Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technologies

FEM CULS Prague

Bachelor Thesis

User perception's and behavioural intentions towards privacy and security online

Amrin Zhakhat

Czech University of Life Sciences Prague
Faculty of Economics and Management

BACHELOR THESIS TOPIC

Author of thesis:	Zhakhat Amrin
Study programme:	Informatics
Thesis supervisor:	John Phillip Sabou, Ph.D.
Supervising department:	Department of Information Technologies
Language of a thesis:	English

Thesis title:

User perception's and behavioral intentions towards privacy and security online

Objectives of thesis:

The main objective of the thesis is to adapt an existing model of user's perceptions towards cyber-security policy in Kazakhstan. To explore this, the thesis will conduct a survey of IT students in universities in Kazakhstan.

Research Focus

- To discern how the average, young citizen in Kazakhstan feels about cyber-security policy development.
- To understand what are the existing government and industrial responses to rising cyber-security challenges.
- To explore the role and/or suggested solutions of young citizens in the future of cyber security policy development towards strengthening government, IT industries, and e-commerce as consistent with global standards.

Methodology:

The methodology of this thesis will be focusing on a questionnaire survey and a series of interviews conducted in a focus group, which will then be converted into statistical representation of responses. This qualitative data will show a detailed picture of user perception's and behavioral intentions towards privacy and security online in Kazakhstan. To obtain data, I will use tools such as Google Surveys and interviews in a focus group. To organize the data, I will use Microsoft Excel and Word and Graph builder to interpret the data and model the user's perceptions and behavioral tendencies towards privacy and security online.

The proposed extent of the thesis: 40-50

Keywords: User perceptions, behavioral intent, privacy, security, social media

Recommended information sources:

1. Akhmetov, B. (2018). Status, perspectives and main directions of the development of cybersecurity of information and communication transport systems of kazakhstan. Republic of Kazakhstan, 23.
2. Boranbayev, A., Boranbayev, S., Nurusheva, A., & Yersakhanov, K. (2018). The modern state and the further development prospects of information security in the Republic of Kazakhstan. Information Technology-New Generations, 33-38.
3. Boranbayev, A., Boranbayev, S., Seitkulov, Y., & Nurbekov, A. (2020, November). Proposing recommendations for improving the reliability and security of information systems in governmental organizations in the republic of Kazakhstan. In Proceedings of the Future Technologies Conference (pp. 854-868). Springer, Cham.
4. Ismailova, R., Muhametjanova, G., Medeni, T. D., Medeni, I. T., Soylu, D., & Dossymbekuly, O. A. (2019). Cybercrime risk awareness rate among students in Central Asia: A comparative study in Kyrgyzstan and Kazakhstan. Information Security Journal: A Global Perspective, 28(4-5), 127-135.
5. Symbat, I., & Yesseniyazova, B. M. (2019). Cyber Security Issues in Digital Kazakhstan. In NISPA Organization. URL: https://www. nispa. org/files/conferences/2019/e-proceedings/system_files/papers/cyber-security-issues-issabaeva. pdf.

Expected date of thesis defence: 2022/23 SS - FEM

Electronically approved: 22. 6. 2022
doc. Ing. Jiří Vaněk, Ph.D.
Head of department

Declaration

I declare that I have worked on my bachelor thesis titled "User perception's and behavioral intentions towards privacy and security online" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the bachelor thesis, I declare that the thesis does not break any copyrights.

In Prague on 15 March 2023 ____________________________

Acknowledgement

I would like to thank John Phillip Sabou and Miloš Ulman, for their advice and support during my work on this thesis.

User perception's and behavioural intentions towards privacy and security online

Abstract

Kazakhstan is currently creating and deploying new digital services to raise the general population's level of living. The government of Kazakhstan is performing a digital change. During the period of modernization, maintaining cybersecurity in cyberspace is one of the most crucial challenges, not just for Kazakhstan but also for other nations. This study's objectives include determining the Republic of Kazakhstan's citizens' access to high-quality digital services as well as the level of public understanding of and readiness for state-implemented programs and projects within the framework of national cybersecurity and digitalization policy. The research will include theoretical and empirical analysis to ascertain Kazakhstan's level of cybersecurity and digitalization. The research subject will also look at the experiences of successful nations and unions, such the US and the EU. By conducting an online survey of Kazakh students, the paper will use a quantitative research methodology. The survey looks at the population's capability, comfort, and knowledge about the usage of digital technology and cybersecurity. By conducting an interview of People working in the cyber-security field, the paper will use a qualitative research methodology. The interview looks at the specialists' views on the level of cyber security in the country, its weaknesses and strengths, and a possible future. Both the survey and the interview will be conduct within the context of Kazakhstan's accepted state program and regulatory legislation. Practical and methodological suggestions for further enhancing Kazakhstan's cybersecurity and digital policy will be made based on the findings of the qualitative and quantitative study. The suggested solutions may be helpful not just for Kazakhstan but also for other nations going through a digital transition. Furthermore, as post-Soviet countries have a common history of independence growth and construction, it may be beneficial for the nations of the former USSR.

Keywords: cybersecurity, younger generation, Kazakhstan, information security awareness, computer literacy

Table of content

1 Introduction

As the internet has become an integral part of daily lives of citizens all around the world, concerns over privacy and security have become increasingly important. With the rise of cybercrimes and online threats, it is crucial to understand how users perceive the importance of privacy and security when using the internet. Kazakhstan is a developing country where cyber security is just gaining importance. Unfortunately, not all people in Kazakhstan are familiar with the Internet. Consequently, students and young citizens are the best target audience to explore user perceptions and behavioural intentions regarding privacy and security online in Kazakhstan because they are active internet users, that represent a future of Kazakhstan. Understanding their attitudes and behaviours towards online privacy and security can provide valuable insights into the challenges and opportunities related to online safety in the country.

The aim of this bachelor work is to investigate the user perceptions and behavioural intentions towards privacy and security online through young citizens in Kazakhstan. The study will explore the young people awareness of online threats and the measures they take to protect their privacy and security online. Additionally, the research will examine the factors that influence their attitudes towards online privacy and security, such as age, gender, and previous experiences.

The survey and interview methods will be used to achieve these research objectives. The survey will provide quantitative data that can be analysed statistically, while the interview will allow for a deeper exploration of participants' experiences, beliefs and attitudes. By combining both methods, this study aims to provide a comprehensive understanding of young citizens' and students' perceptions and behaviour regarding online privacy and security in Kazakhstan.

The importance of this study is that it can inform policymakers, internet service providers and other and other organisations and individuals related to cyber security of individuals as well as the public about the need to improve online security and privacy policies. In addition, the findings of this study may also help to raise awareness among young people about the importance of protecting their personal information online. Ultimately, this study can contribute to a safer online environment for all users.

2 Objectives and Methodology

2.1 Objectives

Nowadays, there are many threats and dangers caused by the Internet and use of it services. From scammers who want to get your money directly to hackers stealing your identity to use it for further illegal purposes. These individuals use different technologies and methods to fulfil their crimes. Depending on people's awareness of cyber security and the basic steps they need to take online, they may be protected from these threats. There are many models of people's behaviour towards cyber-security policy, which differ depending on age, knowledge, professions, and place of residence.

This work sets as the main objective to study of existing models of user’s perceptions towards cyber-security policy and adapt them to the realities of Kazakhstan and its residents. To achieve this goal, it is necessary to collect the opinions of the residents of Kazakhstan, but since Kazakhstan is a developing country, and the digitalization and technification of the country is currently in progress, the collection of opinions of the entire population can mispresent the real existing model of user’s perceptions towards cyber-security policy in Kazakhstan.

Therefore, I decided to conduct a survey of IT students in universities in Kazakhstan. Because of this decision, we will be able to see what the condition of cyber-security awareness among the younger generation of Kazakhstan is, who are already familiar with new technologies and use them in everyday life. Moreover, IT students in universities in the future will be the base for the development of IT area in Kazakhstan, they will occupy working positions both in medium and small businesses, and in government structures. Their model of user's perceptions towards cyber-security policy is the most accurate representation of the model for the whole of Kazakhstan.

Research Focus

- To discern how the average, young citizen in Kazakhstan feels about cyber-security policy development.
- To understand what the existing government and industrial responses are to rising cyber-security challenges.
- To explore the role and/or suggested solutions of young citizens in the future of cyber security policy development towards strengthening government, IT industries, and e-commerce as consistent with global standards.

This thesis will aim to answer the following research questions:

- *RQ1: "What is the state of cyber security in Kazakhstan?"*
- *RQ2: "How do university students in Kazakhstan perceive the utility of cyber-security?"*
- *RQ3: "What is the future of cyber security in Kazakhstan and what can be done to improve it?"*
- *RQ4: "At what level is the model of user's perceptions towards cyber-security policy?"*

2.2 Methodology

Since we need to collect the opinions of the people of Kazakhstan the methodology of this thesis will be focusing on two specific methods. The first is a questionnaire survey, which will allow us to collect opinions from many people. The survey will be mixed-method survey. It will involve a questionnaire with scalable answers in order to collect quantitative data, and it will also have descriptive questions with to collect qualitative data. This data, after analysis, will help us build universal models of user's perceptions towards cyber-security policy show a detailed picture of user perceptions and behavioural intentions towards privacy and security online in Kazakhstan.

The second is a series of focus group interviews that will then be converted into a statistical representation of the responses. The focus groups will be made up of both students and graduates of IT universities and people already working in the IT field in Kazakhstan. This qualitative data will provide a detailed picture of user perceptions and behavioural intent regarding online privacy and security in Kazakhstan. To obtain data, I will create questions, which I will post on the corresponding resource. I will use tools such as Google Surveys where the target audience can answer them. I will also create preliminary questions for the interview and conduct in a focus group/ To organize the data, I will use Microsoft Excel and Word and Graph builder. This will allow to interpret the data and model the user's perceptions and behavioural tendencies towards privacy and security online in Kazakhstan for its further analysis and appropriate conclusions.

3 Literature Review

3.1 What is cyber security?

In order to fully open this topic, we need to answer several critical questions. One of them is: "What is cybersecurity?". According to the article "Defining Cybersecurity" written by "Dan Craigen, Nadia Diakun-Thibault, Randy Purse", the term "cybersecurity" (Dan, et al., 2014) does not have a short and laconic definition covering the multidimensionality of cybersecurity that would be widely accepted. In authors opinion, this could potentially hinder the technological and scientific progress, through the spread and evasion of a predominantly technical view of cybersecurity, preventing the development of other disciplines that must act in concert to solve complex cybersecurity problems. Based on their literary analysis, they concluded that the term "cybersecurity" has been the subject of popular and academic literature in which it is widely used, and its definitions vary widely, depend on context, are often subjective and sometimes uninformative. For instance:

> *"The art of ensuring the existence and continuity of the information society of a nation, guaranteeing and protecting, in Cyberspace, its information, assets and critical infrastructure."* (Canongia & Mandarino, , 2014)

Morten Bay suggests in his article *“What is Cybersecurity? In search of an encompassing definition for the post-Snowden era”* (BAY, 2016) that the term cybersecurity is very broad and covers many different areas.

To determine the meaning, the author used the online version of the Oxford English Dictionary, in which, he defined what the word "security" means, part of the compound word cybersecurity. (Oxford Online Dictionary, n.d.) defined security as “the state of absence of danger or threat”. However, the author does not agree with this simple definition, as it contradicts the complexity of the actual use of this word, especially when it comes to cybersecurity, because this term is constantly used by politicians, computer scientists, IT managers, tech entrepreneurs, healthcare professionals and homeland security operators, etc., it seems almost impossible that so many people would agree with the definition. Everyone on the list has their own take on what cybersecurity is. *"The term is used to cover the measures government institutions take to protect the public and the institutions themselves from threats in the 'cyber'-domain, also known as 'cyberspace'"* (BAY, 2016). However, the author clarifies that the term is also used at a level that is somewhat closer to the individual when it refers to protecting against viruses and other malware on a computer, whether it is personally owned or used in a work situation.

3.2 Why is cybersecurity so important?

Once we've sorted out what cyber security is, we need to understand why it's so important. In the article "Cybersecurity.... How Important Is It?" by The American Bar Association magazine from 2012, written by Judge Herbert B. Dixon Jr., the author discusses and describes the importance of cybersecurity based on several events united around the theme of cybersecurity. Below we look at a part of this article that discusses an article written by U.S. President Barack Obama in the Wall Street Journal in the summer of 2012, in which he called for the passage of a cybersecurity bill that was pending in the Senate. This bill establishes cyber security standards to prevent large-scale cyber-attacks on the national network.

In it, the President noted the frightening possibilities of unknown hackers infiltrating the computer networks of private sector companies that run much of the transport, water, finance, energy and government and other critical infrastructure and security structures. He also stated in the article that foreign governments, crime syndicates and individuals are checking their defence daily, and to prove his point he described a recent intrusion into the networks of companies operating water plants and gas pipelines. Subsequently, the article described the President's concern that computer systems were becoming increasingly vulnerable in other critical sectors of the economy, including the nuclear and chemical industries. The President concluded this thought by assuming that a financial crisis could be triggered by the failure of vital banking systems; a public health emergency or functioning hospitals could be triggered by a lack of clean water; and loss of electricity could bring businesses, cities, and entire regions to a standstill. (Jr, 2012)

According to a report monitoring cyberthreats by the FBI[1], the number of successful attacks skyrocketed across the U.S. by 600% and across the globe by 300% since the beginning of the COVID-19 pandemic (Borkovich & Skovira, 2020). Similarly in 2022, there was a joint advisory report and guidelines from the United Kingdom's National Cyber Security Centre (NCSC) and the United States Department of Homeland Security (DHS) Cyber Security and the Infrastructure Security Agency (CISA) on issues such as phishing, malware, and DDoS attacks that have risen and become a pervasive element of the digital ecosystem (Pranggono & Arabo, 2021)

3.3 How are governments – laws and regulations, regulating Data Protection and Privacy around the world?

The next step is the state the art in data protection and privacy. We will use case examples from Europe and USA. First, consider Europe Data Protection and Privacy. In Europe Data Protection and Privacy regulated by the European Union's General Data

[1] See: https://www.ic3.gov/

Protection Regulation (GDPR), which came into force on 25th May 2018 across the European region. The texts of GDPR contains eleven[2] chapters and 99 Articles to deal with the specific matters in terms of governance and implementation framework. One of the main provisions of the GDPR is that it strongly advocates the minimization of data, not only in terms of collection, but also in terms of storage and long-term storage of data. In the GDPR a data subject has legal rights which are listed in some articles. A few basic articles are listed below.

- The right to the protection of personal data concerning him or her, the right of access by the data subject (GDPR, 2019, Art. 15)
- The right to rectification (GDPR, 2019, Art. 16)
- The right to erasure (or right to be forgotten) (GDPR, 2019, Art. 17)
- The right to restriction of processing (GDPR, 2019, Art. 18)

The GDPR has also given a broader definition of personal data in relation to sensitive data, which includes religious or philosophical beliefs, political views, sexual orientation, trade union activities, past criminal, or non-social behaviour, medical or health data, and data on the race or ethnicity of a living person. The GDPR also details the structure of cross-border data transfers when doing business with European individuals, organisations, and

[2] Chapters of the GDPR

(I) General Provisions

(II) Principles

(III) Rights of the Data Subject

(IV) Controller and Processor

(V) Transfers of Personal Data to Third Countries or International Organizations

(VI) Independent Supervisory Authorities

(VII) Cooperation and Consistency,

(VIII) Remedies, Liability and Penalties

(IX) Provisions Relating to Specific Processing Situations

(X) Delegated Acts and Implementing Acts

(XI) Final Provisions

institutions. The GDPR also takes care of data anonymisation and data pseudonymisation. It ensures that the processing of children's data requires parental consent (Das, 2018).

Second, consider USA Data Protection and Privacy. In the United States, there is no comprehensive federal legislation ensuring the privacy and protection of personal data. Instead, legislation relies on an industry-wide approach to protecting data privacy. Their approach consists of a combination of federal and state legislation, administrative rules, and industry self-regulatory guidelines. It is worth noting that these laws apply only to specific sectors, such as "health, education, communications and financial services, or, in the case of online data collection, children (Boyne, 2018). Their approach is also interesting for our research, because although comparative law experts are likely to dismiss the US system of privacy protection as less robust than the European approach, in some respects the US system provides more greater protection than the European approach (Boyne, 2018). Six federal sectoral acts are summarised in the table below.

Table 3-1 Key Features of Sector-Specific Legislation (Boyne, 2018)

NAME OF LEGISLATION	***DEFINITION PERSONAL DATA***[3]	***DATA CLASSIFICATIONS***	***PROCESSING OF INFORMATION***
Financial Services Modernization Act (Gramm–Leach–Bliley Act): Protects consumers' "non-public" personal information when used by financial institutions	*"Non-public personal information" means personally identifiable financial information that is provided by a consumer to a financial institution; resulting from a transaction with the consumer or from a service provided to the consumer; or otherwise obtained by the financial institution.*	*Non-public personal information is protected. Publicly available personal information is not protected.*	*Financial institutions may transfer personal information to other companies if it is necessary to the performed financial services. Information may be shared with credit reporting agencies or financial regulatory agencies.*[30]
Health Insurance Portability and	*"Protected health information" means*	*Under the Act there is protected health information*	*The Security Rule establishes the minimum requirements*

[3] The legislative enactments in this Table are not based on sector-specific protections rather than on a broad right to personal data protection as exists in the European Union.

