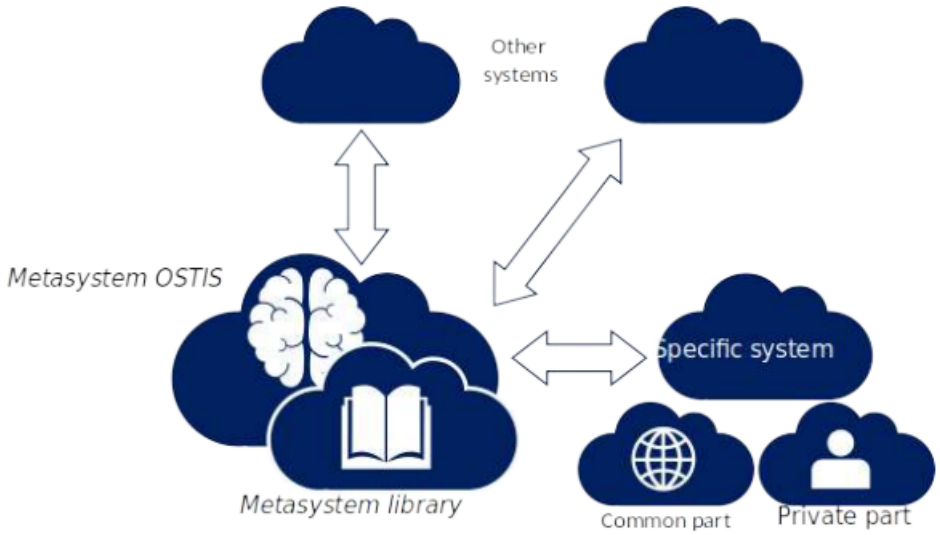

Figure 1: OSTIS Ecosystem Architecture

[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.