A.U. Nussipova[1*] ID, G.K. Slanbekova[2] ID

[1]International Educational Corporation, Almaty, Kazakhstan
[2]Karagandy Buketov University, Karaganda, Kazakhstan
*e-mail: arai_nussipova@mail.ru

SOCIAL MEDIA LANDSCAPE IN THE REPUBLIC OF KAZAKHSTAN: NAVIGATING YOUTH BEHAVIOR AND ENSURING INFORMATION SECURITY

In today's digitally interconnected world, social media has emerged as a prominent force shaping the behaviors, attitudes, and interactions of youth populations worldwide. This research endeavors to explore the intricate relationship between social media engagement and cybersecurity within the context of the Republic of Kazakhstan.

The primary purpose of this scientific inquiry is to investigate the ways in which Kazakhstani youth engage with social media platforms and to assess the associated cybersecurity challenges and implications. Through a multidimensional approach, the study aims to delineate the main directions and ideas underlying the intersection of youth behavior on social media and the imperative of information security.

This research holds significant scientific and practical importance by shedding light on the evolving dynamics of social media usage among Kazakhstani youth and the corresponding cybersecurity risks. By identifying key patterns, vulnerabilities, and protective measures, this study seeks to inform policymakers, educators, and stakeholders about the urgent need for comprehensive strategies to safeguard the digital well-being of young individuals.

Employing a mixed-method research methodology comprising surveys, interviews, and data analysis, this study provides a comprehensive examination of social media dynamics and cybersecurity resilience among Kazakhstani youth. The main results and analysis reveal insights into the prevalent behaviors, perceptions, and attitudes of youth towards social media, alongside an assessment of cybersecurity vulnerabilities and mitigation strategies.

The research underscores the importance of proactive measures to enhance cybersecurity awareness, digital literacy, and regulatory frameworks to address the emerging challenges posed by social media usage among Kazakhstani youth. By contributing empirical evidence and actionable insights, this study enriches the relevant field of knowledge and informs policy interventions aimed at fostering a safer and more secure digital environment for youth in Kazakhstan and beyond.

Key words: Information security, cyber threats, online behavior, youth, digital technology, cyberbullying.

А.У. Нусипова[1*], Г.К. Сланбекова [2]

[1]Халықаралық білім беру корпорациясы, Алматы қ., Қазақстан
[2]Академик Е.А. Бөкетов атындағы Қарағанды университеті, Қарағанды қ., Қазақстан
*e-mail: arai_nussipova@mail.ru

**Қазақстан Республикасындағы әлеуметтік желілер:
Жастардың мінез-құлқын бағдарлау және
ақпараттық қауіпсіздікті қамтамасыз ету**

Қазіргі цифрлық әлемде бұл зерттеу әлеуметтік желілерге қатысу мен Қазақстан жастары арасындағы киберқауіпсіздік арасындағы күрделі байланысты зерттейді. Сауалнамалар мен деректерді талдауды қамтитын аралас зерттеу тәсілінің көмегімен зерттеу қазақстандық жастар арасында әлеуметтік желілерді пайдалануға байланысты заңдылықтарды, осалдықтарды және қорғау шараларын ашуға бағытталған.

Зерттеу екі мақсатқа қызмет етеді: жастардың мінез-құлқын, қабылдауын және әлеуметтік желілерге қатынасын түсіну және олардың онлайн әрекеттеріне тән киберқауіпсіздік тәуекелдерін бағалау. Осы аспектілерге тереңірек үңіле отырып, зерттеу саясаткерлерге, оқытушыларға және мүдделі тараптарға құнды ақпарат береді, бұл киберқауіпсіздік, цифрлық сауаттылық және нормативтік-құқықтық база туралы хабардарлықты арттыру үшін белсенді шаралар қабылдаудың шұғыл қажеттілігін көрсетеді.

Бұл зерттеудің нәтижелері маңызды ғылыми және практикалық мәнге ие, өйткені олар қазақстандық жастар үшін неғұрлым қауіпсіз цифрлық ортаны құруға бағытталған стратегиялық

шаралар үшін негіз болады. Эмпирикалық деректер мен практикалық ұсыныстардың арқасында зерттеу осы саладағы білімді кеңейтуге ықпал етеді және жастардың әлеуметтік желілермен өзара іс-қимылына және оның Қазақстандағы киберқауіпсіздік үшін салдарына байланысты өзекті мәселелерді шешеді.

Сайып келгенде, бұл зерттеу әлеуметтік желілердің динамикасы туралы түсінігімізді байытып қана қоймайды, сонымен қатар киберқауіпсіздік тәуекелдерін азайту және Қазақстанда және одан тыс жерлерде жастардың цифрлық әл-ауқатын қорғау жөніндегі мақсатты шараларды әзірлеуге ықпал етеді.

Түйін сөздер: Ақпараттық қауіпсіздік, киберқауіптер, желідегі мінез-құлық, жастар, цифрлық технологиялар, кибербуллинг.

