AJSIHD
GLOBAL RESEARCH NETWORK

**AMERICAN Journal of Science on Integration and Human Development**
*Volume 02, Issue 02, 2024 ISSN (E): 2993-2750*

# Concept of Cyber Security

**Khilola Ergasheva**

Westcliff University MBA student

**Abstract:** The content of this scientific article is that the concept of cyber security, cyber security event, cyber security object, cyber security subject, cyber protection, cyber attack, ISO/IEC 27001

**Key words:** cyber security, cyber security event, cyber security object, cyber security subject, cyber protection, cyber attack, ISO/IEC 27001, electronic document circulation, authorization and authentication, management of information security incidents.

## INTRODUCTION

• **cyber security** - the state of protection of the interests of individuals, society and the state from external and internal threats in cyberspace;

• **cyber security incident** - an incident that led to interruptions in the operation of information systems in cyberspace and (or) violations of the openness, integrity and free use of information in them;

• **cyber security object** - a set of information systems, including important information infrastructure objects, used in activities to ensure cyber protection of information and cyber security of national information systems and resources;

• **cyber security entity** - a legal entity that has certain rights and obligations related to the possession, use and disposal of national information resources and the provision of electronic information services, information protection and cyber security. and (or) an individual entrepreneur, including subjects of important information infrastructure;

• **cyber protection** - legal, organizational, financial and economic, engineering and technical measures aimed at preventing cyber security incidents, detecting and protecting against cyber attacks, eliminating the consequences of cyber attacks, restoring the stability and reliability of telecommunication networks, information systems and resources, as well as a set of cryptographic and technical data protection measures;

• **cyber attack** - an action that threatens cyber security, carried out intentionally using hardware, software and software tools in cyber space;

Therefore, information sorting is becoming more complicated, and it is not always possible to protect against harmful information. In simple interpersonal relationships, dangerous information can cause sharp conflicts. Now, when considered at the scale of organizations, agencies, and large state structures, the issue of information security acquires an important social and political significance.

## MAIN PART

Taking into account the wide range of tasks assigned to state authorities and management bodies in the main areas of activity, it is very important for them to properly organize the process of providing them with the necessary information. Because this allows state bodies to be provided with complete and reliable information on ensuring the rights and freedoms of citizens, the legal interests of society and the state.

In this regard, international standards have been developed on how to ensure information security for government bodies and various other agencies and business activities.

ISO/IEC 27001 is an international information security standard jointly developed by the International Organization for Standardization and the International Electrotechnical Commission. The certificate includes information security requirements for creating, developing and maintaining an information security management system (ISMS).

ISO/IEC 27001 is one of the most popular standards in the world and meets the requirements of information security management systems (ISMS). What is information security management systems? BIS is a systematic approach to managing confidential information in a company so that it is secure. This mechanism helps small, medium and large enterprises to ensure information security.

According to data, since 2005, more than 25,000 companies worldwide have received ISO/IEC 27001 certification.

Such certification is a useful tool for building trust. That is, the activities of the organization that has received such a certificate, the information and information it provides and distributes are undoubtedly considered reliable at the international and local levels.

· assessment of the risks faced by the organization (threats to resources, their vulnerability and the possibility of threats, as well as determination of possible damage);

· compliance with legal, regulatory and contractual requirements to be fulfilled by the organization itself, its business partners, contractors and service providers;

Forming a set of information processing principles, goals and requirements developed by the organization to support its activities.

· protection against unauthorized access to systems (NSD);

· including internal protection against unauthorized access of the organization's employees;

· authorization and authentication;

protection and integrity of data transmission channels;

· ensuring the relevance of information when exchanging information with clients;

· electronic document circulation;

· management of information security incidents;

· business continuity management;

· internal and external audit of the information security system.

The certificate of compliance with the requirements of ISO/IEC 27001:2013 of the information security management system is the only generally accepted confirmation of compliance with international requirements in world practice.

Organizations with this certificate will have uniform requirements for ensuring information security, and mutual cooperation between management and employees will be established correctly. The trust of partners and other interested parties increases in organizations that have established an information security mechanism according to this certificate, which acts as an impetus for international recognition of the organization.

Another important aspect is that the company's opportunities to participate in large state contracts will expand.

## CONCLUSION

In general, the concept of "Information protection" itself is interpreted by the international standard as ensuring the confidentiality, integrity and availability of information. The basis of the ISO/IEC 27001 standard is the information risk management system. Such a risk management system provides guidance to organizations on which areas of information security to focus on. In short, the organizations that have received such a certificate are the organizations that work most correctly with information.

The certificate is an important recognition for many companies, ministries and agencies. Usually, this group includes, for example, service providers, insurance companies, banks, telecommunications companies, IT companies, etc. But it is important for state bodies - ministries and agencies to have such a certificate in the current conditions to ensure information security and gain trust in relations with citizens. For this, of course, the work of state bodies must have been open, transparent and fair, this has been recognized and the society has fully felt it. Only such bodies are considered worthy of ISO/IEC 27001.

Laws on information security in our country "On principles and guarantees of freedom of information", "On information provision", "On electronic digital signature", "On electronic commerce" and there are several legal documents "On electronic document circulation", "Cyber security" and other similar legal documents, which are important normative legal documents in ensuring information security.

In addition, legal protection of information security not only by national, but also by international norms, obtaining international certificates, mastering international standards is the most correct way in the current conditions.

## LIST OF REFERENCES

1. Ismailov, A., Jalil, M. A., Abdullah, Z., & Abd Rahim, N. H. (2016, August).

A comparative study of stemming algorithms for use with the Uzbek language. In2016

3rd International conference on computer and information sciences (ICCOINS) (pp. 7-12). IEEE.

2. Jalil, M. M., Ismailov, A., Abd Rahim, N. H., & Abdullah, Z. (2017). The Development of the Uzbek Stemming Algorithm. Advanced Science Letters, 23(5), 4171-4174.

3. Abdurakhmonova, N., Alisher, I., & Sayfulleyeva, R. (2022, September). MorphUz: Morphological Analyzer for the Uzbek Language. In 2022 7th International Conference on Computer Science and Engineering (UBMK) (pp. 61-66). IEEE.

4. Ismailov, A. S., & Jorayev, Z. B. Study of Arduino microcontroller board.

5. Ismailov, A. S., Alijanov, D. D., Jorayev, Z. B., & Kurbanov, M. U. Research on renewable energy sources in Uzbekistan.

6. Ismailov, A. S., Shamsiyeva, G., Abdurakhmonova, N., & Navoi, A. Statistical machine translation proposal for Uzbek to English.

7. Abdurakhmonova, N. Z., Ismailov, A. S., & Mengliev, D. (2022, November). Developing NLP Tool for Linguistic Analysis of Turkic Languages. In 2022 IEEE International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON) (pp. 1790-1793). IEEE.

8. Abdurakhmonovaa, N., Alisher, I., & Toirovaa, G. (2022, September). Applying Web Crawler Technologies for Compiling Parallel Corpora as one Stage of Natural Language Processing. In 2022 7th International Conference on Computers Science and Engineering (UBMK) (pp. 73-75). IEEE.

9. Abdurakhmonova, N., Tuliyev, U., Ismailov, A., & Abduvahobo, G. (2022). UZBEK ELECTRONIC CORPUS AS A TOOL FOR LINGUISTIC ANALYSIS.