International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Development of Specialized Method for Increasing the Level of Security on Information and Communication Systems

Saparova Gaukhar, Gulomov Sherzod

Abstract: Abstract: ***This article proposes a method for increasing the level of security of a corporate network by its structure that meets the specified security requirements and distinguishes them from well-known attack type invariant structural units of the network - security domains. Hierarchy of security levels in the form of rings is represented allow more effectively protect a network that requires more security. The method allows to get output data only when the initial data allows to do this. In other words, if it is possible to improve the security level of a given network structure, then the method does this. A graph of the dependence of the security level on the ratio of the number of domains to the maximum number of objects in the domains is developed. A weighted domain allocation algorithm, which will increase the overall security on information and communication systems is proposed. For increasing the overall level of security, the splitting of the network into a larger number of security domains with as few services as possible is given. In accordance the weight of properties with modern data from the theory of information security vulnerability of a particular service is selected.***

Index Terms:violation of the security, overlap, allocation,consolidation, vulnerability, domains, border protection, communication lines.

I. INTRODUCTION

The rapid growth in the popularity of Internet technologies is accompanied by an increase in serious threats of the disclosure of personal data, critical corporate resources, state secrets, etc. Every day, hackers and other attackers endanger information and communication systems, trying to gain access to them with the help of special attacks. These attacks are becoming more sophisticated in impact and uncomplicated in execution. Two main factors contribute to this.

The first is the widespread penetration of the Internet. Today, millions of computers are connected to this network. Many millions of computers will be connected to the Internet in the near future, so the likelihood of hackers accessing vulnerable computers and information and communication systems is constantly increasing.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
Saparova Gaukhar*, Information Security Department, Tashkent University of Information Technologies of Nukus branch named after Muhammad al-Khwarizmi, Nukus, Uzbekistan
Gulomov Sherzod, Providing Information Security Department, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan

In addition, the widespread use of the Internet allows hackers to share information globally. Secondly, this is the universal distribution of easy-to-use operating systems and development environments. This factor sharply reduces the requirements for the level of knowledge of the attacker.

Previously, a hacker needed good programming knowledge and skills to create and spread malware.

The problems of ensuring information security in information and communication systems are caused by security threats for local workstations, local networks and because of attacks on corporate networks that have access to public data transmission sections.

II. METHOD FOR INCREASING THE SECURITY LEVEL OF COMPUTER NETWORK BY ITS STRUCTURE

Each computer network requiring protection will be called a security object. Security levels are defined as a hierarchical attribute that can be associated with a security object to indicate its sensitivity in the sense of security. This degree of sensitivity may indicate, for example, the degree of damage from a violation of the security of a given object [1-2]. When such hierarchical relationships exist in the network, a certain mechanism is required that marks the main contents of the network so that its sensitivity in terms of security is known. One way to achieve this is to associate every component of a computer network with a level of security.

The term security domain is defined as a collection of security objects located in the same network and satisfying the same level of security through some common element. This definition is given in the most general form and additionally includes the concepts of “subject of security” and “security administrator”. Here it is narrower and more specific.

The security domain cannot always be clearly defined. In most cases, there are several security domains on the network, and most often they overlap. The ideal case is when security domains do not cross anywhere. This is the purpose of the method of increasing the security of the corporate network described in this paper.

The boundaries of security domains are difficult to determine in some cases. This is especially true when considering client-server applications. Here, the client and server are distant from each other and their joint work on the network should be well thought out in terms of security.

The outer ring corresponds to the lowest level of security, the inner to the highest.

To move an object from the outer ring to the inner ring, appropriate protective equipment must be used.

As an example that clearly shows which security objects can be included in one security domain, we can consider network interaction based on the trust relationship of objects. The NFS client expects the NFS server to respond appropriately to a file request. It is unacceptable that the client does not receive the expected response due to errors in the security system. Therefore, it is obvious that both the server and the client must belong to the same security domain. Similar trust relationships arise during the operation of the *X* Windows system.

Another example of the use of security domains can be determined based on traffic between computers on the network [3]. If a system that requires a higher level of security is connected to a public access network (external access), then the direct danger of an invasion of this system is obvious.

A more formally proposed concept can be represented in the form of rings is shown in Figure 1.

