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:**