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, p. 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,.* Taganrog : no. 34, pp. 916–921, 2022.;

[5]] A. Ostroukh, Intellektual'nye sistemy: monografiya. Krasnoyarsk: Nauchno-innovatsionnyi tsentr, 2020. pp. 245–250, 2017, (In Russ.).

[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

Semantic Approach to Designing Applications with Passwordless Authentication According to the FIDO2 Specification

Anton Zhidovich and Alexei Lubenko and Iosif Vojteshenko and Alexey Andrushevich
Belarusian State University
Minsk, Belarus
anton.zhidovich, alexeilubenko02@gmail.com, voit, andrushevich@bsu.by

***Abstract*—*In* this paper, a semantic approach to designing applications with the FIDO2 specification-based passwordless authentication using OSTIS technology is proposed. Obtained results will improve the efficiency of the component approach to the development of applications with passwordless authentication, as well as provide the ability to automatically synchronize different versions of components, increasing their compatibility and consistency.**

***Keywords*—FIDO2 technology, passwordless authentication, OSTIS technology, biometrics**

I. INTRODUCTION

When building an intelligent system, it's necessary to accord special priority to the issue of access to system resources and the differentiation of user rights. The key concept here is authentication – a procedure of identity verification to ensure that the user is the subject whose identifier he uses. The issue becomes more complicated when designing different semantically compatible intelligent systems [1], requiring a unified authentication apparatus: easy to use and integrate, as well as the most secure.

The authentication system is only a component, and therefore the development of a unified approach to its design is required. There are various authentication standards, many of which may not provide a high level of security and, moreover, may be compatible only with a certain software class or be proprietary.

II. ANALYSIS OF AUTHENTICATION METHODS

Let's take a look at the most common authentication methods. These methods can be encountered both in everyday life, with the use of messengers, online banking or other online services, and within corporate systems where data is accessed by company employees and delineated according to their position.

A. *Password-based authentication*

Being the most common because of its ease of implementation, password-based authentication method is vulnerable to the most types of attacks: brute-force, range attacks, dictionary attacks, key-logging, social engineering such as phishing, man-in-the-middle and replay attacks.

B. *Trusted third-party authentication*

The method is based on the fact that the service (provider) that owns the user's data, with his permission, provides third-party applications with secure access to this data. The provider is usually a service such as Google, GitHub, Facebook or Twitter. The most common implementation is the OAuth 2.0 protocol.

The OAuth 2.0 specification defines a protocol for delegating user authentication to the service that hosts a user account and authorising third-party applications to access that user account [2].

In [2] the main participants of OAuth 2.0 authentication and their interaction are described. Although this method is one of the most user-friendly and, moreover, implemented in most online resources, it is still vulnerable to a man-in-the-middle attack, which is a common and effective way to gain unauthorised access to a system.

C. *One-time password (OTP)*

OTP, which is used in many systems as a second or first authentication factor, can be a number or some string that is generated for a single login process. When authenticating, the OTP can be sent to the user via SMSmessage, push notification or in a special application. The most secure tool for generating one-time passwords is a token (software, such as Google Authenticator, or hardware).

OTP quickly becomes invalid, which provides resistance to replay attacks. However, most attacks on authentication systems with OTP target the way the user receives it. For example, OTP transmitted via SMS can be intercepted by software such as FlexiSPY or Reptilicus.

One-time passwords are protected against phishing in the classic sense: users cannot reveal long-term credentials. However, the man-in-the-middle attack can be used to retrieve a currently valid one-time password.

D. *Passwordless authentication methods*

Passwordless authentication allows a user to access an information system without entering a password or answering security questions. Instead, the user provides