А.У. Нусипова[1*], Г.К. Сланбекова[2]
[1]Международная образовательная корпорация, г. Алматы, Казахстан
[2]Карагандинский университет им. акад. Е.А. Букетова, г. Караганда, Казахстан
*e-mail: arai_nussipova@mail.ru

Социальные сети в Республике Казахстан: регулирование поведения молодежи и обеспечение информационной безопасности

В нынешнем цифровом мире это исследование исследует сложную взаимосвязь между участием в социальных сетях и кибербезопасностью среди молодежи Казахстана. С помощью смешанного исследовательского подхода, включающего опросы и анализ данных, исследование направлено на расшифровку закономерностей, уязвимостей и защитных мер, связанных с использованием социальных сетей среди казахстанской молодежи.

Исследование служит двойной цели: понять поведение, восприятие и отношение молодежи к социальным сетям, а также оценить риски кибербезопасности, присущие их онлайн-деятельности. Углубляясь в эти аспекты, исследование предоставляет ценную информацию политикам, преподавателям и заинтересованным сторонам, проливая свет на острую необходимость принятия упреждающих мер по повышению осведомленности о кибербезопасности, цифровой грамотности и нормативно-правовой базы.

Результаты этого исследования имеют важное научное и практическое значение, поскольку они служат основой для стратегических мер, направленных на создание более безопасной цифровой среды для казахстанской молодежи. Благодаря эмпирическим данным и практическим рекомендациям исследование способствует расширению знаний в этой области и решает насущные проблемы, связанные с взаимодействием молодежи с социальными сетями и его последствиями для кибербезопасности в Казахстане.

В конечном итоге, это исследование не только обогащает наше понимание динамики социальных сетей, но и способствует разработке целевых мер по снижению рисков кибербезопасности и защите цифрового благополучия молодежи в Казахстане и за его пределами.

Ключевые слова: информационная безопасность, киберугрозы, поведение в сети, молодежь, цифровые технологии, кибербуллинг.

Introduction

From the point of view of the security object, information is a strategic resource and a critical element for its functioning, therefore, it must be properly protected at every stage of its processing: from its receipt to its transmission, storage, analysis, or use, respecting all elements of confidentiality. Information security issues have always been at the heart of government (Nussipova et al., 2023).

The rapid advancement of technology and the widespread accessibility of digital platforms have significantly transformed the landscape of communication and information dissemination in contemporary society. With this evolution comes a pressing concern regarding the influence of mass media, particularly on the youth demographic. The choice of this topic stems from the recognition of the critical role that mass media plays in shaping the worldview, values, and behavior of young people, and the inherent need to understand and address its impact.

The relevance of investigating the influence of mass media on youth behavior and information security is underscored by the increasing prevalence of digital communication channels and their pervasive presence in the daily lives of individuals, particularly the younger generation. Recognizing the lack of comprehensive research in this area, coupled with the emergent nature of new media platforms,

emphasizes the significance and timeliness of exploring this topic.

This study aims to define the object and subject of inquiry as the influence of mass media on the behavior and perceptions of youth in the Republic of Kazakhstan. The overarching goal is to examine the implications of mass media exposure on youth behavior, social values, and information security within the context of the modern digital landscape. To achieve this, the research will employ a multi-disciplinary approach, drawing from fields such as communication studies, political science, psychology, sociology, and media literacy.

The objectives of this study include:

Analyzing the patterns and content of mass media consumption among young people.

Investigating the impact of mass media exposure on the formation of youth behavior, social values, and perceptions.

Identifying the risks and challenges associated with information security in the digital age, particularly concerning youth engagement with online platforms.

Assessing the effectiveness of existing strategies and interventions aimed at promoting media literacy and enhancing information security among young people.

The research methodology will involve a combination of qualitative and quantitative methods, including surveys, content analysis and etc. These approaches will enable a comprehensive understanding of the complex dynamics between mass media, youth behavior, and information security.

Overall, this study seeks to contribute to the existing body of knowledge by shedding light on the intricate relationship between mass media influence and youth behavior, while also providing insights and recommendations for addressing the challenges posed by the digital media landscape.

Materials and methods

This article used a descriptive type of research to describe the characteristics of a group or individuals and their adoption of social media and the impact of the Internet on youth. During the research, surveys were conducted and opinions of young people were considered.

Participants: A total of 621 participants from various higher education institutions across Kazakhstan were surveyed. Participants were selected using a stratified random sampling technique to ensure representation from diverse geographical regions and educational backgrounds. A significant num-

ber of respondents in the survey were young people aged 18-25 (85.1%), as well as 26-35-year-olds (4.2%), 36-45-year-olds (3.2%), 44-55-year-olds (4.4%), and those aged 56 and older (2.9%).

