ISSN 2708-2032
e-ISSN 2708-2040

INTERNATIONAL
UNIVERSITY

INTERNATIONAL JOURNAL OF INFORMATION & COMMUNICATION TECHNOLOGIES

Volume 2, Issue 4
March 2021

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF EDUCATION AND SCIENCE OF THE REPUBLIC OF KAZAKHSTAN

ХАЛЫҚАРАЛЫҚ УНИВЕРСИТЕТІ
IT
МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ
INTERNATIONAL UNIVERSITY

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

Том 2, Выпуск 8
December 2021

Издание зарегистрировано Министерством информации и общественного развития Республики Казахстан. Свидетельство о постановке на учет No KZ82VPY00020475 от 20.02.2020 г.

Журнал зарегистрирован в Международном центре по регистрации сериальных изданий ISSN (ЮНЕСКО, г. Париж, Франция)

Выходит 4 раза в год.

УЧРЕДИТЕЛЬ:
АО «Международный университет информационных технологий»

ISSN2708-2032 (print)
ISSN2708-2040 (online)

СОДЕРЖАНИЕ

ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И КИБЕРБЕЗОПАСНОСТЬ

ЦИФРОВЫЕ ТЕХНОЛОГИИ В ЭКОНОМИКЕ И МЕНЕДЖМЕНТЕ

ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ

МАТЕМАТИЧЕСКОЕ И КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ

CONTENTS

INFORMATION AND COMMUNICATION NETWORKS, CYBERSECURITY

DIGITAL TECHNOLOGIES IN ECONOMICS AND MANAGEMENT

INTELLIGENT SYSTEMS

MATHEMATICAL AND COMPUTER MODELING

МАЗМҰНЫ

АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ЖЕЛІЛЕР, КИБЕРҚАУІПСІЗДІК

ЭКОНОМИКАДАҒЫ ЖӘНЕ МЕНЕДЖМЕНТТЕГІ ЦИФРЛЫҚ ТЕХНОЛОГИЯЛАР

ИНТЕЛЛЕКТУАЛДЫ ЖҮЙЕЛЕР

МАТЕМАТИКАЛЫҚ ЖӘНЕ КОМПЬЮТЕРЛІК МОДЕЛЬДЕУ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 2. Is. 4. Number 08 (2021). Pp. 12–17
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2021.08.4.002

UDC 004.56

Mubarakova S.R. *, Amanzholova S.T., Uskenbayeva R.K.
International Information Technology University, Almaty, Kazakhstan
*E-mail: mubarakova.saltanat@gmail.com

RELEVANCE OF CYBERSECURITY IN THE MODERN WORLD

Abstract. This article discusses one of the most pressing issues of today: relevance of cybersecurity in the modern world. It presents the main facts about cybersecurity, the concept and historical aspect of the development of cybersecurity and analyzes the current state of cybersecurity in Kazakhstan. The relevance of this article lies in the fact that it clearly highlights the role of cybersecurity and its relevance for modern society. In this connection, the article provides up-to-date data on cyberattacks and cybersecurity of our time.

Keywords: cybersecurity, Information Technology, cyberattacks, cybercrime.

Introduction. Today it is difficult to overestimate the importance of cybersecurity in the modern world. This is important because cybersecurity measures are designed to protect against theft and subsequent use of confidential data, personal medical information, intellectual property, government and industry information systems, everything that is stored and managed using information technology. At the moment, the risk of becoming a victim of cybercriminals is quite high. Everyone, from the most popular Internet users to large companies, uses different cloud services to store various personal data. The days when companies could trust antivirus programs and firewalls to protect their information are long gone. In modern reality, the services of cybersecurity specialists are not sufficient for organizing reliable protection. Any office worker, without knowing it, can easily turn into a "tool" of cybercriminals. The role of computer systems and cybersecurity protection measures in modern conditions is enormous [1].

With the development of Internet technology, even electric kettles have "learned" how to receive, process, generate and send digital data over the network. And the more we surround ourselves with high-tech devices, the higher is the risk of becoming a victim of cybercrime. At the same time, cybersecurity is also becoming increasingly important - both as an area of information technology and as a set of tools to ensure the protection of confidential data.

The relevance of the research topic lies in the fact that the number of cybercrimes worldwide has grown enormously over the past few decades, the motives and goals of cybercriminals have changed over time, and the cybercrime rate is rising from year to year. This is evidenced by the huge financial losses of legal entities and structures, as well as the increase in cybercrimes against individuals. This rapidly growing problem requires an effective and speedy solution, as the level of cybercrime and the complexity of crime are increasing, while the processing of cases and the effectiveness of work against criminals in cyberspace are decreasing. This topic is relevant today because the costs of preventing and disposing cybercrimes are growing, more and more legal entities and individuals are trying to protect themselves in advance, but criminals in cyberspace are not stagnating, and methods and types of crimes are getting more and more complicated. Therefore, this area requires constant monitoring and search for solutions.

