ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 5, Issue 6 , June 2018

Investigation of Models of the Infringer and Evaluation of Damage of Confidential Information

M.M.Karimov, S.M.Sagatova, N.F.Akhmedova, B.Sh.Yashnarov

Doctor of technical sciences. Professor in Tashkent State Technical University, Tashkent, Uzbekistan
Student in Tashkent State Technical University, Tashkent, Uzbekistan
Student of Faculty «Computer engineering» Tashkent University of Information Technologies, Uzbekistan
Teacher in the Qibray College of Finance and Economics, Qibray district, Tashkent region, Uzbekistan

ABSTRACT: The article considersthe models of the violator and the assessment of the damage to confidential information, which allows determining the likely violators for the organization and developing recommendations for the protection of information. A model of threats for conducting confidential negotiations is proposed, which allows solving problems of technical protection of information systematically.

KEYWORDS: Confidential information, Model of threats, Infringer of the security, Information systems, Attacker

I.INTRODUCTION

Information processing systems are becoming popular and used universally. Information systems are designed to ensure the operability of the information infrastructure of the organization, the provision of various types of information services, the automation of financial and production activities, as well as the business processes of the organization. They allow reducing both temporary, financial and labor costs. In the information system, significant amounts of information of varying degrees of secrecy are stored and processed, so the issue of the security of this information system from various threats to information security is acute. The definition of security threats relevant to a particular information system makes it possible to develop and create an information security system. The system for protecting confidential information is effective if it neutralizes the current threats to its security.

The model of a likely infringer of the security of information systems is necessary to systematize information on the types and capabilities of the subjects, the purposes of unauthorized influences and the development of adequate organizational and technical countermeasures.

II. METHODOLOGY

When developing a model of the infringer of information systems, the following are taken into account:

- assumptions about the categories of persons to whom the offender may belong;
- the type of intruder;
- assumptions about the motives of the offender's actions;
- assumptions about the qualification of the offender and his technical equipment (about methods and means used to commit the violation);
- limitations and assumptions about the nature of possible actions of violators;

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 5, Issue 6 , June 2018

- the nature of information threats.

Due to the right of permanent or one-time access, violators are divided into two types: violators who do not have access to information systems that implement threats from external public communication networks and (or) international information exchange networks; violators who have access to information systems, including users who implement threats directly into information systems, internal violators. Table 1.1 gives the types of violators and the categories of persons related to them.

Table 1.1.

Types of intruders and categories of persons

Type of intruder	**Categoriesofpersons**
External (N)	- State Intelligence Services; criminal structures; - Representatives of competing organizations (or persons acting on their instructions); - unscrupulous partners; - clients (representatives of organizations, citizens); - visitors (invited for any reason); - representatives of organizations interacting on the issues of ensuring the life of the organization (energy, water, heat, etc.); - persons who accidentally or intentionally violated the access regime; - any person outside the controlled territory.
Internal (M)	- IS users; - IP administrators; - personnel serving technical facilities; - employees of departments; - technical personnel serving buildings (cleaners, electricians, plumbers and other employees who have access to buildings and premises); - security officers; leaders of various levels of the job hierarchy.

External offender has the following options:

- to carry out unauthorized access to communication channels that go beyond office premises;
- to carry out unauthorized access through automated workplaces connected to public communication networks and (or) networks of international information exchange;
- to carry out unauthorized access to information using special software effects through software viruses, malicious programs, algorithmic or program bookmarks;
- to carry out unauthorized access through the elements of the information infrastructure of information systems, which in the process of their life cycle (modernization, maintenance, repair, utilization) are outside the control zone;
- to carry out unauthorized access through the information system of interacting departments, organizations and institutions when they are connected to information systems.

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 5, Issue 6 , June 2018

In organizations, in order to reduce the likelihood of unauthorized access both to the territory of the enterprise and to separate units, the method of creating protection lines is used[1,2]. The organization's territory is divided into several zones, ranked by the degree of secrecy and accessibility for employees or visitors. As a result, there is an opportunity to differentiate access to important information resources of the enterprise, which ensures the protection of information. An example of the organization of protection boundaries is shown in Fig.1.1.