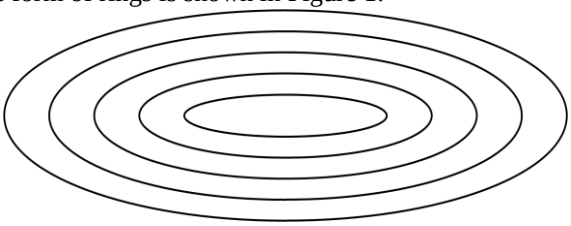


Figure 1- Hierarchy of security levels in the form of rings

Thus, the placement of equipment requiring public access on one network, and equipment requiring increased security in another network [5], allows it to more effectively protect a network that requires more security.

The method consists in isolating and subsequently combining security domains.

It is represented the network in the form of a graph $G(U,V)$, where U - many vertices of the graph, V - set of edges of the graph. In our case $U = \sum_{i=1}^{n} u_i$ – network objects, V - many communication lines connecting them.

III. SECURITY DOMAIN ALLOCATION

Providing security domains is a complex task. The first step is to complete the tasks, namely:

1. identify network objects u_i, requiring protection (computers, servers, routers);

2. specify the level of values t_i ($i = 1,...,n$) each object u_i throughout the network structure; this will help to further assess the level of security of a particular object;

3. determine the type of attacks that can take place for each object;

4. Based on the previous paragraph, determine the types of vulnerabilities w_k ($k = 1,...,s$, $s \in N$) each object u_i, which may arise or cause the implementation of the attacks defined above (the degree of damage from the implementation of the attack will be determined by the type of vulnerability);

5. determine probability $P(w_k)$ ($k = 1,...,s$, $s \in N$) the most common types of vulnerabilities;

6. comparing vulnerabilities and their likelihood $P(w_k)$ ($k = 1,...,s$, $s \in N$), and also, taking into account the degree of value, we can calculate the losses from a particular attack.

Thus, having completed the above tasks, we can conclude that certain security objects belong to specific security levels. We get many $S(u_i)$ – object security level u_i, $i = 1,...,n$.

Further, objects with the same level of security are combined into one network - security domains are obtained. That is, the graph is divided into subgraphs $G_1,...,G_q$ so that

$$S(u_i) = S(u_j) \ \forall i, j = 1,...,m(G_I),$$ where

$m(G_I)$ – number of subgraph security objects G_I, $I = 1,...,q$.

It may happen that two (or more) objects need a different level of security, but they are in the same domain. This cannot be allowed.

Most organizations combine a set of services on one computer system because of the low cost of this approach. The main security rule in this case suggests that combining services with different levels of security in one place is strictly prohibited [6]. In this case, in order to avoid big problems in the future, it will be cheaper to buy two servers and sort all the required set of services into them. But the best option would be to carefully place the services on separate computer systems, placing services with the same level of security on the same system.

IV. SECURITY DOMAIN CONSOLIDATION

As a result of the domain allocation operation, a certain set of security domains is obtained (graphs G_I, $I = 1,...,q$). Then they are combined into one network (graph G_p), but between security domains, means of protecting domain boundaries are included - objects d_f, $f = 1,...,r$, $r \in N$. Insert Objects d_f should occur without violating the initial network structure, that is, if the object u_i was associated with the object u_j in the graph G, then they should also be logically connected in the new column G_{p1} although an object can be physically inserted between them d_f ($f \in N$).In figures 2 and 3,

you can see the connection between the objects. u_i and u_j before (Figure 2) and after (Figure 3) the insertion of an object d_f .

Figure 2- Connections between objects u_i and u_j before inserting an object d_f

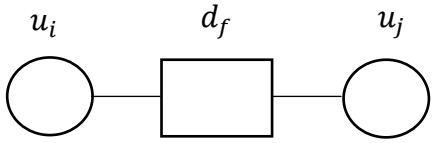


Figure 3- Connections between objects u_i and u_j after inserting an object d_f

The interaction of the obtained domains must be clearly and strictly defined. This is achieved by using various types of gateways or firewalls or other software and hardware to protect domain boundaries. For example, e-mail can be an acceptable solution for domain interaction, and all other traffic should be prohibited.

All attempts to circumvent the protection of domain boundaries should be documented and investigated [7].

The combination of two or more security domains in one network or on one system or the incorrect allocation and combination of security domains leads to a decrease in the overall level of security of the entire network and, as a rule, to a decrease in the level of each of the basic security requirements: confidentiality, integrityandavailability.

Using the analogy with rings, it can see the incorrect association of security domains (Figure 4).

One more important rule should be noted when working with security domains: one requirement of security in favor of another cannot be neglected.

