TECHNICAL SCIENCE
RESEARCH IN UZBEKISTAN
ISSN (E): 2992-9148 SJIF 2024 = 5.333
ResearchBib Impact Factor: 9.576 / 2024
VOLUME-2, ISSUE-7

DATA SECURITY AND MICRO-PROGRAMS

Karshi State University
Faculty of Mathematics and Computer Science
4th grade student of applied mathematics
Narzullayev Dilshod Almurod o‘g‘li

Abstract: Topics devoted to the theoretical foundations and priorities of security and technology science are covered. These topics describe the essence of security and technology concepts, threshold parameters for security detection and assessment, security and technology mechanisms, micro-programs and instructions.

Keywords: Security, technologies, economic security, technicalization of society, economy, politics, BIOS, science and technology, technological products, program.

Before explaining the meaning and essence of the concept of security and technology, it is necessary to touch on the concept of national security. Because security and technology were considered an integral part of national security. National security, as a general form of protection of interests, expresses all ideas about satisfaction of interests and needs, enjoyment of material, spiritual, universal human values and pursuit of well-being. The national security of the country is aimed at protecting its national interests from the influence and threats of various political, military, economic, ecological, ideological and other factors.

Information security (English: Information Security, also English: InfoSec) is the practice of preventing unauthorized access, use, disclosure, destruction, modification, research, recording or destruction of information. This universal concept applies regardless of the form the data is in (eg, electronic or physical). The main goal of information security is to protect the confidentiality, integrity and availability of information in a balanced way, taking into account the appropriateness of the application and without harming the organization's activities. This is achieved primarily through a multi-step risk management process that identifies fixed assets and intangible assets, sources of threats, vulnerabilities, potential impacts and existing risk management options. This process is carried out in conjunction with an assessment of the effectiveness of the risk management plan.

In order to standardize this activity, scientific and professional communities work on the basis of continuous cooperation aimed at developing basic methodology, policy and network standards in the field of technical information security measures, legal liability, as well as user and administrator training

ISSN (E): 2992-9148 SJIF 2024 = 5.333
ResearchBib Impact Factor: 9.576 / 2024
VOLUME-2, ISSUE-7

standards. This standardization is largely influenced by a wide range of laws and regulations governing the access, processing, storage and transmission of data. However, if the culture of continuous improvement is not properly formed in the organization, the introduction of any standards and methodologies can have a superficial effect.

Information security as an employment field has developed and grown significantly in recent years. He has developed many professional specialties including network and related infrastructure security, software and database protection, information systems auditing, business continuity planning, electronic records discovery and computer forensics. Information security specialists have high stable employment and high demand in the labor market.

In computing, firmware is a specific class of computer software that provides low-level control for a device's specific hardware. Firmware, such as a PC's BIOS, can contain basic device functions and provide hardware abstraction services for higher-level software, such as operating systems. For less complex devices, firmware is the device's complete operating system and can perform all control, monitoring, and data manipulation functions. Typical examples of devices that contain firmware are embedded systems (embedded software), home and personal appliances, computers, and computer peripherals. According to some reports, the various firmware components are as important as the operating system on a running computer. However, unlike most modern operating systems, the firmware rarely has a well-developed automatic mechanism to update itself to solve any functional problems discovered after the device is shipped. The BIOS can be updated "manually" by the user through a small utility. Conversely, firmware on mass storage devices (hard drives, optical drives, flash drives, such as solid-state drives) is rarely updated even when flash memory (instead of ROM, EEPROM) is used for firmware.

Most computer peripherals are special purpose computers themselves. Devices such as printers, scanners, webcams, and USB flash drives contain firmware; some devices may also allow you to update their firmware. Some low-cost peripherals no longer include non-volatile memory for firmware and instead rely on the host system to transfer the device driver from a disk file or CD.

Today, the complex of social technologies in various forms is wide and developed, and its role in society is incalculable. In the last period, great changes are taking place in the technological environment. These changes create the need for paperless technology. This, in turn, will lead to a wider development of the EHM. Artificial intelligence systems are created and controlled by humans, and in some places the need for the human factor is mandatory, because machines cannot or

ISSN (E): 2992-9148 SJIF 2024 = 5.333
ResearchBib Impact Factor: 9.576 / 2024
VOLUME-2, ISSUE-7

cannot go beyond commands that cannot determine and confirm the authenticity of a suspected attack.

References

1. "Chernye kabinety". M.: Novoe literaturnoe obozrenie, 2015.

2. Opler, Ascher (January 1967). "Fourth-Generation Software". Datamation. 13 (1): 22–24.

3. "Safety of vital activity" O. Kudratov, T. G'aniyev., 111:. "Labor" - 2004 u