ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 06,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

DIGITAL SECURITY ISSUES AND WAYS TO PROVIDE IT

A.Kh.Djumayev
Senior Lecturer, Department of Digital Economics
jumayevaskar@sies.uz

Annotation. This article discusses the growing importance of cybersecurity in the era of digital development. It analyzes major threats in cyberspace such as fraud, phishing, ransomware, and data theft, and outlines preventive measures. The article highlights Uzbekistan's position and progress in international cybersecurity rankings, provides statistical insights, and suggests measures for further improvement. The necessity of legal regulation and the development of a national cybersecurity strategy is emphasized.

Keywords: Cybersecurity, digitalization, internet threats, cryptography, cyberattacks, data protection, national strategy, technological security

Annotatsiya: Mazkur maqolada raqamli texnologiyalar rivojlanayotgan bir davrda kibermakonda xavfsizlikni ta'minlashning dolzarbligi yoritilgan. Internetdagi firibgarlik, fishing, viruslar, shaxsiy ma'lumotlarning o'g'irlanishi kabi tahdidlar tahlil qilinib, ularni oldini olish choralari ko'rib chiqilgan. O'zbekistonning kiberxavfsizlikka oid xalqaro reytinglardagi o'rni va yutuqlari bayon etilib, mavjud muammolar, statistik tahlillar va ularni bartaraf etish bo'yicha takliflar berilgan. Kiberxavfsizlik sohasida qonunchilik asoslarini mustahkamlash, milliy strategiyani ishlab chiqish zarurati ta'kidlangan.

Kalit so'zlar: Kiberxavfsizlik, raqamlashtirish, internet tahdidlari, kriptografiya, kiberhujumlar, axborot himoyasi, milliy strategiya, texnologik xavfsizlik

Аннотация: В статье рассматривается актуальность обеспечения кибербезопасности в условиях стремительного развития цифровых технологий. Анализируются основные угрозы в киберпространстве, такие как мошенничество, фишинг, вредоносные программы, кража персональных данных, а также предлагаются меры по их предотвращению. Освещаются достижения Узбекистана в международных рейтингах по кибербезопасности, приводятся статистические данные и рекомендации по совершенствованию системы. Подчёркивается необходимость правового регулирования и разработки национальной стратегии кибербезопасности.

Ключевые слова: Кибербезопасность, цифровизация, угрозы в интернете, криптография, кибератаки, защита данных, национальная стратегия, технологическая безопасность

Introduction

Developing security in our republic is currently one of the most important tasks. Security measures are implemented in the network in such a way that there is no single point of denial, not only confidentiality, but also the non-repudiation of any action and authentication are ensured. Hacking attacks, theft of personal information, fraud, cyberbullying, phishing, spam, malicious programs, virus-scammers - all this threatens the security of a person in society. The

ORIGINAL ARTICLE
INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE
ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 06,2025
Journal: https://www.academicpublishers.org/journals/index.php/ijai

early days of the Internet, instead of making many processes transparent and making human rights violations more difficult, did not increase the security of individuals, institutions, and economic activity. The average Internet user often hoped that simple passwords would protect their e-mail and accounts, since providers or employers did not require more secure passwords.
Digital currency is not stored in a simple file. It is reflected in transactions marked with a cryptographic hash. Users own their own
cryptocurrencies and conduct transactions directly with each other. For such security, each of them must be responsible and reliably protect their private keys. The early Internet era created many wonders for many people. However, a large part of the world's population remains unconnected, having no access to technology, no financial system, and no economic opportunities. Moreover, the hope that the new communication tool would bring prosperity to all has not been justified. Yes, the Internet has allowed companies in developed countries to provide jobs to millions of people in developing economies. It has lowered barriers to entry for many entrepreneurs and has provided new opportunities and access to basic information to the underprivileged.

Literature review.

When a lot of information is transferred to a digital format and stored in electronic form, only then does the issue of information and cybersecurity become relevant. The head of our state has set such a requirement for specialists in the field of ensuring information security that they should not only study and eliminate the unpleasant incidents that have occurred in this regard, but also be able to foresee such a situation, that is, try to prevent it.
The concepts of digitization and cybersecurity always go hand in hand. Because along with the digitization of all systems and processes, it is important to ensure their technically perfect and error-free operation and security. The more attention is paid to the development of the digital economy in our country, the more importance is attached to ensuring cybersecurity. A vivid example of this is the high position of our country in the international global rating on cybersecurity, which is published annually by the International Telecommunication Union.
The Global Cybersecurity Index is a joint project of ABI Research and HEI (International Telecommunication Union). The index allows you to assess the level of participation of countries in the field of cybersecurity. The level of commitment is assessed in five areas: legal measures, technical measures, organizational measures, capacity development and international cooperation. According to the 2019 global cybersecurity rankings, Uzbekistan ranks 90th in the National Cyber Security Index, 52nd in the Global Cybersecurity Index, and 95th in the ICT Development Index.
Uzbekistan is strengthening its position in the Global Cybersecurity Index. In 2017, our country ranked 93rd in this ranking, and in 2019 it rose to 52nd place. Cybersecurity in a broad sense is a set of measures aimed at protecting information technologies, namely devices, programs, information systems and data. That is, maintaining the confidentiality of data, protecting their integrity, and ensuring the full functioning of programs and information systems without disruptions. This serves to increase production efficiency.