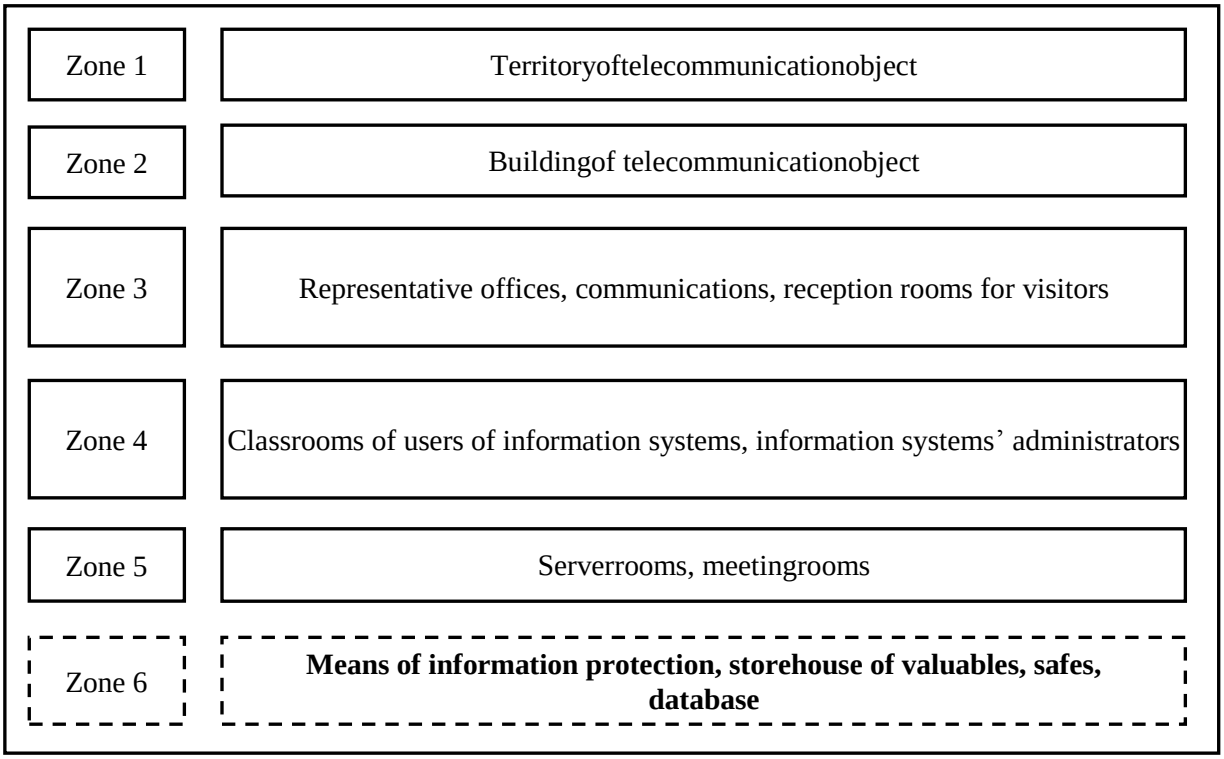

Fig.1.1. Organization of boundaries (zones) of protection

After the knowledge of the alleged infringers for the information system for processing confidential information was systematized, a model of threats to information security is being developed. When constructing a model of threats to the security of confidential information, the frequency (probability) of the implementation of threats is determined. Under the frequency (probability) of implementation is understood as an expertly determined indicator characterizing the probability of realizing a specific threat to information security for a given information system in the emerging conditions. Defining the frequency (probability) of the implementation of threats, it is necessary to take into account the possibilities of violators.

The concept of a mathematical model for assessing the damage to confidential information from external threats. Information on the resource that is consumed without a balance cannot be directly attributed. Therefore, it is impossible to determine the value of information when considering the model of its use only at the information level. To establish the price of information, it is necessary to establish a link between its content and the resource that is spent without remainder [3]. For this, it is necessary to relate the content of information to values of a higher level for which the conservation laws are satisfied or there aremore simplebalance ratios.

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 5, Issue 6 , June 2018

As such a value, it is advisable to take the value of the potential of information, which is a generalized quantitative characteristic of the power of information achieved by means that are consumed without a remainder. Since the content of power is complex and multidimensional, the potential is the simplest scalar approximation, the accuracy of which is sufficient for a comparative evaluation of the effectiveness (importance, value) of providing "things", which includes information.

