CYBERSECURITY IN UZBEKISTAN: THREATS, CONSEQUENCES, ECONOMIC IMPACT, AND PROTECTION MEASURES

Xidirov Behzod
University: TUIT, Faculty of Cybersecurity Engineering
Email: hidirovbehzod003@gmail.com
https://doi.org/10.5281/zenodo.15003960

ARTICLE INFO

Qabul qilindi: 01- Mart 2025 yil
Ma’qullandi: 06- Mart 2025 yil
Nashr qilindi: 11- Mart 2025 yil

KEY WORDS

Cybersecurity, cyber threats, Uzbekistan, information security, economy, digital economy, cybercriminals

ABSTRACT

This article examines the current cybersecurity threats facing Uzbekistan and their potential consequences for citizens and the national economy. The impact of cyber threats on economic growth and international relations is discussed. Examples of countries that have achieved prosperity through the development of cybersecurity are provided.

Introduction:

Despite the importance of cybersecurity, there is very little research in this area in our country. There is a lack of local publications, which makes it difficult to understand the threats and protection methods relevant to Uzbekistan. Even in the world, most data is presented in online resources, and they often do not take into account local characteristics. Therefore, more research is needed to better understand this important topic.

Security has always been a key issue in people's lives. For centuries, societies have sought to protect their borders, resources, relationships, and especially information. In the digital age, information security has become especially important, as modern technologies make it more vulnerable to cyber threats. Today, cybersecurity is becoming critical, as the amount of data that needs to be protected grows every year, both at the level of individuals and at the level of entire countries.

In this article, I will look at the main cyber threats that our country faces, their consequences, and possible risks if we do not develop the cybersecurity industry. I will also provide examples from other countries that demonstrate how the development of cybersecurity can positively affect economic development.

***Research Objective*:** To describe the main cyber threats faced by Uzbekistan and analyze how the development of cybersecurity can influence the country's economic stability and growth.

***Research Tasks*:**

- To consider the main cyber threats present in Uzbekistan.
- To analyze the consequences of cyber attacks for public and private structures.
- To assess what measures to strengthen cyber security can improve the economic situation.
- To provide examples from the experience of other countries for comparative analysis.

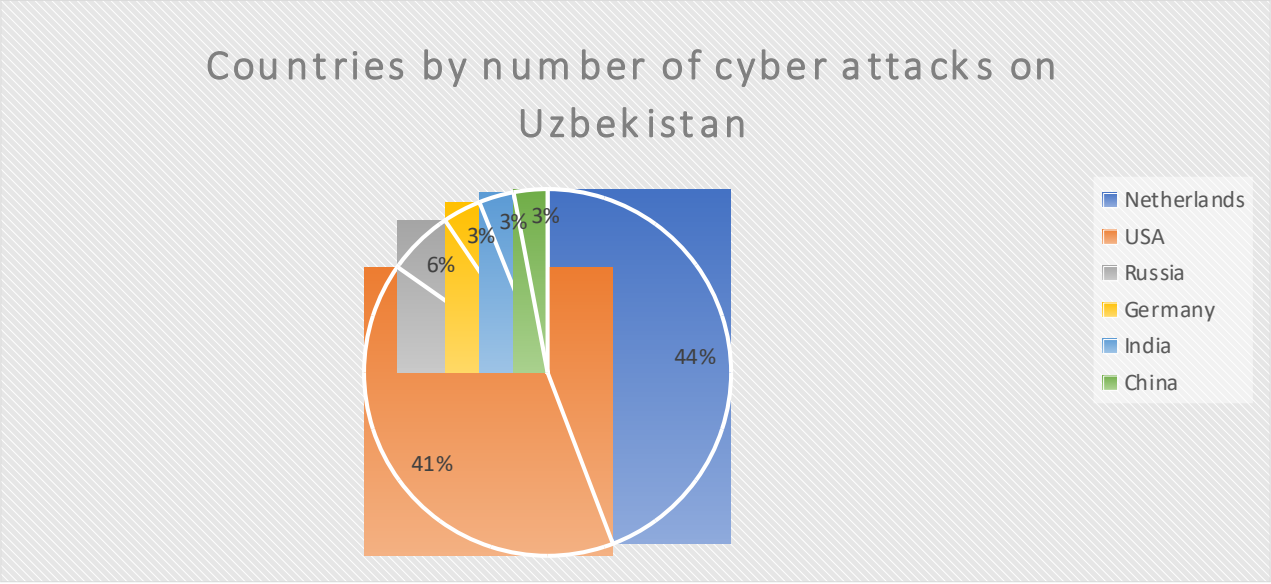
Major Cyber Threats in Uzbekistan

Given the average salary in Uzbekistan ($335.86), many users have limited access to expensive devices and computer technology, making mobile phones the primary means of accessing the Internet. This makes mobile devices the main target of cyberattacks. Hackers use methods such as:

- **Phishing** – Sending fraudulent SMS messages or instant messages containing links to malicious sites that can steal user data.
- **Mobile viruses** – Programs that people can install on their phones by downloading apps from unverified sources. These programs can steal personal data or block access to devices until the user pays a ransom.