Accountability Act (HIPAA)	*individually identifiable health information: (1) Except as provided in paragraph (2) of this definition,*[31] *that is: (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium.*	*(PHI) and “electronic Protected Health Information” (e-PHI). While HIPAA protects PHI, there are additional requirements that apply to e-PHI.*	*for all health care entities and contractors which require all data processors to adopt administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of the information; (2) report security incidents.*
Controlling the Assault of Non-solicited Pornography and Marketing Act (CAN-SPAM Act)	*Regulates the collection and use of e-mail addresses. Covers all commercial messages, which the law defines as “any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service,” including e-mail that promotes content on commercial websites.*	*Regulates “commercial” and “transactional or relationship” e-mails. Commercial e-mail must include non- deceptive sender and subject information; opt-out provisions; sender's address; and clear and conspicuous identification that the e-mail is an advertisement or solicitation.*	*The Act imposes criminal penalties on individuals who: harvest e-mail addresses or generate them through a dictionary attack.*[36]
The Fair Credit Reporting Act (15 U.S.C. § 1681) (and the Fair and Accurate Credit Transactions Act (Pub. L. No. 108-159) which amended the Fair Credit Reporting Act*)*	*Applies to consumer reporting agencies, those who use consumer reports (such as a lender) and those who provide consumer-reporting information (such as a credit card company).*	*“Consumer reports” are any communication issued by a consumer reporting agency (CRA) regarding a consumer's creditworthiness, credit history, credit capacity, character, and general reputation that is used to evaluate a consumer's eligibility for credit or insurance.*	*A CRA must, “follow reasonable procedures to assure accuracy of the information. Where data are “inaccurate or incomplete or cannot be verified,” a CRA must immediately correct the data.*
Electronic Communications Privacy Act (18 U.S.C. § 2510*)*	*Prohibits wiretaps of communications of others without court approval without a party's prior consent. Prohibits the use or disclose any information acquired by illegal*	*Interception “means the aural or other acquisition of the contents” of various kinds of communications by means of “electronic, mechanical or other devices.”*	*“Content” means “information concerning [its] substance, purport, or meaning.” The Act defines “damage” as “any impairment to the integrity or availability of data, a*

	wiretapping or electronic eavesdropping.		*program, a system, or information.*
Computer Fraud and Abuse Act (18 U.S.C. § 1030)	*Seeks to prevent and punish hacking- related activities which the Act defines as "unauthorized access" to protected computers.*[43] *In addition, the Act bars individuals or entities from exceeding the scope of their "authorized access."*[44]	*"Protected computers" includes: those used by financial institutions, the U.S. government, and computers used in or affecting interstate or foreign commerce or communication.*	

These data management and cyber security policies are a useful metric for baselining the strategic creation of national cyber security policy in Kazakhstan.

3.4 Data Protection Laws in Kazakhstan

To answer this question, we will use information from the source named "Cyber Security issues in digital Kazakhstan" written by Isabaeva Symbat and Botagoz M. Yesseniyazova in 2019. The authors of this article state that Kazakhstan is in a state of digital transformation, which consist of developing and implementing new digital services in order to improve the standard of living of the population. However, the majority of Kazakhstanis are vulnerable to cyber-attacks. In their opinion, the reasons for this lie in the lack of knowledge, skills, and awareness in cybersecurity (Symbat & Yesseniyazova, 2019).

- *In March 2019, the President of the Republic of Kazakhstan adopted the Law "On ratification of the Agreement on cooperation of the member States of the Collective security Treaty organization in the field of information security"* (Ministry of Justice of the Republic of Kazakhstan. Institute of legislation and legal information, n.d.)
- *The "National Infocommunication Holding Zerde" was established in July 2008.* (*Cyber Security Issues in Digital Kazakhstan*, 2019, page 4)

- *In 2009 the "National Infocommunication Holding Zerde" created a master plan for the development of E-government and E-services for 2010-2014, as well as a package of regulations on E-government and information security infrastructure. (Cyber Security Issues in Digital Kazakhstan, 2019, page 4)*
- *In October 2011, Zerde holding organized the international conference "Digital communication 2012" and took part in the international exhibition "GITEX technology week". (Cyber Security Issues in Digital Kazakhstan, 2019, page 4)*
- *In 2012, the ICT development Fund was established on the initiative and with the support of the Ministry of transport and communications. (Cyber Security Issues in Digital Kazakhstan, 2019, page 4)*
- *Since 2012 on the basis of holding the Technical Committee on standardization No. 34 "Information technologies" on the basis of which standards and also normative documentation on standardization in ICT are developed and coordinated functions. (Cyber Security Issues in Digital Kazakhstan, 2019, page 4)*
- *In 2013, the Holding took an active part in the development of the state program "Information Kazakhstan – 2020". (Cyber Security Issues in Digital Kazakhstan, 2019, page 4)*
- *In 2014, as part of the "Global e-Government Forum", the Holding jointly with JSC "international IT University" held the first international Scientific and practical Conference "SmartGovernment: Science and Technology". (Cyber Security Issues in Digital Kazakhstan, 2019, page 4)*
- *October 25, 2015, president of the Republic of Kazakhstan N. Nazarbayev signed a new Law "On Informatization". (Cyber Security Issues in Digital Kazakhstan, 2019, page 4)*
- *In 2016, as part of the implementation of the Law "On Informatization" by the government of Kazakhstan, the holding was determined as a service integrator of "electronic government". (Cyber Security Issues in Digital Kazakhstan, 2019, page 4)*
- *In addition, in 2016, in order to develop human capital and improve digital literacy of the population, JSC "Holding Zerde" held an off-site event in 6 cities of the Republic of Kazakhstan to teach students of 9-11 grades and teachers of the*

subject "Informatics". As a result of the event, 117 teachers and 130 pupils schoolchildren were trained. (Cyber Security Issues in Digital Kazakhstan, 2019, page 4)

- *In November 2016, JSC "National Info-communication Holding "Zerde" was determined by Kazakhstan's government by the National Institute of development in the field of information and communication technologies* (Official website Joint Stock Company "Zerde", Official website Joint Stock Company "Zerde").

3.4.1 JSC "National information technologies"

JSC "National information technologies" is one of the largest companies in Kazakhstan's IT market that operating in Kazakhstan since 2000 ("National Information Technologies" JSC, 2019). Currently JSC "NIT" is working on the development of a single information space in the Republic of Kazakhstan. Within its competence, JSC "NIT" performs the following tasks of the operator of information and communication "E-government" infrastructure:

- *ensuring compliance with uniform requirements in the field of information and communication technologies and information security, as well as the rules for the implementation of the service model of Informatization;* (Government of the Republic of Kazakhstan, 2016) *page 3*
- *implementation of system maintenance and maintenance of Internet resources of state bodies and objects of information and communication infrastructure of "E-government" in accordance with the list approved by the authorized body;* (Government of the Republic of Kazakhstan, 2016) *page 4*
- *provision of information and communication services to public authorities on the basis of information and communication infrastructure of "E-government" in accordance with the catalogue of information and communication services;* (Government of the Republic of Kazakhstan, 2016) *page 4*
- *ensuring the security of storage of state electronic information resources placed on the information and communication infrastructure of "E-government",*

assigned to the operator; (Government of the Republic of Kazakhstan, 2016) *page 5*

- *ensuring the security of storage of state electronic information resources in the provision of information and communication services;* (Government of the Republic of Kazakhstan, 2016) *page 5*
- *ensuring rapid response to the identified shortcomings in the provision of information and communication services, as well as public services in electronic form and taking measures to address them;* (Government of the Republic of Kazakhstan, 2016) *page 5*
- *implementation of integration and connection of local, departmental and corporate telecommunications networks of state bodies to the information and communication infrastructure of "E-government»;* (Government of the Republic of Kazakhstan, 2016) *page 6*
- *provision of data transmission services to state bodies, their subordinate organizations, local self-government bodies, as well as other subjects of Informatization, determined by the authorized body and connected to the unified transport environment of state bodies, for the functioning of their electronic information resources and information systems;* (Government of the Republic of Kazakhstan, 2016) *page 6*
- *creation and development of information and communication platform of "E-government" and unified transport environment of state bodies;* (Government of the Republic of Kazakhstan, 2016) *page 7*
- *support and system maintenance of the national gateway of the Republic of Kazakhstan;* (Government of the Republic of Kazakhstan, 2016) *page 7*
- *information content of the E-government web portal.* (Government of the Republic of Kazakhstan, 2016) *page 7*

3.4.2 Commission under the President of the Republic of Kazakhstan and E-government

For the implementation of digitalization in the Republic of Kazakhstan, the decree of the President of the Republic of Kazakhstan in January 2018 formed a Commission under the President of the Republic of Kazakhstan on the (hereinafter – the Commission) (Ministry of Justice of the Republic of Kazakhstan. Institute of legislation and legal information, n.d.). The Commission works as an “advisory body” under the President of the Republic of Kazakhstan, whose task is to develop proposals on the introduction of digitalization and information technologies in the Republic of Kazakhstan. The two main tasks that the Commission works with to accomplish this task are:

- *makes recommendations on the implementation of digitalization and digital technologies in the Republic of Kazakhstan.*
- *conducts monitoring on the effective implementation of the State program “Digital Kazakhstan” and undertaken by governmental agencies and other organizations of measures for implementation of the adopted decisions on the introduction of digitization in the Republic of Kazakhstan.*

In addition, in 2008 Kazakhstan introduced a single mechanism of interaction between the state and citizens, as well as state bodies with each other, ensuring their consistency with the help of information technologies to improve the efficiency of government bodies and the availability of public services. This tool named E-government. Electronic government has gone through four stages of formation and development and now occupies high positions in international rankings. Here are a few nominations that e-government has received:

- WSIS Project Prizes 2013
- First World Govtechineers Race-2017
- WSIS Prizes-2017

Even though the E-government system is estimated as “developing”, we can already conclude that it is successful. According to the International Institute for Management Development's World Digital Competitiveness ranking Kazakhstan consistently over the last 2 years (2017-2018) occupies 38th position in the global ranking.

3.4.3 Suggested ways to improve the level of cybersecurity in Kazakhstan

According to the results of 2017 analysis of indicators related to cybersecurity among the countries of the former USSR, Kazakhstan is ahead only of Tajikistan, Uzbekistan, Kyrgyzstan, Armenia, and Turkmenistan. This is one of the worst development results that Kazakhstan has received, which can negatively affect the present and future of the country. Now the IT sphere concerns all areas of business, and such a result will repel foreign investors, thereby reducing the economic and social opportunities of Kazakhstan. Government needs to take this indicator as a signal that it is already necessary to take certain actions to improve the level of cybersecurity.

in June 2017, the Concept of cybersecurity framework “cyber-Shield of Kazakhstan” was developed in accordance with the message of the President of the Republic of Kazakhstan “the third modernization of Kazakhstan: global competitiveness” with the approaches of the Strategy “Kazakhstan - 2050” on the entry of Kazakhstan into number of 30 most developed countries of the world. The action Plan for its implementation was thought out until 2022, covering organizational, legal, technical, and educational activities was approved as part of the implementation of the cybersecurity Concept at the end of 2017 (Official Information Source of the Prime Minister of Kazakhstan, 2017).

The international experience is used to complete this action plan. Particular attention is paid to the implementation of experience in Protection of national information and communication infrastructure of the leading states and the use of ICT to achieve the goals of socio-economic development. Additionally, Committee on information security of the Ministry of defence and aerospace industry of the Republic of Kazakhstan was formed in accordance with the decree of the President of the Republic of Kazakhstan to improve the level of cybersecurity in Kazakhstan (Ministry of Justice of the Republic of Kazakhstan. Institute of legislation and legal information, n.d.).

Another entity that is involved in improving the level of cybersecurity is KZ-CERT. KZ-CERT is a single centre for users of national information systems. *The main task of KZ-CERT is to reduce the level of cyber security threats to users of the Kazakh segment of the Internet* (KZ-CERT, 2019) by providing collection and analysis of information on computer incidents, advisory and technical support to users in the prevention of computer security threats.

In 2016, The Ministry of information and communication of the Republic of Kazakhstan revealed that 16,576 cyber incidents occurred in 9 months: 688 of them were detected in relation to state institutions. In the same year, the Committee on legal statistics and special records of the General Prosecutor's office of the Republic of Kazakhstan revealed that 106 cybercrime criminal cases were registered for 10 months (National Computer Incident Response Service, 2016).

In 2017 Kazakhstan does not change its position and remains at the same 38th place as in the World Digital Competitiveness ranking. At that time, there were frequent reorganizations that could serve as a barrier to the development and application of digital technologies, as well as the overall effectiveness of government programs in the field of digitalization and cybersecurity. Therefore, we can conclude that to achieve effective results and achieve long-term goals, it is necessary to form in public administration a stable structure of the government and take all necessary measures to minimize the leakage of personnel.

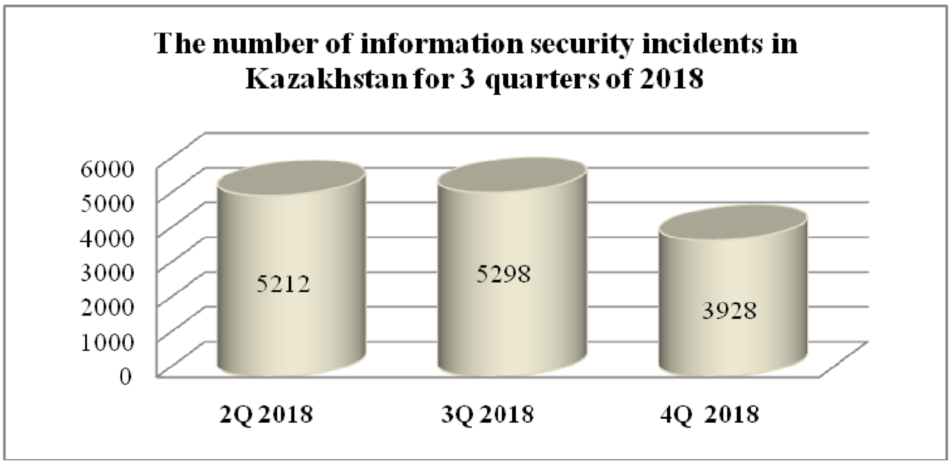


Figure 1. information security incidents

In 2018, Government of Kazakhstan presented data with positive trend in the number of information security incidents, which you can see in the chart developed by author. In this year, Kazakhstan in the field of cybersecurity has a huge breakthrough. Kazakhstan in a short period of time raised its rating from 83rd position to 40th position according to Global Cybersecurity Index. Kazakhstan has achieved a mark - 0.778 and exceeded its own goals to develop the cybersecurity index by 2008 - 0.300, by 2019 - 0.400, by 2020 - 0.500, by 2021 - 0.550, by 2022 - 0.600, which were set in the Concept of cybersecurity. Consequently, the government is faced with the task of updating the Concept of cybersecurity by introducing new goals and objectives. You can see Comparative diagram between WDC 2018 and GCI 2018 indicators on the following diagram developed by the author. (IMD Business School, 2018)

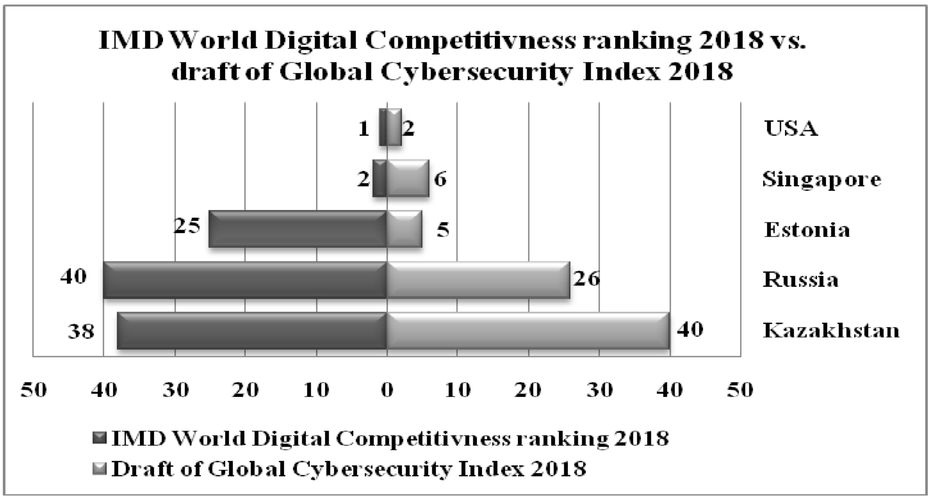


Chart № 1 Comparative diagram between WDC 2018 and GCI 2018 indicators. Chart developed by author

The next step to train future cybersecurity specialists under for 2018-2020 at the expense of the national budget, as part of the program "Provision of personnel with higher and postgraduate education" by framework of the Kazakhstan's cybersecurity Concept (Ministry of Justice of the Republic of Kazakhstan. Institute of legislation and legal information, n.d.).

