelligent systems are to ensure the safety and confidentiality of information, protection and guarantee of the availability, reliability and integrity of information, avoiding information leakage, minimizing damage from events that threaten information security.

It should be noted that since the new generation of intelligent systems 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: to ensure the safety of the semantic compatibility of information, to protect the reliability and integrity of information, to ensure the availability of information at different levels of the intelligent system, to minimize damage from events that threaten 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, IP 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 violating information security;

- the principle of complexity - to ensure security in the whole variety of structural elements, threats and channels of unauthorized access, all types and forms of protection should 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. Alarm 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 should reliably block all penetration routes and possible channels of information leakage;

- the principle of universality - security measures should block the paths 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 security in the work of the process of providing services should be implemented with a sufficient degree of perseverance;

- the principle of qualification of service personnel - maintenance of equipment should be carried out by employees trained not only in the operation of equipment, but also in technical issues of ensuring the security of information;

– 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 main directions of ensuring information security of semantic intelligent systems

Consider the architecture of the Ecosystem OSTIS (Open Semantic Technology for Intelligent Systems), which is shown in Figure 1.

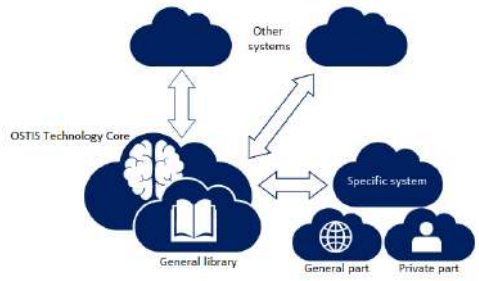

Figure 1. The architecture of the Ecosystem OSTIS.

The core of OSTIS technology includes: – OSTIS semantic knowledge base: it can describe any kind of

knowledge, while it is easy to supplement it with new types of knowledge.

– OSTIS problem solver: Based on a multi-agent approach. This approach makes it easy to integrate and combine any problem solving models.

– interface of the OSTIS system: it 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, the components are updated automatically;

– each owner of the OSTIS Ecosystem application can share part of their knowledge for a fee or for free.

In the considered Ecosystem OSTIS, it is required to organize information security at each level: 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 violation of links in the database knowledge. It should be noted that for some areas of ensuring the information security of semantic systems, methods and algorithms developed within the framework of traditional intelligent systems will be applied. For intelligent systems of the new generation, a number of aspects can be distinguished, within which the development of new algorithms and methods for ensuring information security is required. Let us present the main directions of ensuring the information security of semantic intelligent systems.

A. Restriction of information traffic analyzed by the intelligent system

The exponential growth of the amount of information circulating in information flows and resources under the conditions of quite definite 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 useless information is carried out through the use of axiological filters that implement the functions of numerical evaluation 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].

B. Knowledge base access control policy

Mandatory security policy (MAC - mandatory access control) 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].

1) 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.

2) Application of semantic metric: On a set of information units, in some cases it is useful to set a relation that characterizes the situational proximity of information units, i.e. the strength of the association between information units. It could be called the relevance relation for information units [9]. 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.

3) 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 different 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].

4) 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 communications can become a source of deliberate distortion of information.

IV. Conclusion

Currently, there are no semantic knowledge bases in which internal interpretability, structuring, coherence would be fully implemented, a semantic measure would be introduced, and knowledge activity would be ensured. The methods of ensuring information security considered in the article are extremely important when analyzing the level of security of new generation intelligent systems. Systems that comply with the semantic security model will be resistant to attacks based on plain texts.

References

[1] V. V. Golenkov, N. A. Gulyakina, I. T. Davydenko, and D. V. Shunkevich, "Semantic technologies of intelligent systems design and semantic associative computers," *Doklady BGUIR*, vol. 3, pp. 42–50, 2019.

[2] S. Isoboev, D. Vezarko, and A. Chechel'nitskii, "Intellektual'naya sistema monitoringa bezopasnosti seti besprovodnoi svyazi na osnove mashinnogo obucheniya," *Ekonomika i kachestvo sistem svyazi*, vol. 1(23), pp. 44–48, 2022.

[3] V. A. Chastikova and A. I. Mityugov, "Metodika postroeniya sistemy analiza intsidentov informatsionnoi bezopasnosti na osnove neiroimmunnogo podkhoda," *Elektronnyi Setevoi Politematicheskii Zhurnal «Nauchnye Trudy Kubgtu»*, vol. 1, pp. 98–105, 2022.

[4] D. D. Abdurakhman, "Iskusstvennyi intellekt i mashinnoe obuchenie v kiberbezopasnosti," *Sovremennye problemy lingvistiki i metodiki prepodavaniya russkogo yazyka v vuze i shkole*, vol. 34, pp. 916–921, 2022.

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

[6] A. Palagin, "Semanticheskie aspekty informatsionnoi bezopasnosti: kontsentratsiya znanii," *Istoriya i arkhivy*, vol. 13(75), pp. 38–58, 2011.

[7] K. Khoang and A. Tuzovskii, "Resheniya osnovnykh zadach v razrabotke programmy podderzhki bezopasnosti raboty s semanticheskimi bazami dannykh," *Doklady TUSURa*, vol. 2(28), pp. 121–125, 2013.

[8] V. V. Golenkov, N. A. Gulyakina, I. T. Davydenko, and D. V. Shunkevich, "Semanticheskaya model' predstavleniya i obrabotki baz znanii," in *Data analytics and management in data-intensive fields: a collection of scientific papers of the XIX International Conference (DAMDID/RCDL'2017)*. Moscow: Federal'nyi issledovatel'skii tsentr "Informatika i upravlenie" Rossiiskoi akademii nauk, 2017, pp. 412–419.

[9] A. V. Dement'ev, "Metriki semanticheskikh dannykh," *Molodoi uchenyi*, vol. 24(419), pp. 48–51, 2022.

[10] V. V. Golenkov, N. A. Gulyakina, and D. V. Shunkevich, "Tekushchee sostoyanie i napravleniya razvitiya tekhnologii iskusstvennogo intellekta," in *Informatsionnye tekhnologii i sistemy 2018 (ITS 2018): materialy mezhdunarodnoi nauchnoi konferentsii [Information Technologies and Systems 2018 (ITS 2018)]*. Minsk : BSUIR, 2018, pp. 11–16.

[11] V. N.Druzhinina and D. V. Ushakova, *Kognitivnaya psikhologiya. Uchebnik dlya vuzov*. Moscow: PER SE, 1974.

Информационная безопасность интеллектуальных семантических систем

Чертков В. М.

Развитие искусственного интеллекта обуславливает переход на семантические технологии обработки информации, которые требует формирование новых подходов к обеспечению информационной безопасности таких систем. Статья посвящена обзору подходов и принципов обеспечения безопасности в интеллектуальных системах нового поколения. Приводиться современное состояние обеспечения информационной безопасности в интеллектуальных системах и представлены сформированные основные цели и направления по развитию обеспечения информационной безопасности. Рассмотренные в статье методы обеспечения безопасности информации являются чрезвычайно важными при анализе уровня защищённости интеллектуальных систем нового поколения.

Received 01.11.2022