ISSN 2278-3091
Volume 9, No.4, July – August 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse356942020.pdf
https://doi.org/10.30534/ijatcse/2020/356942020

Processes for Detecting Information Vulnerabilities in Distance Learning Systems

Shamshieva Barno Makhmudjonovna[1], Nasrullaev Nurbek Bakhtiyorovich[2], Fayzieva Dilsora Salimovna[3],
[1]Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan, shamshievabarno83@gmail.com
[2]Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan, n.bakhtyarovich@gmail.com
[3]Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan, dilsora.salimovna@gmail.com

ABSTRACT

This paper describes the process of managing information security risks and threats in distance learning systems. The scheme shows the relationship between the parameters of information security threats to assess the risks and the protected asset, as well as the architecture of the general threat tree for the protected asset. The a priori possibility of implementing threats to information security based on dynamic expert decision support systems in distance learning systems is applied. The scheme of data interaction model of the information security risk and threat management process, a descriptive model of an information security intruder and an algorithm for managing security risks in distance learning systems are proposed.

Key words: Asset, vulnerability, distance learning systems, risk, damage, destructive impact, dynamic expert systems.

1. INTRODUCTION

Today, educational institutions widely use electronic information, computer technology, information systems, Internet resources and distance learning systems in their activities. These dough systems interact with each other and the participants in the educational process, forming a virtual socio-technical system, which allows ensuring the continuity of learning and the interactivity of the teacher and student interaction outside of time and space. Distance technologies make it possible to expand the possibilities of full-time education by increasing the mutual accessibility of learning subjects, information data sets and virtual educational objects.

At the same time, access points to distance learning systems can be both automated workstations inside an educational institution and remote devices, which in turn gives rise to a number of sources of cyber threats and system vulnerabilities. As a result, a violation of the security of the distance learning system as a result of the impact of threats of various natures often leads to a violation of information security in a segment or the entire information system of an educational institution.

To prevent various scenarios of information security breaches and minimize damage to the distance learning system and the information system of an educational institution, it is necessary to apply a set of measures and means of protecting information at various levels of the system's functioning, as well as identify and control potential information security risks. Since it is the control of risks that will reveal unacceptable violations and develop an adequate management strategy.

2. INFORMATION SECURITY RISK AND THREAT MANAGEMENT PROCESS IN DISTANCE LEARNING SYSTEMS

The process of managing risks and threats to information security is one of the key aspects in ensuring information security in organizations of various kinds of activities. At the moment, there are a huge number of methods that allow you to determine, identify and assess information security risks in distance learning systems, each method is invariably based on the concept of "information security threats". Often, information security threats are understood as a set of conditions and factors that can create a threat of violation of one of the information security properties. Thus, the concepts of "information security risk" and "information security threat" are mutually complementary concepts, and are continuously connected in the formation of requirements for information security. This approach to information security management is commonly called the risk approach. It should be understood that various methodologies are often based on the specifics of specific activities of the organization, which gives a more complete picture of the types of protected assets, the degree of criticality of information security properties for a specific type of asset, and most importantly, the cost of losing an asset or violating information security properties. Thus, information security risk becomes a tool for determining the consequences of a threat and has a pronounced commercial nature. This approach is applicable to organizations engaged in commercial activities, the main purpose of which is to make a profit. In connection with these circumstances, the risk-oriented approach receives very significant contradictions. The fact is that if it is impossible to determine the value of an asset, it is simply impossible to assess the loss of this asset in quantitative terms. An example of such information might be:

- information constituting a state secret;
- personal data;
- information related to professional activities;
- information constituting the secret of the investigation and legal proceedings.

These types of information, for each organization, as well as the carriers containing them, will be protected information assets, while the protection of such information will be dictated not only by the wishes of the organization itself, but also by the relevant legislative requirements. Thus, the issue of information security risk management must be directly considered in relation to information security threat management. It is generally accepted that there are always threats to information security, however, depending on a number of conditions, the implementation process and the degree of danger of this threat can vary significantly.

The main purpose of the information security risk and threat management process is to determine, analyze and control measures that take into account the likelihood of the implementation of information security threats, and, depending on the type and composition of the protected information asset, to make it possible to mathematically calculate the possible amount of losses associated with the implementation of the threat. The determination of such consequences and losses is characterized by two main components: the value of the asset and the danger of the threat being realized [1]. Based on the above facts, the concept of "asset value" is further replaced by a more general concept - "asset importance", which will be characterized by three verbal meanings: "High asset importance", "Average asset importance", "Low asset importance".

