Development of measures to ensure information security in structural division of the university

*Elena Boltynkova**, *Andrey Andreev* and *Alexander Doronin*

Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia

Abstract. In this paper we have determined the place of information security in the national security system of the Russian Federation and analyzed information processed in higher education institutions. The categorization of the processed information in the information system of the Higher School of Technosphere Safety is carried out. The estimation of the potential violator of information security is executed and an improved threat model is made, on the basis of which we have formulated practical proposals for the protection of information in the structural unit of the University.

1 Introduction

In the work of Maltsev D. N., Genson E. M. and Repetskiy D. S. identified the most important elements of the educational process in higher education institutions of the Russian Federation, in particular, self-study and the ability to use information technology [1]. Deryabina S. A. And Dyakova T. A. established that electronic resources play an important role in education, as they allow easy access to educational materials for independent or indirect study and have an ordered, systematic structure, presented in a convenient form for study, providing ease of perception of the educational material, its completeness and visual representation [2].

However, in the study of scientific works in the field of information security, it can be concluded that in addition to educational materials in the information systems of the University, work with use of limited access information can be carried out [3, 4, 5]. In particular, the Higher School of Technosphere Security of Peter the Great St. Petersburg Polytechnic University (hereinafter – the HSTS) processes personal data of students and employees, academic performance, various types of achievements of students and masters, data on salaries of employees, scientific works (containing valuable information and currently not actually made public), vacation timetables of employees, program licenses, orders of higher school management, as well as other official documents in limited access.

According to staff structure of HSTS [6] the position of the specialist in the field of information security is not provided, therefore, consideration of the questions deals with ensuring information security is implemented by forces of another staff members.

Thus, the relevance of this work is due to the need to protect the information processed in the structural unit of the University. Therefore, the purpose of this work is to study the security of information processed by the

information system of the structural unit of the St. Petersburg Polytechnic University of Peter the Great (on the example of the HSTS).

Based on the scientific works of foreign experts in the field of information protection [7-9] it is fair to establish that the goal can be achieved by performing the following tasks:

1. Determining the place of information security in the national security system of the Russian Federation;
2. Analysis and classification of information processed in HSTS;
3. Building a model of a potential information security violator;
4. Evaluation of the possible expense of safety;
5. Analysis of information systems of the structural unit of the University, the definition of possible vulnerabilities;
6. Elaboration of a recommendation on the protection of information;
7. Evaluation of the effectiveness of the developed recommendations.

2 Methods

Information security in information systems is an area of scientific knowledge that studies the vulnerabilities of information systems and ways to influence information, developing appropriate methods of protection against internal and external threats in any conditions of its processing and storage. This science based on scientific achievements and practical developments in the field of computer network security, database security, software and hardware information security tools, etc.

In connection with this, various methods of scientific knowledge from other fields of science are widely used in research activities aimed at ensuring the comprehensive security of information processed in the information systems of the HSTS SPbSTU. [10] In this

* Corresponding author: elenaboltynkova0098@mail.ru

case, the main reference point for the choice of methods of scientific research should be its objectives. It is the tasks and questions posed to the work that determine the ways to solve them, and therefore the choice of appropriate methods.

Thus, the following methods of scientific research, built in a logical sequence: problem statement – the study of literature, documents and results of activity – analysis of the current state of information security – synthesis – modeling – idealization.

3 Results

An important step in the process of identifying potential threats to the security of information is the identification of persons and events as a result of actions that may violate the confidentiality, integrity or availability of information processed in the information system. Threats are divided into intentional (network attacks, malware distribution, internal intruder activity) and unintentional (denial of service, personnel error).

In any case, the implementation of the threat entails adverse consequences. For example, a failure in the fire-fighting system can lead to inaction of fire-fighting equipment and alert the fire brigade, therefore, to the death of people and destruction of material resources.

Another example is in Venezuela in 2019 was the most large-scale power outages due to cyber attacks. "The attack was aimed at the automatic control system of hydroelectric station "Guri". And one example is the massive spread of WannaCry malware in 2017. The Spread of the worm has blocked the work of many organizations around the world: hospitals, airports, banks, factories, etc.

Depending on the potential required to implement threats to the security of information, violators are divided into:

1. Low (basic potential);
2. Medium (basic increased potential);
3. High potential.

The ratio of violator types, their potential and possibilities of implementation of security threats are given in table 1.

Information security threat is relevant (U_jA) if there is a possibility of the threat by the violator, and its implementation will lead to a violation of the confidentiality, integrity or availability of information.