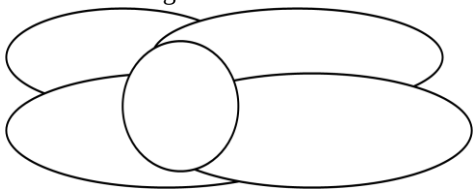


Figure 4 - Overlapping rings of security

V. EVALUATING THE PROPOSED METHOD

Currently, under the conditions of a clear planning of the enterprise's financial resources and the development of such a promising business line as e-commerce, the effectiveness of the method can be evaluated based on two points of view: economic efficiency and efficiency in terms of security.

Cost-effectiveness of the method. The proposed method is not ideal in the sense of the need for additional resources, so the logical question is how much will the total price of all (active and inactive) equipment increase compared to the original?

To answer the first question, it turns to the method itself presented above. Note that the method can be applied both to the existing network structure and to the projected one. Naturally, the second case is more preferable, since the use of the method will be cheaper.

The method allows it to get output data only when the initial data allows you to do this. In other words, if it is possible to improve the security level of a given network structure, then the method does this. And this in turn means the inclusion of at least three additional elements (one active and two passive): border protection d_f ($f \in N$) domain and its two communication lines.

Next, consider Figure 5. It shows the simplest network structure of the elements.

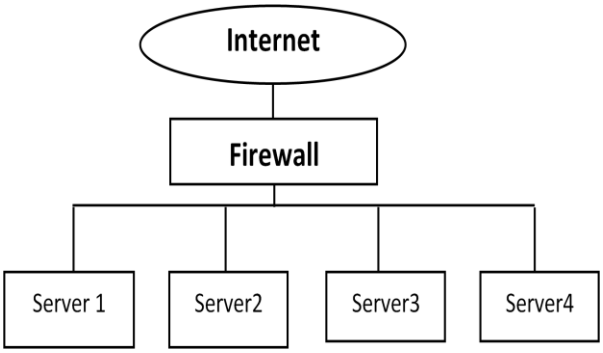


Figure 5 - An example of a corporate network segment used in assessing the economic efficiency of applying the method

It is easy to see that the minimum number of additional network elements (active and passive) that can be added according to the previous output is equal, and the maximum - $3*(n-1)$ (to be precise enough, then $3*n$, but then we get the most non-optimal case, when each security domain consists of one element of the network structure, this case will not be considered). Taking into account only the active part of the total number of additional elements, we obtain $n-1$.

Consider the cost of equipment. A modern corporate computing system costs at least once more than any network security tool. This applies only to the cost of the hardware. The cost of software can exceed the hardware by several tens of times. But this software needs to be configured, debugged, monitored, etc. This fact will not be taken into account due to the fact that network protection tools also need attention.

Thus, the cost of one network protection tool is 13-40 (50) times cheaper than the network object it protects. But the network protection tool in most cases does not protect objects, but a collection of objects in the form of security domains [8]. Consequently, the price of the remedy will be even lower compared to those whom it protects and can reach two orders of magnitude.

Assume that the price of each of the network objects shown in Figure 6 is equal to C . Then, taking into account the "most expensive" case,

we assume that each network protection tool will cost $C/10$, all of them $k \le n-1$. We get that the acquisition of all network protection means will cost $(n/k)*10$ times cheaper, but this value is always obtained ≥ 10.

All of the above applies to the case when the network does not contain data, which in turn is often much more expensive than the entire hardware and software M in time. Number M varies to a sufficiently large extent that, in the event of disappearance, cause permanent damage to an enterprise or corporation. Therefore, the application of the method, and, consequently, the acquisition and installation of network protection tools, pays off in a fairly short period of time, depending on the size of the enterprise and its turnover.

VI. THE EFFECTIVENESS OF THE METHOD IN TERMS OF SECURITY

The concept of the effectiveness of the method in terms of security implies that we must quantify the increase or decrease in the overall level of network security. The method of increasing the security of a corporate network by its structure is to isolate and subsequently combine security domains using the means of restricting access to the DDoS attacks [9]. Before the procedure for allocating security domains, based on the initial data, it should be determined how the network is divided into domains in its current state. Then, after highlighting the domains, compare the result with the initial breakdown into domains. Let us explain all this in more detail.

Denote by D_{beg} number of domains of the source network and through $\overline{T}_{beg}$ vector of property (service) vectors of each security domain of the source network. Similarly D_{end} and $\overline{T}_{end}$ - the number of domains and the vector of property (service) vectors of each domain of the resultant network, respectively.

