ENHANCING FOREIGN LANGUAGE LEARNING THROUGH TECHNOLOGY-FOCUSED CONTENT: AN EDUCATIONAL APPROACH TO CYBERSECURITY AND CYBERCRIME

M.R.Mukhitdinova
English Language Department
University of World Economy and Diplomacy
Tashkent, Uzbekistan
mmuxitdinova@uwed.uz
M.Nurmatilloyev Nurmatilloyevmuhammadali535@gmail.com
M.Muzaffarbekov muzaffarbekov05@icloud.com
J.Obidov jasurbekobidov1155@gmail.com
N. Asadbek ferexalone76@gmail.com
University of World Economy and Diplomac,
International Law students,

Abstract: This article discusses the growing threat of cybercrime in the modern world, where globalization and technology are rapidly developing. The paper focuses on different types of cybercrimes, such as cyberterrorism, financial fraud, online gambling among youth, spreading viruses, hacking passwords, and stealing credit card or bank information. It also presents ways to prevent these threats, ensure information security, and create a safe and trusted digital environment.

Keywords: Cybercrime, Cybersecurity, Information security, Digital literacy, Internet fraud, Personal data protection, Legal analysis, Cyber threat, Information technology, Cyber attacks, National security, Survey analysis, Uzbekistan legislation, Cyber prevention, Cybersecurity policy.

Introduction

In today’s era of globalization and digital technology, cybercrime has become one of the most serious global threats. With the development of the Internet, mobile communication, and artificial intelligence, crime has also moved into cyberspace, becoming more complex and widespread. Cybercrime refers to crimes committed through computer networks and information technologies. These include fraud, identity theft, spreading malware, financial attacks, and online threats. In Uzbekistan, this issue is also important — the laws “On Cybersecurity” and “On Information Security” provide a legal framework for fighting cybercrime. (Kalbayeva, E. 2022). Cybersecurity is a set of technical, legal, and organizational measures to protect personal and government information. Its main goals are to ensure the confidentiality, integrity, and availability of information. The relevance of this topic lies in the fact that as the number of cybercrimes grows, it is necessary to increase digital literacy and strengthen protection mechanisms.

In recent years, both in Uzbekistan and globally, cybercrimes have become more frequent and sophisticated. Criminals now target not only financial systems but also government databases and personal data. This shows the existence of legal gaps, technical weaknesses, and a lack of digital literacy among users.

The increase in cybercrimes has led to the need for the concept of cybersecurity. Cybersecurity is the protection of computer systems, networks, and digital data from unauthorized access, damage, theft, or loss. Its main principles are confidentiality, integrity, and availability. (Akbarova, M. Sh. 2023). Today,cybersecurity is not only an IT issue but also a matter of national security, economic stability, and public trust. Many countries such as the USA, the UK, and South Korea have developed national cybersecurity strategies. In 2001, the first international document against cybercrime was adopted.

B.Shokirov said: “Efforts to exploit the internet for destabilizing countries are increasing. Social networks and their backers sometimes interfere in domestic affairs under the guise of freedom and openness. Consequently, experts are now suggesting transitioning to a new internet model that limits user anonymity, which would help curb online crimes. Countries like China and Russia are already developing or implementing closed, state-controlled network systems”. (Shokirov, B. 2023). This idea that highlights growing concerns about the misuse of the internet to influence or destabilize states. It argues that social networks and the actors behind them may intervene in a country’s internal affairs while claiming to promote openness and freedom. As a response, some experts propose a new internet model with reduced user anonymity, aiming to limit cybercrime and external manipulation. The text also notes that countries such as China and Russia are already moving toward tightly controlled, state-regulated internet systems, illustrating a global trend toward digital sovereignty and stricter information governance. (Karimov, A. & Tursunova, N. 2023).

Large companies like **Google, Microsoft, and Meta** are introducing new technologies to protect user privacy. Uzbekistan has also joined this process — since 2020, several laws such as “On Informatization” and related regulations have been adopted. (Law of the Republic of Uzbekistan, 2022).The **Ministry of Internal Affairs** and the **State Security Service** have created special cybersecurity departments.

The term *cybercrime* first appeared in the 1980s. According to British criminologist **David Wall**, cybercrimes are divided into three main groups: Crimes **against** computers, Crimes **using** computers, and Crimes **where computers are the object** of the offense. (Pollach, I. 2021).

Research Methodology

The study used **qualitative** and **empirical** methods. The main methods include:

1. **Legal analysis** – analysis of key laws and regulations in Uzbekistan.

2. **Comparative analysis** – comparing Uzbekistan's experience with that of the USA, Russia, and European countries.
3. **Empirical method** – based on a survey of 31 participants conducted via Google Forms.
4. **Theoretical basis** – includes Rational Choice, Opportunity, Social Control, and Routine Activity theories.

The survey was anonymous and intended only for research purposes. It consisted of 12 questions divided into four parts:

a) General social information (Q1–2)
b) General questions about cybercrime (Q3–6)
c) Internet problems and legal issues (Q7–9)
d) Responsibility for identifying cybercrime (Q10–12)

Participants and General Awareness

Item	Result
Number of respondents	31 people
Gender	More males than females
Main age group	Mostly 15–20 years old
Older age groups	Fewer participants (21–25, 26–30, 30+)
Understanding of cybersecurity	83.9% understand it correctly
Do not clearly understand	About 9.7% still confuse it with other tec concepts

Most respondents are young and already understand cybersecurity well.

