UDC 327
https://doi.org/10.48371/ISMO.2023.54.4.005
IRSTI 11.04

CYBERSECURITY: IMPORTANCE FOR KAZAKHSTAN AND INTERNATIONAL EXPERIENCES

*Jekebayeva M.[1], Iztaeva V.A.[2], Anassova K.[3], Manapbayev N.[4]
*[1]candidate of philosophical sciences, associate professor of Kazakh Ablai khan University of International relations and world languages, Almaty, Kazakhstan, e-mail: 81makpal@mail.ru
[2]candidate of philosophical sciences, associate professor of Kazakh Ablai khan University of International relations and world languages, Almaty, Kazakhstan, e-mail: iztaeva.venera@mail.ru
[3]candidate of philosophical sciences, associate professor of Satbayev KazNRTU, Almaty, Kazakhstan, e-mail: anasova_76@mail.ru
[4]doctaral student of Abai KazNPU Almaty, Kazakhstan, e-mail: nur.ak.80@mail.ru

Abstract. This article examines the issue of cyber security and the main threats that young people face in the digital age, and offers recommendations and strategies for ensuring cyber security. The article is written based on the results of the analysis of the survey data among young people. The article also considers the role of the state, educational institutions and the private sector in ensuring cyber security, as well as the importance of international cooperation. Since cyber security is a field related to the protection of information and data from unauthorized access, use and destruction, the importance of international practices in Kazakhstan and abroad is deeply studied.

The main idea and goal of the authors of the article is to inform young people about the processes of cyber security prevention measures, educate and engage them in digital literacy, and provide a safe digital environment. In the article, the authors draw conclusions about the need to develop effective measures to increase awareness among young people of Kazakhstan and foreign international practices that provide cyber security and ensure security in the digital space.

Keywords: cybersecurity, digital age, strategy, information, security, viruses, hacker attacks, cyberbulling

Basic provisions

In today's digital world, where information technology is rapidly developing, cyber security is a very relevant issue. This is because cyber security includes not only protecting data, but also preventing cyber attacks, ensuring the confidentiality, integrity and availability of information. Cyber security includes aspects such as protecting personal data, preventing phishing attacks, fraud and malware, ensuring safe use of social media, and protecting against cyber espionage. In the modern digital world, where information technologies permeate all spheres of our life, cybersecurity is becoming one of the most urgent and important problems. The relevance of the problem of cybersecurity in the world and Kazakhstan is not controversial.

As a country with a dynamically developing digital infrastructure, Kazakhstan has also become the target of cyber threats. The spread of the Internet and mobile devices among young people has led to an increase in the number of users who have

been subjected to various cyber attacks. Insufficient awareness of cybersecurity and the misuse of technology make young people vulnerable. Therefore, studying the problem of cybersecurity among young people in Kazakhstan is an urgent task.

Introduction

The main concept of article is to find out the opinions and experiences of young people regarding cyber security, to know the questions covering various aspects of digital security, awareness of risks, protection methods, behavioral habits and acceptance of the importance of security in the online environment, to make a number of recommendations and strategies that contribute to the improvement of cyber security. Hackers, cyberattacks, identity theft, and the spread of malware all threaten not only financial institutions and large corporations, but also every single user on the Internet. Cybercrime has become an international problem that requires joint efforts on the part of States, organizations and society as a whole.

Cyber security is an important area concerned with protecting information and data from unauthorized access, use and destruction. For describing the conception about cyber security we must to develop the theoretical basis of information and lectures on this issue for students and people of any age to form their political and ethical literacy about "cyber security" and cyberbullying in the digital society. We also must to search for materials from literature and libraries developed and studied by domestic and foreign social and humanitarian sciences on the issue of the article on "cyber security" in the digital society. Nowadays most important thing to determine the level of awareness of young people about the possible risks associated with the use of the Internet and digital technologies.

Description of materials and methods

The purpose of this study is to analyze and study the problem of cybersecurity among young people in Kazakhstan. Main research objectives:

- determine the level of awareness of young people about the possible risks associated with the use of the Internet and digital technologies.
- to study young people's perception of the importance of protecting their personal data and privacy in an online environment.
- identification of the main threats and problems facing young people in the field of cybersecurity.
- analysis of the effectiveness of existing measures to ensure cybersecurity among young people in Kazakhstan.
- study the opinions and preferences of young people regarding methods and means of protection in the digital age.
- develop recommendations and strategies to raise awareness and protect young people in the field of cybersecurity.