Since the price of information obtained in this way will not be absolute, but comparative, i.e. which is valid only under certain conditions, then in addition to the property of partial adequacy, the visibility property of the obtained estimate is important. In this regard, a clear assessment of the value of information can be obtained by using a simpler model of potential - the disclosed potential, which depends on the effectiveness of information protection. It is equal to the product of the value of the total potential of information taken before the start of the simulation – U_{common} , the probability of unauthorized access to confidential information, determined by the mathematical model of the operation of the system – $P_{unautorit\ hedaccess}$

$$U_p = U_{common} \cdot P_{unautorit\ hedaccess} \quad (1.1)$$

Under the general potential of information U_{common} we shall mean that positive effect (material or moral) that can be obtained by using it on the specified time interval. At the same time, the formal basis of the rivals' relationship with unauthorized access to information and its protection is the maximum task:

$$max_r max_z U_p(r, z|S) \quad (1.2)$$

where, U_p is the value of the open potential; r, z-strategies for unauthorized access to confidential information and information protection, respectively, implemented in the conditions of the system S.

Analysis of external parameters of the model for assessing the damage to confidential information from external threats. The damage assessment model is not closed. As is known, to fully reflect reality, the model must take into account many external parameters, that is, data from the environment of the model's functioning [4]. However, in practice, it is impossible or difficult to take into account all the possible parameters that influence the outcome of the simulation to some extent or so complicated that the modeling itself becomes an unprofitable task.

One of the main external factors can be identified qualifications of the attacker: the higher it is the greater the chance of unauthorized access. Under identical other conditions, the probability of unauthorized access will be greater for that attacker who has higher qualifications. Since this value does not have a well-defined unit of measurement and, moreover, is an abstract characteristic, then, in the case under consideration, we will limit the qualification of the attacker to a number in the range from 0 to 1, with 0 indicating the professional illiteracy of the attacker, and 1 about him full professionalism.

Another no less important parameter is the time spent by an intruder over the implementation of an unauthorized access attempt. The more time, the greater the chance that the attempt will end in success, but the greater the chance that the attacker will be caught red-handed. In practice, for this quantity, Markov processes with discrete states and continuous time will be used in this model, which, as is well known, are in most cases characterized by two intensity parameters λ_i and μ_i, where the parameter λ_i characterizes the intensity of direct transitions between the components S_i, and the parameter μ_i of reverse transitions (Fig.1.2).

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 5, Issue 6 , June 2018

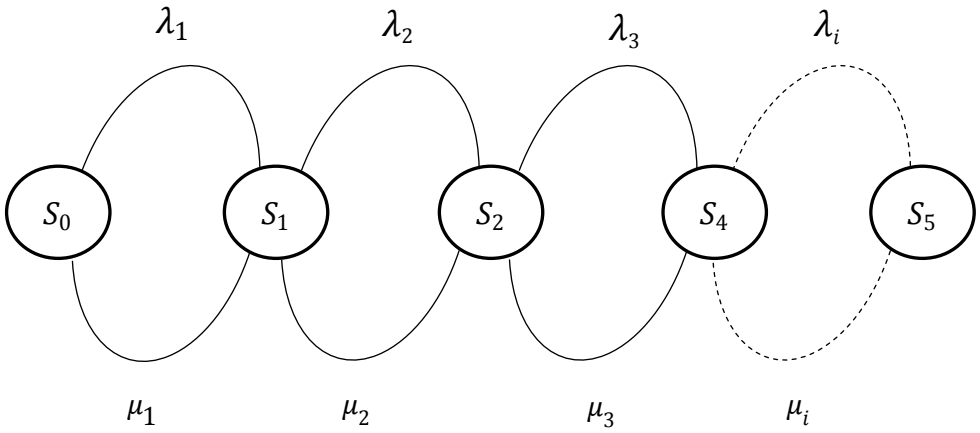

Fig.1.2. Example of the graph of the Markov process

In addition, it is also necessary to consider the number of intruders. The more their number, the more likely the case of unauthorized access to the protection object. When there is an assessment of damage while simultaneously unauthorized access of several intruders. In our case, this fact will be taken into account when using the maximin problem, when among the possible damages the maximum applied by the most qualified attacker will be selected.

It should also be noted that any confidential information also has a physical component, which characterizes the protection of confidential information from the physical side. For example, if the information is on the network, the technical equipment of the attacker plays an important role in unauthorized access to confidential information. The higher it is, the more imperceptible, lighter and better it can realize the threat. In the mathematical model, for each of its components it will be necessary to determine the so-called energy probability of detecting confidential information, depending on the technical equipment of the attacker. In addition to the parameters associated with the actions of intruders, the model also uses parameters related to different probability distribution laws. The values of these parameters are determined using statistical methods. The constraints imposed on these parameters are related to the distribution laws themselves.