Based on a detailed analysis of existing risk assessment methods and determining the relevance of information security threats, each threat can be characterized by the following main parameters:

1. Object of impact of the threat (asset \ asset type).
2. The source of the threat.
3. Vulnerability used in the implementation of the threat.
4. A way to implement a threat through the use of its inherent vulnerability.
5. Destructive impact arising in the process of threat implementation.
6. The likelihood of the threat being realized.
7. Danger of threat realization.

Based on numerous surveys of experts in the field of information security, it was found that each of the parameters is related to others; these relationships are presented in Figure 1.

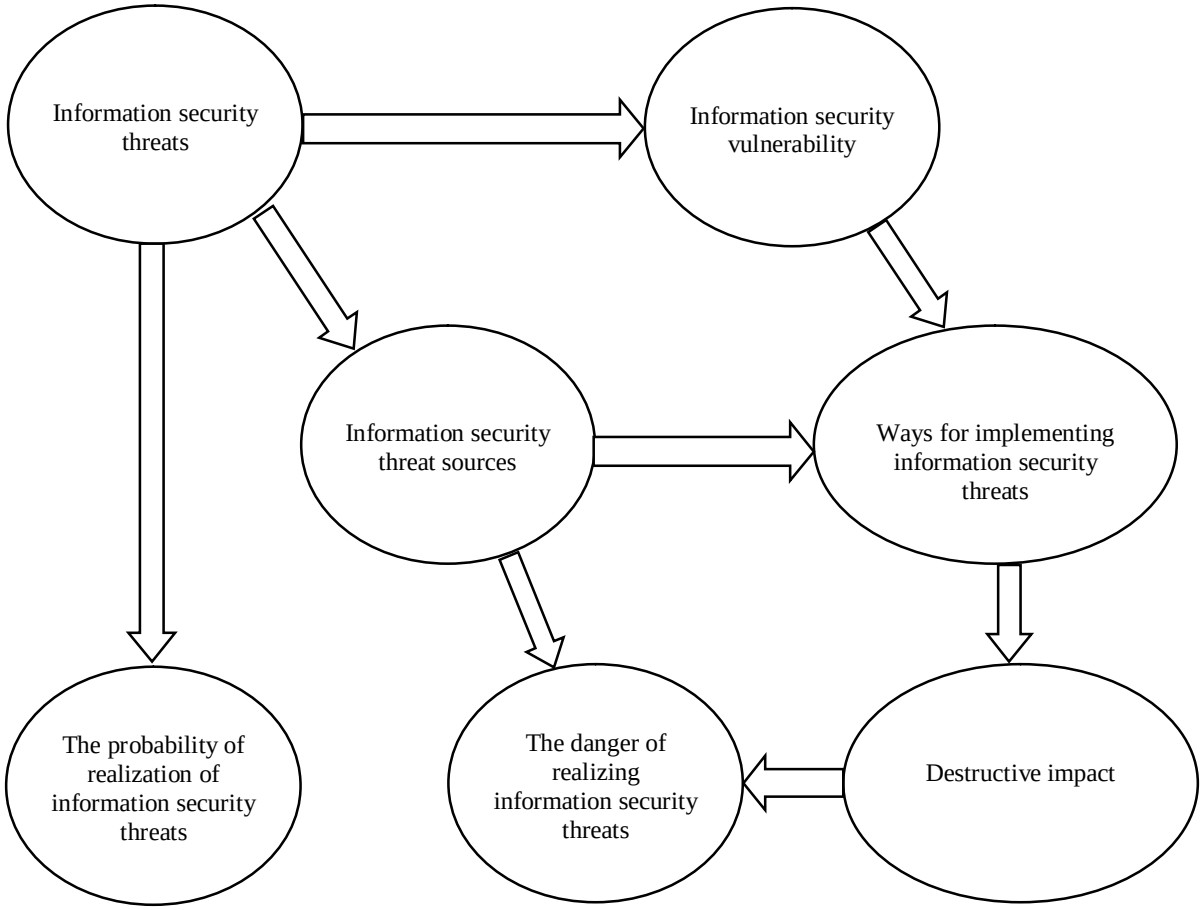

Figure 1: Linking information security threat parameters

Taking into account the previously described parameters necessary for assessing the risks and threats to information

security for the protected asset, the following scheme of the relationship between the parameters of information security threats is obtained, shown in Figure 2.