Survey Instrument: The survey was conducted using Google Forms, an online survey platform provided by Google. A structured questionnaire was designed to collect data on participants' social media usage patterns, attitudes, and perceptions, as well as their awareness of cybersecurity risks. The questionnaire comprised both closed-ended and open-ended questions, allowing for quantitative and qualitative analysis of responses. Prior to administration, the questionnaire underwent pilot testing with a small group of students to ensure clarity and validity.

Procedure: The survey link was distributed to potential participants via email and social media channels, inviting them to complete the questionnaire using Google Forms (Google Forms [Online survey platform]). Participants were given the flexibility to respond at their convenience within a four-week period. Reminders were sent periodically to encourage participation and maximize response rates.

Research Methodology: The study employed a mixed-methods approach, combining quantitative analysis of survey data with qualitative insights from open-ended responses. Quantitative data analysis involved descriptive statistics to characterize social media usage patterns and cybersecurity awareness among participants. Qualitative data analysis entailed thematic coding of open-ended responses to identify recurring themes related to social media behavior and cybersecurity concerns.

Research Results: Analysis of the survey data revealed diverse patterns of social media usage among Kazakhstani youth, alongside variations in cybersecurity awareness. While a significant proportion of participants reported high levels of social media engagement, cybersecurity awareness varied considerably, with some expressing limited knowledge or concern about online security risks. These findings underscore the importance of targeted interventions to enhance cybersecurity education and promote responsible social media behavior among youth in Kazakhstan.

Literature review

Our research aims fall into two main categories:

Initially, we aim to construct a theoretical framework to guide the development of cybersecurity education initiatives. This framework hinges on

factors influencing cybersecurity awareness, knowledge, and behavior, which we investigated through a series of research questions, progressing from broad to specific:

Does Social Media Have a Positive or Negative Impact on Adolescents and Young Adults?

What is the extent of cybersecurity awareness among internet users?

What strategies do online users, particularly youths, adopt to counter cyber threats?

Furthermore, our study endeavors to provide practical suggestions for enhancing the effectiveness of cyber education programs, drawing on the findings derived from the theoretical framework.

Thanks to the proliferation of mobile internet, social networks have emerged as the primary source of information for a significant portion of the population, particularly among the younger demographic. Sociological studies conducted in 2021 revealed that 45.2% of respondents prefer to obtain information through social media platforms. The advent of global messengers and online platforms has fundamentally reshaped the landscape of the media industry. This transformation has coincided with a notable surge in the politicization of certain social networks, rendering them arenas for the dissemination of misinformation (Tokaev, 2023).

During the last decade, information technology such as mobile devices and digital applications have transformed daily life, facilitating diverse lifestyles in many areas. The ease of technology usage as well as the increased demand for online connectivity (in education, retail, tourism, and even autonomous vehicles) has expanded opportunities for internet usage on a global scale. Indeed, some of these uses include reading digital newspapers, surfing the web, utilizing search engines to find desired content, assisting recommender systems in the form of decision support tools, and using social media to name only a few (Zwilling et al., 2022).

Adults frequently blame the media for the problems that younger generations face, conceptually bundling different behaviors and patterns of use under a single term when it comes to using media to increase acceptance or a feeling of community. The effects of social media on mental health are complex, as different goals are served by different behaviors and different outcomes are produced by distinct patterns of use. The numerous ways that people use digital technology are often disregarded by policymakers and the general public, as they are seen as "generic activities" that do not have any specific impact. Given this, it is crucial to acknowledge the complex nature of the effects that digital technology has on adolescents' mental health. This empirical uncertainty is made worse by the fact that there are not many documented metrics of how technology is used. Self-reports are the most commonly used method for measuring technology use, but they can be prone to inaccuracy. This is because self-reports are based on people's own perceptions of their behavior, and these perceptions can be inaccurate. At best, there is simply a weak correlation between self-reported smartphone usage patterns and levels that have been objectively verified (Khalaf et al., 2023).

As a result, it is evident that the effects of digital technology, particularly social media, on adolescents' mental health are multifaceted and complex. While adults often attribute problems faced by younger generations to media use, it is essential to recognize that different behaviors and patterns of use yield varying outcomes. Unfortunately, policymakers and the general public often overlook the diverse ways in which individuals engage with technology, viewing them as generic activities with little specific impact. Moreover, the empirical uncertainty surrounding the effects of technology on mental health is exacerbated by the lack of documented metrics for measuring technology use. Self-reports, the most common method for assessing technology usage, may be prone to inaccuracies due to individuals' subjective perceptions of their behavior. Therefore, while self-reports provide valuable insights, their reliability may be limited. Moving forward, a nuanced understanding of the complexities involved in technology use and its impact on mental health is crucial for developing effective interventions and support systems for adolescents navigating the digital landscape.