The study uses survey and data collection methods to obtain representative information about the opinions and experiences of young people regarding cybersecurity. The survey includes questions covering various aspects of digital security, such as risk awareness, security practices, behavioral habits, and acceptance of the importance of security in an online environment.

The results of the study will be analyzed in order to identify the main problems and trends in the field of cybersecurity among young people in Kazakhstan. Based on the data obtained, recommendations and strategies will be developed to help raise awareness and protect young people in the digital age. These guidelines and strategies can be used as a basis for developing educational programs, awareness campaigns, and legal activities aimed at improving cybersecurity among young people.

The problem considered in this article was analyzed and studied on the basis of library and Internet materials using historical analytical and descriptive methods from the point of view of sociology, law, ethics, philosophy, and politics. Currently, inaccordance **with Article 20 of the Constitution of the Republic of Kazakhstan,** within the framework of information culture, an analysis of the ideas of information literacy introduced by the International Association of School Libraries (IASL) in 2006 ideas is carried out, the approach of each researcher to the formulation "Information Society" analysed. About cybersecurity and cyber bulling were written by R. Ayris, D. Bell, W. Dysard, M. Castells, J. Martin, E. Toffler, a well-known sociologist of the Japanese country Y. Masuda in his work "Information Society as a post-industrial society". A historical comparison and comparison, a historical description and methods of analysed to the main factors that influenced the formation of changes and intellectuals that became its driving force are carried out.

Results

Cybersecurity: key concepts and threats

Cybersecurity is an important area related to the protection of information and data from unauthorized access, use and destruction. In today's digital world, where more and more spheres of life are becoming dependent on information technology, ensuring security in the online environment is becoming an indispensable task.

The definition of “cybersecurity” includes not only data protection, but also the prevention of cyber attacks, ensuring the confidentiality, integrity and availability of information. Cybersecurity includes aspects such as protecting personal data, preventing phishing attacks, fraud and malware, ensuring safe use of social networks, and protecting against cyber espionage [1].

In the digital age, there are a number of major threats and dangers facing both individual users and organizations. These include cyber attacks, including viruses, Trojans, malicious codes, and the file-of-attack service. In addition, there are threats in the form of identity theft, phishing, social engineering, and cyber espionage. The spread of disinformation and fake news is also a serious problem in the digital environment.

Young people play an important role in cybersecurity. With the increasing use of information technology and social media among young people, they are becoming particularly vulnerable to various cyber threats. In addition, young people are one of the main forces behind the creation and application of innovative approaches and technologies in the field of cybersecurity. Therefore, informing, educating and involving young people in cybersecurity processes are important steps towards ensuring a secure digital environment.

Young people need to be aware of the potential dangers and dangers in the online world, and have the knowledge and skills necessary to protect their personal information and data. Regular educational programs and cybersecurity trainings help young people develop skills in recognizing phishing emails, using passwords securely, protecting their devices from malware, and much more.

In addition, young people can actively participate in public debates about cybersecurity, introduce new technologies and methods of protection, and contribute to the creation of policies and legislation aimed at ensuring security in the digital environment. Young professionals in the field of information security can become an important link in the development and implementation of innovative solutions for data protection and prevention of cyber attacks [2].

Thus, young people's understanding of the importance of cybersecurity and their active involvement in this area is crucial to creating a secure and reliable digital era. Joint efforts of the state, educational institutions, organizations and young people will help achieve significant results in the field of information and data protection in Kazakhstan.

Awareness level: The majority of respondents are not sufficiently aware of the potential dangers and risks in the online environment. Some survey participants do not know how to protect their personal data and doubt the reliability of the online platforms they use.

1. *Security practices*: Despite the low level of awareness, many respondents stated that they take certain measures to ensure their cybersecurity. These measures include using complex passwords, restricting access to devices and accounts, and installing antivirus programs.

2. *Perception of threats*: the survey results showed that the majority of respondents understand that threats exist in the online environment. They identified various types of threats, including viruses and malware, hacker attacks, cyber fraud, and privacy breaches. This demonstrates a certain level of awareness and vigilance among young people regarding cybersecurity.