The probability of successful implementation of the attack. The calculation of the probability of response of certain users of the network to the social and engineering attacking influences of the attacker makes it possible to judge the security of this "node" of the system, that is, the user, but not the security of the system as a whole. To calculate the total probability of security of the information system from the social-engineering attacks of the attacker several heuristics can be used.

The process of assessing the security of the allocated premises from technical channels of information leakage. To assess the security of the premises, the confidential information contained in the technical information leakage channels (TILC) the modelof threats is created, and then, based on it, the most dangerous TILC is selected. After a special study of the selected room is carried out for the chosen TILC, at the output of which the signal-to-noise ratios at the selected control points and some other information are obtained. This data is entered into the

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 5, Issue 6 , June 2018

program, which not only calculates the security of the premises, but also gives practical advice on how to eliminate the detected inconsistencies.

The threat model and the choice of the most dangerous technical channel for information leakage. The expert, according to the results of constructing the threat model, fills out a special table, so filling it is purely subjective assessment of the expert of certain parameters of the security of the premises under examination. The basis of the threat model is the basic model of threats to the security of personal data when processing them in information systems [5]. As the main leakage channels, we will take the side electromagnetic emissions and interference, acoustic and species threats corresponding to its channels of leakage. Thus, the table of the threat model will look like it is shown in Table 1.2.

Table 1.2.

General view of the model of threats to confidential information

Threat	Topicality of threat	Coefficient of the feasibility of threat
Threats of leakage through acoustic (vibroacoustic) channel		
Interception with the use of equipment recording acoustic waves	Not relevant /relevant	[0;1]
Interception with the use of equipment that detects vibroacoustic waves	Not relevant /relevant	[0;1]
Interception with the use of equipment that registers electromagnetic radiation and electrical signals	Not relevant /relevant	[0;1]
Interception with the use of special electronic devices for the removal of voice information connected to communication channels	Not relevant /relevant	[0;1]
Interception with the use of special electronic devices for the removal of voice information embedded in the premises.	Not relevant /relevant	[0;1]
Interception with the use of special electronic devices for the removal of voice information connected to communication channels	Not relevant /relevant	[0;1]
Leakage by means of interception of paging messages and cellular communication	Not relevant /relevant	[0;1]

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 5, Issue 6 , June 2018

Threats of leakage through the species channel		
Interception at the expense of viewing confidential information by means of optical means from displays and other means of computer facilities	Not relevant /relevant	[0;1]
Viewing confidential information using special electronic pick-up devices that are embedded in office space.	Not relevant /relevant	[0;1]
Viewing confidential information using special electronic pickup devices secretly used by individuals when they visit office space.	Not relevant /relevant	[0;1]
Threats of leakage through the channel of spurious electromagnetic emissions and pickups(SEEAP)		
Due to spurious electromagnetic emissions	Not relevant /relevant	[0;1]
Due to interference over power circuits	Not relevant /relevant	[0;1]
Due to radio waves modulated by the information signal	Not relevant /relevant	[0;1]
With the help of means of removal of induced informative signals from power supply circuits	Not relevant /relevant	[0;1]

Any threat can be either irrelevant or urgent. The criterion of the urgency of the threat is the possibility of realizing this threat in specific confidential information, as well as its danger for confidential information. As a factor of feasibility of the threat, an indicator determined by an expert way is taken, which characterizes the probability of realizing a specific threat to the security of confidential information in the current situation. The coefficient of feasibility of each threat is expressed by the expert numerically in the interval from zero to one - zero is assigned if the expert considers the implementation of this threat impossible, unit in case the expert considers the probability of realizing this threat as guaranteed. If not relevant, the threat is discarded, the coefficient of feasibility is not considered.

In order to increase the level of objectivity of the special study, it is proposed to involve several experts to determine the threat model - each expert makes a separate model, putting, according to his experience, the coefficients of feasibility of threats, and further, using the mathematical method of Saaty's weighted expert assessments, which

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 5, Issue 6 , June 2018

allows determining the best alternative of possible, the final model of threats is made. The use of the Saati method begins with the construction of a hierarchical structure of the problem under consideration. It, in general, should consist of three levels - goal, criteria and alternatives. The choice of the alternative is directly affected by the relative weight of each criterion, determined at the stage of model building.

