AMERICAN JOURNALS
Open Access, Peer Reviewed Journals

American Journal of Technology and Applied Sciences
ISSN (E): 2832-1766 Volume 25, June - 2024

IMPROVING THE EFFICIENCY OF INFORMATION SECURITY IN THE CONSTRUCTION AND OPERATION OF VARIOUS CONTROL SYSTEMS

Xikmatulla Nigmatov 1, a)
Kurbon Rakhmanov 2, b)
1 Department of Modern of ICT, International Islamic Academy of Uzbekistan, Tashkent, Uzbekistan
2 Department of Modern of ICT, International Islamic Academy of Uzbekistan, Tashkent, Uzbekistan
a) Corresponding author: khikmatulla@mail.ru
b) raxmanov@gmail.com

ABSTRACT

In this article, the increase in the number and types of cybercrimes occurring in the world as a result of the development of the Internet has a significant impact on big data, the issue of storing large amounts of data and ensuring security in communication channels is focused on. In this process, proposals are made to ensure the security of big data and prevent its loss. In particular, in the construction of any intellectual system of information security management, it is envisaged to take into account the total costs and losses of the object receiving the information.

KEYWORDS

Cybercrime, information security, digital transformation, information systems, information protection, intelligent information security management system, operation of various control systems, symmetric and asymmetric coding methods.

Introduction

As everyone knows, the number of cybercrimes on the international Internet has increased dramatically recently. Naturally, this is due to the accelerated increase in the number of modern mobile communication information systems, processing large volumes of various types of information. Such a rapid development of the Internet leads to great problems of ensuring security from various cyber threats. Therefore, the problem of ensuring the transmitted, processed and stored data requires the development of more modern systems for protecting this data. Data centers or data processing centers that specialize in hosting specialized computer devices designed for storing large amounts of data, processing information, as well as providing customers with communication channels for access to the Internet.

According to statistics, according to Steve Morgan, editor-in-chief of Cybersecurity Ventures: Cybercrime is predicted to cost the world $8 trillion USD in 2023, according to Cybersecurity

Ventures. If it were measured as a country, then cybercrime would be the world's third largest economy after the U.S. and China [1].

In this case, users of which can be both state-owned enterprises, organizations, institutions, and commercial enterprises using various virtual services. A huge amount of heterogeneous information with a certain value is transmitted through these virtual channels. Currently, with the transition to market relations, any information becomes a commodity (product) for the recipient, and each one individually may have a different value in terms of semantic content. As is known, information security is understood as the protection of information and supporting infrastructure from accidental or intentional impacts of a natural or artificial nature that can cause unacceptable damage to subjects of information relations, including owners and users of information and supporting infrastructure. And information protection is a set of measures aimed at ensuring information security.

Currently, information security tools in computer systems and networks can be divided into [2-3]:

- organizational (organizational – technical and organizational – legal) means of protection;
- technical, i.e., electronic, electromechanical and other hardware means of protection;
- software protection tools; - legal remedies;
- physical means of protection;
- means of information protection during transmission via communication channels;
- special means of protection against various computer viruses and others.

Sometimes cryptographic means of information protection are singled out separately, although they can be conditionally attributed to software and technical means of information protection. For all of the above information security tools, there are currently quite a lot of developments dedicated to software, organizational, technical, legal and cryptographic security tools. As everyone knows, solving the problem of ensuring information security in telecommunication networks, computer information processing systems is a complex and complex task.

The protection of information in the transmission, processing and storage of data is becoming an important task in the modern world. Workstations of a particular organization can be reliably protected, but when data is transferred outside the perimeter closed from penetration, the probability of leaks increases. Very often, the use of insufficiently effective means of protection causes the loss of personal data of citizens, their bank card numbers, information having the nature of a trade secret. The use of modern methods of information protection should be the main goal of creating an information security system.

In order to ensure the security of information, it is necessary to purposefully and regularly use methods and tools, as well as the implementation of various measures to maintain a given level of information security across the entire set of indicators and security conditions. For a scientifically-based choice of information security policy, it is necessary to answer the following questions:

- what is the risk of losing this or that type of information;
- what information should be protected and from whom;
- what degree of protection is required for each type of information;
- what organizational, technical and software protection tools should be used;
- what will be the costs of protecting this information, etc.

When creating information security systems, it is necessary to study in detail the object for which it is being created, to develop a private model of the violator. The next stage is the development of

requirements for the information security system, which should take into account the goals and objectives set for the system, the technical requirements of the customer and the real threats of the information resource of the object, on the basis of which the information security system is being developed. At the same time, the most advanced, promising methods and means of information protection must be analyzed.

