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 ostissystems 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; systems.
- 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 nonstandard 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) — sys305 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