According to data from the according to the Cybersecurity Center of the State Security Service of Uzbekistan, the biggest threats target web resources, especially government sites and platforms. In 2023, over 11 million cyberattacks on Uzbekistan's web resources were recorded. These attacks included:

- **SQL Injection** – Hackers input malicious commands into website forms (such as login or password fields) to access site databases.
- **Protocol exploitation** – Attacks exploiting vulnerabilities in network protocols.
- **Remote code execution** – Attackers force a server (the computer running a website) to execute malicious programs, taking control of the system.
- **Unauthorized file access** – Hackers gain access to hidden or protected files on websites, potentially leading to data leaks.



These cyberattacks primarily originated from IP addresses in the Netherlands (759.5 thousand), the USA (696.6 thousand), Russia (100 thousand), Germany (58 thousand), India (53 thousand), and China (51 thousand). This underscores the global nature of cyber threats and the necessity of international cooperation to enhance protection levels.

Most attacks were enabled by the following website issues:

- **Lack of user content verification – Websites do not check what users input in forms or upload, allowing attackers to insert harmful data.**

- **Programming flaws** – Errors in website code can lead to vulnerabilities that hackers exploit. Security issues related to outdated plugins or weak password protection can make websites easy targets.
- **Weak passwords** – Using simple passwords makes websites and systems vulnerable, as these passwords are easy to guess or crack.

Consequences of Cyberattacks for Uzbekistan

Cyberattacks and cybersecurity shortcomings can have severe consequences for Uzbekistan. Key aspects include:

1) Economic Impact – Cyberattacks can cause significant financial losses for the government and businesses. When hackers access financial data or disrupt website operations, companies may face:

- System recovery costs, requiring time and resources.
- Compensation for data breaches or reputational damage.
- Ransom payments to restore access to data in case of extortion.

An example of one of the large-scale cyberattacks WannaCry, which in total affected more than 500 thousand computers in more than 200 countries, belonging to individuals, commercial organizations and government agencies. The spread of the worm blocked the work of many organizations around the world: hospitals, airports, banks, factories, etc. In particular, in a number of British hospitals, scheduled medical procedures, examinations and urgent operations were postponed. The damage from this attack was estimated at billions of dollars, which showed how quickly cyber threats can spread.

2) Loss of trust. Cyber attacks on government institutions and companies can lead to a loss of trust among citizens and businesses. If users perceive that their personal data is not protected, they may begin to avoid using online services, making it more difficult to go digital. Estonia as an example: In April 2007, Estonia was the target of a series of powerful cyber attacks that lasted for several weeks. These events occurred against the backdrop of political tensions between Estonia and Russia over the Estonian government’s decision to move a monument to Soviet soldiers (the “Bronze Soldier”) from the center of Tallinn to another location. This caused protests both inside and outside Estonia, especially among Russian-speaking citizens and the Russian government. These cyber attacks paralyzed many online services in the country, which was a serious blow to Estonia, as the country was already known as one of the most digitally advanced in Europe.

3) Impact on national security. Insufficient protection against cyber threats can weaken national security. Cyber attacks can target not only financial institutions, but also important government structures, such as:

- Healthcare systems.
- Energy companies.
- Communication infrastructure.

The example of Ukraine, a cyber attack on the Ukrainian power supply system in 2015 left more than 225,000 people across the country without power for 3 hours, highlighting the serious risks to national security. Although the power outages lasted only a few hours, some critical equipment at Ukrainian substations could not be controlled remotely for a long time, requiring manual control.

International Experience in Cybersecurity Development

Many countries have recognized the importance of investing in cybersecurity to ensure economic growth and national security. Let's look at some examples:

The United States has long been a leader in this area. It has implemented a cybersecurity strategy that includes not only protecting government and commercial entities, but also incentivizing technology companies. This has allowed the United States to strengthen its key economic sectors and increase investor confidence, which has contributed to the country’s prosperity.

Israel is known as one of the world's leading centers in the field of cybersecurity. The state is actively developing the cyber technology sector, which not only allows the country to protect itself from external threats, but also attracts significant investment, stimulating economic development.

Estonia, after a series of cyber attacks in 2007, invested heavily in building a resilient digital infrastructure. They established cyber defense centers, such as the NATO Cyber Center in Tallinn, and provided a high level of protection for the public and private sectors. This allowed Estonia to develop a digital economy, become an example for other countries in introducing digital services, such as online voting and digital healthcare. Thanks to this, the country attracted the attention of investors and created favorable conditions for economic growth.