The next stage of the research is the construction of the hierarchical structure specifically of our problem - in this case, the goal will be to identify the most dangerous TILC in the views of the individual expert, the threats will be the criteria, and the coefficient of feasibility that the expert appropriated to a certain threat -is the weight of the criterion[6].Finally, all the criteria are divided into three groups according to their TILC, and the hierarchical model of the problem acquires the form shown in Fig. 1.4.

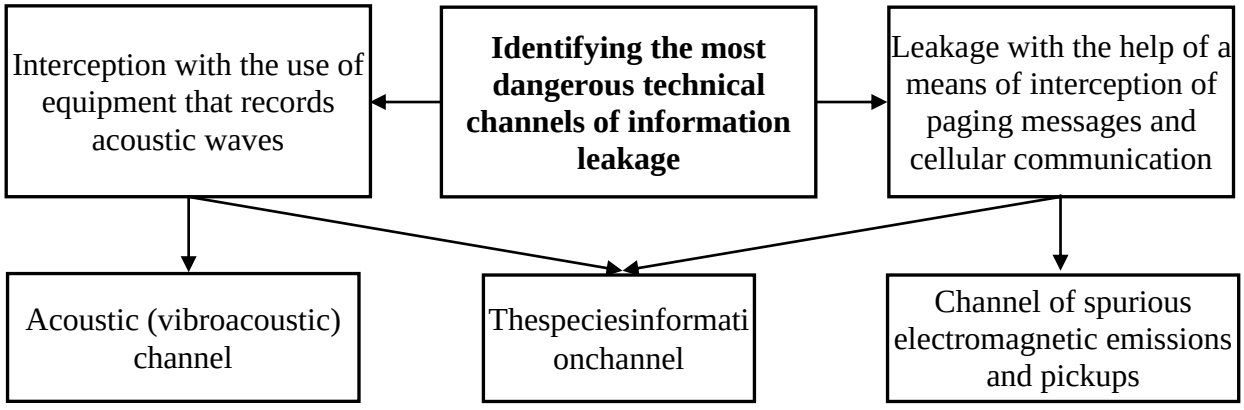

Fig.1.4. Hierarchical structure of the problem of identifying the most dangerous technical information leakage channels

Model of threats to conduct confidential talks. The subsystem of technical protection of information is the most important component of the information protection system of information objects in the enterprise. Along with this, the actualization of the subsystem of technical protection of information in accordance with the real operating conditions of the protection object is possible only based on the development of a model of threats to the information security of the subsystem [7]. Existing known models do not clearly formulate an idea of the composition and content of the model of threats to information security in the enterprise, which determines the need for its development.

The model of threats to information security is defined as a physical, mathematical, descriptive representation of the properties or characteristics of threats to information security. At the same time, the factor is a phenomenon, an action or a process, the result of which can be leakage, distortion, destruction of the protected information, blocking access to it.

Figure 1.5 shows a model of threats intended for conducting confidential negotiations.