Analysis and results.

According to the analysis of the State Unitary Enterprise "Cybersecurity Center", in 2019, 268 cybersecurity incidents were detected on websites of the national segment of the Internet. This means that the number of violations in the digital world decreased by 44% compared to the previous year. Of these, 222 were unauthorized content uploads, 45 were defacements (a

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 06,2025
Journal: https://www.academicpublishers.org/journals/index.php/ijai

hacking attack that replaces a website page with another, for example, a page with advertising), and one was hidden mining (hidden activity on a cryptocurrency platform).
Compared to 2018, the number of incidents that occurred in the national segment of the Internet decreased significantly in 2019, which indicates that the work carried out in the field of cybersecurity has yielded positive results. 69% of incidents were detected on websites hosted by hosting providers in Uzbekistan, and the remaining 31% were on sites hosted by hosting providers in foreign countries relevant. 80 cases were investigated and practical recommendations were given to eliminate the identified vulnerabilities, the remaining 188 cases were eliminated independently by the website owners.
Security problems in cyberspace are caused by managing content with security errors in the code, working with outdated versions of software, easy access passwords, templates downloaded from unsafe sources, managing websites on computers infected with viruses, etc.

Conclusions and recommendations:

Legal strengthening of cybersecurity standards is extremely necessary. The digital world has not yet been able to clearly define its legal status. The fact that new types and forms of threats are emerging every day requires their reflection in legislation. The development of a national cybersecurity strategy will regulate activities in the field of combating crime in the national cyberspace. After all, the harm and danger of crime in the virtual world are no less than in the real world. According to the national cybersecurity strategy for 2020-2023, a unified cybersecurity system and a legal framework will be formed in the field of protecting critical infrastructure from cyberattacks.
The Law "On Cybersecurity" is expected to reflect the protection of the information and communication technology system from modern cyber threats, the introduction of modern mechanisms for cybersecurity for systems at various levels, the definition of the rights and obligations of state bodies, enterprises and organizations in this area, and the coordination of their activities.
At the heart of all reforms being carried out in our country is the goal of creating convenience for our people. Special attention to ensuring cybersecurity is becoming a prerequisite for the reliable and safe use of digital opportunities. The digitization of all sectors of the economy provides an opportunity to integrate into the global community, gain a place in the global market, gain economic stability, and create convenience for the population. It is gratifying that this is a key issue on the agenda of our country. Uzbekistan is taking bold steps towards digitization.
In our country, comprehensive measures are being implemented to actively develop the digital economy, widely introduce modern information and communication technologies in all sectors and areas, primarily in public administration, education, healthcare and agriculture.
In particular, the implementation of more than 220 priority projects has been launched, which include improving the e-government system, further developing the local market for software products and information technologies, establishing IT parks in all regions of the republic, as well as providing the industry with qualified personnel.

REFERENCES:

1. International Telecommunication Union. (2021). Global Cybersecurity Index 2020. Retrieved from https://www.itu.int

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 06,2025
Journal: https://www.academicpublishers.org/journals/index.php/ijai

2. ABI Research & ITU. (2019). National Cyber Security Index: Global Assessment. Retrieved from https://www.ega.ee
3. O‘zbekiston Respublikasi Prezidentining Administratsiyasi. (2020). Raqamli iqtisodiyotni rivojlantirish strategiyasi 2020–2030. Tashkent: Uzinfocom.
4. Cybersecurity Ventures. (2020). Cybersecurity Market Report 2020. Retrieved from https://cybersecurityventures.com
5. Davlat Unitar Korxonasi “Kiberxavfsizlik markazi”. (2020). O‘zbekiston Respublikasi veb-saytlarida 2019-yilgi kiberxavfsizlik holati tahlili. Tashkent: DUK “Kiberxavfsizlik markazi”.
6. O‘zbekiston Respublikasi Vazirlar Mahkamasi. (2020). Kiberxavfsizlik to‘g‘risidagi qonun loyihasi. Tashkent: Lex.uz
7. U.S. Department of Homeland Security. (2019). Cybersecurity Strategy. Washington, DC: DHS.
8. OECD. (2020). Digital Economy Outlook 2020. Paris: OECD Publishing.
9. Zetter, K. (2015). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. New York: Crown Publishing Group.
10. Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W. W. Norton & Company.