South Korea and Singapore have also been actively developing their cyber defense systems, which has allowed them to protect key infrastructures and attract international companies and investors, promoting economic prosperity.

Application of experience for Uzbekistan

International experience in cybersecurity provides many valuable lessons that can be adapted to the conditions of Uzbekistan. The development of cybersecurity in our country is not only of great strategic importance for data protection, but can also contribute to strengthening the digital economy, increasing trust in government and commercial online services, and creating new jobs in the IT sector.

1. Economic benefits of cybersecurity development. One of the main lessons that can be learned from the experience of countries such as Israel and the United States is that the development of cybersecurity is directly related to economic growth. In Uzbekistan, where digitalization is only gaining momentum, investing in cybersecurity can contribute to the accelerated development of the digital economy. The introduction of reliable data protection

mechanisms will create a safer environment for business, which in turn will attract foreign investment.

To this end, the government and the private sector need to actively develop cybersecurity programs aimed at protecting banking systems, e-commerce platforms, and government online services. For example, creating national cybersecurity standards and supporting startups specializing in information security will help to form a strong digital ecosystem.

2. Protecting critical infrastructure and national security. The experiences of Estonia and South Korea highlight the importance of protecting critical infrastructures such as energy, transport, and healthcare. In Uzbekistan, as in other countries, these sectors are increasingly dependent on digital technologies and networks. Implementing best global practices in protecting such infrastructures can help avoid serious consequences from cyberattacks.

The example of Ukraine, where a cyberattack on the power grid caused serious power outages, shows that such threats are real and can be aimed at weakening national security. For Uzbekistan, protecting critical infrastructures should be a priority. An important step could be the creation of specialized cyberattack response centers that will monitor and prevent cyber threats.

3. Increasing citizen and business trust in digital services. As the experience of Estonia has shown, cyberattacks can undermine citizen trust in government and commercial online services. In Uzbekistan, where the digitalization of government services is just beginning to develop, it is essential to create reliable security systems so that citizens and companies can be confident in the security of their data.

To this end, the government should focus on creating a comprehensive data protection system, from encrypting user information to regular security audits. State programs to train employees in cybersecurity and encourage the introduction of digital security passports for companies will also help build trust in the country's digital infrastructure.

4. Developing human resources. Investing in human capital is one of the key factors in the success of Israel and Singapore. Uzbekistan also needs to focus on training cybersecurity specialists. Universities and educational institutions should develop specialized training programs that will help create a qualified workforce in this area. This will create the conditions for the formation of its own domestic market for cybersecurity solutions.

Developing educational programs on cybersecurity at the level of universities and specialized IT schools can help Uzbekistan not only provide protection against cyber threats, but also export this knowledge outside the country, which will contribute to economic development.

5. Cooperation with international organizations. Given the global nature of cyber threats, it is important for Uzbekistan to establish close cooperation with international organizations in the field of cybersecurity. The experience of the United States and European countries shows that effective protection is possible only through the exchange of experience and coordination of efforts with other states.

Uzbekistan can benefit from cooperation with organizations such as the European Cybersecurity Agency (ENISA) or the NATO Cyber Center. Information exchange, participation in international cybersecurity forums and joint exercises can help improve the level of protection of critical facilities.

References:

1. https://ru.wikipedia.org/
2. https://cyberpark.uz/news/bolee-13-mln-kiberatak-v-god-v-uzbekistane-viyavili-skachok-chisla-xakerskix-atak
3. https://cyclowiki.org/wiki/%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0_%D0%BD%D0%B0_%D1%83%D0%BA%D1%80%D0%B0%D0%B8%D0%BD%D1%81%D0%BA%D1%83%D1%8E_%D1%8D%D0%BD%D0%B5%D1%80%D0%B3%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%83_2015_%D0%B3%D0%BE%D0%B4%D0%B0
4. https://www.bbc.com/ukrainian/vert-fut-russian-40509165
5. https://cys-centrum.com/ru/news/black_energy_2_3
6. https://www.golosameriki.com/a/estonia-un-cyber-security/5432333.html
7. https://baltnews.com/v-ehstonii/20240411/1026267002/Rekordnaya-kiberataka-na-estonskie-sayty-obyavlena-okhota.html
8. https://www.epravda.com.ua/rus/news/2022/08/18/690548/
9. https://www.xabar.uz/ru/xorij/ucheniya-po-kiberbezopasnosti-nato-nachalis-v-estonii
10. https://rus.err.ee/1609445360/kiberataki-na-gosuchrezhdenija-jestonii-osuwestvila-rossijskaja-voennaja-razvedka
11. https://www.rbc.ru/society/25/05/2017/592644ee9a79477171fea588
12. https://huntsmansecurity.com/blog/wannacry-petya-et-al-protecting-your-organisation-from-ransomware/.