If taken for $\|\overline{T}_{beg}\|$ the number of all properties in all vectors of the initial network and beyond $\|\overline{T}_{end}\|$ the number of all properties in all vectors of the finite network, and beyond $|\overline{T}_{beg}|$ the number of vectors of the initial network and beyond $\|\overline{T}_{beg}\|$ the number of vectors of a finite network, it is obvious that

$$\|\overline{T}_{beg}\| = \|\overline{T}_{end}\|, \quad |\overline{T}_{beg}| \ne |\overline{T}_{end}|.$$

In this case, the inequality

$$D_{beg} \le D_{end}$$

Let's consider two limiting options for network security: absolutely secure and absolutely unprotected packet [10].

In the first embodiment, the dimension of each vector $|\overline{T}_{end}\, j| = 1$, $\forall j \in [1, D_{end}]$. Or, in other words, in each security domain there is only one service.

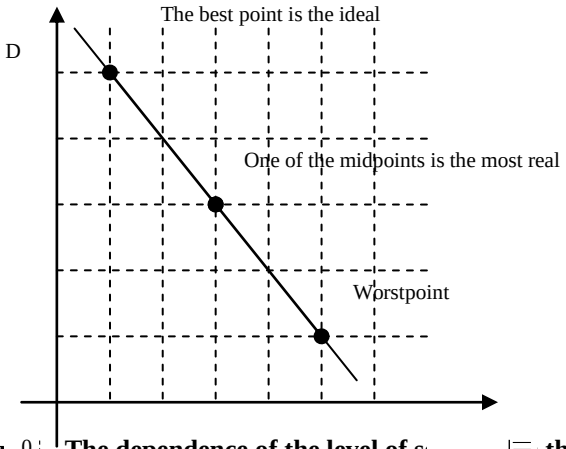
In the second option $D_{end} = 1$, that is, all services are in the same domain.

Any other case considered between these two is more secure (if we strive for an ideal case) with the following conditions:

$D_{beg} \to \max$ and $|\overline{T}_{beg}\, j| \to 1$, at the same time.

It's obvious that $\max(D_{beg}) = \|\overline{T}_{beg}\|$.

On the graph (Figure 6) you can see all of the above [11]. The highest point is ideal, and the lowest is the worst in terms of security. By Ox plotted $\max|\overline{T}_j|$ (the maximum of the number of properties of each of the property vectors), and by Oy - D.



Figu 0 - The dependence of the level of s ratio he number of domains to the maxi $\max|\overline{T}$ nber of objects in domains

VII. WEIGHTED SECURITY DOMAIN ALLOCATION ALGORITHM

The initial data for this algorithm coincides with the initial data for the comparative algorithm. That is, it has a graph $G(U,V)$ of n vertex, where $U = \sum_{i=1}^{n} u_i$ - many network objects, V - many communication lines connecting them. The number of properties of each network object is of course, their number is the same for all objects and is equal to m. It is known that each property has a vulnerability in the sense of security. Therefore, the properties differ among themselves - one is more secure, the other is less secure. It can say that each property has a weight, if we consider them from the point of view of security. All specific properties are determined empirically based on the value (importance) of the network object. Denote by $\bar{t} = \{t_1, \ldots, t_m\}$ network object properties vector. Let the properties t_i represent the numerical value of the weight of this property.

That is, $t_i = \begin{cases} p, & weight\ \ property\ \ object \\ 0, & property\ \ not\ \ present \end{cases}$,

where $p \in N$.

Weight p for the most important property t_k is chosen in such a way that the sum of the weights of the properties is less than or equal to t_k :

$$t_k \le \sum_{i \ne k} t_I \quad , \quad i = 1,...,m$$

Thus, it obtains for each object a set of properties, each property being a numerical value of its vulnerability and therefore, its importance for the object or network as a whole. Based on the obtained sets of properties, it concludes about the level of security of the object. This is achieved by a simple summation of the properties:

$$S(u_i) = \sum_{j=1}^{m} t_j^i \quad ,$$

where t_j^i – j -th property of the object u_i.

Taking into account the received damage to the security of objects, it combines them into domains. Objects that fall into the same domain have either the same or different by δ level of security. Value δ is determined based on the obtained values of the security levels of network objects.

The result of all the above operations - a set of security domains - is combined into one network using security tools between domains.

The weighting algorithm has several disadvantages. Firstly, the determination of property weights is a rather time-consuming operation. Secondly, the search is not an easy task [12-13]. It is possible to significantly simplify the implementation of algorithms in a machine version by introducing a dialogue with the user.

