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;
- 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:**

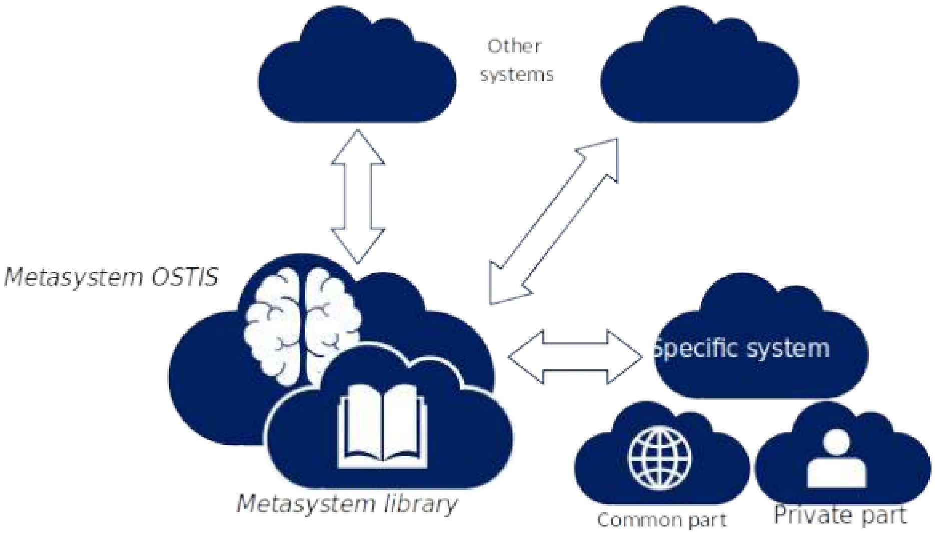

Figure 1: OSTIS Ecosystem Architecture

[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.