The purpose of the study is to analyze the relevance of cybersecurity in the modern world.

In accordance with the purpose of the study, we set the following tasks:

1) To study the existing trends in information technology and cybersecurity;

2) To substantiate the relevance of this topic;

3) To study the current status quo in the cybersecurity area;

4) To analyze the cybersecurity situation in Kazakhstan.

The object of the work is the cybersecurity of Kazakhstan at the present time. The subject of the study is cybersecurity in the modern world.

In accordance with the purpose and objectives of the study, the main research methods are:

- study of popular science literature on this problem;
- analysis and synthesis of the collected information;
- analysis of the legal framework;
- analysis of statistical data;
- systematization and generalization of materials, conclusions on this problematic issue.

The scientific significance lies in the fact that the research contributes to the study of the relevance of cybersecurity in the modern world, particularly in Kazakhstan. The practical significance of the work lies in the fact that the results of this work can be used in the efforts to remedy the cybersecurity situation in Kazakhstan and in practical classes on information technology.

The hypothesis of our research: "Currently, cybercrime on the web is growing every year. And despite all the external struggle with this, the problem exists to this day. Moreover, this becomes a global problem for modern man. Cybercrime can grow into a more global problem and become more serious than domestic crimes. Therefore, it is very important to study this phenomenon" [2, p. 63-65].

Methods and materials. The main research methods are: text analysis in the form of analysis of scientific literature related to the topic of information technology and cybersecurity, comparative analysis in the form of studying and summarizing information obtained during the study; statistical methods and synthesis. Comparison and generalization are also used as auxiliary methods of empirical research. To search for existing research, numerous literature search methods were used, including searching in electronic databases and major journals, as well as manually searching for links to identified articles. The main electronic databases were Pubmed, SCOPUS, Web of Science and Science Direct. During the initial search, 51 articles on cybersecurity were found. These articles were further examined using the following three selection criteria: firstly, the studies included in the review should directly address the human factors related to cybersecurity and its consequences; secondly, the studies should be published in peer-reviewed journals; and thirdly, the studies should not focus on the technological dimension of cybersecurity. After applying these three criteria, 50 questions were selected, which were considered in four main areas: cyberattacks, contributing factors and strategies to combat them, cybersecurity in Kazakhstan [3, p. 10-12].

Literature review. Information and cybersecurity is not a new topic for research, as a matter of fact it has been a serious national problem for more than 20 years, which has led to a rapid growth of scientific literature over the past 10 years. A significant contribution to the disclosure of the problems of the formation and development of the information society was made by the socio-philosophical theories of foreign scientists: D. Bell, W. Dayzard, M. Castels, M. McLuhan, J. Masuda, T. Stonier, E. Toffler and others. Given the rapidly growing body of literature on the current cybersecurity issues, the purpose of this review article is to summarize the current literature for researchers, policy makers, practitioners and even the general public. As a result of this review, 51 relevant publications in leading journals on information systems in the period from 2010 to 2020 have been found and analyzed. In particular, there were identified nine main areas of concentration (for example, legal issues, supervision and morality, vulnerabilities, risks and detection), which constituted a substantive basis for the theoretical justification of the basic structures and their interrelations in the study of information systems security. This review has hopefully made an important contribution to cybersecurity research, summarizing the existing literature and providing an exhaustive framework. This review aims to make a new contribution to the synthesis of knowledge in cybersecurity research in three dimensions [4, p. 34-42].

Results and discussions. In the modern world organizations of the commercial, financial, medical, processing and energy sectors, including all government agencies, organize the collection, storage and processing of all information necessary for work, as well as personal data of employees, users, customers and visitors. In principle, all this information should be protected, as it is confidential, and its possible loss or theft can have unpredictable consequences for people and organizations. Organizations that directly provide the infrastructure of entire cities, countries and the global community as a whole are more likely to be subjected to a multi-level complex cyberattack [5].

The very concept of cybersecurity refers to a set of technologies, methods and processes designed to protect the integrity of programs, networks and data from cyberattacks. In other words, cybersecurity is a set of conditions that guarantee protection of all components of information systems from the maximum number of threats and undesirable influences at the physical, financial, emotional, mental, spiritual, educational, political and professional levels. Such influence, or negative consequences in case of errors, accidents, incidents and other damage in cyberspace are considered undesirable [6].