In January 2017, the first president of the country N. Nazarbayev announced a new goal for the third modernization. The new goal is improving the global competitiveness with five main priorities of modernization. These priorities designed to implement steady progress in the number of 30 advanced countries, by ensuring the growth rate of the economy above the world average. Including accelerated technological modernization of the economy is a turning point of third modernization. (Ministry of Justice of the Republic of Kazakhstan. Institute of legislation and legal information, n.d.).

Also in December 2017, the state program "Digital Kazakhstan" was adopted with an implementation period of 2018-2022. The main goal of the program is to improve the quality of life and the competitiveness of the economy of Kazakhstan. To achieve this goal, the method of progressive development of the digital ecosystem is used. In addition, Kazakhstan is reorienting from a raw material to a production and service model by diversifying the national economy through the development of digital technologies and improvingthe provision of public services using information and communication services, which leads to the use of new labour market opportunities. Kazakhstan aims to increase the level of digital literacy of 83% of the population, increasing productivity in the priority areas of the economy, creating jobs, and increasing investment in start-ups by 2022 year.

According to the author, who is based on the results of his own analysis, it is necessary to improve the awareness of the population and their skills in the use of digital, information and communication technologies, in order to minimize the negative consequences of cyber-attacks. It is necessary, in the course of the digital transformation of Kazakhstan, to study and adapt the experience of other states, which will also serve to minimize possible risks, and most importantly, not to repeat the faults have been made by other countries.

Currently, Kazakhstan is continuing to spread advanced technologies for their effective use in public administration. This has a positive impact not only on the overall effectiveness of the government, but also on the social situation and the economic situation of the country. However, the implementation of technologies with that value carry their own risks associated with their protection and security, so the authors propose that it is necessary to consider the possibility of restricting access through reducing the tariff for mobile services and the Internet. In addition, the author suggests that the government and business with the involvement of civil society should control the process of mastering new technologies in order to reduce the risks of inequality of implemented technologies. Only through such control it is possible to achieve a certain goal:

1. universal recognition
2. trust of the population
3. successful implementation of strategic objectives.
4.

Isabaeva Symbat and Botagoz M. Yesseniyazova, during their analysis, were unable to determine a clear trajectory of the strategic plan on cybersecurity in the country. Government identified only the main directions without their implementation assessment. Therefore, Kazakhstan needs to develop and adopt a cybersecurity strategy for a thorough study of the strategies of successful countries. An important part of this step is the adaptation of these strategies considering Kazakh national, cultural, and mental characteristics.

Another cybersecurity problem in Kazakhstan that the authors highlight is the lack of highly qualified, certified experts in cybersecurity. Therefore, they propose a state policy to focus on attracting such specialists from other countries, as well as on training highly qualified specialists in information security within the country. It will also be effective if the heads of state bodies devote time for their employees for their self-training and self-development, through learning from the best practices of the world. These steps with a high probability will make it possible to avoid faults and risks faced by other nations. On the other hand, we cannot underestimate the current achievements of Kazakhstan over the years of independence in the field of cybersecurity and digitalization, but we should understand that there is still a lot of areas for development. Also, in the course of the analysis, despite all the similarities, it was noted that Kazakhstan focused on general issues of digitalization, while the Russian Federation is more focused on the digitalization of the economy in general with achieving goals on a global mass time.

"After analysing the existing performance indicators in international rankings and their impact on socio-economic development of the country, and with the view discussed in the article the achievements of foreign countries, the authors come to the conclusion about the necessity of active measures by Kazakhstan to development of digitization and cybersecurity" – quote from article (Symbat & Yesseniyazova, 2019). For the development of digitization and cybersecurity, we need additional funds that can be obtained through attract foreign investors. It is also necessary to create appropriate conditions for business development in the IT industry for domestic and foreign companies to attract foreign investors and the overall development of healthy competitive development in the IT industry.

However, the author acknowledges in the conclusion that additional further deep study is needed in order for the adoption and implementation of national projects and programs in terms of cybersecurity and digitalization to be risk-free and with minimal threats.

3.5 How do people view or feel about protecting their data in the public domain, .e.g., on the internet?

The analysed source could answer the question. Source name "Cybercrime risk awareness rate among students in Central Asia" (Ismailova, et al., 2019) written by Rita Ismailova, Gulshat Muhametjanova, Tunç Durmuş Medeni, Ihsan Tolga Medeni, Demet Soylu & Omar Azimbek Dossymbekuly in 2019 as part of the Information Security Journal:

A Global Perspective. The authors believe that organizations and countries forgetting to raise awareness among users while investing in and developing the technologies. And without awareness among users is impossible to assure information security.

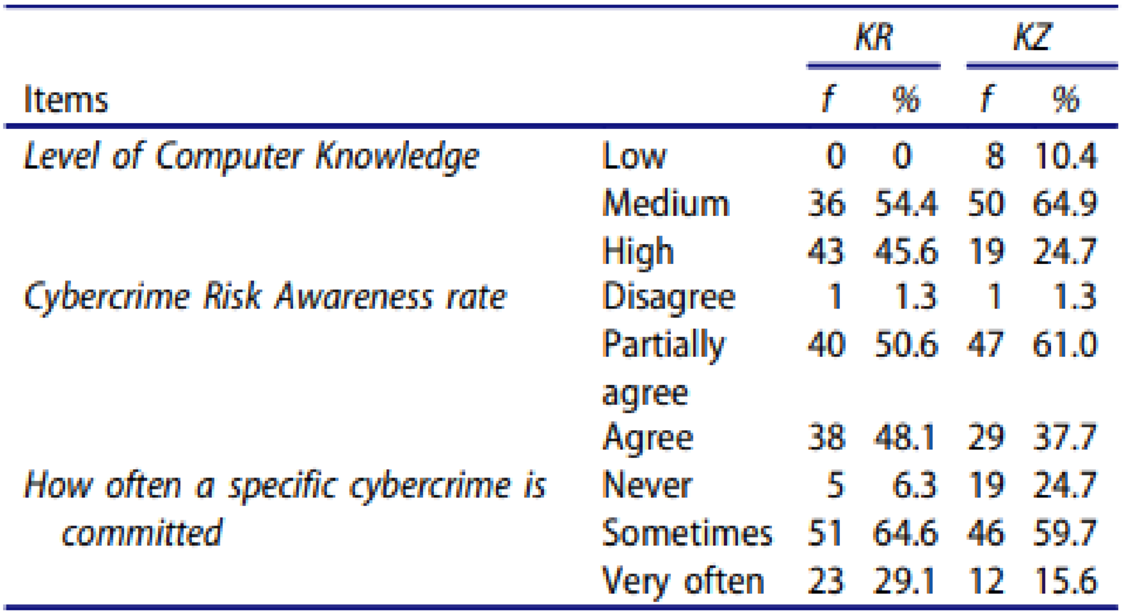
In general, we can say that among young people the level of awareness of users about information security is still extremely low. And this is a threat, because we can already conclude committing crimes in cyberspace no longer require complex skills or techniques, since the Internet has spread to all areas of life, and there are many programs and uncontrolled forums discussing malicious software. Moreover, as it turned out in the course of a study in one of the countries, young people did not perceive cybercrime as something illegal. (Ismailova, et al., 2019). Therefore, the authors believe that it is necessary to raise the level of awareness in the field of information security, especially among young people.

According to the International Telecommunication Union survey In Central Asia, in 2017, Kyrgyzstan is in 'Initiating' stage, Kazakhstan is in 'Maturing' stage. Kazakhstan is ranked #83 with 0.352 points and Kyrgyzstan #97 with 0.270 points (the International Telecommunication Union, 2017). Both states are described with respect to the Global Cybersecurity Index, which is based on the following pillars:

1. Legal
2. Technical
3. Organizational
4. Capacity Building
5. Cooperation

But despite the higher position of Kazakhstan, it has low scores on 'Public Awareness Campaigns'. Public Awareness Campaigns are part of the capacity building. In this study, the authors tried to find out whether there is an influence of place of residence and characteristics of nations, histories on the information security awareness rate of students. To achieve this goal the quantitate approach was used. Survey conducted in public universities in Almata (Kazakhstan) and Bishkek (Kyrgyzstan). In the questionnaire, there were a total of 51 questions[4]

The first were questions in which you need to choose one of several answers to a question related to general knowledge level analysis. According to the results 64.9% Kazakhstan and 54.4% Kyrgyzstan participants perceive themselves as having a medium level of computer knowledge, 10.4% Kazakh and 0% Kyrgyz students think they have low level of computer knowledge. You can see the results in the table.



		KR		*KZ*	
Items		*f*	%	*f*	%
Level of Computer Knowledge	Low	0	0	8	10.4
	Medium	36	54.4	50	64.9
	High	43	45.6	19	24.7
Cybercrime Risk Awareness rate	Disagree	1	1.3	1	1.3
	Partially agree	40	50.6	47	61.0
	Agree	38	48.1	29	37.7
How often a specific cybercrime is committed	Never	5	6.3	19	24.7
	Sometimes	51	64.6	46	59.7
	Very often	23	29.1	12	15.6

Table 3-2 General knowledge level analysis made by the author. Table developed by author

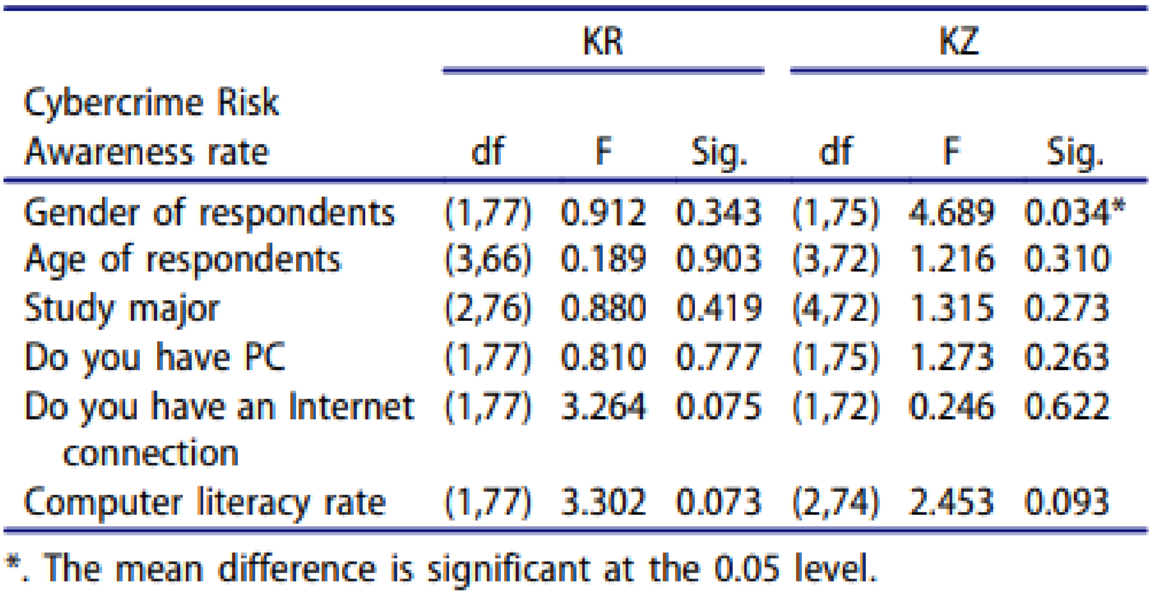
To answer the following questions, students were asked to determine how much they agree or disagree with statements related to understanding of how often a specific cybercrime is committed. The frequency analysis results look like this:

- 64.6% of Kyrgyz students and 59.7% of Kazakh students have chosen “committed sometimes”, this was the medial answer;

[4] 6 questions are demographic ones, 6 questions are on general computer literacy, 29 questions on cybercrime risks awareness, in 10 questions students were asked to answer how often, in their opinion, certain crimes are committed.

- 29.1% of respondents from Kyrgyzstan and 15.6% of respondents from Kazakhstan stated that is a specific cybercrime occurs very often;
- 6.3% of Kyrgyzstan students stated that cybercrimes never take place, while for Kazakhstan the percentage is higher – 24.7%

As a next step, the authors conducted several separate One-way Analysis of Variance (ANOVA) for each country separately. First, in order to check which independent variables, have an impact on the cybercrime risk awareness rate of students. As independent variables: gender of respondents, age of respondents, study major, having PC, having an Internet connection and computer literacy rate were used. You can see the results in the table.



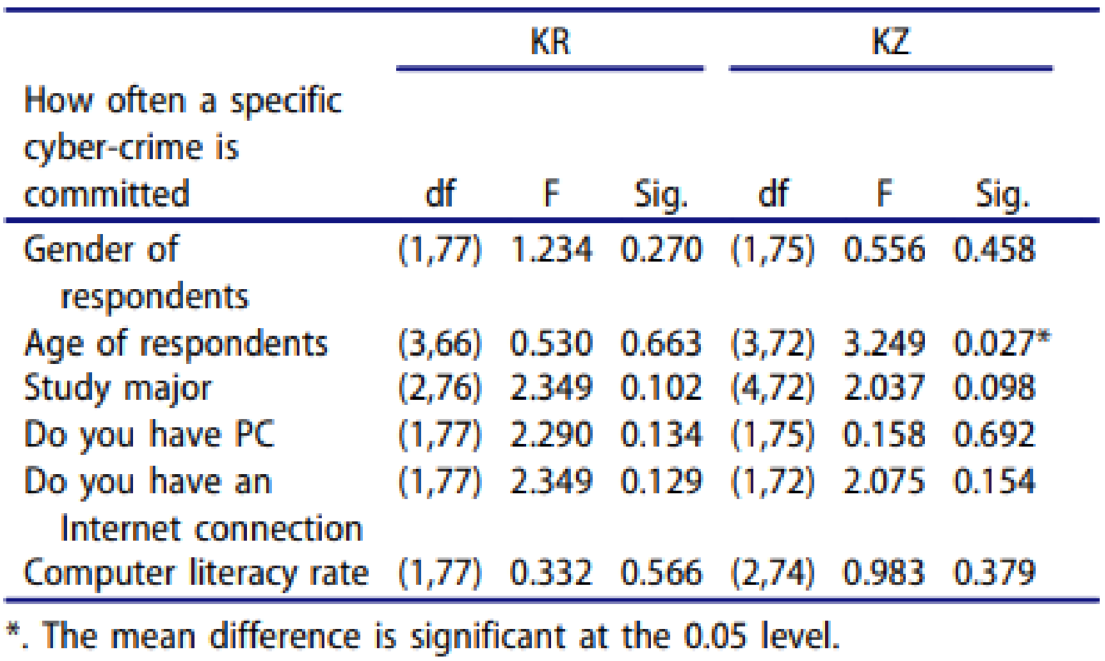
	KR			KZ		
Cybercrime Risk Awareness rate	df	F	Sig.	df	F	Sig.
Gender of respondents	(1,77)	0.912	0.343	(1,75)	4.689	0.034*
Age of respondents	(3,66)	0.189	0.903	(3,72)	1.216	0.310
Study major	(2,76)	0.880	0.419	(4,72)	1.315	0.273
Do you have PC	(1,77)	0.810	0.777	(1,75)	1.273	0.263
Do you have an Internet connection	(1,77)	3.264	0.075	(1,72)	0.246	0.622
Computer literacy rate	(1,77)	3.302	0.073	(2,74)	2.453	0.093

*. The mean difference is significant at the 0.05 level.

Table 3-4 Cyber security awareness rates differences between Kazakhstan and Kyrgyzstan students made by the author. Table developed by author

The test result is as follows: in Kazakhstan there is a statistically significant difference between cybercrime risk awareness rate of male and female students with F (1, 75) = 4.689, $p < .05$ and mean difference of −0.191. Which means female students have higher cybercrime risk awareness rates than male students. For Kyrgyz students did not show statistically significant differences in terms of all independent variables, as well as for other Kazakhstan data.

Second, to check which independent variables, have an impact on the how often cyber-crimes committed rtes. As independent variables: gender of respondents, age of respondents, study major, having PC, having Internet connection and computer literacy rate on knowledge of how often a specific cybercrime is committed. The test result is like the previous ones and looks like this: in Kazakhstan there is a statistically significant difference between specific cybercrime is committed of age groups male and female students with F (3, 72) = 3.249, p < .05. To find the highest means, the post-hoc analysis was carried out. The results look like this, 19–20 age groups have the highest means. One can sum it up to the conclusion that students of this age group have a better understanding of crime frequency committed over cyberspace. You can see the results in the table.



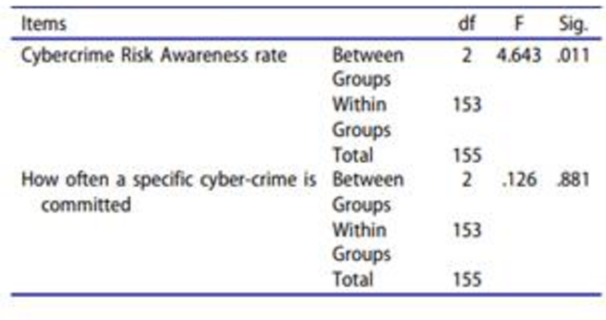
	KR			KZ		
How often a specific cyber-crime is committed	df	F	Sig.	df	F	Sig.
Gender of respondents	(1,77)	1.234	0.270	(1,75)	0.556	0.458
Age of respondents	(3,66)	0.530	0.663	(3,72)	3.249	0.027*
Study major	(2,76)	2.349	0.102	(4,72)	2.037	0.098
Do you have PC	(1,77)	2.290	0.134	(1,75)	0.158	0.692
Do you have an Internet connection	(1,77)	2.349	0.129	(1,72)	2.075	0.154
Computer literacy rate	(1,77)	0.332	0.566	(2,74)	0.983	0.379

*. The mean difference is significant at the 0.05 level.