3. *Interpretation and analysis of the obtained data*

Explaining the survey results will provide a better understanding of the current cybersecurity situation among young people in Kazakhstan. A low level of awareness and incomplete understanding of how to protect your data is a serious problem that requires further action. However, the positive aspect is that young people are aware of the threat and are interested in protecting their cybersecurity [3].

Due to the fact thatақалаthis topic is quite extensive, recommendations and strategies for strengthening cybersecurity among young people in Kazakhstan will be studied and proposed in the future. The analysis of the obtained data will be used in the development of these proposals, taking into account the needs and characteristics of the youth audience.

Cyber security issues in Kazakhstan

Vulnerabilities and threats in cyberspace in Kazakhstan

Kazakhstan, like many other countries, faces various vulnerabilities and threats in cyberspace. One of the main vulnerabilities is the lack of awareness of users about the methods of protecting their data and the general rules of safe behavior

on the network. Many young people are unaware of the risks associated with using the Internet and do not have sufficient knowledge of cybersecurity measures.

Kazakhstan is also experiencing an increase in cases of cybercrime, including hacker attacks, phishing attacks, cyber fraud and identity theft. Cybercriminals actively use the latest technologies and methods to carry out their malicious activities. The presence of vulnerabilities in Kazakhstan's cyber infrastructure creates additional risks for citizens and organizations.

Shortcomings in cybersecurity legislation and policies

Despite some achievements in the field of cybersecurity, Kazakhstan still has shortcomings in the legislation and policies governing this area. Some legislative acts do not meet modern challenges and technological changes, which weakens the effectiveness of cybersecurity measures.

In addition, there is a mismatch between the public and private sectors in the field of cybersecurity. A clear lack of understanding of the role and responsibilities of each sector leads to a lack of separation and coordination in the actions taken.

The role of the State and the private sector in ensuring cybersecurity

Effective cybersecurity efforts in Kazakhstan require cooperation and collaboration between government agencies and the private sector. The State should develop and implement strong and comprehensive policies that ensure adequate protection of the country's cyberspace.

Government organizations should actively work to improve legislation, as well as develop cybersecurity strategies and plans. It is important to ensure that sufficient financial and human resources are available to effectively implement these strategies.

However, the state cannot clearly solve all cybersecurity problems. The private sector should also be actively involved in ensuring security in the digital age. This includes developing and applying cutting-edge technologies, investing in employee training, building collaboration networks, and sharing information about cyber threats.

It is also necessary to raise awareness and knowledge of young people in the field of cybersecurity. It is important to conduct educational programs, seminars and trainings that will help young people develop safe online behavior skills and protect their data.

As a result, effective cybersecurity in Kazakhstan requires joint efforts of the state, the private sector and young people. Only through cooperation, education and sustainable development can we successfully counter the threats of the digital age and ensure the security of our country [4].

Discussion

Cybersecurity recommendations and strategies

The first thing to do when it comes to cybersecurity recommendations and strategies:

- it would be more correct to teach zh Astar the basics of cybersecurity on the network;

- Educational institutions, including schools, higher education institutions and training centers, should implement specific cybersecurity programs that include the basic principles of safe online behavior, personal data protection, detection and prevention of cyberthreats;

- Regular training events and seminars should be held in Astara to preserve knowledge and skills about cybersecurity;

on cooperation between public authorities, the private sector and educational institutions орнатқан жө;

- effective security management requires cooperation and partnership between government agencies, the private sector and educational institutions.

public authorities should actively cooperate with representatives of the private sector and educational institutions, exchange information on new threats and trends in cyberspace;

- it is necessary to create a platform for public dialogue and exchange of experience, where different parties can jointly develop cybersecurity strategies and policies;

- new technologies and tools need to be developed to prevent threats.

The rapid development of technology requires the constant development of new tools and methods for preventing and detecting cyber threats. Innovative solutions such as artificial intelligence systems, analytical tools, and automated security systems can significantly improve the effectiveness of network protection. The State and private sector should invest in research and development of new technologies and tools, as well as in supporting startups and innovative projects in the field of cybersecurity. This approach not only increases the level of protection against cybersecurity, but also contributes to the development of the domestic cybersecurity industry [5].

