INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCHERS
ISSN: 3030-332X Impact factor: 8,293 Volume 8, issue 2, November 2024
https://wordlyknowledge.uz/index.php/IJSR worldly knowledge
Index: google scholar, research gate, research bib, zenodo, open aire.
https://scholar.google.com/scholar?hl=ru&as_sdt=0%2C5&q=wosjournals.com&btnG
https://www.researchgate.net/profile/Worldly-Knowledge
https://journalseeker.researchbib.com/view/issn/3030-332X

MILITARY APPLICATION OF COMMUNICATIONS AND INFORMATION SECURITY

Madina Rustamqulova

rustamovamadina200@gmail.com

Keywords: Military communication, Information Security,Confedential information,Special department

Abstract: Cyber-attacks and cyber-threats are one of the urgent problems in the world today. This article discusses the prospects of information security and cyber-security in the military sphere. The role of information security in military organizations is widely covered.

Military communication is a process of mutual information exchange and coordination of military structures. These communications include radio, telephone, computer networks and other communication equipment. So much for the effective transfer of military communications, protection and supply of production.

Information security means protection from material and deliberate attacks. This field is a multifaceted field of activity, in which only systematic and complex production can be created. There are no absolute systems for this, but reliable devices in the sense of "trusted system" are not possible. From enough hardware and devices, one software is a device processing device using various image downloads.

Confidential information and confidential information are prohibited documents.

Confidential Information - Documented information that does not include access to legislation of the Republic of Uzbekistan, information on state secrets. The Cabinet of Ministers of the Republic of Uzbekistan "On measures to implement the decision of the President of the Republic of Uzbekistan "On National Additional Measures" dated July 8, 2011 PQ-1572" dated July 7, 2011 - in November 296, the above sentence is officially ready. Information is very important in the military field. Data Protection, Communication Power, Cyber Security, Information Privacy of Civilian and Military Personnel, System Continuity are all protected by security. Inadvertent capture or disclosure of military information, plans and strategies, and internal information may lead to an enemy.

It is necessary to protect information systems, networks and data, and of course, military organizations against cyber attacks. This is mainly done by Cyber Security personnel. A clear example of this is the activity of the Cyber Security Center, the increasing number of Cyber Security courses in universities, and the growth of qualified specialists. In particular, qualified military cyber security specialists are being trained in the Special Department of Tatu named after Muhammad Al Khorazmi. Students who have completed this course will attain the rank of lieutenant, cyber security specialist with special military training. Muhammad Al-Khorazmi Higher Education is among the number of higher education institutions in the field of training security specialists. Signing practical programs with prestigious Khori higher education institutions for higher education. Providing quality education to students and training mature personnel of the time is one of the high qualifications of education.

Specialists mainly work on Cyber protection systems, Encryption, security communication systems on a legal and regulatory basis. Cyber security systems: Special programs and systems are implemented in military installations to combat cyber threats. These systems are designed to detect, recover and recover from cyber attacks. Encryption: Encryption technologies and management in data management and administration. This is necessary to ensure the security of the data and to prevent its accidental use. Technological systems: There are special production communication channels and systems for military communication. These systems allow military support to reliably correct data. Monitoring and analysis systems: Improving the effectiveness of monitoring and analysis to provide information. This allows for early and rapid response to potential damages. Training and Treatment: Regular training in military health information is required. This is to monitor the readiness of the new ones to the court and follow the observation. Physics: View physical support in military and facilities to provide information base. This helps prevent unauthorized access to data. Legal and regulatory framework: To ensure the information framework, military equipment storage and regulatory documents must be developed. It helps to organize and support processes. Documents related to obtaining information at the secondary level. It is the development and use of information resources, the organization of an organization and business processes. Examples of this include data resources, communication, use of cryptographic support, content filtering, and others. Such documents are the internal technical and organizational policy (standards) of the organization. Central information system to store all documents. Information security in English (English: Information Security, loosely, InfoSec) is the process of obtaining unauthorized access, disclosure, loss, research, recording or access to information. The three universal concepts apply regardless of the form of data (e.g., electronic or physical). The main purpose of the uninformed is information, health1, means of application[2]. This is achieved through a multi-step capability management process that identifies priority capabilities and intangible assets, potential contamination sources, vulnerabilities, impacts, and existing asset controls. This work is carried out together with the planning of planning

Organizational tools in the development of a reliable information protection mechanism. Legal and regulatory frameworks: Legal and regulatory documents must be developed in military installations to ensure information security. This helps streamline processes and increase security.

Organizational measures play an important role in creating a reliable information protection mechanism, because unauthorized use of confidential information is mainly not technical. but also users and employees who do not take into account the elementary rules of protection

It is related to criminal irresponsibility.

Organizational support is the strengthening of executive production and interaction, which does not allow access to confidential information or creates serious difficulties.

During the operation of the information protection system, the activity of the security administrator consists of timely change of user authorizations and adjustment of network systems. The problem of managing user rights and configuring the information protection system in computer networks. eg centralized use of the network

can be solved based on the use of the system. In the implementation of such a system, a special user management server working on the main server of the network is used. This server automatically synchronizes the database of central security authorities with the database of local security authorities. All this is done sequentially. Information security is achieved by providing a minimal need-to-know status. In other words, the authorized person can only be required to have the information necessary to manage his activities, such as the crimes against privacy mentioned above. . One of the most important measures to ensure privacy is to classify data for internal access through strict guidelines. Encrypting information is a typical example of one of ensuring confidentiality. Security policy consists of amalgam maintenance and direct control. Configuration of systems installed in the chat partition may require tweaks, so system and network administrators should work to implement the patch.

In conclusion, in today's era, when cyber-attacks and cyber-threats are becoming more and more intense, there is a high demand for professional cyber-security specialists. Therefore, the role of information security personnel and information security in general is indispensable in the military sector as well.

References:

1. G’aniyev S. K. ,Karimov M. M., Tashev К. A. AXBOROT XAVFSIZLIGI Toshkent 07
2. S.S. Qosimov Axborot texnologiyalari xaqida o’quv qo’llanma Toshkent 07
3. G’aniyev S.K.Karimov M.M. Hisoblash tizimlari va tarmoqlarida axborot xavfsizligi TDTU
4. http://www.kaspersky.ru/
5. http://www.viruslist.ru/
6. http://www.citforum.ru/internet/infsecure/its2000_01.shtml/
7. http://www.osp.ru/lan/2001/04/024.htm/
8. http://www.osp.ru/lan/2001/03/024.htm/
9. www.nasa.gov/statistics/
10. www.security.uz/
11. www.cert.uz/
12. www.uzinfocom.uz/