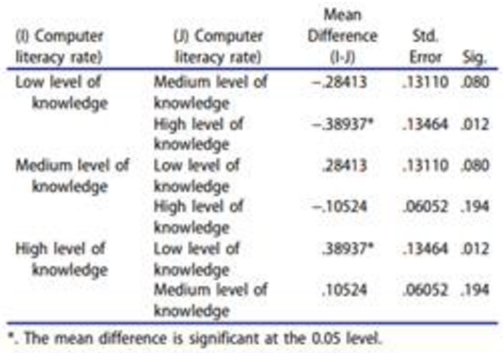
Table 3-5 Cyber security awareness rates differences in terms of factors between Kazakhstan and Kyrgyzstan students made by the author. Table developed by author

Third, ANOVA testing showed that how often a specific cybercrime is committed does not depend on their computer literacy, but cybercrime risks awareness of students depends on their computer literacy. The difference was found to be significant in a 95% confidence interval. The further analysis showed that the mean difference of cybercrime risk awareness rate was significant between students with low level and high level of computer literacy.

There is a clear pattern showing the increase of cybercrime risk awareness rate as the computer literacy rate increases. You can see the results in the tables.



Items		df	F	Sig.
Cybercrime Risk Awareness rate	Between Groups	2	4.643	.011
	Within Groups	153		
	Total	155		
How often a specific cyber-crime is committed	Between Groups	2	.126	.881
	Within Groups	153		
	Total	155		



(I) Computer literacy rate)	(J) Computer literacy rate)	Mean Difference (I-J)	Std. Error	Sig.
Low level of knowledge	Medium level of knowledge	−.28413	.13110	.080
	High level of knowledge	−.38937*	.13464	.012
Medium level of knowledge	Low level of knowledge	.28413	.13110	.080
	High level of knowledge	−.10524	.06052	.194
High level of knowledge	Low level of knowledge	.38937*	.13464	.012
	Medium level of knowledge	.10524	.06052	.194

*. The mean difference is significant at the 0.05 level.

Table 3-6 ANOVA testing results in the increase of cybercrime risk awareness rate and the computer literacy rate dependency made by the author. Table developed by author

The last was an independent samples t-test, to understand if there is a difference in cybercrime risks awareness rate, understanding of how often a specific cybercrime is committed and the computer literacy rate in terms of students' country of residence. Results the mean score of Kyrgyz and Kazakh students was 2.4733 and 2.3980 out of 3, respectively. The cybercrime risks awareness rate of Kyrgyz and Kazakh students does not differ. This means that most students from both countries are aware of crimes committed over cyberspace and they can clearly define these crimes. However, there are differences in defining the frequency with which these crimes are committed between Kazakh students (1.9334 out of 3) and Kyrgyz students (2.318 out of 3). Kazakhstan residence fail in defining the frequency with which these crimes are committed.

The author believes that It can be concluded that students from both countries are aware of crimes committed in cyberspace and can clearly identify these crimes, as more than 98% of students agreed or partially agreed with the statements during the survey, thus showing a high level of awareness without a statistically significant difference between countries. However, some differences in the answers appeared during the study: 24.7% of Kazakh students and 6.3% of Kyrgyz students stated that cybercrimes have never happened, it can be concluded that they cannot determine the frequency with which these crimes are committed. If in Kyrgyzstan this is a relatively low percentage, then for Kazakhstan a quarter of students are not aware of cyber-attacks.

The authors found that respondents had a relatively high level of awareness of cybercrime but did not appear to have more advanced knowledge in the area, leading respondents to state that online crime occurs infrequently. Considering all of the above, it can be concluded that Kazakh users are less aware of the risks. However, the authors believe that a more detailed study is needed to assess the depth of knowledge of Kyrgyz users. Another observation made by the authors is that the level of computer literacy of respondents and awareness of the risks of cybercrime are directly dependent on each other. This proves a clear pattern in which cybercrime risks awareness increases as the level of computer literacy increases. Speaking of factors that may affect the level of awareness of cybercrime, two conclusions are drawn based on observations:

- *Kazakh female students have higher rates of awareness of the risks of cybercrime than male students.*
- *Students in the 19-20 age group have a better understanding of the frequency with which this or that crime is committed in cyberspace.*

In conclusion, the authors consider that students in the two countries of Central Asia have the same level of information security knowledge, despite a statistically significant difference in cybercrime awareness. In their opinion, there is a need to continue to raise awareness, by implementing a security tool in higher education institutions.

3.6 What challenges does Kazakhstan face about cybersecurity?

We will look at the answer to this question through the source “Status, perspectives and main directions of the Development of cybersecurity of information and Communication transport systems of Kazakhstan” (Akhmetov, 2018) written by Berik Akhmetov in 2018 as part of the Reports of the national academy of sciences of the republic of Kazakhstan. The reason for choosing this article is that for Kazakhstan, these issues and the problem of information protection and information and cyber security are even more important due to the size of the territory and the geopolitical location of Kazakhstan, with political and socio-economic policies aimed at further strengthening of sovereignty. Therefore, this means that the active expansion of the information technology and critical information transport systems in Kazakhstan is accompanied by the appearance of new cyber threats, which are important to pay attention to already at this moment of development.

The author believes that transport industry is passing through the stage of transformation and adaptation to new digital technologies in the whole world and modern Kazakhstan. This transformation makes transport systems already are more vulnerable to cyberattacks because they have an active connection to the Internet both in the vehicles themselves and in the components of the transport infrastructure. It could be video surveillance cameras, information boards, smart stops, cloud infrastructure, etc.

According to the author source, only during the period from March 2015 to May 2016 information and communication transport systems has been compromised to DoS attacks and other destructive influences by computer intruders more than 44 times (IBM, n.d.). This information is outdated, but it's still important to understand that cyberattacks are nothing new and require increased attention, almost all elements of the information and communication transport systems can become objects of cyberattacks. And in turn, insufficient attention to the problem of cybersecurity can lead to negative consequences, such as:

a. to loss of control and its interception by strangers
b. failures in the operation of transport dispatch control systems
c. in the worst case, there may be consequences with human casualties
d. As a result, Akhmetov stated the following conclusions (Akhmetov, 2018):

1. *"was shown that in order to carry out effective information security and cyber security policy for information and communication transport systems, for the selection and implementation of information security systems, it is necessary to analyse cyber threats and vulnerabilities for such systems taking into account the specificity of each type of transport."*
2. *"it is necessary to develop a unified methodology for the creation of protected situational centres of the transport adapted to the conditions of potential targeted cyber-attacks."*

3. *“it is necessary to continue comprehensive research on the modelling of potential intruder strategies for the implementation of complex targeted cyberattacks directed against information and communication transport systems. This will allow more effective evaluation of the reliability of the operation of information security systems for information and communication transport systems.”*

4 Practical Part

The practical work aims to fulfil several objectives. The main objective of the thesis is to adapt an existing model of user's perceptions towards cyber-security policy in Kazakhstan. To do this, we have divided this objective into several separate priorities in the form of Research Focus. The first is "To discern how the average, young citizen in Kazakhstan feels about cyber-security policy development". To complete this objective, we conducted a survey among students of departments related to cybersecurity and IT.

The second objective is "To understand what the existing government and industrial responses are to rising cyber-security challenges. To understand this model, we conducted a literature review that described the stages of cyber-security development in Kazakhstan and the actual situation. Moreover, we conducted focus group interviews with cyber security professionals in Kazakhstan to gain a broader understanding of the problem.

The final task is "To explore the role and/or suggested solutions of young citizens in the future of cyber security policy development towards strengthening government, IT industries, and e-commerce as consistent with global standards". To meet this objective, we also conducted focus group interviews with cybersecurity professionals and cybersecurity and IT students.

Since we collected the surveys, we need to analyse them statistically. To do this, we used a proper tools and methods.

4.1 Methodology

4.1.1 Questionnaire survey

To conduct a survey, several tools were used to collect, create, distribute and analyze the data. Firstly, Microsoft Word was used to collect information on the topic and to create question templates. This involved researching the specific topic of the survey and identifying relevant questions that would provide the necessary data for the study. The question templates were then created, which included closed-ended questions, multiple choice questions, and open-ended questions.

Next, Google Forms was used to create the online survey using the already created questions. Google Forms allowed for easy creation of the survey and customization of the questions. The online platform also allowed for pre-collection of answers, meaning respondents could fill in the survey at their convenience. Once the survey was created, it was time to distribute it to potential respondents. Facebook, WhatsApp, and Telegram were used as social media platforms to distribute the link with access to the survey. These platforms allowed for a wide reach and enabled the survey to be distributed to a large number of people, making it more likely to gather a representative sample.

Finally, Microsoft Excel was used to store and pre-analyze the survey results. The responses were downloaded from Google Forms and imported into Excel, where they were cleaned and sorted. Basic descriptive statistics such as mean, mode, and median were used to summarize the data. This allowed for the identification of patterns and trends in the data, which could then be used to draw conclusions and make recommendations.

In summary, a combination of Microsoft Word, Google Forms, Facebook, WhatsApp, Telegram, and Microsoft Excel were used to create, distribute, and analyze the data collected through the survey. This approach allowed for a thorough and detailed analysis of the data, enabling the researcher to draw meaningful conclusions and make informed decisions.

4.1.2 Semi-structured interviews

To gather information through interviews, Microsoft Word was used for various purposes. Firstly, it was used to collect information on the topic and to highlight relevant questions related to the model. These questions were compiled into templates which could be used during the interviews. Secondly, it was used to store the results of the interviews after they were conducted. This helped to ensure that all responses were recorded accurately and in a timely manner.

Invitations to the interviews were sent out via email using both Gmail and Mail.ru. These emails included the date and time of the interview, as well as any other relevant details such as the location or method of the interview (e.g. in-person or via video call). To coordinate the details of the meeting, Facebook, WhatsApp, and Telegram were used. These communication platforms allowed for easy communication and coordination with the interviewees. This included confirming the time and location of the interview, as well as any other relevant details such as the agenda or topics to be covered during the interview.

During the interviews, notes were taken on Microsoft Word to ensure that all responses were recorded accurately. The notes included both direct quotes and summaries of the responses provided by the interviewees. These notes were later used to identify themes and patterns in the data and to draw conclusions based on the responses received.

Overall, the use of Microsoft Word, Gmail, Mail.ru, Facebook, WhatsApp, and Telegram allowed for a streamlined process of gathering data through interviews. These tools were effective in coordinating with the interviewees and recording their responses accurately, which in turn helped to ensure the quality of the data collected.

4.1.3 Analysis framework

To analyse the collected data, I used a combination of IBM SPSS Statistics, Excel, and Google Forms. Firstly, I imported the data collected from the survey into Google Forms with pre-analysis from Google framework. This involved organizing the data into Excel and cleaning any errors or inconsistencies in the data. I then used organized data to create graphs and visualizations, which helped me to quickly identify trends and patterns in the data.

Next, I used IBM SPSS Statistics to conduct descriptive statistics on the data, which helped to provide a more in-depth analysis of the data. This included calculating the mean, median, and standard deviation of the data, as well as creating frequency tables and charts to display the distribution of the data. Using these statistical tools, I was able to identify key trends and patterns in the data and gain a deeper understanding of the relationships between different variables.

Finally, I used Excel to create additional graphs and visualizations based on the results of the IBM SPSS analysis. These graphs and visualizations helped to further illustrate the trends and patterns in the data and provided a clearer picture of the overall findings of the analysis.

4.2 Questionnaire survey

To adapt an existing model of user's perceptions towards cyber-security policy in Kazakhstan we need to collect the opinions of the residents of Kazakhstan on how the model currently exists, in addition we have the task "To discern how the average, young citizen in Kazakhstan feels about cyber-security policy development". To achieve the second of these goals and partially achieve the first goal we conducted a survey among students of departments related to cybersecurity and IT via the Internet using the tool Google Forms.

The main reason I decided to conduct a survey among IT students at Kazakhstan universities is that Kazakhstan is a developing country, and the country is currently undergoing digitalization and technicalization, hence collecting the views of the entire population may distort the actual model of user perception of cybersecurity policy, due to their lack of awareness of cybersecurity and IT. In my opinion, IT students' model of user perception of cybersecurity policy is the most accurate representation of the model for all of Kazakhstan now and in the future, because IT students will be the foundation for the future development of the IT sphere in Kazakhstan, they will take up employment positions in both medium and small businesses and government agencies. We hoped to get over 100 responses to our mixed-method survey, which involve a questionnaire with scalable answers to collect quantitative data, and descriptive questions with to collect qualitative data.

Ultimately, by conducting this survey, we were able to analyse it to determine the state of cybersecurity awareness among Kazakhstan's younger generation, already familiar with new technologies and using them in their daily lives. The algorithm for creating and conducting survey was as follows:

1. First step, we selected our target audience.
2. Second step, I identified the topics and questions that would help us analyse the existing model.
3. The third step, I compiled questions of several types that relate to the highlighted topics in the previous step and fit our target audience.
4. Step four, I uploaded my questions to Google Forms.
5. The fifth step, through social media and messengers I distributed the link to the survey.
6. Sixth step, waiting for the results.
7. Seventh, collecting all the results and preparing for later analysis.
8. Below are the questions we used, as well as screenshots of the questionnaire in Google forms, and our results in an Excel document.

The first type of question was needed to identify basic information about the respondents to use this information for further analysis, even though the questions were asked anonymously.

«Age group»

- *12-16*
- *17-21*
- *22-26*
- *27-31*
- *31+*

«Gender»

- *Male*
- *Female*

«Occupation (faculty, year of study/ work, position) »

The next type of question was needed to identify the computer literacy of respondents, so that the results could be scaled up to the entire computer-literate population of Kazakhstan.

«Do you have a PC with internet connection? »

- *I have PC with internet connection*
- *I have PC without internet connection*
- *I don't have PC, but I have internet connection*
- *I don't have PC and internet connection*

«Please show as the level of computer knowledge - Rate your knowledge on the scale from 1 to 10, with 1 – being weak and 10 being strong»

- *Knowledge of PC*
  - *1-10*
- *Knowledge of hardware*
  - *1-10*
- *Knowledge of OS*
  - *1-10*

«How confident, if at all, do you feel that you know how to keep your personal devices and online accounts secure? »

- *Very confident*
- *Confident*
- *Neither confident nor unconfident*
- *Unconfident*

- *Very unconfident*

A third type of question was needed to determine the respondents' awareness of cybercrime and cybersecurity

«Which of the following applies to cybercrime?»

- *Hacking*
- *Cyber terrorism*
- *Malwares*
- *Online gambling*
- *Cyber stalking*
- *Virus dissemination*
- *Phishing*
- *Salami attack*
- *Child pornography*
- *Spoofing*
- *None of the Above*

«How safe do you feel about your information when you are online?»

- *Very safe*
- *Safe*
- *Not safe*
- *Don't know*

«Do you feel it is essential to be safe online? »

- *Strongly agree*
- *Agree*
- *Strongly disagree*
- *Disagree*
- *Neutral*

«Is the password for your email account being used for any other online accounts?»

- *Yes*
- *No*

«Are you currently using your web browser or a password manager app to save or create passwords?»

- *Yes*
- *No*

Next, the question type of question was needed to determine how often respondents' encounter cybercrime on the Internet in Kazakhstan

«How many times have you been a victim of a cybercrime?»

- *Never*
- *1 time*
- *2-5 times*
- *More than 5 times*
- *Question Title*

«Have you ever experienced any of these situations?»

- *Trojan or malware*
- *Auto generated mails to your inbox*
- *Publishing obscure material on your profiles*
- *Confidential reports/information being hacked*
- *Loss of personal data*
- *Never experienced such situation.*

The next type of question was needed to determine the respondents' attitudes towards cyber security laws.

«Do you think that the laws in effect are able to control cyber criminals?»

- *Strongly agree*
- *Agree*
- *Strongly disagree*
- *Disagree*
- *Neutral*

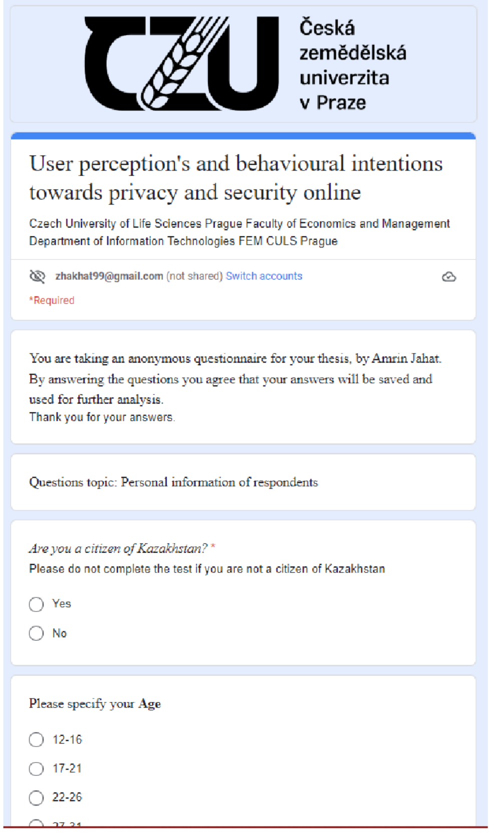
«Were you aware that victims of fraud and cybercrime should report it to Action Fraud?»