International cooperation in the field of cybersecurity

In the digital age, when cyber threats are blurring borders, international cooperation is becoming a key factor in ensuring cybersecurity. The global community is aware of the need to join forces to prevent and counter cyber threats. In this chapter, we will explore the importance of international cooperation and its-role in combating cyber threats.

Initially, international cooperation plays an important role in sharing information about recent threats and attacks. Thanks to the exchange of experience and threat data, you can quickly respond to new methods and tactics of cybercriminals. Coordination of actions and joint response to events are possible thanks to international cooperation. Organizations and Governments can share information about events, vulnerabilities identified, and successful cybersecurity practices.

In addition, the development of international standards and regulations plays an important role in ensuring cybersecurity around the world. Common standards and accepted norms allow you to establish common rules of the game and consistent ways to protect information and networks. International organizations and forums such as the International Telecommunication Union (ITU), the United Nations (UN),

and the International Telecommunication Union (ITU) are actively working to develop and adopt cybersecurity standards [6].

Thus, international cooperation is an integral part of the effective fight against cyber threats. The exchange of information, coordination of actions and development of international standards will strengthen collective efforts to ensure cybersecurity at the global level. Only through joint action and collaboration can we effectively protect our digital systems and data from cyber threats.

In the sociological survey "**How do you understand cybersecurity and cyberbullying?**" took part 87 students of KazUIRand WL 1-2 course and 8 teachers.

Date of the survey :11-18.11.2023.

After f**ocus-group interview and** sociological survey, we get information about cybersecurity and cyberbullying.

Question No. 1 Indicate the life values closest to you from among the proposed ones?

1) What is cyberbullying? How do you understand?

- is bullying and harassment using digital technology.

-It can be on social networks, messaging applications, gaming platforms and mobile phones.

2)What is the purpose of cyberbullying?

These are repeated episodes whose purpose is to intimidate, anger, or humiliate the harassed and are accomplished by

- spreading false information or posting indecent photos of someone on social networks;

send harassing messages or threats through messaging platforms;

- impersonate another person and send obscene messages on their behalf.

3) How does online harassment affect a person?

When a person is being harassed online, it feels like they are being harassed everywhere, even at home.

It seems to him that there is nowhere to hide from those who hurt him.

Such actions can have long-term consequences:

- Psychological - a person feels sad, uncomfortable, looks stupid to himself and becomes angry.

- Emotional - a person becomes ashamed of his hobbies or loses interest in them.

- Physiological - suffer from adverse conditions such as fatigue (sleep problems) or stomach ache and headache.

Fear of being ridiculed or persecuted by others can prevent sufferers from talking about or solving problems

4) Reasons for cyberbullying

- Psychological factors: Some people may choose to use cyberbullying to release negative emotions related to their insecurities, moods, or other psychological issues. Attacking others can be a way for them to cope

- Group effect: When some people see others engaging in aggressive behavior online and that behavior is supported or unchecked by others, they may be motivated to engage in similar behavior.

Conclusion

In this article, we want to summarize our article on cybersecurity among young people in Kazakhstan and draw some conclusions based on the results.

In the survey, we found that there is a significant lack of knowledge and awareness among young people about the potential dangers associated with the use of the Internet and digital technologies. The majority of respondents do not know how to protect their personal data and do not fully understand the importance of cybersecurity.

The relevance of the problem of cybersecurity among young people is indisputable. In our digital society, which is closely connected to the Internet and network technologies, the protection of personal information and countering cyber threats are becoming an integral part of our lives. In addition, given the rapid development of technologies and the constant emergence of new threats, it is important to understand that ensuring cybersecurity is an ongoing process that requires constant updating of knowledge and skills.

Based on the research results of the article, we have identified a number of recommendations and strategies that contribute to improving cybersecurity among young people in Kazakhstan. First, it is necessary to actively implement educational programs and courses aimed at raising awareness of cybersecurity among young people. This may include training in the basics of safe Internet use, protecting personal data, and detecting phishing attacks.

Secondly, to create an effective system of protection against cyber threats, it is important to develop cooperation between government agencies, the private sector and educational institutions. This includes sharing information about emerging threats, developing common strategies and action plans, and supporting and supporting the implementation of innovative technologies and tools.

Finally, an effective fight against cyber threats requires active cooperation at the international level. This includes the development of international standards and regulations, joint trainings and exercises, as well as the exchange of experience and best practices between different countries.