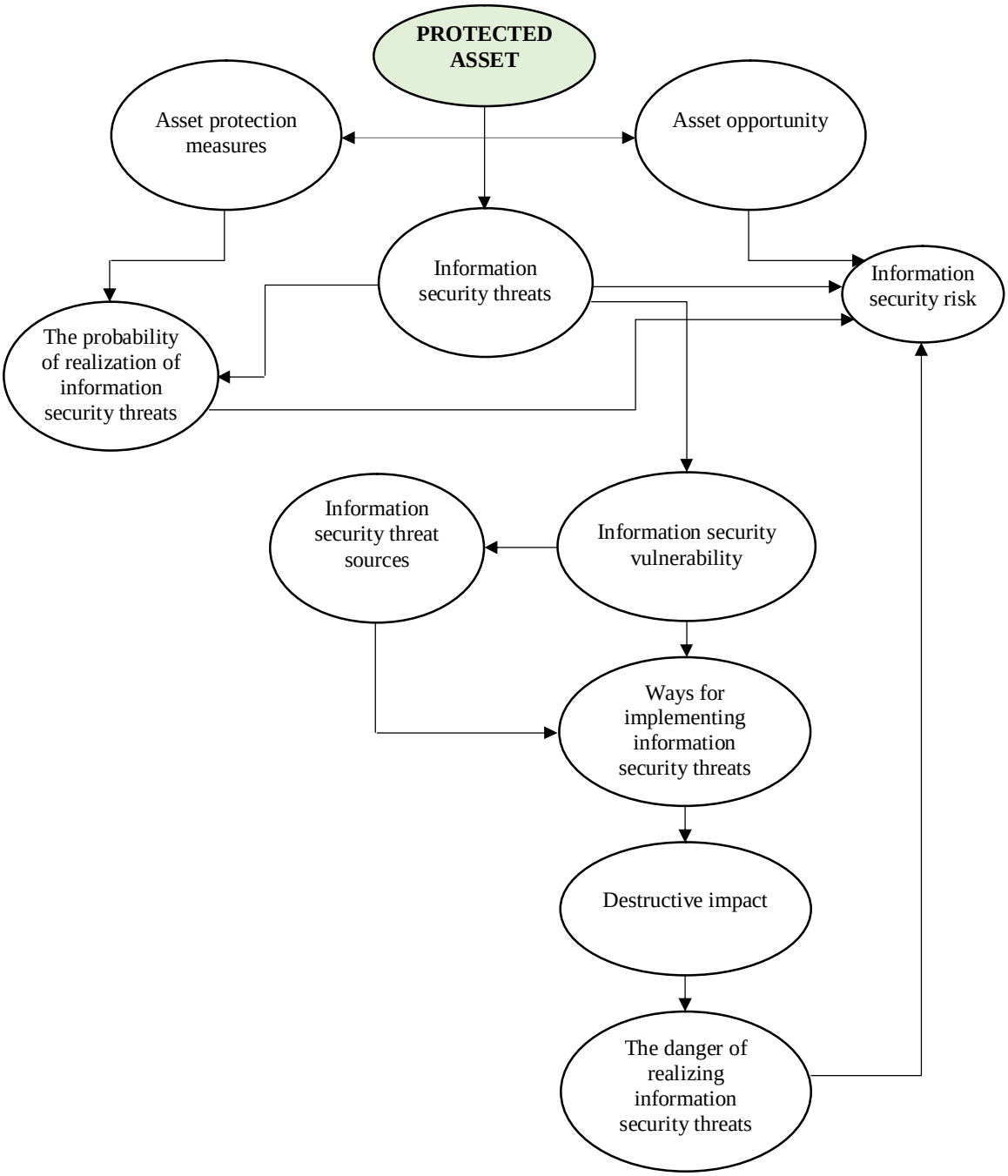

Figure 2: Scheme of the relationship between the parameters of information security threats

Thus, regardless of the chosen methodology for assessing risks and identifying threats to information security, in the process of managing risks and threats to information security, it is possible to build a common tree of risk-threats for a specific selected asset, which gives a complete picture necessary for their analysis. The architecture of this tree is shown in Figure 3.

