MODELING OF THE METHOD OF ESTIMATION AND ANALYSIS OF PROTECTION OF INFORMATION RESOURCES IN DISTRIBUTED SYSTEMS

Botirov.X.N assistant
B.I.Yusupaliyev a student
F.E.Qodirov a student
Karshi branch of TUIT named after Muhammad Al-Khorezmi

Key words: information security, threat, threat assessment, distributed system, linear encryption, algorithm.

Modern methods of processing, transmission and accumulation of information contributed to the emergence of threats associated with the possibility of loss, distortion and disclosure of data. Therefore, ensuring information security is one of the leading directions in the development of information technology. There are the following prerequisites, or the causes of threats:

- objective (quantitative or qualitative insufficiency of the elements of the system) - not directly related to people's activities and causing random by nature of the threat;

- subjective - directly related to human activities and causing as intentional (the activity of intelligence services of foreign countries, industrial espionage, the activities of criminal elements and unfair employees), and unintentional (poor psychophysiological state, insufficient training, low level of knowledge) threats to information.

Implementation of threats to information security can be done:

• through agency sources in the bodies of commercial structures, public administration, having the opportunity to obtain confidential information;

• by bribing individuals who work in the enterprise or in structures directly related to its activities;

• by interception of information circulating in means and communication systems and computer facilities, by means of technical reconnaissance and software-mathematical influences on it during processing and storage;

• by eavesdropping of negotiations conducted in office premises, vehicles, in apartments and in cottages;

• through negotiation processes with foreign or domestic firms, using non-cautious handling of information.

• Through "initiators" from among employees who want to improve their well-being by "earning" money or take the initiative for other material or moral reasons.

Along with the development of methods and methods of transformation and transmission of information, the methods of ensuring its security are constantly developing. The current stage in the development of this problem is characterized by a shift from the traditional view of it as a problem of protecting information to a broader understanding - the problem of information security, which consists in its integrated solution in two main areas.

The first can include protection of state secrets and confidential information, providing mainly the impossibility of unauthorized access to them. At the same time confidential information means information of limited access of a public nature (commercial secret, party secret, etc.).

The second direction concerns protection from information, which has recently acquired an international dimension and a strategic character. At the same time, three main areas of protection from the so-called information weapon (impact) are distinguished:

- on technical systems and facilities;

- society;

- the human psyche.

To achieve this goal, the intermediate environment must provide services for the interaction of the components of the distributed system. To such services are:

- provision of a unified and independent mechanism for the operation of other software components by some software components of the system;
- provision of security of the distributed system: authentication and authorization of all users of the components' services and protection of information transmitted between components from reading and reading by third parties;
- providing data integrity: managing transactions distributed between remote system components;
- Load balancing on servers with software components;
- Detection of remote components.

To ensure the security of a distributed system, the intermediate environment must support the three general-purpose functions necessary to create a system without dangerous systems.

1. Verify the authenticity of the user of the services of the component of the distributed system (authentication1). Verification of authenticity can be one-sided, when only the server is convinced of the authenticity of the client, or two-tone, when the client also convinces of the authenticity of the server.

Restriction of access to the services of the component, depending on the results of authentication (authorization). To solve this problem, the intermediate environment must support the access restriction, which is based on so-called roles (røle baced security). Because component developers can not designate access levels through specific users or user groups of the system, they must use some abstract roles that, when the component is deployed, will be linked by the system administrator to the system user accounts.

Protection of data transmitted between components of the system, from viewing and changing by third parties. For this, messages transmitted between the components must be signed by an electronic signature and encrypted both by the client and the server. As a standard safety model, the CIA model is often cited:

- Confidentiality of information - co-funding (mandatory for the person who has access to certain information to comply with the requirement not to transmit such information to third parties without the consent of its owner);
- Integrity;
- availability (avialability).

To protect the information transmitted to the communication channels, a set of methods and means of protection are used to block possible threats to information security.

The most reliable and universal method of protecting information in communication channels is encryption. Encryption at the subscriber level allows you to protect operational information from loss of confidentiality and the imposition of false information.

Linear encryption allows, in addition, to protect the service information. Without access to the service information, the attacker can not record the fact of transmission between specific subscribers of the network, change the address part of the message in order to redirect it.

Counteraction to false connections of subscribers (processes) is provided with application of a number of procedures of mutual authentication of subscribers or processes authenticity. Against deletion, overt distortion, reordering, transmission of duplicate messages, the mechanism of acknowledgment, numbering of messages or use of information about the time of sending messages is used. These service data must be encrypted. The intensity of the exchange can be hidden by adding special messages to the workflow.