Particular attention should be paid to the formulation "socio-psychological characteristics" – the not yet fully formed psyche and the inability to fully analyze information make young people one of the structures most susceptible to the influence of the media and mass culture. On the one hand, almost every representative of young people is a formed personality, but on the other hand, their worldview and values are largely changeable and easily change their vector under the influence of various factors. The media is just one of them. This is a source of a large amount of information, constantly updated, which actively notifies a person about the realities of the world around him, the most striking social processes and phenomena, which makes the media a tool for regulating public opinion, a means of manipulation. In the modern world, the degree of involvement of young people in the field of media

influence is higher than ever before, since now every person has the opportunity to use different types of channels for obtaining information. Young people here again act as a special social group due to their mobility and flexibility – they easily master new information channels, easily navigate the Internet, which allows for easy transition through various online media. That is, young people, having the opportunity to view as many media channels as possible, thereby subscribe themselves to even greater influence from these same channels. Young people spend the lion's share of their leisure time scrolling through social network feeds, watching videos and reading articles – it is obvious that the media are an integral part of the system that forms the hierarchy of value orientations and attitudes of modern youth (Dmitruk, 2022).

From another perspective, it is crucial to acknowledge the socio-psychological characteristics of young people, which render them particularly susceptible to the influence of media and mass culture. While adolescents may possess partially formed personalities, their worldview and values are often malleable and easily influenced by various factors, with media being a significant contributor. Media serves as a constant and dynamic source of information, shaping perceptions of the world and informing individuals about social processes and phenomena. Moreover, the media functions as a tool for regulating public opinion and can be used for manipulation.

With the advancement of digital technology, individuals have gained numerous new opportunities, encompassing communication, sharing experiences, entertainment, and learning. These technologies not only cater to everyday needs but also fulfill higher aspirations.

However, along with these opportunities come new hazards on the internet, particularly for teenagers. Threats can be categorized into three groups.

The first group pertains to instances of aggression, cyberbullying, and exposure to inappropriate content not suitable for minors. According to former Mazhilis deputy Sauytbek Abdrakhmanov, 140 thousand cases of cyberbullying were reported in the country in 2021(Kunafin, 2024).

The second danger is linked to internet addiction. A report by the international agency We Are Social revealed that, on average, individuals spent 2 hours and 23 minutes per day solely on social networks last year. Given that 98.7% of young people in Kazakhstan regularly use the internet, Kazakhstanis may be particularly vulnerable to this risk (Kemp, 2024).

The third group of problems involves the spread of fake information, which necessitates the application of critical thinking skills to counteract.

Addressing these new threats against minors constitutes a complex and multifaceted process that requires the collaboration of online platforms, regulatory bodies, and internet users themselves (Kunafin, 2024).

In summary, the digital age has ushered in a myriad of opportunities for individuals, spanning communication, entertainment, and learning. However, these advancements also bring forth new challenges, particularly for adolescents and young adults navigating the online landscape. Cyberbullying, internet addiction, and the proliferation of fake information pose significant threats to the well-being of minors. Addressing these issues requires a multifaceted approach involving collaboration between online platforms, regulatory bodies, and internet users themselves. Furthermore, it is imperative to acknowledge the socio-psychological characteristics of young people, which render them susceptible to the influence of media and mass culture. Understanding the complexities of digital technology's impact on mental health is essential for developing effective interventions and support systems.

Results and discussion

In the course of the research work, a survey was conducted between March and May 2023 titled "Social Networks in the Republic of Kazakhstan: Regulating the Behavior of Youth and Ensuring Information Security" to explore the influence of social networks on Kazakhstani youth and the measures necessary to regulate their behavior while ensuring information security. A total of 621 respondents participated in the survey.

The results of the social survey conducted among the population on information security issues:

A significant number of respondents in the survey were young people aged 18-25 (85.1%), as well as 26-35-year-olds (4.2%), 36-45-year-olds (3.2%), 44-55-year-olds (4.4%), and those aged 56 and older (2.9%). At the same time, most of the respondents (79%) study at special secondary, or higher educational institutions, while 21% work in organizations or independently. These target groups (by age and occupation) are currently active consumers and distributors of information.

Regarding the question 'Where do you first look for the information that interests you?', 94.5% of respondents answered 'on the Internet', 2.1% chose 'in newspapers and magazines (periodicals)', 1.3%

selected 'on radio and television, at an educational institution, in training courses', 7.5% indicated 'in scientific, educational, fiction, technical literature', and 26.5% mentioned 'through communication with people'. Only 1% of respondents provided their own answer.