The algorithm is more complicated compared to comparative algorithms, but it can help where the application of the comparative algorithm did not give a significant result, since a completely different approach is used here.Now consider the practical application of the above algorithm.Take, for example, a network whose structure is shown in Figure 7.

The depicted network has access to a public access network and this creates the possibility of unauthorized access to the network under study. Therefore, it was decided to use a filtering router, which is located in front of the entrance to the public network. Inside the organization there is a database server, which the organization needs to provide services to its customers. This server is further protected by a firewall [14]. Also on the network is the server of the development team, the DNS server.

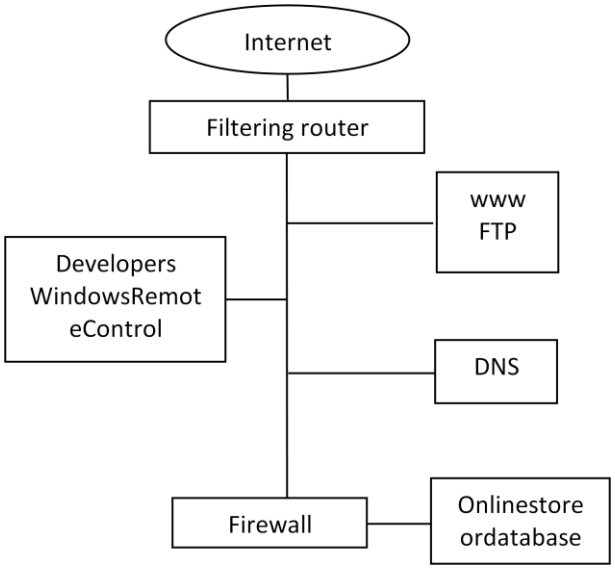


Figure 7 - Algorithm usage example - Initial network

At first glance, it seems that the network is quite secure. But this does not take into account the fact that services such as DNS, WWW, FTP are used to provide access from the Internet and they are on the same network as the development team. This creates a danger of data loss or data theft.Let's try to apply an algorithm to increase security to this network.

VIII. APPLICATION OF THE COMPARATIVE ALGORITHM

It will be considered a network whose structure can be changed according to the received security domains. Database server does not get

under consideration, since it is already in a separate security domain and is separated from other means of protection - a firewall.

So, we have three objects on the same network: the DNS server, the WWW and FTP server, the development server with its services - u_3.

It is considered the number of services used by all servers as a whole: DNS, WWW, FTP, remote service. Take the initial data for the algorithm: $n = 3$ (number of objects), $m = 4$ (number of services). It is composed a matrix of objects - properties. It is had:

$$\begin{array}{c} \\ u_1 \\ u_2 \\ u_3 \end{array} \begin{array}{c} \begin{array}{cccc} t_1 & t_2 & t_3 & t_4 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

The matrix clearly shows that there are no columns with more than one unit. Therefore, following the algorithm, we conclude that each object deserves its own security domain. Between these domains, the most appropriate security features should be included.

The network structure obtained as a result of the weighting algorithm coincides with the result of the comparative algorithm and is shown in Figure 8.

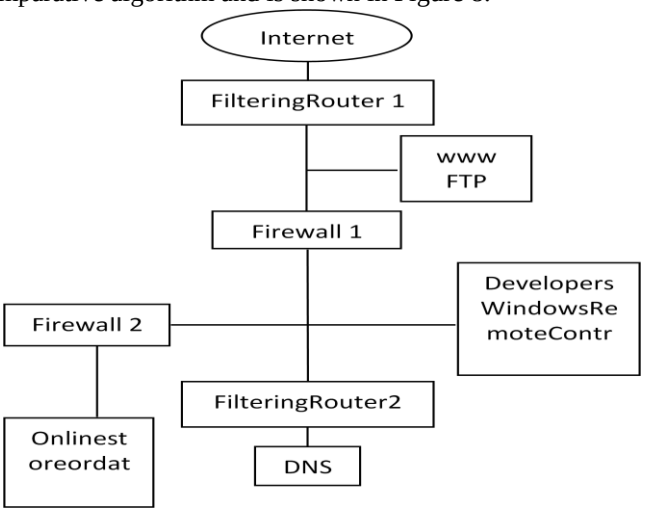


Figure 8-An example of using algorithms is the result of applying algorithm

*Application of the weight algorithm.*The initial data for this algorithm are the same as for the previous one: (number of objects), (number of services). Let the properties of objects in the property vector be arranged as follows: $t = \{t_1, t_2, t_3, t_4\} = \{\text{DNS, WWW, FTP, Remote Control (RC)}\}$,