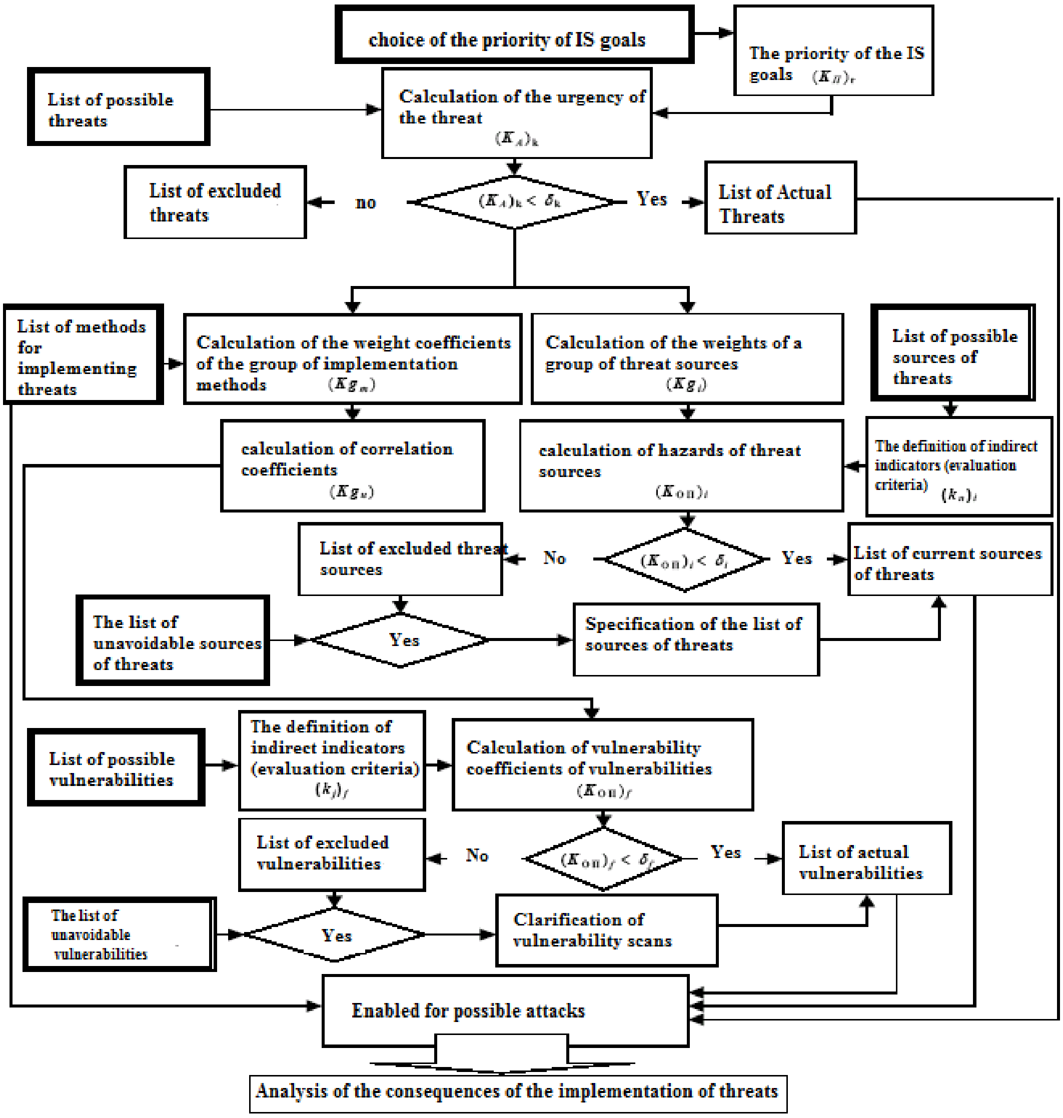
choice of the priority of IS goals
The priority of the IS goals $(K_П)_r$
List of possible threats
Calculation of the urgency of the threat $(K_A)_k$
List of excluded threats
no
$(K_A)_k < \delta_k$
Yes
List of Actual Threats
List of methods for implementing threats
Calculation of the weight coefficients of the group of implementation methods (Kg_m)
Calculation of the weights of a group of threat sources (Kg_i)
List of possible sources of threats
calculation of correlation coefficients (Kg_u)
calculation of hazards of threat sources $(K_{оп})_i$
The definition of indirect indicators (evaluation criteria) $(k_n)_i$
List of excluded threat sources
No
$(K_{оп})_i < \delta_i$
Yes
List of current sources of threats
The list of unavoidable sources of threats
Yes
Specification of the list of sources of threats
List of possible vulnerabilities
The definition of indirect indicators (evaluation criteria) $(k_j)_f$
Calculation of vulnerability coefficients of vulnerabilities $(K_{оп})_f$
List of excluded vulnerabilities
No
$(K_{оп})_f < \delta_f$
Yes
List of actual vulnerabilities
The list of unavoidable vulnerabilities
Yes
Clarification of vulnerability scans
Enabled for possible attacks
Analysis of the consequences of the implementation of threats

Fig. 1. Algorithm for analyzing and assessing threats

Thanks to this approach, it is possible:

- establish priorities for security objectives for the subject of the relationship;
- determine the list of current sources of threats;
- determine the list of actual vulnerabilities;
- assess the relationship between vulnerabilities, sources of threats, the possibility of their implementation;
- determine the list of possible attacks on the object;
- develop scenarios for possible attacks;
- describe the possible consequences of implementing threats;
- Develop a set of protective measures and a system for managing the economic and information security of the enterprise.

The results of the assessment and analysis can be used to select the appropriate optimal methods for parrying threats, as well as when auditing the real state of information security of the facility.

To create an optimal information security system for an enterprise, it is necessary to correctly assess the situation, identify possible risks, develop a security concept and policy, on the basis of which the model of the system is built and appropriate mechanisms for implementation and functioning are developed.

Литература

1. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 2. Распределенные системы, сети, безопасность; Бином-Пресс - Москва, 2011. - 704 с
2. Васильков, А.В. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум, НИЦ ИНФРА-М, 2013.
3. Васильков, А.В. Информационные системы и их безопасность: Учебное пособие / А.В. Васильков, А.А. Васильков, И.А. Васильков. - М.: Форум,
4. Ерохин, В.В. Безопасность информационных систем: Учебное пособие / В.В. Ерохин. - М.: Флинта,
5. Астахов А.Н. Анализ защищенности корпоративных систем. /Открытые системы, 2002, № 7,8/
6. Трифаленков И., Зайцева Н. Функциональная безопасность корпоративных систем. /Открытые системы, 2002, № 7,8, С12/