Depending on the importance of the asset, the likelihood of the threat and the source of the threat, the branches of the tree will change for each specific threat, based on the type of asset and the intruder's model. In the general case, the likelihood of the threat and the degree of its danger will affect the relevance of the threat, and in the case of a

risk approach, the possible consequences of the destructive impact on the asset in question will be taken into account. As can be seen from Fig. 3, when using such an approach to the process of managing information security risks and threats, the more detailed the chosen methodology describes information threats and the higher the competence of the information security analyst who determines the relevance of threats and the magnitude of risks, the more branches in the tree. One of the key tasks in managing information security risks and threats is control and accounting of measures to ensure asset protection. In many terminologies, these measures, when considered in relation to threats, are called countermeasures [2]. Depending on the threat, the set of countermeasures to cover a given threat can vary significantly.

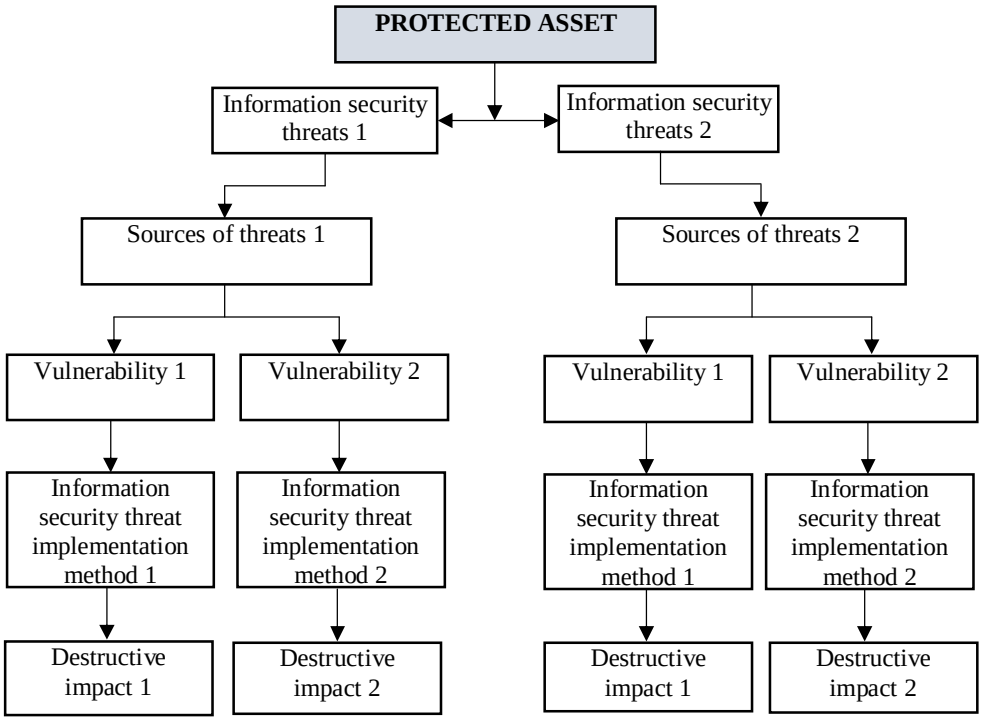

Figure 3: Architecture for constructing a common threat tree for a protected asset

Depending on countermeasures and their parameters, information security analysts can judge the likelihood of a particular threat, the value of which is key, both when building a threat model and when calculating risks. In the general case, such a calculation is made on the basis of the aggregate opinion of experts, using the method of expert assessment. This approach has a number of significant disadvantages, namely:

- subjective assessment based on the expert's personal experience;
- fragmentation of parameters used by experts;
- routine of the process;
- the length of the evaluation period.

Thus, the most common approach used in the methods of risk assessment and determination of the relevance of information security threats has a number of significant problems and inconveniences for use. The solution to these problems can be the development of a new method for assessing the possibility of implementation and the danger of threats using automation tools, based on dynamic expert decision support systems. The proposed method formalizes the main features affecting the determination of the possibility of implementation and the danger of information security threats, obtained as a result of knowledge engineering and a corresponding survey of experts in the field of information security.

3. DETERMINATION OF THE A PRIORI POSSIBILITY OF IMPLEMENTATION OF INFORMATION SECURITY THREATS IN DISTANCE LEARNING SYSTEMS

The a priori determination of the probability of implementation of information security threats will be based on the method of expert assessment and the principle of averaging the coefficients for minimization accompanying the method of expert assessment of shortcomings. Based on this logic, the primary relationship of the parameter was determined, which most fully describes the influence of a specific threat source on the possibility of implementing the threat itself [3]. This parameter is directly related to both the threat source itself and the threat under consideration, and directly affects the possibility of threats emerging - the way of implementation.