As an indicator of the relevance of information security threats a two-component vector is accepted, the first component is the probability of threat realization (A_j), and the second is the degree of damage in case of its realization (R_j):

$$U_jA = [A_j; R_j] \quad (1)$$

The probability of threat realization will be determined based on the analysis of statistical data on the frequency of information security threats in information system, and the degree of damage in case of its implementation is determined based on the assessment of the degree of consequences of security violations. In the absence of statistical data on the implementation of threats to the security of information in the information system is determined based on the assessment of the possibility of implementation threats to the security of information (D_j - the level of protection of in information system and the potential of the offender, required for the implementation of security threats):

$$U_jA = [D_j; R_j] \quad (2)$$

Under the probability of implementation of the threat of information security is understood to be defined by an expert indicator that characterizes how likely is the

Table 1. Dependence of potentials and possible threats.

Potential	Type of violator	Opportunities to implement information security threats
Low	External entities, persons providing the operation of information systems or serving the infrastructure of the operator, users of the information system, former employees, persons involved in the installation, adjustment, commissioning and other works.	Have the opportunity to get information about the vulnerabilities of the information system. Have the ability to independently create methods and means of implementing attacks and the implementation of attacks on the information system.
Medium	Competing organizations, developers, manufacturers, software, hardware and software vendors, information system administrators, and security administrators.	Have all the capabilities of offenders with basic capacity. Are aware of the information security measures used in the information system of this type. Have the opportunity to obtain information about the vulnerabilities of individual components of the information system by carrying out, using the available free access software, analysis of application software code and individual software components of system-wide software. Have access to information about the structural and functional characteristics and features of the information system.
High	Special services of foreign States.	Have all the capabilities of offenders with basic and high potentials. Have an opportunity to carry out unauthorized access from the allocated (departmental, corporate) communication networks to which physical access (unprotected by organizational measures) is possible).

Table 2. Calculating potential violator.

Indicator of the capabilities of the offender		Values for vulnerability identification	Values when using the vulnerability
The time	< 0,5 hour	0	0
	< 1 day	2	3
	< 1 month	3	5
	> 1 month	5	8
Technical competence of the infringer	Non-professional	0	0
	Specialist	2	3
	Professional	5	4
Knowledge of the project and information system	Lack of knowledge	0	0
	Limited knowledge	2	2
	Knowledge of sensitive information	5	4
Ability to access the information system	< 0,5 hour or undetectable access	0	0
	< 1 day	2	4
	< 1 month	3	6
	> 1 month	4	9
	Impossible	0	0
The sophistication of the violator	Not present	0	0
	Standard equipment	1	2
	Specialized equipment	3	4
	Equipment made to order	5	6

implementation of the j -th threat to the security of information in the information system.

The ability to implement the j -th information security threat (D_j) is evaluated based on the level of security of the information system (D_s) and the potential of the offender (D_h) necessary to implement this threat to the security of information in the information system:

$$D_j = [D_s; D_h] \quad (3)$$

For the purpose of calculation of potential of the violator numerical values of the specified indicators according to table 2.6 are defined. Obtained on the basis of table 2.6 values of the characteristics of the potential of the offender are summarized. The resulting sum of the characteristic values corresponds to the ranges of values given in table 2.7, according to which the potential of the violator necessary to implement the threat to the security of information is determined.

Table 3. Quantitative assessment of the offender's potential.

Range of values	The potential intruder
<10	Potential is insufficient to implement a security threat
10-17	Basic (low)
18-24	Basic elevated (medium)
>24	High

At the next stage, it is necessary to build an improved mathematical model of threats based on the formalization of the actions of the offender.

Let N be the number of computers that are vulnerable to attack, and $\langle N_0 \rangle$ be the average number of computers

attacked in a given unit of time. Let $a(t)$ be the proportion of vulnerable machines that were successfully attacked in time t , then $N \cdot a(t)$ is the total number of successfully attacked computers each of which will potentially be used to carry out subsequent attacks with an average number of $\langle N_0 \rangle$.

Since some computers have already been successfully attacked (their share is $a(t)$), each new captured computer will produce no more than $\langle N_0 \rangle (1 - a(t))$ new successful attacks. Thus, the number of captured computers for the period of time dt is equal to:

$$n = aN \cdot (1 - a)dt \quad (4)$$

$$Nda = aN \cdot (1 - a)dt \quad (5)$$

$$da/dt = \langle N_0 \rangle a(1 - a) \quad (6)$$

The solution of formula 6 leads to the following form:

$$a = \frac{e^{\langle N_0 \rangle (t-T)}}{1 - e^{\langle N_0 \rangle (t-T)}} \quad (7)$$

where T is the time parameter characterizing the greatest growth of attacks.

Note that each object can send, receive and process data over the network - network traffic. Network traffic can be divided into service and application traffic. The traffic in the network can be described in a private form using the matrix $TQ \times Q$, where $Q = P + 1$ [9].

Taking into account the load matrix, the consideration of the basic model can be generalized for Autonomous systems as follows. Let's introduce P_j - probability that the captured computer in a subnet will

attack computers in the same subnet, then $1 - P_j$ – probability that the attacked computer will be out of this subnet.