Thus, ensuring cybersecurity among young people is an urgent and important task. In the field of cybersecurity, all necessary measures should be taken to inform, educate and support young people. Only through joint efforts of the state, educational institutions, the private sector and society as a whole can we ensure a safe and reliable digital space for young people and society as a whole.

REFERENCES

[1] Cavelty M., Wenger A. Cybersecurity politics. Socio-technological transformations and political fragmentation. - New York, Routledge, 2022. - 286 p.

[2] Назарбаев Н. Стратегия становления постиндустриальногообщества и партнерство цивилизаций. – Москва: Экономика, 2008. - 398 с.

[3] Шаймарданова З.Д. Трансформация подходов к обеспечению безопасности // Известия КазУМОиМЯ имени Абылай хана", серия "Международные отношения и регионоведение". - 2018. - № 4.- С.7-13.

[4] Белгібаев Д.Т. Ақпараттық қоғам және мәдениет // ҚазҰУ хабаршысы. Философия сериясы. Мәдениеттану сериясы. Саясаттану сериясы. – 2011. - № 1 (36). – 166 –б.

[5] Джекебаева М.А. Тұңғыш Елбасы саясатындағы «Цифрлы Қазақстан» бағдарламасы және заманауи технологиялар // Известия КазУМОиМЯ имени Абылай хана", серия "Международные отношения и регионоведение". – 2019. - № 3 (37). - 40-48 бб.

[6] Джекебаева М.А., Турсунбаева С., Рсалдина Г. «Цифрлы Қазақстан», заманауи технологиялар және жастар» // Асфендияров атындағы ҚазҰМУ Хабаршысы. 2018. - № 4. -300-303 бб.

REFERENCES

[1] Cavelty M., Wenger A. Cybersecurity politics. Socio-technological transformations and political fragmentation. New York, Routledge, 2022.

[2] Nazarbaev N. Strategija stanovlenija postindustrial'nogoobshhestva i partnerstvo civilizacij [Strategy for the formation of a post-industrial society and partnership of civilizations]. Moskva: Yekonomika, 2008 [in Russ.].

[3] Shaymardanova Z.D. Transformatsiya podkhodov k obespecheniyu bezopasnosti [Transformation of approaches to ensuring security]. Izvestiya of Kazakh Ablai khan University of IR and WL, seriya «Mezhdunarodnyye otnosheniya i regionovedeniye», 2018, № 4, s.7-13 [in Russ.].

[4] Belgıbaev D.T. Aqparattyq qoğam jäne mädeniet [Information society and culture]. QazŪU habarshysy. Filosofia seriasy. Madeniettanu seriasy. Saiasattanu seriasy. 2011, No.1 (36), b.166 [in Kaz.].

[5] Jekebaeva M.A. Tungysh Elbasy saiasatyndagy «Sifrly Qazaqstan» bagdarlamasy jane zamanaui tehnologialar ["Digital Kazakhstan" program and modern technologies in the policy of the first Head of State]. Izvestiya of Kazakh Ablai khan University of IR and WL, seriya «Mezhdunarodnyye otnosheniya i regionovedeniye», 2019, No.3 (37), b.40-48 [in Kaz.].

[6] Jekebayeva M.A., Tursunbaeva S., Rsaldina G. «Sifrly Qazaqstan», zamanaui tehnologialar jäne jastar». ["Digital Kazakhstan", modern technologies and youth"]. Asfendiarov atyndağy QazŪMU Habarshsy, 2018, № 4, b.300-303 [in Kaz.].

КИБЕРҚАУІПСІЗДІК: ҚАЗАҚСТАН ҮШІН МАҢЫЗЫ ЖӘНЕ ХАЛЫҚАРАЛЫҚ ТӘЖІРИБЕ

*Джекебаева М.А.[1], Изтаева В.А.[2], Анасова Қ.Т.[3], Манапбаев Н.[4]

*[1]философия ғылымдарының кандидаты, Абылай хан атындағы ҚазХҚжӘТУ қауымдастырылған профессоры, Алматы, Қазақстан
e-mail: 81makpal@mail.ru

[2]философия ғылымдарының кандидаты, Абылай хан атындағы ҚазХҚжӘТУ доценті, Алматы, Қазақстан, e-mail: iztaeva.venera@mail.ru