Taking into account the structure of dynamic expert systems, the a priori determination of the possibility of implementing threats will consist in:

1. Concretization of the investigated problem area, to exclude a combinatorial explosion.
2. Selection of experts.
3. Engineering knowledge experts.
4. Formation of a working database.
5. Formalization of decision making when obtaining results.

To apply an a priori assessment of the possibility of implementing a threat, it is necessary to first analyze all information security threats considered within the framework of the used approach for calculating the relevance of threats to determine all the accompanying implementation methods, in the absence of this classification within the framework of the approach itself.

To determine the parameters of interaction between the threat source and the implementation method, experts need to fill in the intersection of the columns and rows of the matrix based on the following considerations:

- impossible (H\B) - the value is assigned to the intersection if the expert believes that this implementation method cannot be applied by the given threat source;
- low (H) - the value is assigned to the intersection if the expert believes that the given implementation method has low applicability to the given threat source;
- medium (C) - the value is assigned to the intersection if the expert believes that the given implementation method has an average applicability to the given threat source;
- high (B) - the value is assigned to the intersection if the expert believes that the given implementation method is highly applicable to the given threat source [4].

To obtain the primary coefficients of the probability of the threat being realized, each of the parameters is assigned a numerical coefficient:

H\B = 0;
H = 0.2;
C = 0.5;
B = 1.

Thus, there is a matrix of the form $\begin{bmatrix} 11 & \dots & 1M \\ \dots & \dots & \dots \\ N1 & \dots & NM \end{bmatrix}_{k_i}$ (1)

where

i – number of experts;
N – number of threat sources;
M – number of ways to implement.

Moreover, the possibility of implementing V_i information security threats i described by the cumulative set of ways to implement this threat $E_i \in M$.

Final matrix k_r the possibility of implementing threats after filling in by all invited experts will have the form:

$$k_r = \sum_{i=1}^{n} \begin{bmatrix} 11 & \dots & 1M \\ \dots & \dots & \dots \\ N1 & \dots & NM \end{bmatrix}_{k_i} \quad (2)$$

Indicator of threat realization possibility (V_t) intruder N is calculated as the arithmetic mean of the total sum of the row indicators N matrix k_r for all E_t.

Depending on the methodology used for calculating the relevance of threats and information security risks, these coefficients are subject to additional interpretation, however, based on the general logic of the method, the spread of possible values of the final indicators should be interpreted:

1. $V_i \in [0, 0.2)$ – unrealizable;
2. $V_i \in [0.2, 0.5)$ – unlikely realizable;
3. $V_i \in [0.5, 0.8)$ – probably realizable;
4. $V_i \in [0.8, 1)$ – very likely realizable.

4. DATA MODEL SCHEME OF THE INFORMATION SECURITY RISK AND THREAT MANAGEMENT PROCESS

The process of managing information security risks and threats in an organization is a fundamental element in information security management [5]. Based on the results of its work, a colossal number of control actions are formed, both during the creation of an information protection system, and at subsequent stages of its existence. This process is based on two basic mechanisms operating in the organization: a mechanism for calculating risks and a mechanism for processing risks, depending on which the main actions with the information protection system will be built.

As part of the implementation of this process in the organization, the following constituent elements should be determined on the basis of existing internal and external regulatory documents:

- the composition of the considered threats to information security;
- prospective objects of influence in the organization;
- the most likely sources of threats;
- the nature of the impact on the objects of protection.

In Figure 4, taking into account the mechanisms chosen by the organization to calculate the risks, should be determined.