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 5, Issue 6 , June 2018

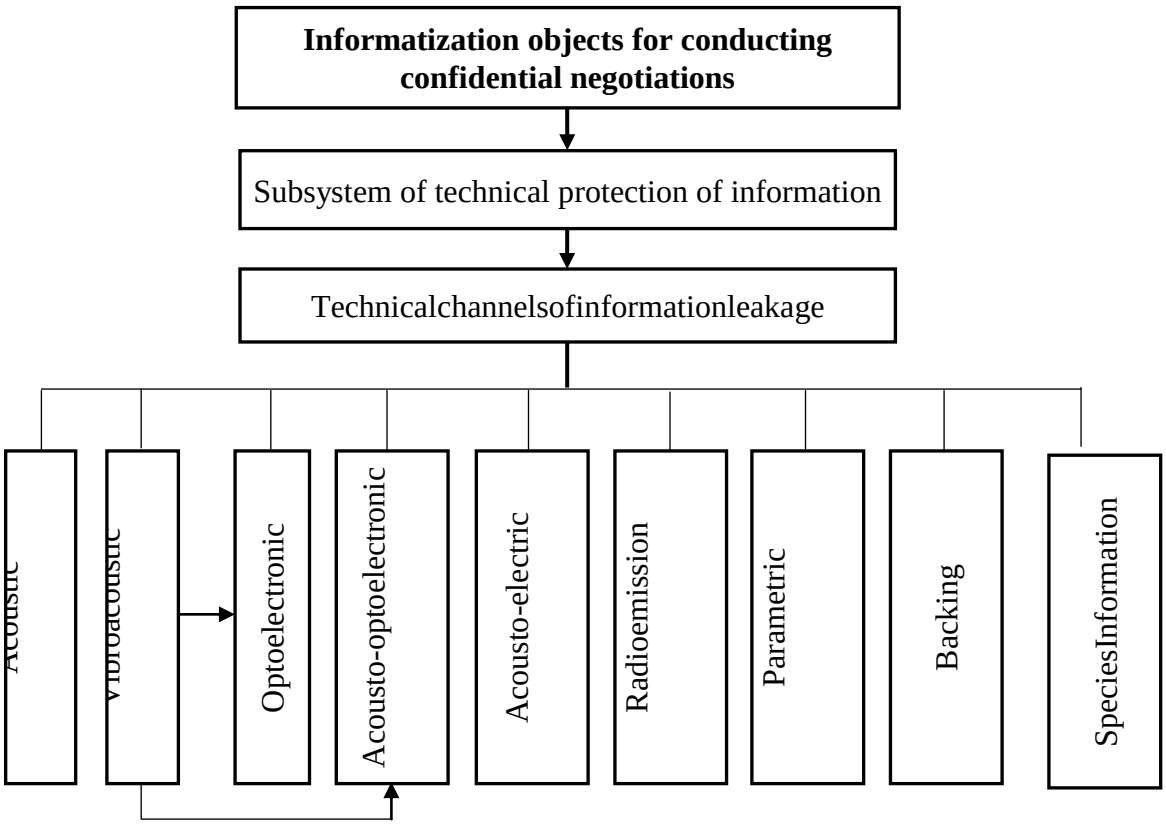

Fig.1.5. Model of the subsystem of technical protection of information intended for conducting confidential negotiations

III. CONCLUSIONS

The proposed threat model for conducting confidential negotiations allows you to select exactly the technical leakage channel that is most vulnerable to intruders, allowing the organization to save on installation and maintenance of irrelevant security measures, and thereby optimize the firm's costs of protecting its confidential information.

REFERENCES

1. Accorsi R. and Wonnemann C. (2011a) "InDico: Information flow analysis of business processes for confidentiality requirements" in 6th International Workshop, Security and Trust Management in Athens, Greece 2010. Springer Berlin Heidelberg, pp. 194-209.
2. XinmingOu, SudhakarGovindavajhala, Andrew W. Appel. MulVAL: A logic-based network security analyzer // InProceedings of the 14th USENIX Security Symposium, Princeton University. 2005. – P.113-128.
3. William Stallings. Network security essentials: Applications and Standards Fourth edition. Prentice Hall, USA, 2011. – P.417.
4. Tanya Aplin, Lionel Bently, Phillip Johnson, Simon Malynicz. Gurry on Breach of Confidence: The Protection of Confidential Information 2nd Edition. Oxford University Press, 2012, pp.976.
5. Albrechsten E, Hovden J (2010). Improving information security awareness and behavior through dialogue, participation, and collective reflection. An intervention study. J. Comput. Secur, 29(4): pp. 432-445.
6. Kotenko and E. Doynikova, "Security assessment of computer networks based on attack graphs and security events," Bali, Indonesia, LNCS, vol. 8047. Springer-Verlag, April 2014, pp. 462–471.
7. WilkoHenecka, Stefan Kogl, Ahmad-Reza Sadeghi, Thomas Schneider, and ImmoWehrenberg. TASTY: Tool for Automating Secure Two-Party Computations. In ACM Conference on Computer and Communications Security (CCS), 2010.

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 5, Issue 6 , June 2018

AUTHOR'S BIOGRAPHY

KarimovMadjitMalikovich

Doctor of technical sciences. Professor in Tashkent State Technical University named after Islam Karimov. Author of 5 monographs, 7 textbooks, 10 patents and more than 200 scientific articles.

SagatovaSitoraMirazizovna

Bachelor degree student in Tashkent State Technical University named after Islam Karimov. Author of more than 9 scientific articles.

AkhmedovaNozimaFarkhodqizi

Master Degree student of Faculty «Computer engineering» Tashkent University of Information Technologies. Author of more than 8 scientific articles.

YashnarobBekhzodSheralievich

Teacher in the Qibray College of Finance and Economics, Kibray district, Tashkent region. Author of more than 4 published scientific articles.