- *I was aware, and I have/would use the service*
- *I was aware, but would not use the service*
- *No, I was not aware.*

The last type of question was needed to determine the respondents' attitudes towards cyber security laws in Kazakhstan.

«Can you identify the main threats to the further development of digital services in the Republic of Kazakhstan?»

- *lack of qualified specialists*
- *threat to respondents is cyber-attacks, i.e., the vulnerability of networks*
- *low level of digital literacy of the population*
- *poorly developed system of service providers no threats.*



Česká zemědělská univerzita v Praze

User perception's and behavioural intentions towards privacy and security online

Czech University of Life Sciences Prague Faculty of Economics and Management Department of Information Technologies FEM CULS Prague

zhakhat99@gmail.com (not shared) Switch accounts

*Required

You are taking an anonymous questionnaire for your thesis, by Amrin Jahat. By answering the questions you agree that your answers will be saved and used for further analysis.
Thank you for your answers.

Questions topic: Personal information of respondents

Are you a citizen of Kazakhstan? *
Please do not complete the test if you are not a citizen of Kazakhstan

○ Yes

○ No

Please specify your Age

○ 12-16

○ 17-21

○ 22-26

Figure 2. Survey |Example

4.3 Semi-structured interviews

The second is a series of focus group interviews that will then be converted into a statistical representation of the responses. The focus groups will be made up of both students and graduates of IT universities and people already working in the IT field in Kazakhstan. This qualitative data will provide a detailed picture of user perceptions and behavioural intent regarding online privacy and security in Kazakhstan. Because of this decision, we will be able to see what the condition of cyber-security awareness among. Moreover, IT students in universities in the future will be the base for the development of IT area in Kazakhstan, they will occupy working positions both in medium and small businesses, and in government structures. After we have compiled the user's perceptions towards cyber-security policy is the most accurate representation of the model for the whole of Kazakhstan based on the younger generation of Kazakhstan is, who are already familiar with new technologies and use them in everyday life. We should consider this issue in more detail by adding details to this motel through focus group interviews.

The interviews took place freely via chat rooms and emails. Because of the nature of this method, in some cases more prepared questions had to be used. On the other hand, in other cases, almost no pre-designed questions were used, as the interviewers showed a high level of awareness of the different topics and were able to talk about different sides of the issue. Before describing the results of this work, I would like to point out that there were limitations that had not been anticipated before studying this issue. After reviewing the literature, a list of interviewees with jobs in different fields related to computer science and cybercrime was compiled. Several questionnaires were sent, which were answered negatively, and some were ignored. Subsequently, it turned out that the questions were ignored and refused to be answered due to the fact that information about cybersecurity in Kazakhstan is a top secret, so interviewers who had previously agreed to cooperate after seeing the list of questions refused to talk about these topics in general. Despite this, our project aims to explore specifically the younger generation's vision of cybersecurity, so the number of interviewees under 26 was increased to fill gaps caused by the refusal of three participants over 26, whose personal information would not be disclosed at their request.

We were interviewed:

- 1 person whose personal information is unavailable because he ignored and did not participate in focus group interviews.
- 2 people whose personal information is unavailable because they refused to answer questions.
- Dauletbek Kaysar Nurlanuly, a mathematics graduate from Nazarbayev University, now works at the Institute of Smart Systems and Artificial Intelligence, developing speech recognition algorithms.
- Maulenov Erzat Mazhituly, graduated from Astana IT University in 2022, now works for KPMG, big4, IT Consultant.
- Bauyrzhanov Bakhtiyar Kuanyshevich, a graduate of Nanjing University of Post and Telecommunications, in Nanjing, China, majoring in Computer Science. Additional Information: Currently staying in Kazakhstan, looking for a job in cybersecurity sphere.
- Kasymkhan Akimbek Talgatuly, graduated from Nazarbayev University, works as an English teacher.
- Khafizov Almaz Erikovich
- Kazihan Margulan Muttahiuly, 1st year master's student majoring in Computer Science in Nazarbayev University ("NU" is a top research-oriented university in Kazakhstan)

Interviews were conducted in Russian, Kazakh and English languages. Examples of responses are given below:

4.3.1 Question "Do you think it is important to be safe online?"

Akimbek Kasymkhan:

"Yes, but unfortunately not everyone knows about it, especially children. Right now, I work as an English teacher in a private IT school, so I feel keenly the need to raise awareness about the dangers of the Internet among people. Because of the specialized

training, our curriculum covers topics such as internet safety and the dangers that it stores, and we also discuss cybersecurity a little bit. Children, who have been studying with me since they are young, use computers and the internet and often spend more time on the internet with their families and parents, but they are not familiar with the basic rules of using the internet and are therefore very vulnerable to scammers. So, it seems to me that one should not only keep an eye on their safety on the internet, but also on the safety of those around them and especially their family. But Kazakhstan is not yet at an IT Education level, so parents themselves are unfortunately not aware of many of the pitfalls, but that's a whole other issue..."

Bauyrzhanov Bakhtiyar

"Yes, the need to be safe online and in cybersecurity is moving to a new level every day in order in direct proportion to the possible dangers that lie in wait for everyone."

An additional subtle question: *"What do you mean by saying that possible dangers are being taken to the next level?"*

"I want to say that the number of threats posed by the Internet and the criminals that are on it is growing, as is the number of possible frauds. This is happening all over the world and in Kazakhstan as well. But the situation in Kazakhstan is slightly different. As we are just going through digitalization and the level of cybercriminals lags behind other countries, but it's not for long. When I left the country, I felt that right now with the development of technology and the level of crime would increase and no longer the ordinary population would be at risk, but companies and even government agencies. That's why I chose this field for my profession, because Kazakhstan needs competent programmers versed in cybersecurity, and there are plenty of jobs and good pay."

4.3.2 Question “What do you understand by the term cyber security?”

Maulenov Erzat

"It's a very broad term, and it seems to me that every profession and area of IT has a different understanding of the term. I will answer the question in my capacity as an IT consultant for one of the Big Four Accounting Firms. In our field cybersecurity is about protecting all personal data of our clients. Because we use off-the-shelf foreign software, we do not have leaks. Another problem is the lack of awareness of some individuals, private businesses, who do not understand that they are also responsible for the security of their data. But such problems are occurring less and less frequently."

An additional subtle question: *"What kind of problems are you talking about, can you share?*

"If I omit all the details, dates and names, I can say that there have been times when clients have complained about leaks and then it turns out that they have leaked information because of a simple lack of diligence".

An additional subtle question: *"What do you think are the reasons for this and why are there fewer and fewer cases?*

"I think it's because of a lack of awareness of how to protect your data and especially how important data is. It is enough to explain how fraudsters can use data, which we do. I would like to believe that the general literacy of the population has increased and therefore there are fewer and fewer such cases."

Kazihan Margulan

"Cybersecurity is a subfield of Computer Science that focuses on data privacy and security. It is not limited to the Network Security, but also works on software architecture, ethics, and governance."

4.3.3 Question "Do you think that current laws are capable of controlling cyber criminals?"

Kazihan Margulan

"Laws are usually made in the administrative structure that is heavily loaded with bureaucracy, that is why the speed of law-making is not able to catch-up with the speed of IT progress. For that reason, most of the professional cyber criminals cannot be controlled."

4.3.4 Question "How do you feel about cyber security in Kazakhstan? Do you think it is at an adequate level? If you agree with the statement, tell why; if you don't agree with the statement, tell us what could be improved."

Dauletbek Kaysar

"I see Kazakhstan actively moving in the development of cyber security. Kazakhstan's hackers take first places in international hacker championships and Kazakhstan's cybersecurity start-ups are successful in the international market."

Bauyrzhanov Bakhtiyar

"In my opinion, modern operating systems with internal pre-installed antivirus are generally sufficient to cope with most viruses and the average user with a sufficient level of care may never encounter a cybercrime. However, identity theft is very common in Kazakhstan. Many cases of theft of personal social networking pages, followed by deception of friends and relatives of the victim take place every year. In my opinion, if such cases are not uncommon, it is scary to imagine the holes in cybersecurity at a higher level."

Kasymkhan Akimbek

"I think so. All that is missing is an education in cyber hygiene."

Kazihan Margulan

"Cybersecurity in KZ was very poor before TSARKA was established. Today it is on the competitive level in comparison with many other neighbouring countries. It is hard to measure the cybersecurity level in a country because Internet unites us. However, in terms of basic laws, jurisdictions and effort Kazakhstan is on a decent level."

Maulenov Erzat

"Based on my experience and that of my colleagues, I would like to say that "we are doing well", but all too often I hear in the news about these or other cyber-attacks and the damage they cause. There are probably many more cyber-attacks that the government is not telling us about. Remember, these reports mostly only talk about "unsuccessful" cyber-attacks once they are detected, the number of successful cyber-attacks is likely to surprise everyone."

4.3.5 Question "What do you think about the implementation of the Cyber Security Concept in Kazakhstan?"

Bauyrzhanov Bakhtiyar

"A much-needed concept. Increasing protection against third-party threats is a necessity that everyone must go through, but in our country cyber security is lagging far behind development. I stayed in close contact with programmers from Kazakhstan while I was training in China, and I can say from personal experience that even the approach to cyber security training in China is much more in-depth and thoughtful than the way the 'shield' of many companies that have government tenders is built. Our country is undergoing a major digital transition, many opportunities to get rid of bureaucracy in favour of digital documents are forcing us to increase Cyber Security of public institutions. On the contrary, apart from petty thefts, no major cybercrimes have occurred in our country, or at least I cannot recall hearing of any major scandal involving cybercrime."

4.3.6 Question "Can you identify the main threats to the further development of digital services in Kazakhstan?"

Kazihan Margulan

"One of the main reasons are the political concerns. IT solutions usually involve fairness and has strict rules, which some governments do not like. Other than that, there is a concern that most of the competitive IT specialists can earn more abroad, that is why they would rather choose to work abroad. But, on the other hand, there is still room for significant improvement. As the number of IT specialists in our country is increasing. I see many new competitions being held across the country, several IT universities have opened and are cooperating with our university. Many foreign teachers are attracted year after year. But it is important to understanding that, once we have many IT specialists, we will have many cyber criminals. We should be ready to control them in the cyberspace. I believe we have a good starting position overall."

Dauletbek Kaysar

"I see a threat in the level of training of IT staff, as well as the inability of the market to meet the needs of actively growing companies."

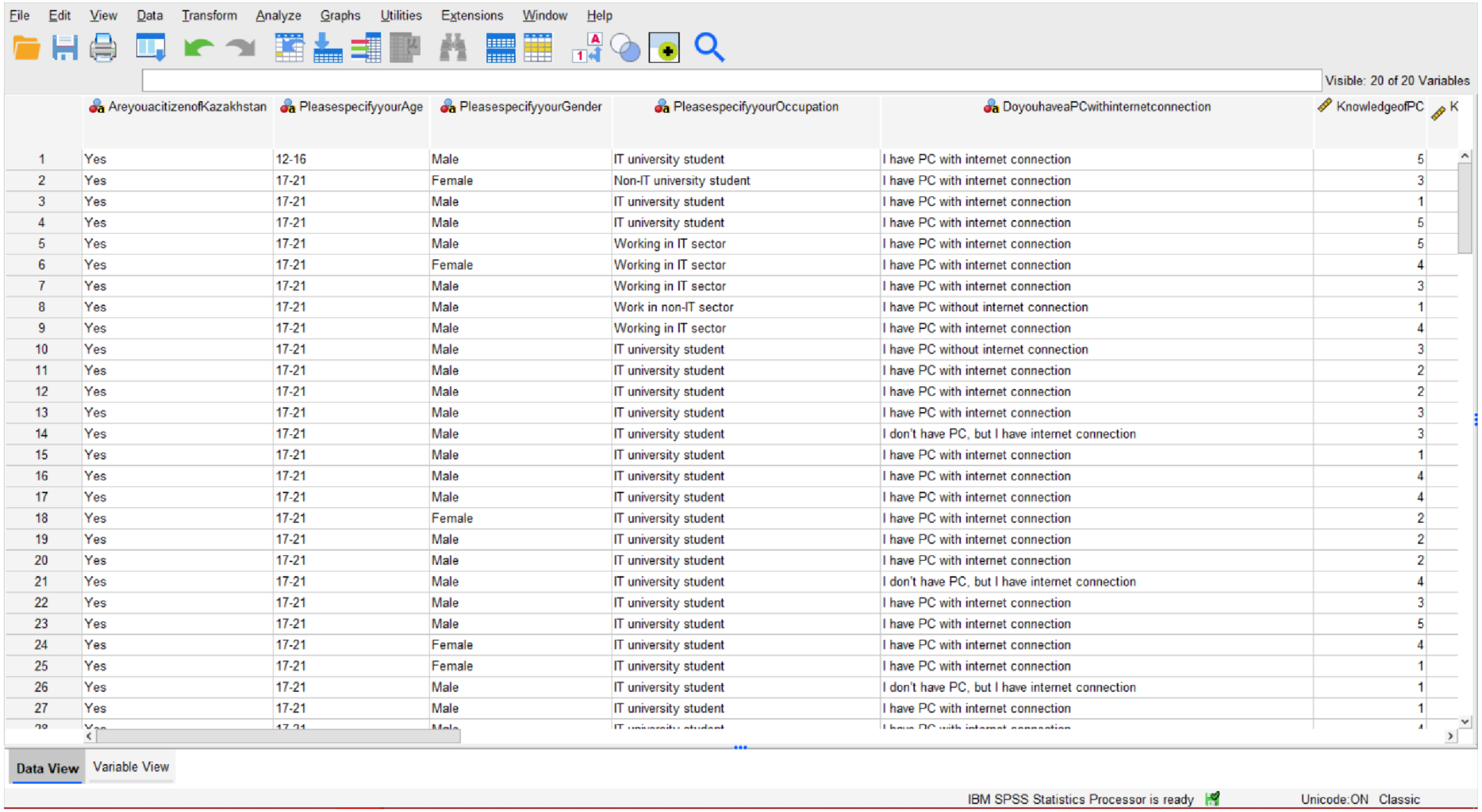
Kasymkhan Akimbek

"At the moment I cannot recall a major scandal involving the theft of personal information in our country. I believe that the explanation for this is either the relatively good cyber security of state institutions, or that cybercrime has not yet grown to a level that would be noticeable at this stage of the state's development. But it seems to me more likely to be the second one."

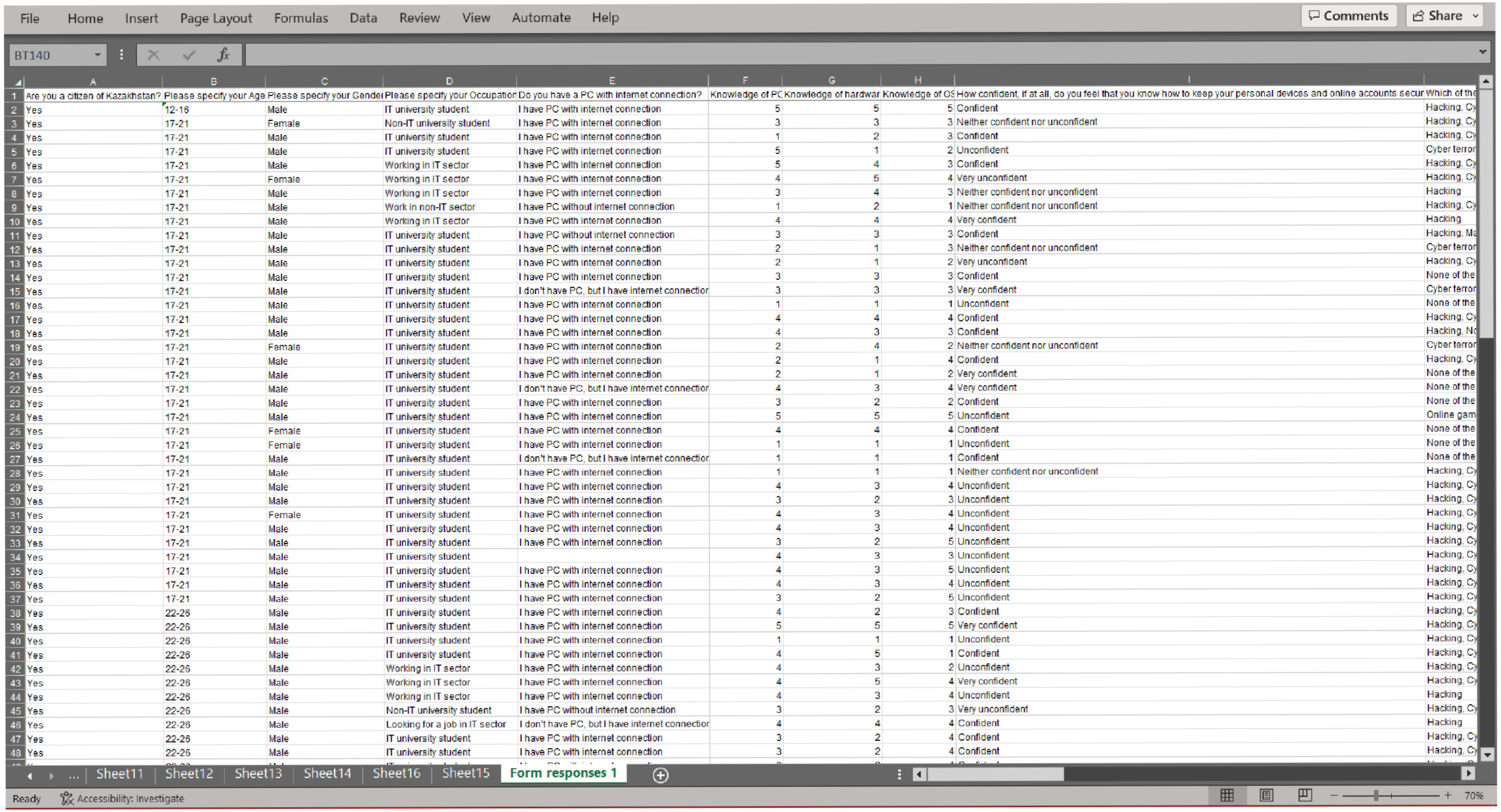
4.4 Analysis framework

We used data about opinions of the residents of Kazakhstan on how the currently model of user's perceptions towards cyber-security policy exists from the results of Questionnaire survey in Google Forms. We will use IBM SPSS Statistics, Excel, and Goggle Forms to analyse the data.