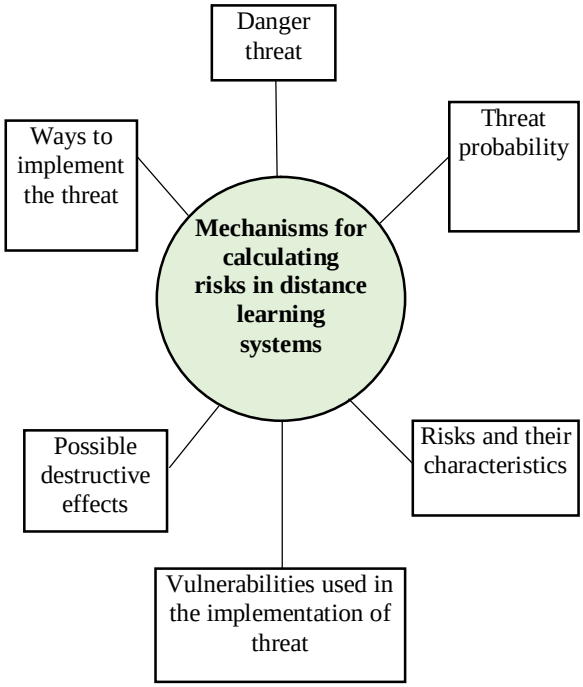

Figure 4: Scheme of risk miscalculation mechanisms in distance learning systems

And taking into account the methods of risk treatment adopted in the organization, appropriate corrective and preventive actions should be formed [6]. At the final stages of the process, a number of critical information is formed, which directly affects the efficiency of the information protection system, the completeness of the implementation of measures to protect information, the correctness and rules for the functioning of information protection tools.

The general scheme of the data interaction model of the information security risk and threat management process in distance learning systems based on dynamic expert decision-making systems is shown in Figure 5.

The implementation of this process is one of the most complex and resource-intensive actions in ensuring information security, however, this process can be significantly facilitated in the case of using automation tools for personnel activities or information security management tools, implemented in accordance with the requirements of the proposed information security management method based on dynamic expert decision support systems.

The information processed and generated as part of this process is transferred for further processing in related information security management processes and will be of key importance in determining the parameters of control, corrective and preventive actions in the organization [7].