"How much time per day do you spend on the internet?" respondents to the question: 1-2 hours – 18 %; 3-4 hours – 33%; 5-6 hours – 27%; 7 or more hours – 22%. Therefore, it was determined that the vast majority of Internet users spend at most 3-4 hours on the Internet.
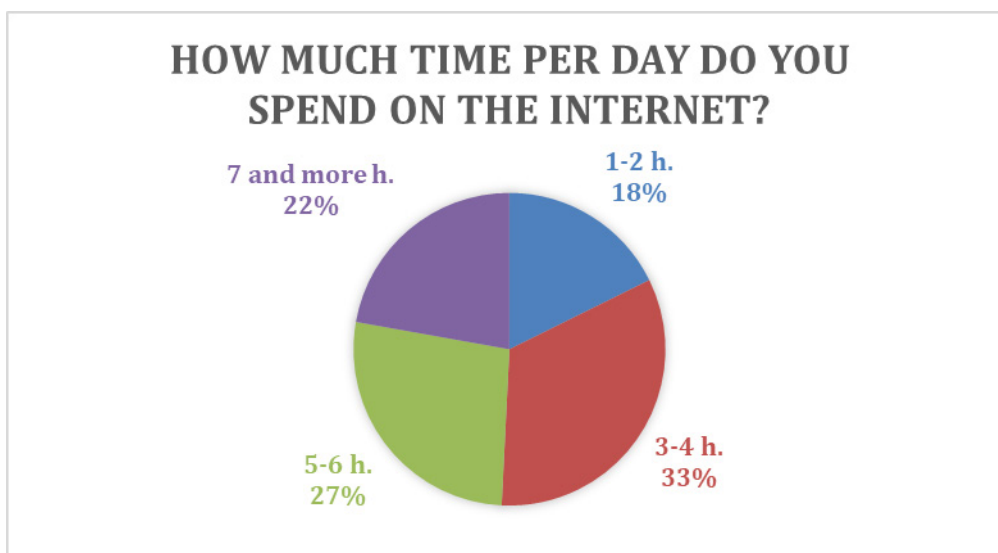

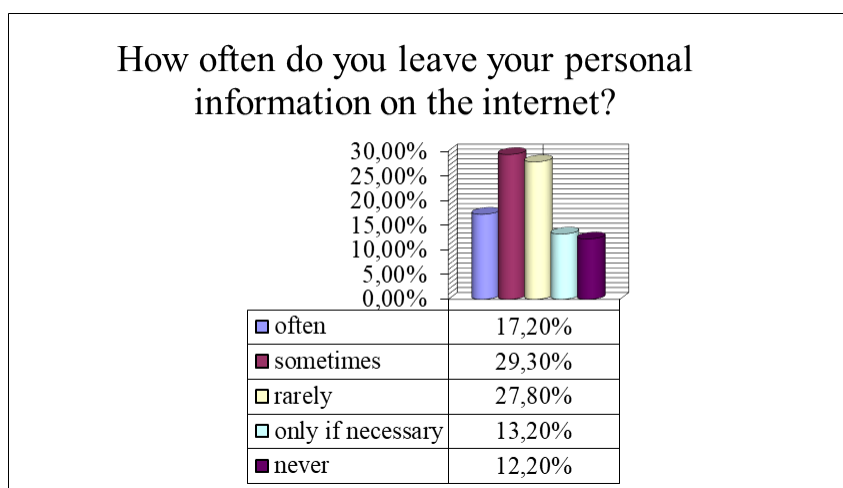**Figure 1** – How much time per day do you spend on the internet?

Figure 2 – How often do you leave personal information on the internet
(registering on various sites, filling out surveys, etc.)?

"How often do you leave personal information on the internet (registering on various sites, filling out surveys, etc.)?" the answer of the respondents to: often (registered in 5 or more social networks, I fill out various questionnaires) – 17.2%; some-

times (registered on 2-4 social networks, etc.) – 29.3%; rare (registered on 1-2 social networks, etc.) – 27.8%; never – 12.2%; only when necessary and only on the websites of state bodies and banks – 13.2%.

Based on the survey data above, we can glean information about citizens' tendencies to leave their personal information online and their attitudes toward security protection.

It was found during the process of processing the answers of the respondents that information security depends on the safety of individuals in the use of information networks. Specifically, the survey revealed several key findings regarding the factors influencing information security:

In the table above, the opinions of citizens regarding the survey conducted regarding the safety of social networks have been processed and grouped. «Have you ever had your social media accounts hacked?» The respondents' votes were divided as follows: My page cannot be hacked because I have a complex password – 14%, Yes – 36.4%, No – 48.8%, Other answers (I trust official sites, tried to hack, 4 times, my pages are linked to social networks) – 0.8%.

Table 1 – responses to survey questions about personal security of citizens in the information space

Questions	yes	no	There are useful and harmful information	I did not meet personally, my acquaintances met	I am a member of such a group	I have a complex password
Do you think that information on the Internet can harm people?	15,60%	9%	73,10%	-	-	-
Have you come across suspicious groups promoting radical movements, suicide, anorexia and etc. on the Internet?	23,30%	84,30%	-	11,90%	0,30%	-
Do you know how to protect yourself on social media?	61,60%	18,90%	-	-	-	-
Have you ever thought about the dangers of social media by posting personal information?	65,10%	21,20%	-	-	-	-
Have you ever had your social media accounts hacked?	36,40%	48,80%	-	-	-	14%
Did you know that your personal data can be stolen and used?	79,90%	7,30%	-	-	-	-

«Have you ever thought about the dangers of social media by posting personal information?» The respondents gave the following answers: 65.1% – Yes; 21.2% – No; I have trouble answering – 13.2%; Their own answers (Sometimes I think about how much, I don't include any information) – 0.5%.

