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