Figure 2 Screenshot of the data from IBM SPSS Statistics


File Edit View Data Transform Analyze Graphs Utilities Extensions Window Help
Visible: 20 of 20 Variables
Data View
Variable View
IBM SPSS Statistics Processor is ready
Unicode:ON Classic

	AreyouacitizenofKazakhstan	PleasespecifyyourAge	PleasespecifyyourGender	PleasespecifyyourOccupation	DoyouhaveaPCwithinternetconnection	KnowledgeofPC
1	Yes	12-16	Male	IT university student	I have PC with internet connection	5
2	Yes	17-21	Female	Non-IT university student	I have PC with internet connection	3
3	Yes	17-21	Male	IT university student	I have PC with internet connection	1
4	Yes	17-21	Male	IT university student	I have PC with internet connection	5
5	Yes	17-21	Male	Working in IT sector	I have PC with internet connection	5
6	Yes	17-21	Female	Working in IT sector	I have PC with internet connection	4
7	Yes	17-21	Male	Working in IT sector	I have PC with internet connection	3
8	Yes	17-21	Male	Work in non-IT sector	I have PC without internet connection	1
9	Yes	17-21	Male	Working in IT sector	I have PC with internet connection	4
10	Yes	17-21	Male	IT university student	I have PC without internet connection	3
11	Yes	17-21	Male	IT university student	I have PC with internet connection	2
12	Yes	17-21	Male	IT university student	I have PC with internet connection	2
13	Yes	17-21	Male	IT university student	I have PC with internet connection	3
14	Yes	17-21	Male	IT university student	I don't have PC, but I have internet connection	3
15	Yes	17-21	Male	IT university student	I have PC with internet connection	1
16	Yes	17-21	Male	IT university student	I have PC with internet connection	4
17	Yes	17-21	Male	IT university student	I have PC with internet connection	4
18	Yes	17-21	Female	IT university student	I have PC with internet connection	2
19	Yes	17-21	Male	IT university student	I have PC with internet connection	2
20	Yes	17-21	Male	IT university student	I have PC with internet connection	2
21	Yes	17-21	Male	IT university student	I don't have PC, but I have internet connection	4
22	Yes	17-21	Male	IT university student	I have PC with internet connection	3
23	Yes	17-21	Male	IT university student	I have PC with internet connection	5
24	Yes	17-21	Female	IT university student	I have PC with internet connection	4
25	Yes	17-21	Female	IT university student	I have PC with internet connection	1
26	Yes	17-21	Male	IT university student	I don't have PC, but I have internet connection	1
27	Yes	17-21	Male	IT university student	I have PC with internet connection	1



	A	B	C	D	E	F	G	H	I	
1	Are you a citizen of Kazakhstan?	Please specify your Age	Please specify your Gender	Please specify your Occupatior	Do you have a PC with internet connection?	Knowledge of PC	Knowledge of hardwar	Knowledge of OS	How confident, if at all, do you feel that you know how to keep your personal devices and online accounts secur	Which of the
2	Yes	12-16	Male	IT university student	I have PC with internet connection	5	5	5	Confident	Hacking, Cy
3	Yes	17-21	Female	Non-IT university student	I have PC with internet connection	3	3	3	Neither confident nor unconfident	Hacking, Cy
4	Yes	17-21	Male	IT university student	I have PC with internet connection	1	2	3	Confident	Hacking, Cy
5	Yes	17-21	Male	IT university student	I have PC with internet connection	5	1	2	Unconfident	Cyber terror
6	Yes	17-21	Male	Working in IT sector	I have PC with internet connection	5	4	3	Confident	Hacking, Cy
7	Yes	17-21	Female	Working in IT sector	I have PC with internet connection	4	5	4	Very unconfident	Hacking, Cy
8	Yes	17-21	Male	Working in IT sector	I have PC with internet connection	3	4	3	Neither confident nor unconfident	Hacking
9	Yes	17-21	Male	Work in non-IT sector	I have PC without internet connection	1	2	1	Neither confident nor unconfident	Hacking, Cy
10	Yes	17-21	Male	Working in IT sector	I have PC with internet connection	4	4	4	Very confident	Hacking
11	Yes	17-21	Male	IT university student	I have PC without internet connection	3	3	3	Confident	Hacking, Ma
12	Yes	17-21	Male	IT university student	I have PC with internet connection	2	1	3	Neither confident nor unconfident	Cyber terror
13	Yes	17-21	Male	IT university student	I have PC with internet connection	2	1	2	Very unconfident	Hacking, Cy
14	Yes	17-21	Male	IT university student	I have PC with internet connection	3	3	3	Confident	None of the
15	Yes	17-21	Male	IT university student	I don't have PC, but I have internet connectior	3	3	3	Very confident	Cyber terror
16	Yes	17-21	Male	IT university student	I have PC with internet connection	1	1	1	Unconfident	None of the
17	Yes	17-21	Male	IT university student	I have PC with internet connection	4	4	4	Confident	Hacking, Cy
18	Yes	17-21	Male	IT university student	I have PC with internet connection	4	3	3	Confident	Hacking, No
19	Yes	17-21	Female	IT university student	I have PC with internet connection	2	4	2	Neither confident nor unconfident	Cyber terror
20	Yes	17-21	Male	IT university student	I have PC with internet connection	2	1	4	Confident	Hacking, Cy
21	Yes	17-21	Male	IT university student	I have PC with internet connection	2	1	2	Very confident	None of the
22	Yes	17-21	Male	IT university student	I don't have PC, but I have internet connectior	4	3	4	Very confident	None of the
23	Yes	17-21	Male	IT university student	I have PC with internet connection	3	2	2	Confident	None of the
24	Yes	17-21	Male	IT university student	I have PC with internet connection	5	5	5	Unconfident	Online gam
25	Yes	17-21	Female	IT university student	I have PC with internet connection	4	4	4	Confident	None of the
26	Yes	17-21	Female	IT university student	I have PC with internet connection	1	1	1	Unconfident	None of the
27	Yes	17-21	Male	IT university student	I don't have PC, but I have internet connectior	1	1	1	Confident	None of the
28	Yes	17-21	Male	IT university student	I have PC with internet connection	1	1	1	Neither confident nor unconfident	Hacking, Cy
29	Yes	17-21	Male	IT university student	I have PC with internet connection	4	3	4	Unconfident	Hacking, Cy
30	Yes	17-21	Male	IT university student	I have PC with internet connection	3	2	3	Unconfident	Hacking, Cy
31	Yes	17-21	Female	IT university student	I have PC with internet connection	4	3	4	Unconfident	Hacking, Cy
32	Yes	17-21	Male	IT university student	I have PC with internet connection	4	3	4	Unconfident	Hacking, Cy
33	Yes	17-21	Male	IT university student	I have PC with internet connection	3	2	5	Unconfident	Hacking, Cy
34	Yes	17-21	Male	IT university student		4	3	3	Unconfident	Hacking, Cy
35	Yes	17-21	Male	IT university student	I have PC with internet connection	4	3	5	Unconfident	Hacking, Cy
36	Yes	17-21	Male	IT university student	I have PC with internet connection	4	3	4	Unconfident	Hacking, Cy
37	Yes	17-21	Male	IT university student	I have PC with internet connection	3	2	5	Unconfident	Hacking, Cy
38	Yes	22-26	Male	IT university student	I have PC with internet connection	4	2	3	Confident	Hacking, Cy
39	Yes	22-26	Male	IT university student	I have PC with internet connection	5	5	5	Very confident	Hacking, Cy
40	Yes	22-26	Male	IT university student	I have PC with internet connection	1	1	1	Unconfident	Hacking, Cy
41	Yes	22-26	Male	IT university student	I have PC with internet connection	4	5	1	Confident	Hacking, Cy
42	Yes	22-26	Male	Working in IT sector	I have PC with internet connection	4	3	2	Unconfident	Hacking, Cy
43	Yes	22-26	Male	Working in IT sector	I have PC with internet connection	4	5	4	Very confident	Hacking, Cy
44	Yes	22-26	Male	Working in IT sector	I have PC with internet connection	4	3	4	Unconfident	Hacking
45	Yes	22-26	Male	Non-IT university student	I have PC without internet connection	3	2	3	Very unconfident	Hacking, Cy
46	Yes	22-26	Male	Looking for a job in IT sector	I don't have PC, but I have internet connectior	4	4	4	Confident	Hacking
47	Yes	22-26	Male	IT university student	I have PC with internet connection	3	2	4	Confident	Hacking, Cy
48	Yes	22-26	Male	IT university student	I have PC with internet connection	3	2	4	Confident	Hacking, Cy

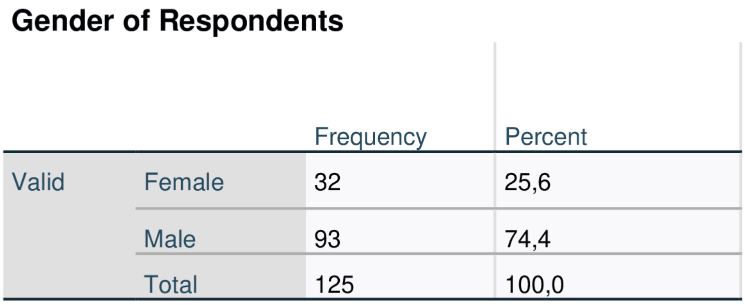
Figure 3 Screenshot of the data from Excel

This illustration shows the data collected from a survey conducted using Google Forms, which was then stored and analysed in Excel and IBM SPSS Statistics. The data consists of responses from participants who have knowledge in the field of the survey topic. The relevance of this data to the thesis is that it provides insights into the opinions and attitudes of a sample population, which can be scaled up to represent the larger population. By analysing this data using statistical software such as IBM SPSS and presenting it in visual form through Excel, trends and patterns can be identified and communicated effectively to support the thesis. The use of these tools ensures that the data is analysed comprehensively and efficiently, which enables the researcher to draw valid conclusions and make informed decisions based on the findings.

4.4.1 Scaling up

The first step in analysing the data is to find out if we can scale our results.
The dataset consists of 121 participants.

Table 4-1 Gender of Respondents

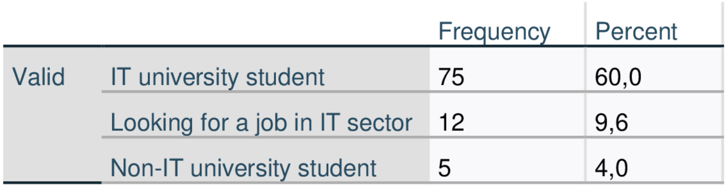


Gender of Respondents

		Frequency	Percent
Valid	Female	32	25,6
	Male	93	74,4
	Total	125	100,0

The participants are divided by gender. The results belong to 74.4% of men, 25.6% of women are given in the results data set. One of the most important conditions for scaling up this work is the occupation of Respondents. Therefore, participants separated by Occupation, too.

Table 4-2 Occupation of Respondents



		Frequency	Percent
Valid	IT university student	75	60,0
	Looking for a job in IT sector	12	9,6
	Non-IT university student	5	4,0

	Work in non-IT sector	3	2,4
	Working in IT sector	30	24,0
	Total	125	100,0

In this *Bar chart* we can see the ratio between occupation of all participants. As we can see, the highest amount of test participants is IT university student, and the second highest number of participants are Working in IT sector.

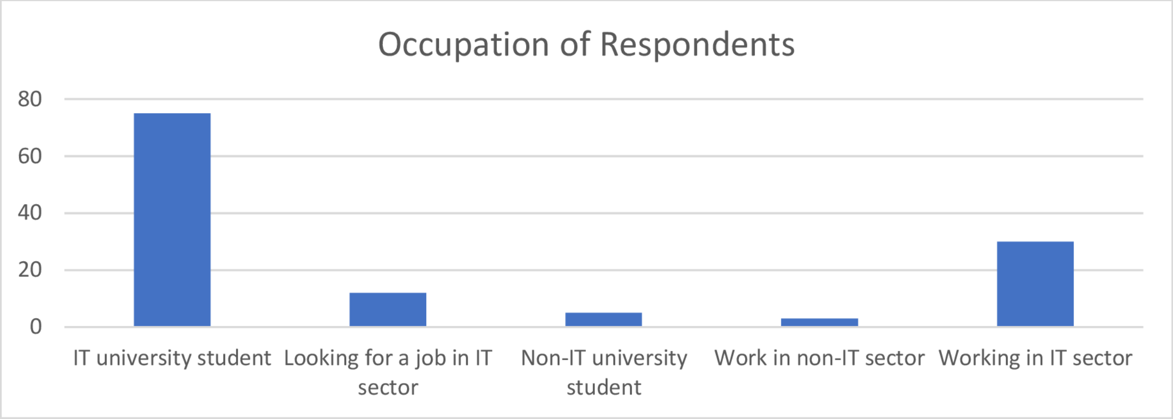


Chart 4-1 Occupation of Respondents. Source: Own Illustration

Despite the occupation, the computer literacy of respondents is also important information for the correct scaled up to the entire computer-literate population of Kazakhstan. Therefore, we wanted data on the respondents' equipment and their self-assessment of knowledge. This category is also listed in dataset.

Table 4-3 Respondents' equipment

Do you have a PC with internet connection?

	Frequency	Percent
Refrained from answering	1	,8
I don’t have PC and internet connection	2	1,6
I don’t have PC, but I have internet connection	16	12,8
I have PC with internet connection	102	81,6
I have PC without internet connection	4	3,2

Total	125	100,0

The results show that 84.8% have a computer and 94.4% have access to the internet, so it could be claimed that our respondents are sufficiently equipped. Next, we need to find out how qualified our respondents are, as they are supposed to represent the qualified side of the nation. To do this, a knowledge self-assessment survey was carried out.

Table 4-4 Sum of point in PC, Hardware, OS Knowledge

Descriptives

			Statistic	Std. Error
Sum of point in PC, Hardware, OS Knowledge	Mean		9,08	,270
	95% Confidence Interval for Mean	Lower Bound	8,54	
		Upper Bound	9,62	
	5% Trimmed Mean		9,09	
	Median		9,00	
	Variance		9,139	
	Std. Deviation		3,023	
	Minimum		3	
	Maximum		15	
	Range		12	
	Interquartile Range		4	
	Skewness		-,112	,217
	Kurtosis		-,257	,430

As we can see, our respondents have average scores for PC, Hardware, OS knowledge, which is sufficient for scaling, as the average value is 9.62 out of the maximum 15. Therefore, we can conclude that our respondents meet the scaling conditions, and the scaling could be done according to the collected data. The same information can be represented in a graph for better understanding.

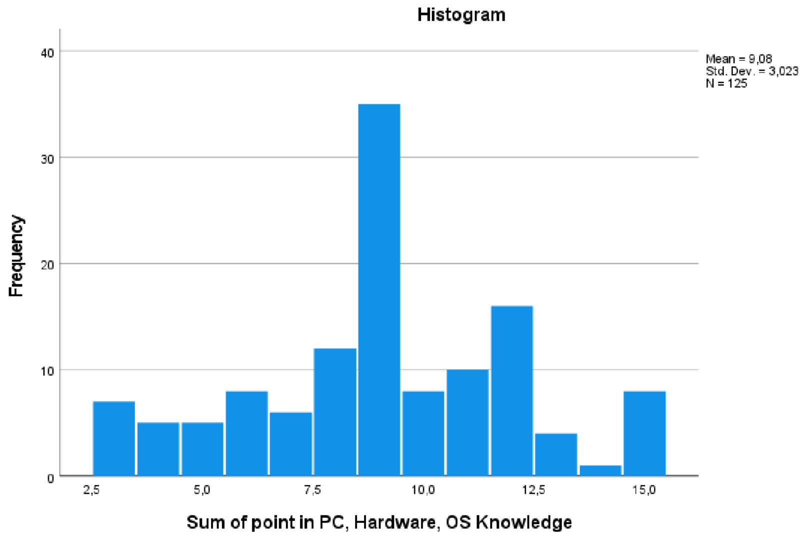


Chart 4-2 Sum of point in PC, Hardware, OS Knowledge. Source: Own Illustration

4.4.2 Assessment of understanding of cyber security among respondents

The next step is to assess their cyber security knowledge. I decided to analyse how well the respondents understand cyber security through a question that encapsulates cybercrime. For each correct answer 1 point is awarded, the answer to none of the above gives 0 points. Maximum is 10, minimum is 0.