«Do you know how to protect yourself on social media?» 61.6% of respondents answered that they know well how to protect themselves on social networks; 18.9% – No; 18.8% – I don't know; My personal answer (Don't download anything more; I want more information; YouTube helps; It's very easy, but many don't know) – 0.7%.

«What do you search/watch on the Internet?» (You can choose several answers) The answers of the respondents were as follows: Goods, services – 46.1%; Work – 16%; Fiction, educational literature – 37.2%; Scientific, educational material – 60.6%; Communication – 37.5%; Music – 65.5%, Movies – 64.1%, and their own answers.

«Do you think information on the Internet can harm people?» Respondents answered: Yes – 15.6%, No – 9%, There is both useful and harmful information – 73.1%, I have trouble answering – 1.7%.

«Have you come across suspicious groups promoting radical movements, suicide, anorexia and etc. on the Internet?» To the question, the opinions of the respondents were divided as follows: Yes – 23.2%, No – 64.3%; I did not meet personally, but my relatives, acquaintances, friends met – 11.9%; Yes, I am in such a group – 0.3%, I immediately write a complaint to such sites – 0.2%.

«Who do you think should take measures to protect children from harmful information that affects their psyche?» The answers of the respondents to the question were divided as follows: 74.3% – Parents, 16.4% – Teachers, educators; 42.3% – The child himself; 31.5% chose the state, and 1.6% chose their own answers.

«Did you know that your personal data can be stolen and used?» To the question, the respondents

gave the following answers: Yes, I know – 79.6%; No – 7.3%; Did not think about it – 12.1%

If we pay attention to the figure above, it is evident that citizens of our country primarily engage in activities such as listening to music and watching movies on the Internet. Following this, searching for scien-

tific and educational materials emerges as the next priority. The survey data indicate a growing interest in online communication. However, literary literature and job searches exhibit relatively low engagement. Therefore, it can be concluded that Internet users predominantly seek entertainment-oriented information.
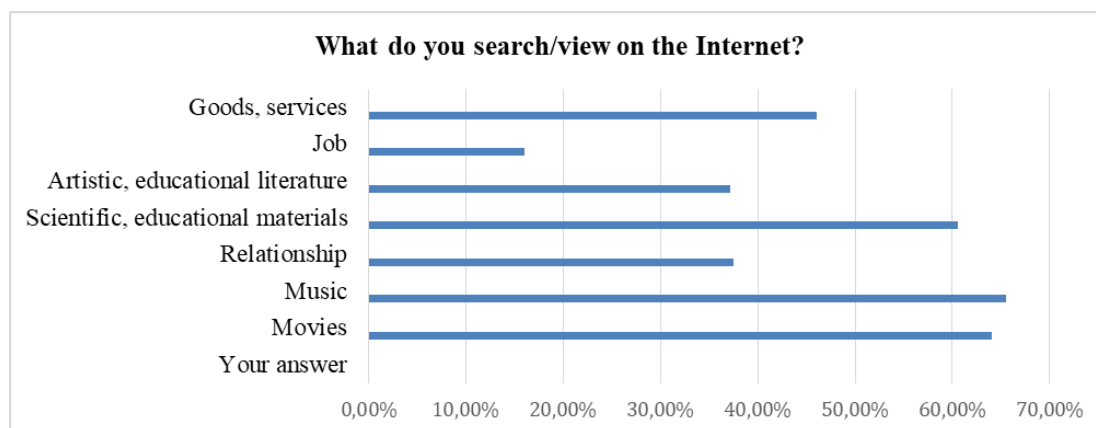

Figure 3 – What do you search/view on the Internet?

"Do you know what to do in case of a leak?" The answers of the respondents to the question were as follows: I seek the help of specialists – 37.4%; I turn to law enforcement agencies or the court – 16.8%, I did not think about it – 44.5%; own answers – 1.3% (I'll go to the programmer, delete the account, I don't know what to do, I won't do anything, I'll decide by myself). Therefore, it is determined that citizens do not think much about their safety. Therefore, it is necessary to increase citizens' knowledge about information security and to raise the culture of information literacy.

In addition, the majority of respondents (70%) do nothing personally to ensure information security. These are very alarming facts that indicate the insufficient awareness of the population about the issue of information security and citizens' understanding of the degree of danger in these issues, as well as the low level of their legal awareness.

The survey also showed that social networks play an important role in the life of a modern person (81%). 85.1% of respondents registered in social networks are aged 18-25. This indicates that the main audience of social networks is undergraduate students who are addicted to social networks(Shingaliyeva и др. 2023).

It should be noted that only 21.3% of respondents do not publish any information about themselves on social networks, and 6% of respondents

upload all possible information. 12.4% of respondents do not think about the danger of social networks; they post personal information on them. It is worth noting that 36.4% of respondents had cases of hacking of their pages in social networks. These facts indicate, on the one hand, poor public awareness, and on the other hand, carelessness and lack of responsibility.