At the time of the experimental test, we fix the matrix $TQ \times Q$ and the values of the function modeling the load in one of the subnets, according to [11] $tf_{j,k}(t)$, $t=t_0$. Then P_j can be represented as a simpler relation:

$$P_j = \frac{\sum_{q=1, k=j}^Q tf_{q,k} t_0 + \sum_{q=j, k=1}^Q tf_{q,k} t_0}{\sum_{q,k} tf_{q,k} t_0} \quad (8)$$

In this case, the system of equations can be written as:

$$\begin{aligned} \frac{da_i}{dt} = & \left[a_0 K \left(\frac{\sum_{q=1, k=j}^Q tf_{q,k} t_0 + \sum_{q=j, k=1}^Q tf_{q,k} t_0}{\sum_{q,k} tf_{q,k} t_0} \right) + \right. \\ & \left. + \frac{\sum_{q=j, k=j}^Q tf_{q,k} t_0}{\sum_{q,k} tf_{q,k} t_0} \right] (1 - a_i) \end{aligned} \quad (9)$$

$1 \leq i \leq Q$

The choice of strategy of formalization of actions of the malefactor defines a type of the received quantitative characteristic of its opportunities.

4 Conclusion

Various structures of the University process both public and confidential information. In the Universities, information is processed with the status "Confidential". Is processing this information require a separate enhanced protection. The most dangerous for IP are internal violators of is, because they have access to the resources of information resources, they have access to information that represents commercial, personal and professional secrets. Also it is impossible to exclude from external violators if information system is connected to information and telecommunication networks. [12]

For the correctness of the degree of threats, an improvement of the mathematical model used in the work to assess the security of information in the information system was carried out. The improvement consists in the representation of interacting subnets as a system of equations forming a complete group of events.

On the basis of the constructed models it is possible to organize a secure LAN within the structural unit of the University, as well as possible to further develop software and use other means of information security in order to ensure the security of information processed in the is of the HSTS on the example [13-18].

References

1. Maltsev D.N., Henson E.M., Repetsky D.S. 2019 Electronic textbooks for applied baccalaureate Higher education in Russia № 4, p. 134-141

2. Deryabina S.A. and Dyakova T.A. 2019 Professiogram of a foreign language teacher in the digitalization of the educational space Higher education in Russia №4, p. 142-149
3. Khurum Nazir Junejo, David Yau 2016 Data Driven Physical Modeling for Intrusion Detection in Cyber Physical Systems Cryptology and Information Security Series, p.43
4. Hieu N. Tran, Robert H. Deng, HweeHwa Pang 2016 Privacy-Preserving and Verifiable Data Aggregation Cryptology and Information Security Series, p.115
5. Razinkina, E., Pankova, L., Trostinskaya, I., Pozdeeva, E., Evseeva, L., Tanova, A. Student satisfaction as an element of education quality monitoring in innovative higher education institution (2018) E3S Web of Conferences, 33, paper № 03043
6. Personalities. High School Technosphere Safety. [Electronic resource] - URL: <https://hsts.spbstu.ru/person/?paging=1> (access date: 03/31/2019)
7. Rudskoy, A.I., Borovkov, A.I., Romanov, P.I. Russian experience in engineering education development (2018) Vysshee Obrazovanie v Rossii, 27 (1), pp. 151-162
8. Mohd Aizuddin Zainal Abidin, Anuar Nawawi, Ahmad Saiful Azlin Puteh Salin Customer data security and theft: a Malaysian organization's experience Information and Computer Security, vol. 27, iss. 1.
9. Carl Young Information Security Science 1st Edition
10. Harrison Stewart, Jan Jurjens Information security management and the human aspect in organizations Information and Computer Security, vol. 25, iss. 5
11. Sychev V.M. Formalization of the model of the internal violator of information security
12. Vasiliev, Y.S., Zegzhda, P.D., Kuvshinov, V.I. Modern problems of cybersecurity (2014) Nonlinear Phenomena in Complex Systems, 17 (3), pp. 210-214
13. Boltenkova E.A. Software to protect computer files from unauthorized access OS Windows Pr. Computer 2018664472 RU No. 2018661775 appl. 10.26.2018; publ. 11/16/2018
14. Skripnuk, D., Kikkas, K., Romashkina, E., E3S Web of Conferences, (2019)
15. Voskresenskaya, E., Vorona-Slivinskaya, L., Mokhorov, D., Tebryaev, A., E3S Web of Conferences, (2019)
16. Sokolova, O.A., Alloyarov, K.V., Baranova, T.A.,) IOP Conference Series: Earth and Environmental Science, (2019)
17. Kulik, S.V., Travkina, E.V., Fedorov, A.S., Rubtsova, A.V., IOP Conference Series: Earth and Environmental Science, (2019)
18. Alloyarova, Y., Alloyarov, K., Kuranova, L., Karpovich, I., IOP Conference Series: Earth and Environmental Science, (2019)