Currently, most of all will be directed to the development of information security tools using intelligent tools, i.e., with the development of knowledge bases and hardware-technical means of protection based on the use of human biological parameters. During identification and authentication, in this case, in addition to the login and password, five most common types of biometrics can be used to enter the subject's information system, such as a fingerprint, a face image, a voice, an iris, and a drawing of the veins of a person's palm and finger. And when transmitting via communication channels, cryptographic means of information protection will be used.

The approach we propose is that when developing the above-mentioned information security management systems and choosing one or another means of protection, it is proposed to take into account the importance of this information, determined by its value [4]. In many specific cases, obtaining distorted, altered information, or not receiving the necessary information due to the impact of deliberate attacks by the violator will be conditionally considered erroneous. If this message is delayed and there is an error in the information received in the systems or objects where it is used, certain processes will proceed in a suboptimal way, i.e., with some losses, which will lead to material damage and can be determined by cost expressions. This expression can be defined both in monetary terms and in labor costs [5-6].

The average value of these losses may be non-linear and may increase rectilinearly, smoothly or instantly, depending on the content and importance of this message. The proposed approach for ensuring information security in computer networks and telecommunications systems is that when developing and building any information systems and information security tools, it is necessary to take into account the cost losses from untimely acceptance or errors of information, taking into account their value determined by the recipient of this information. Since any information is a valuable asset, the possession of which increases the competitiveness of business companies. Its protection becomes the goal not only of market participants and citizens, but also of states and law enforcement agencies. At the level of international law, fundamental documents on the protection of information are being adopted, articles related to crimes in the field of information security have already been introduced into the criminal codes of most countries. The value of the information should be determined by the material effect of saving the generalized labor costs of the recipient object to achieve the goal, i.e., ensuring the required protection of the system information. In general, the achievement of the goal is described by the expression

$$P = P_o - [S_{is} + S_n].$$

where: S_{is}, S_n – respectively the reduced costs of a reliable information system and losses for its construction; P - an indicator characterizing the operation of the combined system (profit, productivity, quality and quantity of products, the degree of completion of the task, etc.); P_o - an indicator P, which takes maximum values with absolutely reliable operation of the information system, ensuring the specified information security. The advantage and advantage of this expression is the fact that P

synthesizes changes in the cost of not only creating a secure information system, but also the losses of the managed object during its operation [10, 12-13].

For optimal construction of information security systems, it is necessary to minimize these total cost losses, taking into account the costs of building the created system as a whole [2]. The main criterion for ensuring any information system that provides reliable protection of information from various external influences is to minimize the above total cost losses depending on the value of the transmitted, processed and delivered to the user of the functioning object. These indicators can be obtained in advance by modeling or experimentally.

The application of this criterion (minimum losses) will create a more reliable information security system with minimal financial and labor costs. Currently, cryptographic means of protecting information in telecommunications networks are very widely used. Therefore, studies have been conducted on the use of various methods of information protection in the transmission of conditional form (open and labeled "DSP") information through communication channels in telecommunications, computer systems and networks.

Various methods of threats and attacks arising in computer networks, possible ways of their definition, methods of cryptographic means of information protection using both symmetric and asymmetric coding methods, as well as methods of information security of various databases are considered. The corporate network was modeled using the example of one university with branches, transmitting information in Uzbek and Russian. Algorithms of the data transmission system for the selected corporate computer network have been compiled in DES (Data Encryption Standard), AES (Advanced Encryption Standard), IDEA (International Encryption Algorithm) and software tools in the algorithmic scripting languages PHP and Java Script. The results obtained showed the correctness of the chosen method of information protection. These results can be used in the design of local, corporate and even regional computer systems and telecommunications networks, as well as in the operation of such information processing systems and networks of various levels and purposes. Based on the above, an effective method of improving the quality of functioning of computer networks and telecommunications systems will be the organization of priority message service, which consists in providing advantages to messages with a higher priority or messages with large cost losses from the delay in delivering information, which we will call a temporary value characteristic (VCC) [2, 7].

The general task of synthesizing an optimal priority system can be formulated as follows: to divide the total flow of messages into n streams and organize their transmission in such a way as to maximize the value of [3,8]:

$$W_E = \frac{\sum_{k=1}^{n} L_k M_k Q_k}{\sum_{k=1}^{n} L_k M_k} \quad (1)$$

where: - W_E is a network efficiency indicator that characterizes the value of the transmitted messages; L_k- relative share of the K-th priority stream; Q_k - probability of timely transmission of messages of the Kth stream. In order to assess the degree of influence of each of the message flow parameters, we will consider separately priority systems by value or by message aging time [13-16].

Let the general flow of messages be characterized by the density of the distribution of the value of messages f (C_0). The first priority will include messages having $C_0 \geq C_1$, the second - having $C_2 \leq C_0 \leq C_1$, etc. The task is to find such values of C_c (k=1, n=1) at which the maximum value of W is provided. In

this case, it is more convenient to use a slightly different expression for W_E (without normalizing the values of messages):

$$W_E = \frac{\sum_{k=1}^{n} L_k(C_0)Q_E}{\sum_{k=1}^{n} L_k M_k(C_0)} \quad (2)$$

It is easy to show that:

$$L_1 M_1(C_0) = \int_{C_1}^{\infty} C_0 f(C_0) dC_0 \,, n \quad (3)$$

$$L_k M_k(C_0) = \int_{C_k}^{C_{k-1}} C_0 f(C_0)\, dC_0 \,, k = \overline{2, n} \quad (4)$$

$$\sum_{k=1}^{n} L_k M_k(C_0) = \int_{0}^{\infty} C_0 f(C_0) dC_0 = M(C_0)\,; \quad (5)$$

$$Q_k = Q_\infty \frac{1-\rho^{k+1} Q_m^{K+1}}{1-\rho^{k+1}\rho}\,. \quad (6)$$

To find Q_k, we use expression (6) to investigate the impact of only the value of messages, let's say, $\mu_k = \mu_1$,

$\nu_k = \nu(k = \overline{1, n})$. Then you can write:

$$Q_k = \frac{1-\sum_{i=1}^{k} \rho_i}{\nu\,[\mu^{-1}+(\nu+6_{k-1}\prod_{k-4}(\nu)^{-1}]-\rho_k}. \quad (7)$$

where: $\rho_i = \frac{\lambda_i}{\mu} = \frac{\lambda \cdot L_i}{\mu} = \rho L_i$;

$$\prod_{k-1}(\nu) = \sum_{i=1}^{k-1} \lambda_i \mu 6_{k-1}^{-1} \left(\nu + 6_{k-1} - 6_{k-1}\prod_{k-1}(\nu) + \mu\right)^{-1} \quad (8)$$

Resolving (8) with respect to $\prod_{k-1}(\nu)$ we obtain:

$$\prod_{k-1}(\nu) = \frac{\nu+\mu+6_{k-1}}{2 6_{k-1}} \pm \sqrt{\left(\frac{\nu+\mu+6_{k-1}}{2 6_{k-1}}\right)^2 - \frac{\mu}{6_{k-1}}} \quad (9)$$

Given that $\prod_{k-1}(\nu)$ must be less than 1, and replacing $\sigma=\nu/\mu$ we get:

$$\prod_{k-1}(6) = \frac{1+\delta+\rho\sum_{i=1}^{k-1} L_i}{2\rho\sum_{i=1}^{k-1} L_i} - \sqrt{\left(\frac{1+\delta+\rho\sum_{i=1}^{k-1} L_i}{2\rho\sum_{i=1}^{k-1} L_i}\right)^2 - \frac{1}{\rho\sum_{i=1}^{k-1} L_i}}\,; \quad (10)$$

$$Q_k = \frac{1-\rho\sum_{i=1}^{k-1} L_i}{\delta\{1+[\delta+\rho\sum_{i=1}^{k-1} L_i(1-\prod_{k-1}(\delta))]^{-1}\}-\rho L_k} \quad (11)$$

$$Q_k = \frac{1-\rho\sum_{i=1}^{k-1} L_i}{\delta\left\{1+\frac{1}{\delta+\rho\sum_{i=1}^{k-1} L_i(1-\prod_{k-1}(\delta)}\right\}-\rho L_k} \quad (12)$$

In particular, let's talk about the work being carried out in Uzbekistan regarding the maintenance of databases of enterprises and organizations. According to the Presidential Decree No. 1989 dated June 27, 2013, large projects planned to be implemented in the field of information technologies were announced. By now, almost all of them have been completed. According to the Presidential Decree No. 1989, it is planned to launch data processing centers in three cities of Uzbekistan: Tashkent, Kokand and Bukhara. In 2022, a data processing center located in the Tashkent region was launched. A system firstly with 20 petabytes of memory has been established in the data center in cooperation with the Chinese company Huawei. It has 580 servers, and diesel generators with a total power of 5 megawatts ensure continuous operation of the system. The building's cooling and fire safety systems also meet all requirements. In general, the Data Center has a TIER III certificate issued by the international "Uptime" institute.

The data center was launched on the strategy of "Digital Uzbekistan – 2030" [17]. The data center will save billions of dollars spent by government agencies on data storage and technical support, and the

quality of services provided to citizens and entrepreneurs will improve. Most importantly, reliable protection against cyberattacks is provided. Taking this into account, starting from March 2024, my.gov.uz - the Single interactive state services portal was also moved to this data center. Gradually, government institutions are moving their sites and information systems to the Data Center to ensure information security, ensure data integrity and avoid cyberattacks. In the future, it is planned to launch Data Centers in the cities of Bukhara and Kokand. This certainly guarantees comprehensive protection of their data from state organizations.

CONCLUSION

The results of the study of the priority system based on the separation of flows of requirements according to their value, allows us to draw the following conclusions:

1. Reduces the generalized costs of the recipient object of information.
2. The gain is obtained with any division of the stream into priorities (even suboptimal), when messages of high value are assigned a higher priority.
3. The gain from the introduction of a priority system increases with an increase in the number of priorities, an increase in the load and with a faster aging of information.
4. Allows you to avoid blocking the system even with large overloads.

Based on the above, when building any intelligent information security management system, we consider it appropriate to take into account the value of the processed and delivered information, taking into account the total cost losses of the recipient object of information.

REFERENCES

1. Steve Morgan, Editor-in-Chief. Cybersecurity facts, figures, predictions and statistics. https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/.
2. H. Nigmatov, Umarov U.A. Analytical simulation methods determining the basic characteristics of a telecommunication network with different communication channels and a changing structure. Bulletin of TUIT: Management and Communication Technologies Volume 4 2021-third number Article 3.
3. H. Nigmatov. To a technique of maintenance of information safety in networks and systems of telecommunication. The Third International Central Asian Conference. In English. ICI-2007 and ITRA-2007 Paris.
4. H. Nigmatov, A.Mukhammadiev. To A Technique of Maintenance of Information Safety in Networks and Systems of Telecommunication. International Journal of Advanced Research in Science, Engineering and Technology Vol. 7, Issue 10, October 2020.
5. H. Nigmatov. Information Security. Information protection in telecommunication networks. Shymkent. Publishing house "ZHEBE", 2013. 188 p.
6. H.Nigmatov, B.B.Gafurov. Methodology and algorithm for managing packages of requirements in switching centers. The magazine of the Ministry of Emergency Situations. Tashkent. 2022.
7. X.Nigmatov, U.A.Umarov Exchange of messages in the telecommunication network with different types of communication channels. International Conference on Information Science and Communications Technologies (ICISCT) 4-5 November 2021.

8. X.Nigmatov, T.B.Tursunbayev. Algorithms of management requirement packages for switching centers. In Volume 2, Issue 5 of International scientific journal of "Science and Innovation". 2023. Pages 191-193.
9. T.A.Valiyev, X. Nigmatov. Towards determining the optimal use of a communication network for data transmission. " Issues of cybernetics ", Edition. 64. Tashkent, 1974.
10. A.Usmanov, Z.T.Adilova, X.Nigmatov. Managing information flows over data networks. Publisher «FAN». Tashkent. .1984.
11. V.N.Roginskiy. On the problem of assessing information in an information network. In the book Problems of information distribution. Moskva. Nauka, 1973. Pp.. 12-18.
12. A.M.Svetlitskiy, L.YE.Yashuk. On the distribution of flows in multi-pole communication networks. In book Information distribution systems. M.: Наука, 1972. Pp . 212-219.
13. N. Frank, Chjou. Topological optimization of computer networks. M.: Mir, 1974, pp. 147-182.
14. B.S. Goldshteyn, A.E. Curly Post-NGN Communication Networks. SPb.: BXB-Petersburg, 2014. 160 p.
15. A.Y. Grebeshkov. Computer technology, networks and telecommunications: a textbook for universities. M.: Hot line – Telekom, 2017. 190 p.
16. V.O. Tixvinskiy, S.V. Terentyev, A.B. Yurchuk. LTE mobile communication networks. Technologies and architecture. – M.: Eko-Trendz, 2010. 284 p.
17. Decree of the President of the Republic of Uzbekistan dated October 5, 2022. No. PF-6079 "On approval of the strategy "Digital Uzbekistan - 2030" and measures for its effective implementation". https://www.lex.uz/uz/docs/-5030957#-5031756.