The analysis shows that some respondents (37.5%) communicate through social networks. At the same time, 37% of the respondents have a positive attitude towards dating on social networks, and 40% have a neutral attitude. A much smaller number (23%) consider such a relationship dangerous. In addition, a third of respondents (31%) go on a date with a virtual friend, and almost half of them note that primarily young people and children do not appreciate the potential or actual dangers of dating on social networks.

Of course, one of the urgent issues is ensuring information security on the Internet. 17.7% of respondents spend 1-2 hours on the Internet, 33.1% – 3-4 hours, 27% – 5-6 hours, and 19.9% – more than 7 hours. At the same time, many people (63%) are looking for entertainment or communication on Internet sites. What we can see from this is the influence of the Internet on their lives and behavior. That is, it can be concluded that the Internet plays a big role in the life of a modern person.

According to the survey, citizens understand that there is both useful and harmful information on the Internet (73.1%). At the same time, 23.2% of those asked watch movies, videos, read content on the Internet, communicate with people who promote wrong or even dangerous lifestyles, etc. 11.9% of them personally or their acquaintances, friends, relatives have experienced radical trends, suicide, anorexia, etc. encountered suspicious propaganda groups.

Protection of children from information harmful to their health and development is a very urgent issue. Due to the current pandemic, it is known that the vast majority of parents allow their children to use the Internet until they reach adulthood, and it is alarming that sometimes even 2-3-year-old children are brought up with the help of the Internet. In addition, most parents give children complete freedom in choosing Internet sites or do not pay special attention to this issue. At the same time, some parents do not know and are not interested in what social networks their children are on (Shingaliyeva и др. 2023).

Also, a significant number of respondents (16.4%) believe that children should be protected from harmful information by teachers, educators, or the child himself, while 3% do not consider this to be an important issue. 31.5% of the respondents believe that the relevant authorities should deal with this issue, and 42.3% believe that the child should monitor it himself. These numbers show that a significant number of parents abdicate all responsibility for their children's information security.

Personal data protection is also an important issue. 87% of respondents register on various sites, social networks, fill out questionnaires, that is, leave their data online. In addition, most respondents (79.6%) know that their personal data can be stolen or used by other people. 34.4% of respondents have faced theft of personal information online. However, their willingness to ignore this fact in the case of personal data theft is questionable.

Copyright protection, complicated by the proliferation of content in the virtual network, is also a pressing issue (Smith, J., & Brown, A. 2019). According to the survey, half of the respondents do not agree or are indifferent to the protection of the copyright of users who post their materials on the Internet, or believe that the authors themselves should protect their copyright, and 15% do not consider the fact of downloading a ready-made essay, report, book, music, film from the Internet to be theft, and 40% consider it theft only if the copyright is registered.

Thus, copyright infringement, direct plagiarism in the scientific environment and educational system, and the low level of loyalty of many citizens to downloading without the consent of the copyright holders continue to exist in our country.

Based on the research, the following recommendations can be made:

- It is necessary to increase the awareness of citizens about the threats to information security, including when receiving, using, and posting information on various Internet sites and social networks, and to train them in the skills of safe online behavior. For this purpose, traditional mass media, educational videos on the Internet, public authorities, and educational institutions should be widely used. It is necessary to explain the need to use antivirus programs, official sources, legitimate programs, and to protect one's accounts and personal data.

- Considering that children and young people are more prone to negative influence, special courses on information security should be introduced in schools, colleges, and universities, or topics related to these issues should be included in the curricula of subjects that cover these issues (e.g., fundamentals of life security, Information Law, etc.). Practical training sessions are also recommended.

- Employees of law enforcement agencies, legal scholars, and teachers of law-related subjects in educational institutions should conduct lectures and explanatory works aimed at forming a negative attitude towards the creation, distribution, and use of false, slanderous information, extremism, radical religious teachings, suicide incitement, incitement to national, racial, social discord, and violation of state secrets, commercial, official, or other legally protected secrets. This will contribute to strengthening citizens' awareness of responsibility for violations of legislation in the field of information.

- It is advisable to install special information stands or displays explaining the rules of safe Internet use in a concise and accessible form in the Public Service Centers of the "Government for Citizens" state corporation. Employees of the centers can provide direct explanations of these rules in the self-service area for citizens when they receive state services.

- School teachers and educators in children's institutions should conduct explanatory work not only with children but also with their parents, especially in families with many children, including deepening the work on monitoring children's registration and communication on social networks.

- Law enforcement agencies should pay special attention to websites that promote suicide, drugs, pornography, pedophilia, anorexia, and take timely

measures to block such sites and bring the culprits to justice. Collaboration with volunteers, organizations dedicated to combating such phenomena, and civil groups is essential in this regard.

- State support should be provided to enterprises involved in information security, including the development of domestic technologies and technical means of information protection, ensuring their availability to the public, and providing special tax regimes, discounts, and preferences.