Cybercrime, Places, and Personal Data

Topic / Question	Main Result
Where cybercrimes happen most	48.4% banking, 45.2% social networks
What is cybercrime?	7.4% say unauthorized account access is crime
Misunderstanding	1% think forgetting a password is cyberc
Where they leave personal data	35.5% state portals, 35.5% nowhere
Reactions to unknown links	54.8% do not open unknown links

People think cybercrime happens mainly in banks and social networks and are careful with personal data.

Education, Responsibility, and Passwords

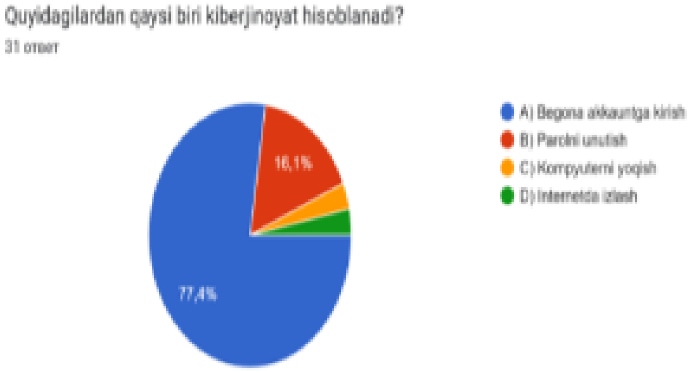
Topic / Question	Main Result
Where cybersecurity should be taught	71% say schools and universities
Who must fight cybercrime?	61.3% say every user is responsible
Who to contact after cybercrime	51.6% police
Understanding of strong passwords	83.9% choose a strong password

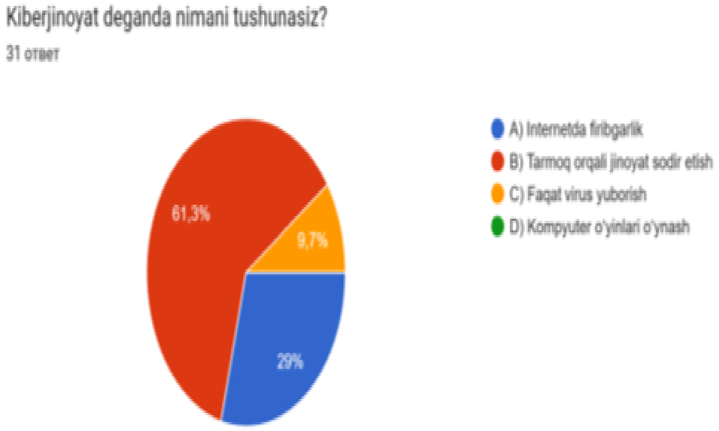
Most people believe cybersecurity education should start early and that every user must stay responsible.

Picture 1. Survey on an Educational Approach to Cybersecurity and Cybercrime

The survey results show the following key findings:

1. **Awareness** – 83.9% of respondents know what cybersecurity means.
2. **Fields of cybercrime** – 48.4% mentioned the banking system, 45.2% said social media.
3. **User behavior** – 54.8% avoid clicking on unknown links.
4. **Responsibility** – 61.3% believe that fighting cybercrime is the duty of every user.
5. **Password security** – 83.9% know the importance of using strong passwords.





Discussion

The findings show that awareness of cybercrime in Uzbekistan is growing, but **practical protection measures** are still insufficient. This is due to **legal gaps**, **technical weaknesses**, and **human factors**.

Around 65% of employees cannot detect suspicious messages, but **training programs** can reduce this risk by 30%. The results confirm the need to include cybersecurity education in academic programs.

International experience shows that in countries like the USA, Japan, and South Korea, effective cybersecurity policies are based on the integration of education, technology, and law. Such an approach would also be effective for Uzbekistan.

Conclusion

Cybercrime is an inevitable problem of modern society. To reduce it, it is important to:Increase digital literacy among citizens, Update the legal framework to international standards, Strengthen technical infrastructure, Introduce cybersecurity subjects into the education system.

In addition, preventive education and international cooperation should be enhanced. Uzbekistan already has a solid legal foundation, but practical implementation needs to be further improved.

References

1. Shokirov, B. (2023). Cybercrime: Social and Economic Risks. https://zenodo.org/record/17021

2. Akbarova, M. Sh. (2023). Cybersecurity Against Cybercrime. https://zenodo.org/record/17021

3. Kalbayeva, E. (2022). Legal Responsibility for Cyber Theft in Uzbekistan. https://zenodo.org/records/15624813

4. Bobokulov, A. (2023). The Impact of Social Engineering on Cybercrime. https://zenodo.org/records/14194717

5. Karimov, A. & Tursunova, N. (2023). Psychological Aspects of Cyber Fraud. https://zenodo.org/records/14194717

6. Pollach, I. (2021). Cybercrime and Human Rights: Legal Responses. https://zenodo.org

7. Law of the Republic of Uzbekistan (2022). On Cybersecurity. https://lex.uz/docs/5959427