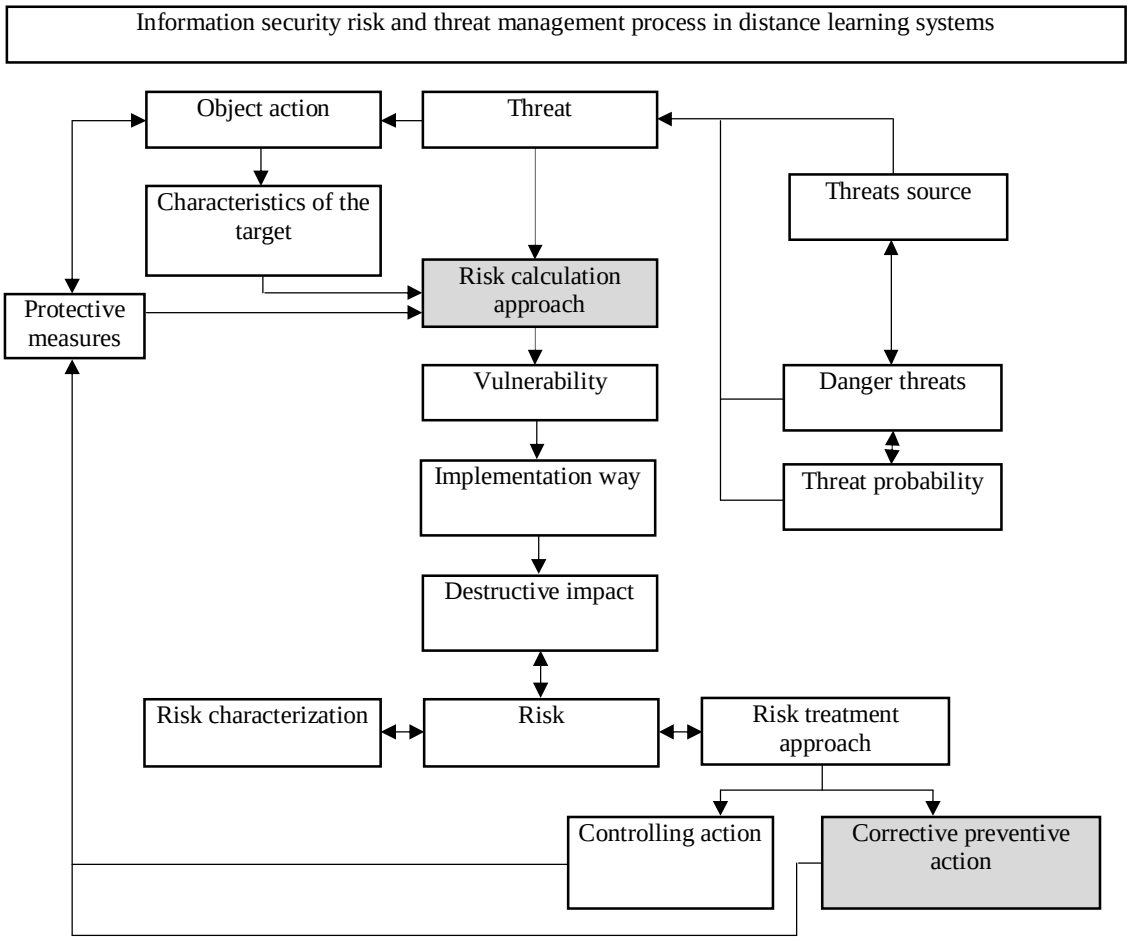

Figure 5: Scheme of the data interaction model of the information security risk and threat management process in distance learning systems

From the point of view of the information security management method based on dynamic expert decision support systems, this process will be one of the constituent parts within the functional group of processes related to the "solver".

5. DESCRIPTIVE MODEL OF INFORMATION SECURITY INTRUDER IN DISTANCE LEARNING SYSTEMS

Taking into account the threat model, a descriptive model of an information security intruder in distance learning systems was compiled as the most dangerous source of cyber security threats (Table 1).

Table 1: Security Intruder Model in Distance Learning Systems

Attacker type	Type	Goal
External actors (individuals)	External	1) Causing financial / reputational damage, desire for self-realization. 2) Identification of vulnerabilities of the distance learning system. 3) Information systems of an educational institution for the purpose of their further sale and obtaining financial benefits. 4) Theft of intellectual property. 5) Obtaining unauthorized access to resources and services of the distance learning system. 6) Violation of the integrity and / or destruction of educational materials and data on the educational process. 7) Violation of the availability of the website and server of the distance learning system. 8) Violation of the availability of information and training course materials for users of the distance learning system. 9) Obtaining unauthorized access to personal data of students and university employees.
Competing institutions	External	1) Obtaining competitive advantages.
Teachers	Internal	1) Obtaining unauthorized access to resources and
Learners	Internal	
Methodists	Internal	

Administrators, developers and technical support of the distance learning system, information security specialists	Internal	services of the distance learning system. 2) Exceeding privileges and gaining control over the distance learning system. 3) Obtaining unauthorized access to the internal information systems of an educational institution through a compromised distance learning system. 4) Theft of scientific materials and intellectual property: educational materials, assessment materials and materials created collectively by participants in the educational process. 5) Obtaining unauthorized access to personal data of students and employees. 6) Obtaining unauthorized access and making changes to the database of educational statements. 7) Obtaining unauthorized access to internal service and other confidential information stored and processed in information systems. 8) Violation of the integrity and / or destruction of educational materials and data on the educational process. 9) Violation of the availability of the website and server of the distance learning system. 10) Violation of the availability of information and training course materials for users of the distance learning system. 11) Causing financial / reputational damage.

The results of the violator's activities are security risks of an informational, operational, financial, reputational nature, some of which may lie in the area of permissible and be accepted by an educational institution, and some of which may be unacceptable [8]. Risk decision making and strategy selection should be carried out as part of an ongoing management cycle.

6. ALGORITHM FOR MANAGING SECURITY RISKS IN DISTANCE LEARNING SYSTEMS

The identified threats to the distance learning system are subject to research for the relevance and the need to use protective equipment and mechanisms aimed at blocking the threat and reducing potential risks of consequences. For this, such characteristics of threats as the probability of implementation and possible damage are investigated. The assessment can be based on processed statistical information about security events, simulations or expert judgment.

To assess the security risks of a distance learning system, an algorithm based on quantitative parameters is proposed. For every threat TR_{ij} from private threat lists, where j – the serial number of the threat in the private list of threats for i –th of the distance learning system [9]. Risk is a probabilistic value; for the calculation, a common two-factor assessment model is used based on the use of an indicator of expected damage – U and the likelihood of the threat being realized – p, formula 3.

$$R(TR_{ij}) = Up \qquad (3)$$

The probability of the threat realization lies in the range [0; 1], the value of the value is directly influenced by the presence / absence of protection measures in this subsystem of the distance learning system and statistically data on the frequency of such a threat – h. To assess the impact of protective measures on the likelihood of a threat in the distance learning subsystem, it is proposed to use 4 levels of protection, each of which is assigned a performance factor:

- no protection measures (QSMlevel=1);
- protective measures create a barrier to the realization of a threat and can reduce the likelihood of its realization (QSMlevel=0.75);
- protection measures create several barriers and significantly complicate the process of threat implementation (QSMlevel=0.5);
- protection measures completely block the threat (QSMlevel=0).