- To facilitate public monitoring of regulatory legal acts, conduct public expertise, and develop proposals for improving legislation in this area, issues of information security should be placed under the consideration of Public Councils under state bodies.

Conclusion

In conclusion, the survey results highlight the pressing need to bolster public awareness of information security and foster responsible online conduct. It is imperative to implement educational programs and integrate information security courses into academic curricula. Additionally, enforcing stringent measures against online threats and promoting parental involvement are crucial steps in safeguarding individuals, especially children, from cyber risks.

The digital era offers unprecedented opportunities for communication, entertainment, and knowledge acquisition. However, alongside these benefits come inherent challenges, particularly for young people navigating the online realm. Cyberbullying, internet addiction, and the dissemination of misinformation pose significant risks to their well-being. Tackling these issues demands a collaborative effort involving online platforms, regulatory bodies, and internet users.

Moreover, recognizing the socio-psychological dynamics influencing young individuals is paramount. Their susceptibility to media and cultural influences underscores the importance of understanding the intricate effects of digital technology on mental health. Developing effective interventions and support systems requires a nuanced comprehension of these complexities, ensuring a safer and more conducive online environment for all.

References

Dmitruk, Anastasia Petrovna. 2022. «Conference Priority areas of social, humanitarian and economic research in the 21st century». The influence of the media on the formation of value orientations of young people, Sociologicheskie nauki, , vyp. 27 (aprel'). https://apni.ru/article/3966-vliyanie-smi-na-formirovanie-tsennostnikh-ori. (In Russian)

«Google Forms [Online survey platform]. Retrieved from». b. d. Google LLC. (n.d.). https://www.google.com/forms.

Kemp, Simon. 2024. «DIGITAL 2024: 5 BILLION SOCIAL MEDIA USERS». Digital 2024. UK. https://wearesocial.com/uk/blog/2024/01/digital-2024-5-billion-social-media-users/.

Khalaf, Abderrahman M, Abdullah A Alubied, Ahmed M Khalaf, i Abdallah A Rifaey. 2023. «The Impact of Social Media on the Mental Health of Adolescents and Young Adults: A Systematic Review». Cureus, August. https://doi.org/10.7759/cureus.42990.

Kunafin, Daniyar. 2024. «Zakon.kz». TikTok dal rekomendacii po bezopasnosti kazahstanskih detej i podrostkov v Seti, 6 fevral' 2024 g., Zakon.kz izdanie. https://www.zakon.kz/obshestvo/6423399-TikTok-dal-rekomendatsii-po-bezopasnosti-kazahstanskikh-detey-i-podrostkov-v-seti.html. (In Russian)

Nussipova, Arailym, Esenzhol Aliyarov, Raushangul Kabilova, Katira Karymsakova, i Botakoz Nuralina. 2023. «Pandemic, Hoaxes and Information Security of Kazakhstan». Journal of Information Policy 13 (November): 140–58. https://doi.org/10.5325/jinfopoli.13.2023.0011.

Shingaliyeva, Akzhan K, Kunimaigul S Smadiyar, Arailym U Nussipova, Katira K Karymsakova, and Gaukhar N Azimbayeva. 2023. «Socio-Psychological Development of Children in a Large Family».

Tokaev, Kassym-Jomart. 2023. On approval of the Information Doctrine of the Republic of Kazakhstan. https://www.akorda.kz/ru/ob-utverzhdenii-informacionnoy-doktriny-respubliki-kazahstan-2025248. (In Russian)

Zwilling, Moti, Galit Klien, Dušan Lesjak, Łukasz Wiechetek, Fatih Cetin, i Hamdullah Nejat Basim. 2022. «Cyber Security Awareness, Knowledge and Behavior: A Comparative Study». Journal of Computer Information Systems 62 (1): 82–97. https://doi.org/10.1080/08874417.2020.1712269.

Smith, J., & Brown, A. (2019). Cybersecurity Awareness among College Students: A Quantitative Study. Journal of Cybersecurity Education, 5(2), 45-58.

Information about authors:

Nussipova Arailym Umarkhodzhaevna (corresponding author) – PhD, associate professor of International Educational Corporation (Almaty, Kazakhstan, e-mail: arai_nussipova@mail.ru);

Slanbekova Gulnara Kobylanovna – PhD, associate professor of the Department of Psychology of Karaganda Buketov University (Karaganda, Kazakhstan, e-mail gulnaraslanbekova1@gmail.com)

Авторлар туралы мәлімет:

Нусипова Арайлым Умарходжаевна (корреспондент автор) – PhD, Халықаралық білім беру корпорациясының ассоциацияланган профессорі (Алматы қ., Қазақстан, e-mail: arai_nussipova@mail.ru)

Сланбекова Гульнара Кобылановна – акад. Букетов атындағы Қарағанды университетінің қауымдастырылган профессоры (Қарағанды қ., Қазақстан, e-mail: gulnaraslanbekova1@gmail.com)