[3]философия ғылымдарының кандидаты, Қ.Сатбаев атындағы ҚазҰТЗУ қауымдастырылған профессоры, Алматы, Қазақстан
e-mail: anasova_76@mail.ru

[4]Абай атындағы ҚазҰПУ докторанты, Алматы, Қазақстан
e-mail: Nur.ak.80@mail.ru

Аңдатпа. Бұл мақалада киберқауіпсіздік мәселесі және цифрлық дәуірде жастар тап болатын негізгі қауіптер қарастырылып, киберқауіпсіздікті қамтамасыз ету бойынша ұсыныстар мен стратегиялар ұсынылған. Мақалада жастар арасында жүргізілген сауалнама деректерін талдау нәтижелеріне негізделе жазылған. Сондай-ақ мақалада киберқауіпсіздікті

қамтамасыз етудегі мемлекеттің, оқу орындарының және жеке сектордың рөлі, халықаралық ынтымақтастықтың маңыздылығы қарастырылған. Киберқауіпсіздік ақпарат пен деректерді рұқсатсыз кіруден, пайдаланудан және жойылудан қорғаумен байланысты сала болғандықтан, Қазақстанда және шетелдік халықаралық тәжірибелердің маңыздылығы терең зерттелген.

Мақала авторларының негізгі ойы мен мақсаты жастарды киберқауіпсіздік алдын алу шаралары процестеріне хабардар ету, цифрлік сауаттылыққа оқыту және тарту, қауіпсіз цифрлық ортаны қамтамасыз ету болып табылады. Авторлар мақалада киберқауіпсіздікті қамтамасыз ететін Қазақстанда және шетелдік халықаралық тәжірибелердің жастар арасында ақпараттандыруды арттыру және цифрлық кеңістікте қауіпсіздікті қамтамасыз ету бойынша тиімді шараларды әзірлеу қажеттігі туралы қорытынды жасайды.

Тірек сөздер: киберқауіпсіздік, цифрлық дәуір, стратегия, ақпарат, қауіпсіздік, вирустар, хаккерлік атакалар, кибербуллинг

КИБЕР БЕЗОПАСНОСТЬ: ЗНАЧИМОСТЬ КАЗАХСТАНСКИХ И ЗАРУБЕЖНЫХ МЕЖДУНАРОДНЫХ ОПЫТОВ

*Джекебаева М.А.[1], Изтаева В.А.[2], Анасова К.Т.[3], Манапбаев Н.[4]
*[1]кандидат философских наук, ассоциированный профессор КазУМОиМЯ им.Абылай хана, Алматы, Казахстан, e-mail: 81makpal@mail.ru
[2]кандидат философских наук, доцент КазУМОиМЯ им.Абылай хана, Алматы, Казахстан, e-mail: iztaeva.venera@mail.ru
[3]кандидат философских наук, ассоциированный профессор КазНИТУ имени К.Сатбаева, Алматы, Казахстан, e-mail: anasova_76@mail.ru
[4] Докторант КазНПУ имени Абая, Алматы, Казахстан
e-mail: Nur.ak.80@mail.ru

Аннотация. В данной статье рассматривается проблема кибербезопасности и основные угрозы, с которыми молодые люди сталкиваются в эпоху цифровых технологий, а также предлагаются рекомендации и стратегии обеспечения кибербезопасности. Статья написана по результатам анализа данных опроса среди молодежи. Также в статье рассматривается роль государства, образовательных учреждений и частного сектора в обеспечении кибербезопасности, а также важность международного сотрудничества. Поскольку кибербезопасность – это область, связанная с защитой информации и данных от несанкционированного доступа, использования и уничтожения, значение международной практики в Казахстане и за рубежом глубоко изучается. Основная идея и цель авторов статьи – информировать молодежь о процессах мер по предотвращению кибербезопасности, обучать и привлекать ее к цифровой грамотности, обеспечивать безопасную цифровую среду.

В статье авторы делают выводы о необходимости разработки эффективных мер по повышению осведомленности молодежи Казахстана и зарубежной международной практики, обеспечивающей кибербезопасность и обеспечение безопасности в цифровом пространстве.

Ключевые слова: кибербезопасность, цифровой век, стратегия, информация, безопасность, вирусы, хаккерские атаки, кибербуллинг.

Статья поступила 07.12.2023