Taking into account formula 3 and the above rules, the amount of risk from each threat in the i –th distance learning subsystem will be calculated according to formula 4.

$$R(TR_{ij}) = U_j h_j QSMlevel_j \qquad (4)$$

The overall risk for each distance learning subsystem will be determined as.

$$R_i = \sum_{j=1}^{m} R(TR_{ij}) = \sum_{j=1}^{m} U_j h_j QSMlevel_j \qquad (5)$$

where

i– distance learning subsystems;

j threat number in each i th distance learning subsystem;

m – the number of threats in the i– distance learning subsystem;

$QSM\,level_i$ – the value of the efficiency factor of protection measures in each subsystem.

To determine the relevance of the threat by the level of risk, it is necessary to compare the obtained ones with the level of acceptable risk, all values less than the acceptable one are subject to acceptance, the rest are subject to insurance, transfer or reduction through the use of measures and means of protection.

7. CONCLUSION

In conclusion, it should be noted that AT developing a scheme of the relationship of information security threat parameters for assessing risks and a protected asset and at constructing the architecture of a common threat tree for a protected asset, it is necessary to develop models and an algorithm for detecting information vulnerabilities in distance learning systems. At the same time, a descriptive model that takes into account the frequency of implementation of the threat, damage and the coefficient of effectiveness of countermeasures to counter the threat and an algorithm for managing security risks in the process of internal security audit are proposed.

REFERENCES

1. Rjaibi N., Rabai L. B. A., Aissa A. B. and Louadi M. (2012). **Cyber Security Measurement in Depth for E-learning Systems**. International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2(11), pp. 1-15.
2. Rabai L. B. A. and Rjaibi N. (2012). **Quatifying Security Threats for E-learning Systems. Education and e-Learning Innovations (ICEELI)**, 2012 International Conference, Tunis, Tunisia, July,2012.
3. Chen Y. and He W. (2013). **Security Risks and Protection in Online Learning: A Survey. The International Review of Research in Open and Distance Learning**, 2013. https://doi.org/10.19173/irrodl.v14i5.1632
4. Mohammed Amin Almaiah, Ahmed Al Mulhem. **Thematic Analysis for Classifying the Main Challenges and Factors Influencing the Successful Implementation of E-learning System Using NVivo. International Journal of Advanced Trends in** Computer Science and Engineering. Volume 9, No.1, January – February 2020. Indexed in Scopus. – P. 142-152
5. Mohamed HALIM, Nouha ADADI, Driss CHENOUNI, Mohammed BERRADA. **Web Services Composition in E-Learning platform**. International Journal of Emerging Trends in Engineering Research. Volume 8. No. 2, February 2020. Indexed in Scopus. – P. 525-532 https://doi.org/10.30534/ijeter/2020/41822020
6. Gulomov Sherzod, Karimova Dilbar, Akbarova Shokhida Azatovna, Qosimova Gulnora Ismoilovna. **Comparative Analysis of Methods Content Filtering Network Traffic**. International Journal of Emerging Trends in Engineering Research. Volume 8. No. 5, May 2020. Indexed in Scopus. – P. 1561-1569 https://doi.org/10.30534/ijeter/2020/15852020
7. Candiwan, NaidaHauraZafira. **An Information Security Awareness Investigation of E-commerce Users: A Case Study of Traveloka**. International Journal of Advanced Trends in Computer Science and Engineering. Volume 9 No.2, March -April 2020. Indexed in Scopus. –P. 1422-1429 https://doi.org/10.30534/ijatcse/2020/79922020
8. Defta, L. (2011). **Information security in E-learning Platforms**, Proceedings of the 3rd World Conference on Educational Sciences, Instanbul, Turkey, 2689 2693. https://doi.org/10.1016/j.sbspro.2011.04.171
9. Kumar, S. & Kamlesh, D. (2011). **Investigation on Security in LMS Moodle**, Proceedings of International Journal of Information Technology and Knowledge Management, Kurukshetra University, Kurukshetra, India, 233-238.