- *Hacking = 1*
- *Cyber terrorism = 1*
- *Malwares = 1*
- *Online gambling = 1*
- *Cyber stalking = 1*
- *Virus dissemination = 1*
- *Phishing = 1*
- *Salami attack = 1*
- *Child pornography = 1*
- *Spoofing = 1*
- *None of the Above = 0*

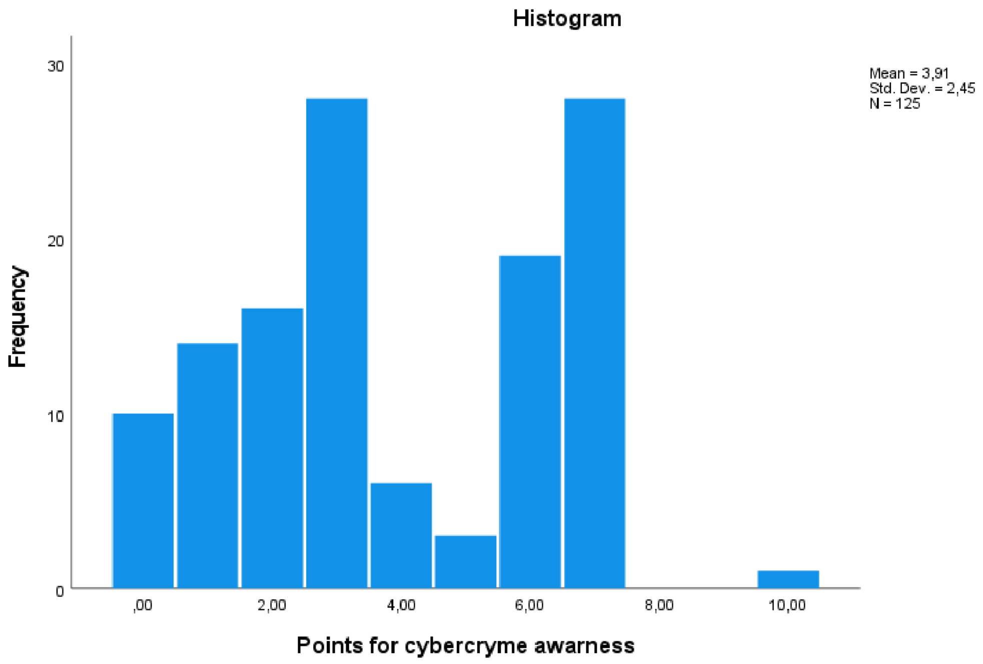


Chart 4-3 Points for cyber-crime awareness. Source: Own Illustration

As a result, we can see that the scores are in high numbers on the right side of the graph, indicating that respondents do not identify cybercrime well. These results are interesting in their own way, as most respondents feel confident that their personal data is safe online.

Table 4-5 respondent's confidence toward personal data in internet

How confident, if at all, do you feel that you know how to keep your personal devices and online accounts secure?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very unconfident	5	4,0	4,0	4,0
	Unconfident	29	23,2	23,2	27,2
	Neither confident nor unconfident	20	16,0	16,0	43,2
	Confident	55	44,0	44,0	87,2
	Very confident	16	12,8	12,8	100,0
	Total	125	100,0	100,0	

The total number of confident and very confident (71 respondents) exceeds the number of not confident and very unsure (34 respondents) by 2.08 times. This can also be seen in the graph.

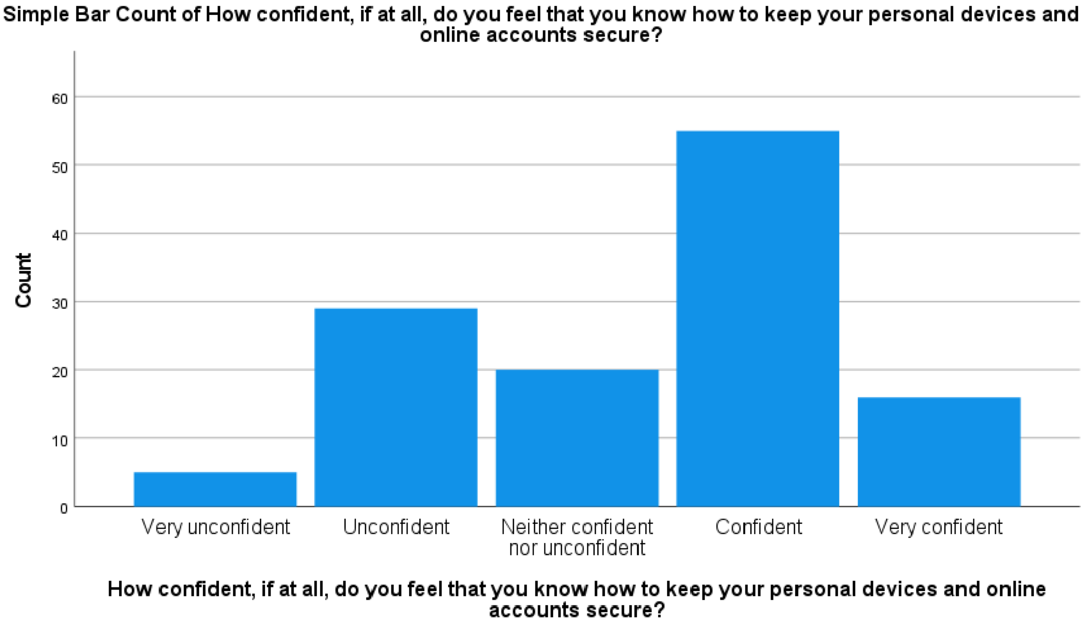


Chart 4-4 respondent's confidence toward personal data in interne. Source: Own Illustration

Another way to assess the extent to which respondents stay safe online is to test them on the frequent mistakes internet users make.

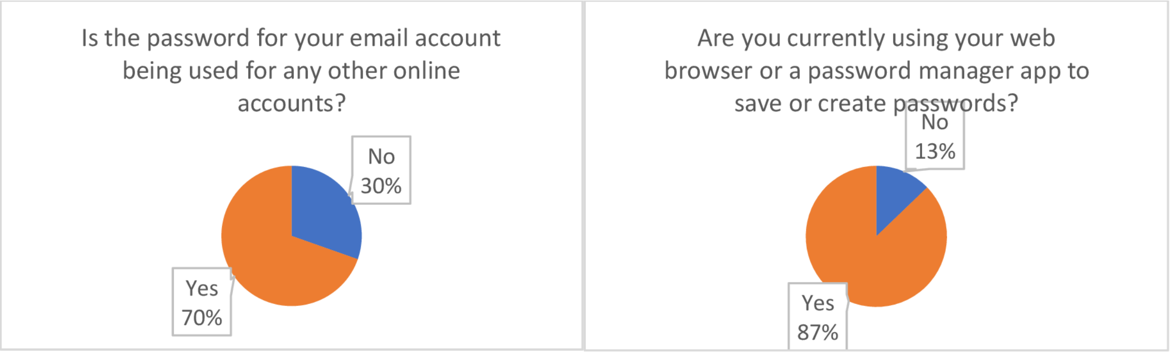


Chart 4-5 respondent's answers from yes/no question from survey. Source: Own Illustrations

Using the same password for multiple accounts or relying solely on a password manager for online security can be a dangerous practice. If a hacker gains access to one password, they would then have access to all accounts associated with that password. This could lead to sensitive personal and financial information being compromised, and even identity theft.

This issue is why we included a question in our survey about password management practices. It is important for individuals to understand the risks associated with using the same password for all accounts or relying solely on a password manager, and to take steps to improve their online security. This may include using unique and complex passwords for each account, enabling two-factor authentication, and regularly updating passwords to prevent potential security breaches. Overall, taking a proactive approach to password management can help protect personal information and prevent cyber-attacks.

Now we need to learn about the state of cyber security in Kazakhstan.

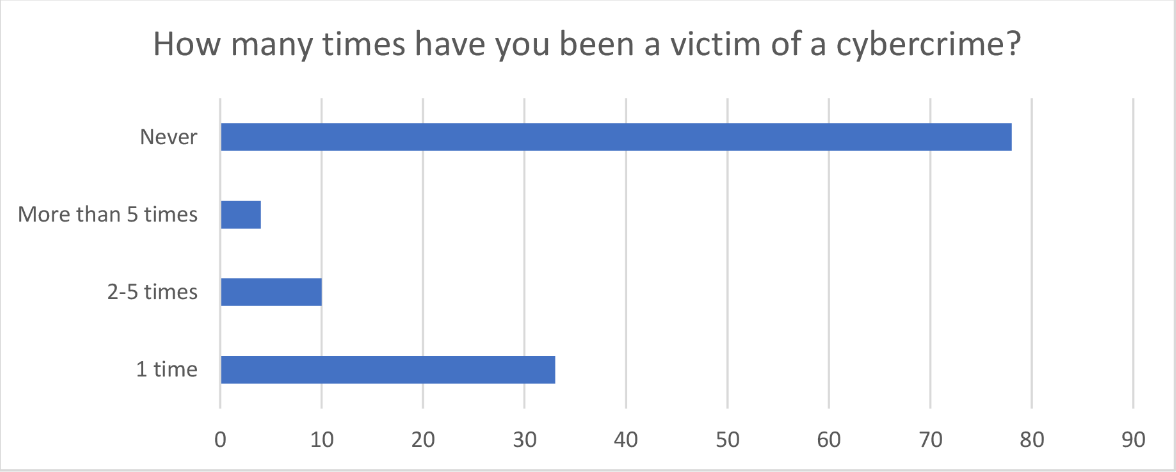


Chart 4-6 The state of cyber security in Kazakhstan. Source: Own Illustration

The question "How many times have you been a victim of a cybercrime" can provide valuable insights into the state of cyber security in Kazakhstan. The answers to this question can reveal the frequency and prevalence of cybercrime incidents among the population, which can in turn indicate the level of cyber security awareness and preparedness in the country. Only a small percentage of respondents report being victims of cybercrime, this could suggest that cyber security measures in Kazakhstan are effective and that individuals are taking necessary precautions to protect their data online.

Based on the survey results, it appears that the respondents have rarely been victims of cybercrime. However, it is still important to analyse which types of cybercrimes are most common in Kazakhstan, even among those that are rarely experienced by the survey participants.

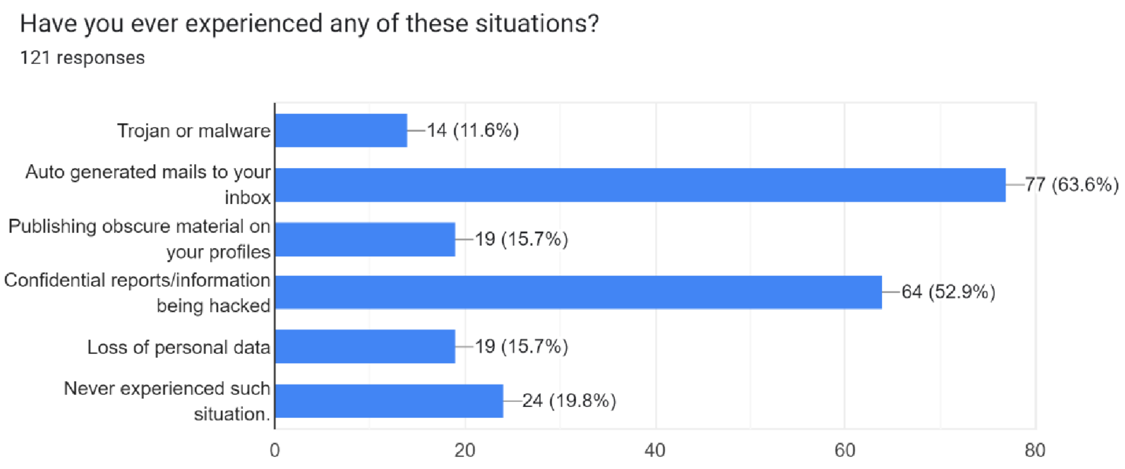


Chart 4-7 Which cybercrimes are most common in Kazakhstan. Source: Own Illustration

The survey data reveals that despite the low incidence of cybercrime witnessed by the respondents in Kazakhstan, they do not hold the state responsible for ensuring cyber security. This is evident from the low rating given to cyber security by the respondents, which was 5.56 out of 10 among 121 participants. It is possible that this result is due to the respondents' lack of trust in legal protection provided by the state. This indicates that there may be a need for greater awareness and education on cyber security issues in the country, as well as a need for stronger legal frameworks to protect citizens' online safety.

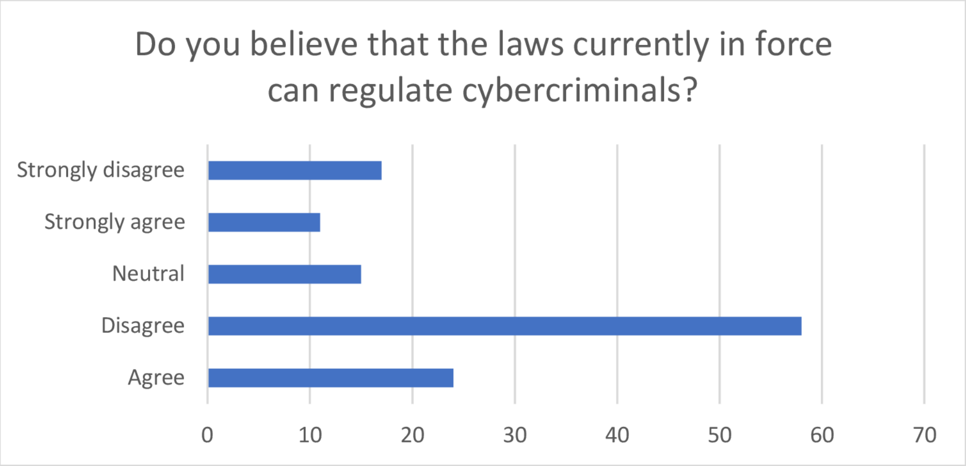


Chart 4-8 Trust level in legal protection

The reasons behind this trend may vary, but based on the data collected from interviews, it appears that a shortage of specialists is one of the primary factors, as evidenced by the graph provided. Another contributing factor, as indicated by the survey, is a low level of digital literacy among the population.

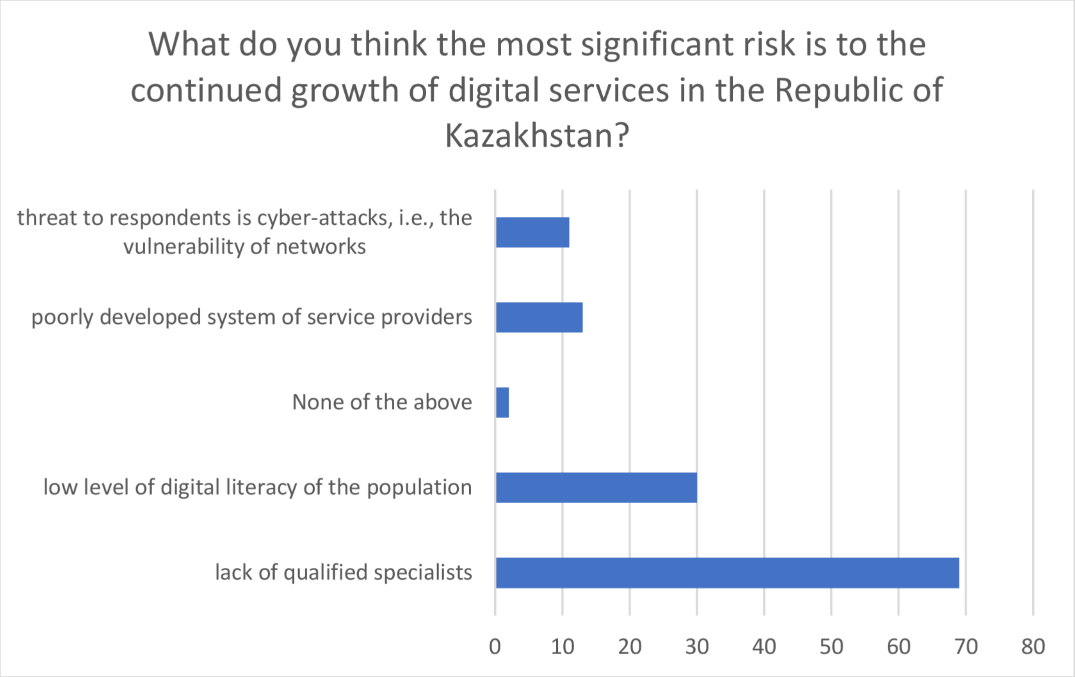


Chart 4-9 the most significant risk is to the continued growth of digital services in the Republic of Kazakhstan

Another reason may lie in the lack of knowledge of the law among residents, as the following graph shows.

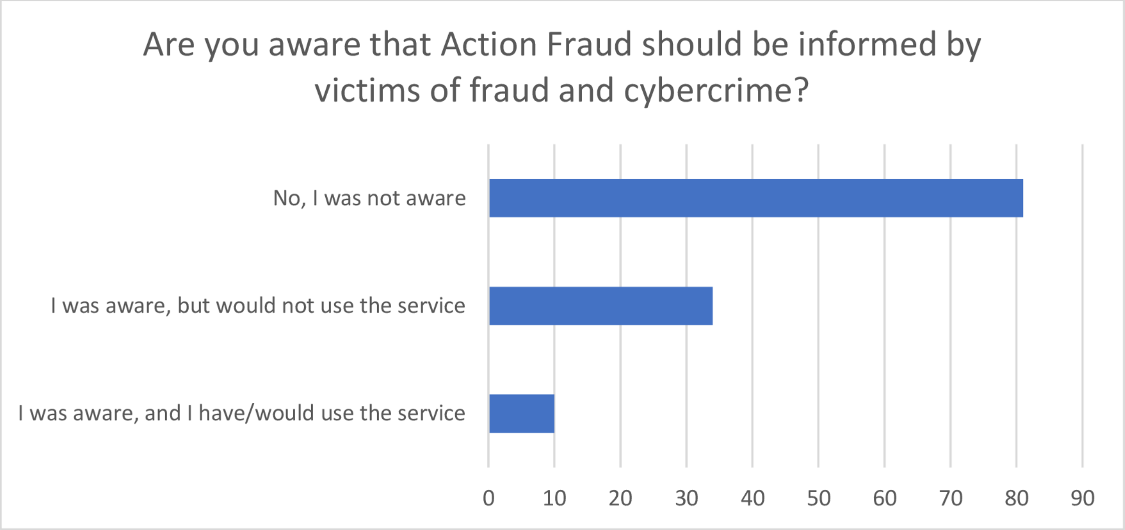


Chart 4-10 Knowledge of the law among residents

Despite this, the survey results tell us that the people of Kazakhstan, as represented by students, value the security of their data. Although they don't think their data is safe.

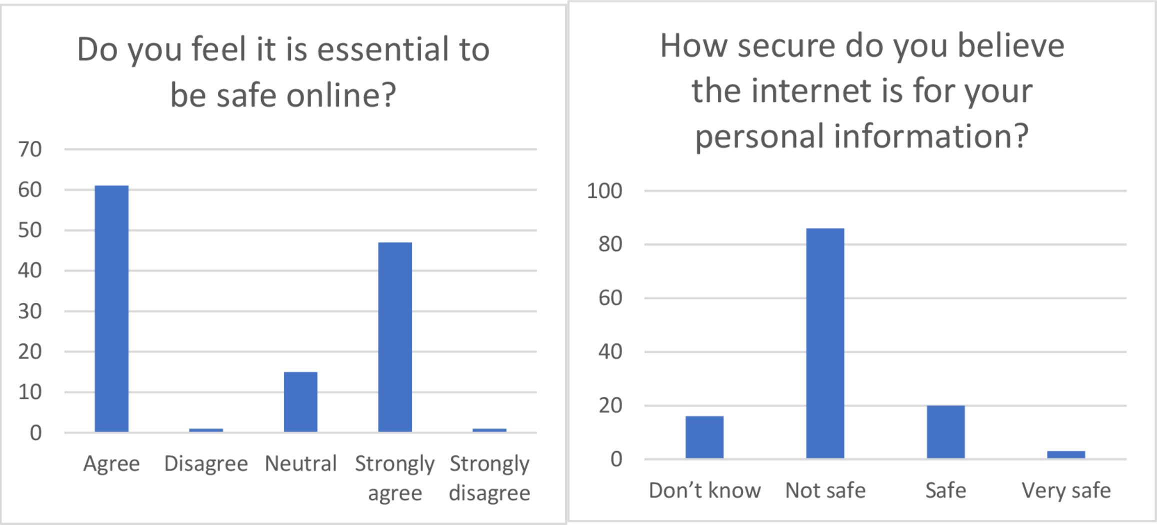


Chart 4-11 The safe level of information in Kazakhstan

4.4.3 Richter magnitude scale

We can use Richter magnitude scale to assess how safe the data of internet users in Kazakhstan is. In this assessment we will use only 3 questions that meet the criteria.

- 5 points for Strongly agree
- 4 points for agree
- 3 for neutral answer
- 2 for disagree
- 1 for Strongly disagree.
- 5 for Very Safe
- 4 for Safe
- 3 for Don't know
- 1 for Not Safe
- 5 for Very Confident
- 4 for Confident
- 3 for Neither confident nor unconfident
- 2 for Unconfident
- 1 for Very Confident

The total dilution looks like this, if the average Kazakh has more than 12 points from 15 then his data is protected, and he understands what he is doing.

Average for question: Do you feel it is essential to be safe online?
4,216
Average for question: How secure do you believe the internet is for your personal information?
1,832
Average for question: How confident, if at all, do you feel that you know how to keep your personal devices and online accounts secure?
2,944
Total
8,992
Percent of satisfaction
60%

Table 4-6 Richter magnitude scale calculations 1-2

The results are very low with only 60% satisfaction, which is below the 12 points that were satisfied. We can also add a question related to the legal intricacies of cybersecurity to find out how well the state is doing to ensure internet security.

Table 4-7 Richter magnitude scale calculations 2-2

Average for question: Do you believe that the laws currently in force can regulate cybercriminals?
2,632
Total
11,624
Percent of satisfaction
58%

It is important to assess the state's performance in ensuring internet security by asking a question related to the legal intricacies of cybersecurity using the Richter magnitude scale because it provides a quantifiable measure of the state's effectiveness in addressing cyber threats and protecting citizens' online safety.

4.4.4 Scoring the test results

Also, we could use the whole point system to determine the average score for a resident of Kazakhstan. You could get 2 points for two yes/no type questions, 1 point for each negative answer and 0 points for each positive answer, 10 points for cyber security knowledge, and you could get 7.5 points for PC, Hardware, and OS knowledge. We will only give the latter points half their value, as it is a self-assessment that we do not additionally check. A total of 19.5 points could be obtained for completing the questionnaire. Unfortunately, we cannot determine the number of points for the variances, as we cannot achieve homogeneity of the variances.

Table 4-8 Scoring the test results

Average for PC knowledge	**Reduced for self-evaluation**
3,112	1,556
Average for Hardware knowledge	
2,608	1,304
Average for OS knowledge	
3,387	1,694
Average for Cybercrime Awareness points	
3,912	
Average points from first Yes/No question	
0,304	
Average points from Second Yes/No question	

0,128	
Total points	
8,8975	

The results of the respondents' assessment through our questionnaire are 8.8975 which is only 46% of the maximum score, a rather low result. If we exclude the results from self-evaluation, we get 4,344 points out of 12 points, which is 36%. Also from this table, we can conclude that, according to respondents, they know the OS best and the Hardware worst. Moreover, we can see very low results of cyber threats identification.

5 Results, Discussion and Recommendations

In modern society, the topic of cyber security is felt most urgently, especially in the realities of developing countries such as Kazakhstan. The need to promote awareness among populations is growing, but even though digitalization in Kazakhstan is reaching its early stages and it seems an ideal time to establish a solid foundation of understanding among the population, practice shows that technology development and spread are far faster than teaching people how to use it. This also applies to the generation that now runs the state and companies, who have had to accept the arrival of technology and add it to their field of activity, often at the expense of process efficiency, as well as to the new generations growing up who seem to be able to use technology but are not prepared to face the dangers that may arise. This problem is made more urgent by the fact that new generations are using the internet in a much higher rate, making it much easier for them to become victims of a scammer. In addition, as the positive effects of technology increase, the opposite side always grows - the number and variability of fraudsters and the quality of their work increase as well. Fortunately, Kazakhstan still has time.

5.1 Results of practice part

5.1.1 Results of Survey

By generalizing the replies of respondents who matched our target audience, we can create a model of attitudes and understanding of cybersecurity in Kazakhstan, which I will call Almaz for convenience of understanding.

Almaz is a man from Kazakhstan who is between 22-26 years old. He is studying for an IT degree or is already working in this field. The following assumptions about Almaz can be identified:

- Almaz has an internet connection even if there is no computer.
- Almaz is confident in their knowledge of computer use.
- Almaz has no developed concept of cybercrime and can only identify some.
- Almaz feels confident about the internet.
- Almaz doesn't take the least ways to protect themselves on the internet.
- Almaz has never been a victim of cybercrime or was unable to determine that it was cybercrime.
- That said, there have been cybercrime incidents with Almaz has had cybercrime incidents.
- Almaz does not believe that the state and the law can deter cybercriminals.
- Almaz believes that lack of expertise is the cause of all the ills.
- Almaz trusts the government.
- Almaz does not report cybercrime to the relevant authorities.
- Almaz thinks their data is not protected on the internet.
- But Almaz thinks they need to be protected on the internet.

5.1.2 Results of Interview

The interviews we conducted only confirm our model, as everything that was said from the interviewees matches Almaz's conclusions, so we can conclude that even though the depth of the "cut" of the survey questions is different from the interview questions, so are the target audiences of the two sources of information - Almaz (the model) understands that there are many problems in Kazakhstan, but he does not know the concrete steps to correct this problem, despite his awareness of his field. It seems to him that Kazakhstan's cybersecurity problem lies in a combination of problems in completely different areas, some of which are only indirectly related to IT.

5.2 Discussion and Recommendations

It is reasonable to agree with our results and the model we have created because cyber security, as shown by the experience of different countries, is an area that involves many areas of governmental activity, private companies and even the life of the common individual. Kazakhstan has managed to develop very significantly over the last 30 years, rising to the top 50 countries of the world, but there is a downside of this. The individual cannot keep up with the changes and developments and therefore becomes vulnerable to those who have already seen the benefits of digitalisation and are exploiting them illegally.

Unfortunately, the country gives limited attention to increasing awareness if even specialists in the field make such mistakes in their daily use of the internet. There may be many different reasons for this, such as the existence of other problems that need to be resolved right now. But unfortunately, if this trend continues in Kazakhstan soon there will be a huge number of cyber criminals, the population is not prepared. The only reason cybersecurity in Kazakhstan has not yet been strongly affected by these problems is because digitalisation in Kazakhstan is just taking its first steps and has not yet touched all areas. Scammers have not become as capable as in neighbouring Russia, for example. But this is a ticking time bomb, and after a while it may cause harm.

Recommendation for the following researchers on this topic.

1. Studying how cybercrime has evolved in Kazakhstan, because already now you can see how people are starting to notice that scammers are becoming more and more tricky than they were a few years ago. Considering that Kazakhstan's cyber criminals still have a lot paths evolve and learning examples.

2. Finding an approach to persuade Kazakhstan's public institutions to share information with cybersecurity experts.
3. Studying the backgrounds of new generations of IT workers to compare the number of students who have studied abroad and in Kazakhstan, as this will help determine the extent to which Kazakhstan invests in IT education.
4. Studying the issue of brain drain and the shortage of specialists in Kazakhstan, comparing it with other areas, and identifying reasons and strategies to address the problem.

6 Conclusion

The aim of the thesis was to adapt an existing model of user's perceptions towards cyber-security policy in Kazakhstan. An additional goal of the work was to discern how the average, young citizen in Kazakhstan feels about cyber-security policy development, to understand what the existing government and industrial responses are to rising cyber-security challenges. Also, explore the role and/or suggested solutions of young citizens in the future of cyber security policy development towards strengthening government, IT industries, and e-commerce as consistent with global standards.

RQ 1: "What is the state of cyber security in Kazakhstan?"

It can be concluded that despite Kazakhstan's great achievements in recent years, there are still many things that need to be corrected and improved. Technological development and digitalisation are moving much faster than the spread of awareness among the population. Existing government and industry responses to the growing cybersecurity challenges are sufficient to meet today's challenges. However, in the near future, unless the situation changes drastically, the government may become vulnerable to advanced hackers. Unfortunately, it was not possible to obtain further comment due to disclosure restrictions.

RQ 2: "How do university students in Kazakhstan perceive the utility of cyber-security?"

As the research results show, young citizens in Kazakhstan do not feel good about cyber-security policy development despite a better understanding of the dangers of the Internet in Kazakhstan. They trust the government, even though they feel that the actions they take are not sufficient to solve all or at least most of the problems.

RQ 3 "What is the future of cyber security in Kazakhstan and what can be done to improve it?"

The most crucial points for development can be highlighted, can be used in further study of this topic and Kazakhstan, based on a suggested solutions of young citizens in the future of cyber security policy development towards strengthening government, IT industries, and e-commerce as consistent with global standards.

RQ 4 "At what level is the model of user's perceptions towards cyber-security policy?"

Therefore, the existing model of user's perceptions towards cyber-security policy in Kazakhstan has an unsatisfactory level of awareness and skill in using the Internet, making mistakes, and not protecting their data. On the other hand, there is awareness of existing problems, which can serve as a starting point for further development.

7 References

"National Information Technologies" JSC, 2019. [Online] Available at: https://www.nitec.kz

Akhmetov, B., 2018. Status, perspectives and main directions of the development of cybersecurity of information and communication transport systems of Kazakhstan. *Reports of the national academy of sciences of the republic of Kazakhstan,* 2(318), p. 23 – 30.

Amoroso, E., 2006. Cyber Security.

BAY, M., 2016. WHAT IS CYBERSECURITY? In search of an encompassing definition for the post-Snowden era. *UCLA Information Studies.*

Bay, P. C. i. I. S. a. U. M., 2016. WHAT IS CYBERSECURITY? In search of an encompassing definition for the post-Snowden era. *UCLA Information Studies.*

Beyza, U. & Patricia, L., 2018. Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences. January.

Borkovich, . D. & Skovira, . R., 2020. Working from home: Cybersecurity in the age of COVID-19. In: *Issues in Information Systems.* s.l.:s.n.

Boyne, S. M., 2018. Data Protection in the United States. July, 66(1), p. 299–343.

Canada, P. S., 2010. Canada's Cyber Security Strategy.

Canongia, C. & Mandarino, , R., 2014. Cybersecurity: The New Challenge of the Information Society. pp. 60-80.

CNSS, 2010. National Information Assurance Glossary. Issue Instruction No. 4009.

Dan, C., Nadia , D.-T. & Randy , P., 2014. Defining Cybersecurity. October.

Das, A. K., 2018. European Union's General Data Protection Regulation: A brief overview. *Centre for Studies in Science Policy, School of Social Sciences Jawaharlal Nehru University,* June, Issue 65, pp. 139-140.

DHS, 2014. A Glossary of Common Cybersecurity Terminology. 1 October.

Government of the Republic of Kazakhstan, 2016. *Law of the Republic of Kazakhstan.* s.l.:s.n.

IBM, n.d. *Featured research.* [Online] Available at: https://www.ibm.com/security/resources/xforce/research.html[19]

IMD Business School, 2018. *World Digital Competitiveness Rankings.* [Online] Available at: https://www.imd.org

Ismailova, R. et al., 2019. Cybercrime risk awareness rate among students in Central Asia: A comparative study in Kyrgyzstan and Kazakhstan. 28(4-5), pp. 127-135.

ITU, 2009. Overview of Cybersecurity. Issue X.1205.

Jr, J. H. B. D., 2012. "Cybersecurity... How Important Is It?". *The Judges' Journal,* 4(51).

Kemmerer, R. A., 2003. Cybersecurity. Issue 705-715.

KZ-CERT, 2019. *Official website of KZ-CERT Kazakhstan.* [Online] Available at: http://kz-cert.kz/en/about

Lewis, J. A., 2006. Cybersecurity and Critical Infrastructure Protection.

Ministry of Justice of the Republic of Kazakhstan. Institute of legislation and legal information, n.d. *Adilet database.* [Online] Available at: https://adilet.zan.kz/eng#

National Computer Incident Response Service, 2016. [Online] Available at: https://sts.kz/en/nsrki/

Official Information Source of the Prime Minister of Kazakhstan, 2017. *Phishing websites, spear-phishing, whaling — Cyber Shield of Kazakhstan improves security systems.* [Online] Available at: https://www.primeminister.kz/en/news/reviews/phishing-websites-spear-phishing-whaling-cyber-shield-of-kazakhstan-improves-security-systems7698

Official website Joint Stock Company "Zerde", Official website Joint Stock Company "Zerde". [Online] Available at: https://zerde.gov.kz/holding/history/

Oxford Online Dictionary, n.d. 1 October.

Pranggono , B. & Arabo, A., 2021. COVID-19 pandemic cybersecurity issues., 4(2),. In: *Internet Technology Letters.* s.l.:s.n., p. p.e247..

Symbat , I. & Yesseniyazova, B. M., 2019. Cyber Security issues in digital Kazakhstan.

the International Telecommunication Union, 2017. [Online] Available at: https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017.aspx

8 List of pictures, tables, graphs, and abbreviations

8.1 List of pictures

8.2 List of tables

8.3 List of charts

8.4 List of abbreviations

GDPR - General Data Protection Regulation

Appendix

Responses List for the Survey - User perception's and behavioural intentions towards privacy and security online