It is selected the weight of each property according to modern data from the theory of security for the vulnerability of a particular service. Let $t_1 = 1$, $t_2 = 3$, $t_3 = 3$, $t_4 = 10$. Object property vectors:

$t^1 = \{1,0,0,0\}$, $t^2 = \{0,3,3,0\}$, $t^3 = \{0,0,0,10\}$

It is determined the level of security of objects by the formula $S(u_i) = \sum_{j=1}^{m} t_j^i$ where t_j^i - j -th property of the object u_i. It has had:

$S(u_1) = 1 + 0 + 0 + 0 = 1,$

$S(u_2) = 0 + 3 + 3 + 0 = 6,$

$S(u_3) = 0 + 0 + 0 + 10 = 10.$

An analysis of the data shows that the difference between the levels of security of objects is large enough to choose a number. Therefore, it is concluded that each object belongs to its own security domain. That is, they received three security domains. They are interconnected through protective equipment.

IX. CONCLUSION

To conclude it should be notedthat application of the above algorithms can give different results. Although the use of both algorithms will significantly increase the overall security of the network, you should choose the one that is most optimal in terms of the cost-protection ratio.

REFERENCES

1. Dileep Kumar G, Manoj Kumar Singh and M.K. Jayanthi. Network Security Attacks and Countermeasures. IndexedIn: SCOPUS |Copyright: © 2016 |Pages: 357
2. Phillip Ferraro. Cyber Security: Everything an Executive Needs to Know. Hardcover – July 6, 2016.
3. Joseph MiggaKizza. Guide to Computer Network Security (Computer Communications and Networks) (2015-02-10).
4. Shangin V. Information security computer. systems and networks. Publisher: Infra-M. Year of publication: 2018
5. Crow V.A., Tikhonov V.A., Mitryakova L.V. The theoretical basis for ensuring the safety of informatization facilities. Textbook for universities. ISBN 978-5-9912-0524-5, 2016, 304 pp.
6. Babash A., Baranova E. Actual issues of information security. Monograph. Publisher: Rior. Year of publication: 2017
7. GulomovSh.R., Abdullaev D.G., Nasrullaev N.B., Zokirov O.Y. Method for determination of the probabilities of functioning states of information of protection on cloud computing. International Journal of Mechanical Engineering and Technology (IJMET) Volume 10, Issue 04, April 2019, India. –P.750–759
8. GulomovSherzod, AbdullaevDilmurod, MalikovaNodira, AkhmedovaHusniya. Construction of Schemes, Models and Algorithm for Detection Network Attacks in Computer Networks. International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-12, October 2019. – P. 2234-2240
9. MohdAzahariMohd Yusof, Fakariah Hani Mohd Ali, and Mohamad Yusof Darus, "Detection and Defense Algorithms of Different Types of DDoS Attacks," International Journal of Engineering and Technology,vol. 9, no. 5, October 2017.
10. A. Bremler-Barr, Y. Harchol, D. Hay, Y. Koral. Deep packet inspection as a service. In CoNEXT, 2014. – P.271–282.
11. William Stallings. Network security essentials: Applications and Standards Fourth edition. Prentice Hall, USA, 2011. – P.417.
12. Pongle, P., & Chavan, G. (2015). Real time intrusion and wormhole attack detection in internet of things. International Journal of Computer Applications, 121(9).
13. Le, Anhtuan, et al. "A specification-based IDS for detecting attacks on RPL-based network topology." Information7.2 (2016).
14. Stavroulakis, P., & Stamp, M. (Eds.). (2010). Handbook of information and communication security. Springer Science & Business Media.

AUTHORS PROFILE

Saparova Gaukhar was born in September 25, 1983 in Nukus city, the Republic of Karakalpakstan. In 2006 graduated«Mathematics» faculty of Azhiniyaz Nukus State Pedagogical Institute. Has more than 30 published scientific works in the form of articles, journals, theses and tutorials in the field Computer networks and Cyber Security. Currently works of the department «Information Security» at the Tashkent University of Information Technologies of Nukus branch named after Muhammad al-Khwarizmi.

Gulomov Sherzod PhD was born in February 26, 1983 in Shakhrisabz city, the Republic of Uzbekistan. In 2009 graduated «Information technology» faculty of Tashkent University of Information Technologies. Has more than 125 published scientific works in the form of articles, journals, theses and tutorials in the field Computer networks and Cyber Security. Currently works of the department «Providing Information Security» at the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi.