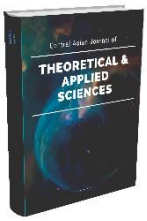

CENTRAL ASIAN JOURNAL OF THEORETICAL AND APPLIED SCIENCES

Volume: 04 Issue: 12 | Dec 2023 ISSN: 2660-5317
https://cajotas.centralasianstudies.org

Humans Factor in Information Security Significance

Sirojiddin Djuraboyevich Uzakov
Andijan State University, Faculty of Mathematics, Teacher of the Department of Informatics

Received 4th Oct 2023, Accepted 6th Nov 2023, Online 27th Dec 2023

Abstract: *In this article, the importance of the human factor in information security will be discussed. In this, the authors rely on technological information and talked about solving the problem using scientific literature some negative aspects of the existing problem are also mentioned.*

Keywords: *Information security, communication, technology, integrity, wholeness.*

In a broad sense, information security is the accidental or intentional exposure of information a set of protection tools. Regardless of the effect: natural factors or man-made causes - the data owner bears the losses.

Principles of information security

The integrity of information means both during the storage of information, retaining its original shape and texture even after repeated transmission ability is understood. Only the owner or the user has the right to change, delete or complete the data. Privacy - access to information resources for a certain group of people a feature that indicates the need for restraint. During actions and operations the data is only entered into information systems and successful from identification will be available to previous users.

Availability of information resources from freely available information resource means that it will be made available to users in a timely and unhindered manner. Reliability means that the data belongs to a trusted person or ownershows that they work as a source of information at the same time. Third parties to ensure and support information security on prevention, monitoring and elimination of unauthorized access by includes a set of different measures. Ensuring information security measures, as well as protection against information corruption, destruction, blocking or copying aimed at doing. It is very important to solve all tasks at the same time, only then will full, reliable protection be ensured.

Comprehensive solution of information security problems by the DLP system is provided. Maximum number of SearchInform CIB data transmission channels controls and internal audits of the company's information security service provides a large set of tools. Hacking or stealing information has a number of serious consequences, financial the main way to protect information if it leads to losses questions are particularly relevant.

Diversity of information security threats An information threat is a potential impact or effect on an automated system, may later harm someone's needs. Today there are more than 100 positions of threats to

the information system and There are types. Analysis of all risks using various diagnostic methods important to do. Based on the indicators analyzed in detail, you system you can build correctly.

Classification of security vulnerabilities

Information security threats are not independent, but the protection system through possible interaction with the weakest links, i.e. through vulnerability factors appears. The threat of disruption in the operation of systems at a particular carrier facility will bring.

The main weaknesses are caused by the following factors:

- imperfection of software, hardware platform;
- different structure of automated systems in information flow characteristics;
- some of the systems' operating processes are defective;
- inaccuracy of information exchange protocols and interface;
- difficult working conditions and location of data.

Often the sources of threats are illegal due to data damage run for profit. But the random action of threats is protection due to the insufficient level and the mass effect of the threatening factor possible. There is a distribution of vulnerabilities by class, they can be:

1) Lens;

2) Random;

3) Subjective.

If you eliminate the effects of vulnerabilities or at least if you reduce it, from a full-fledged threat aimed at the data storage system you can escape.

Objective weaknesses

This type of equipment in the facility that requires direct protection depends on the technical structure and its characteristics. Get rid of these factors completely it is impossible to be, but to partially destroy them engineering and technical methods using the following methods:

Related to technical means of radiation:

- electromagnetic techniques (side options of radiation and cablesignals from lines, elements of technical equipment);
- sound options (with the addition of acoustic or vibrating signals);
- electricity (displacement of signals in the circuit of the electrical network, lines and by pickups in conductors, with uneven distribution of current). Enabled:
- malware, illegal software, "software bookmarks" technological outputs from programs combined with the term;
- equipment labels - directly to telephone lines, electrical factors included in networks or simply in buildings.
- Created with the properties of the protected object:
- Location of the object (controlled around the information object the appearance and absence of the area, the reflection of vibration or sound around the object the presence of the elements of the object, the distant elements of the object availability);

- organization of information exchange channels (use of radio channels,leasing frequencies or using universal networks).
- Those that depend on the characteristics of the carrier elements:
- Parts with electroacoustic modification (transformers, telephone devices, microphones and speakers, inductors);
- objects exposed to the electromagnetic field (carriers,microcircuits and other elements).

Studies have shown that traditional information security training programs often necessary to effectively reduce information security risks to students does not provide knowledge and skills (Kraemer and Carayon, 2007). This Various factors to failure, including interesting and interactive educational materials lack, inability to adapt teaching to the needs of individual students and with limited opportunities for practical application of learned knowledge and skills may be related.

To overcome these limitations, online learning environments are about information security emerged as an effective means of curriculum delivery. That's the research showed that the online learning environment provides students with multimedia materials, interactive and using collaborative learning activities and personalized learning experiences provides an opportunity, which increases student engagement and retention of knowledge.

There are several benefits of online information security training programs evaluated in studies. For example, Chandrasekharan, Krishnan, and Babu (2017) an online study of cyber security awareness among undergraduate students evaluated the effectiveness of the program. The study found that the curriculum significantly improved students' cyber security awareness and knowledge. Similarly, Singh, Pahwa and Chaudhary (2019) among Indian bank employees evaluated the effectiveness of an online cybersecurity training program. That's the research showed that the training program improved employees' cyber security concepts and security significantly improved the ability to detect and respond to threats.

These studies show that online learning environments are about information security can be an effective tool in the delivery of training programs. At the same time, this that programs meet their goals and information security risks to students to ensure that they provide the knowledge and skills necessary to reduce their there is a need to evaluate its effectiveness.

Based on this, it can be concluded that information is effective in the online learning environment safety training uses a range of strategies, including interactive teaching methods, requires customized content and game usage. Students are unique taking into account their needs and using different teaching methods, effectiveness of information security training for teachers in an online learning environment and individuals in the complex and rapidly changing landscape of cybersecurity can help prepare for management.

Nowadays, the number and type of information in the world information flow is very large causing various problems and shortcomings in terms of consumption and safety is issuing. Attacks by various hacker groups on information security, disinformation, massive system and software crash, These are the spread of viruses that reverse information content or destroy it including As we know the power of information, it is people by leading astray, by poisoning the mind, and by corrupting ideas, they with such consequences as creating confusion about current events coming is no secret. Internet networks directly represent the future of the entire humanity, especially the nation. poisoning the minds of the young generation who are the future of the state, ensnaring them in various ways, distance from science, views that are contrary to our national values in various ways serves as a practical means of absorption. In this context, information security we refer to another given definition: "Information security - unacceptable as

a result of its impact Against the effects of internal and external information, intentionally or accidentally, leading to situations stability of the system". What is given in this definition is the system of our own mind and we should form in our society. Among our people, "Knowledge acquired in youth is a stone." There is a proverb that says, "It is like a carved pattern." If we look at it from this point of view, it will grow in the next generation, as above, in the consumption of information and the use of the Internet it is necessary to introduce a complete and continuous system that performs the function of a special defense and filter. This the introduction of the system directly into the general secondary education system and all layers of its youth is an effective means of coverage. First grade introduction of "Information Science" subjects for students, mainly information by teaching information about it in a simple and fluent way, by means of various comparative examples if it is to go and absorb the initial concepts about it, it is relatively for higher classes "Types and Classification of Information", "Information and the Internet: introduction of "culture and security" subjects, mainly world information flow to be able to analyze the characteristics, their types and the level of reliability, if they are needed requirements, to have fundamental knowledge about them, to avoid informational attacks and protect those around you, not to be deceived by fraudulent groups on social networks, from the Internet formation of a culture of use, compliance with moral and spiritual principles in consumption the main task is to inculcate such tasks as doing.

We live in the information age with many conveniences and opportunities He is putting many problems and issues in front of us. World science and to quickly learn about new technological innovations, to use them on the one hand, it contradicted our national mentality and universal human values widespread dissemination of information, false information by malicious people the fact that it leads people astray is a separate aspect. This period is every person and requires vigilance and awareness from the society. Only then will we be sure of our goal we will be a step and no external and internal factors will stop us from high progress can't.

Summary

In conclusion, we would like to say that today information technologies Security in the field has become more relevant than ever. Confidential and personal information of us or the company we work for - The safety of -- is largely dependent on us. Due diligence is the security guarantee of our data.

Books

1. Security in Computing – (3rd Edition) Charles P. Pfleeger, Shari Lawrence Pfleeger. PHI.
2. Cryptography and Network Security – by A. Kahate – TMH.
3. A Sitek and Z Kotulski (2018). POS-originated transaction traces as a source of contextual information for risk management systems in EFT transactions. EURASIP Journal on Information Security 2018,5, Published on: 27 April 2018https://doi.org/10.1186/s13635-018-0076-9.
4. J Navarro, V Legrand, A Deruyver and P Parrend (2018). OMMA: open architecture for operator-guided monitoring of multi-step attacks. Eurasip Journal on Information Security, 2018,6. Published on: 2 May 2018 https://doi. org/10.1186/s13635-018-0075-x.
5. G Jaideep and B.P Battula (2018). Detection of spoofed and non-spoofedDDoS attacks and discriminating them from flash crowds. Eurasip Journal onInformation Security, 2018:9. Published on: 16 July 2018 https://doi.org/10.1186/s13635-018-0079-6.