Cybersecurity is security in relation to information technology. This includes all technologies that store, process, or transmit data, such as computers, data networks, and all devices connected or embedded in a network, such as routers and switches. It should be noted that the concept of cybersecurity is a state or process of protecting computer systems aimed at repelling any kind of cyber threats, be it malware, various network attacks such as brute force attacks and DDoS, or even training staff on the methods of protection against social engineering, phishing and other tricks of cybercriminals. As cybersecurity evolves, attackers evolve to exploit weaknesses in the system for profit or simply to prove their case.

Cybersecurity extends to computers, networks, operating systems, applications, and other configurable and programmable components of the IACS system. The concept of cybersecurity was first introduced in 1991 as part of the generalization of digital network technologies, and goes back to the ancient Greek word "cyber". However, this arms race has been going on since the 1950s. For example, launching a cyberattack two decades after the creation of the world's first digital computer in 1943 was not an easy task. Giant electronic machines were not connected to the network, a limited number of people had access to them, and only a few knew how to work with them, so there were practically no threats. So, the history of cybersecurity begins in 1972 with the ARPANET research project, the forerunner of the Internet.

Cybersecurity is rapidly evolving, hackers and security service providers are constantly competing to get around each other, and new threats and innovative ways to combat them are constantly emerging. This review presents the latest trends in cybersecurity. For example, the Covid-19 pandemic has forced most organizations to transfer employees to work from home, often in a very short period of time. Many studies show that after the pandemic, most employees will continue to work remotely. Working from home involves new risks and is one of the most discussed trends in the field of cybersecurity. Home offices tend to be much less secure than centralized offices, which are usually equipped with firewalls and routers, and access control is regulated by the IT security group. The transition to remote work was carried out in a hurry so as not to disrupt work processes, and the security audit could be carried out with less care than usual. Cybercriminals can take advantage of this. Many employees use personal devices for two-factor authentication, and they may well use mobile versions of instant messaging apps such as Microsoft Teams and Zoom. Blurring the boundaries between personal and professional life increases the risk of confidential information falling into the wrong hands. The development of the Internet of Things has also opened up new opportunities for cybercriminals [7]. As a result, the main trend of cybersecurity is to attract the attention of companies to the security problems that have arisen as a result of the transition to remote work: identifying and eliminating new security vulnerabilities, improving systems, implementing security measures and ensuring proper monitoring and documentation.

Currently, cyberattacks are carried out with the aim of extorting money from people or disrupting production or work processes in companies. Cybersecurity is considered as a component of computer security and information technology. Compliance with the basic requirements of information security allows you to keep physical and digital data intact, protect them from disclosure, use, verification or complete destruction, that is, from unauthorized access to them. According to the international security services in the field of cyber threats, about 12 people are attacked every second in the world and about 556 million cybercrimes are committed annually in the world, the damage from which is more than 100 billion US dollars.

According to international cybersecurity experts, in 2019 cyberattacks around the world occurred every 14 seconds. Along with the increase in the number of cyberattacks, the damage they cause is also growing: in 2018 the losses of companies from various sectors of economy amounted to $ 1.5 trillion, while in 2019, according to experts, they already reached 2.5 trillion dollars. In 2022, according to the forecasts of the World Economic Forum, the amount of damage caused to the planet as a result of cyberattacks could grow to $8 trillion. By the way, anyone can be subjected to cyberattacks - both large companies and ordinary users. Many believe that their televisions and other household appliances may not be of interest to hackers. However, few people pay attention to the fact that thanks to these devices it is also possible to access personal data that can be used for various purposes.

Currently, in the Republic of Kazakhstan, the interaction of the IT industry with domestic business is perceived as a promising direction. The message of the President of the Republic of Kazakhstan "Kazakhstan in a new reality: time to act" reflects the fact that large public and private companies spend tens of billions of tenge on the development and attraction of foreign players. The government should establish mutually beneficial cooperation between industry and the IT industry. This will create digital technology platforms that will be able to fuel the digital ecosystem of any industry and make Kazakhstan one of the international centers for processing and storing data.

There are not so many companies engaged in practical provision of information security in Kazakhstan, no more than ten. The main reason: most of the orders were subcontracted in Russia, Israel or European countries. For example, second-tier banks ordered information security not from Kazakhstani, but from foreign suppliers. There are many distributors of software on the Kazakhstan market that sell foreign antiviruses, firewalls and security systems. The main consumer of cybersecurity services is, of course, the banking sector, since the banks' reputation depends on it. In addition, if the information is disclosed, it will be extremely difficult to avoid financial losses. That is, banks must undergo annual inspections, which cost from 20 thousand dollars. If we talk about small businesses, outsourcing of information security will cost from 1 million tenge per month. At the same time, the costs of companies still hardly pay their way, because the market is growing slowly. The ingenuity of hackers and scammers, as well as the emergence of new ways of processing information, stimulate the development of increasingly stringent standards and requirements for information security (IS), which, according to experts, generate new solutions in this area [8].

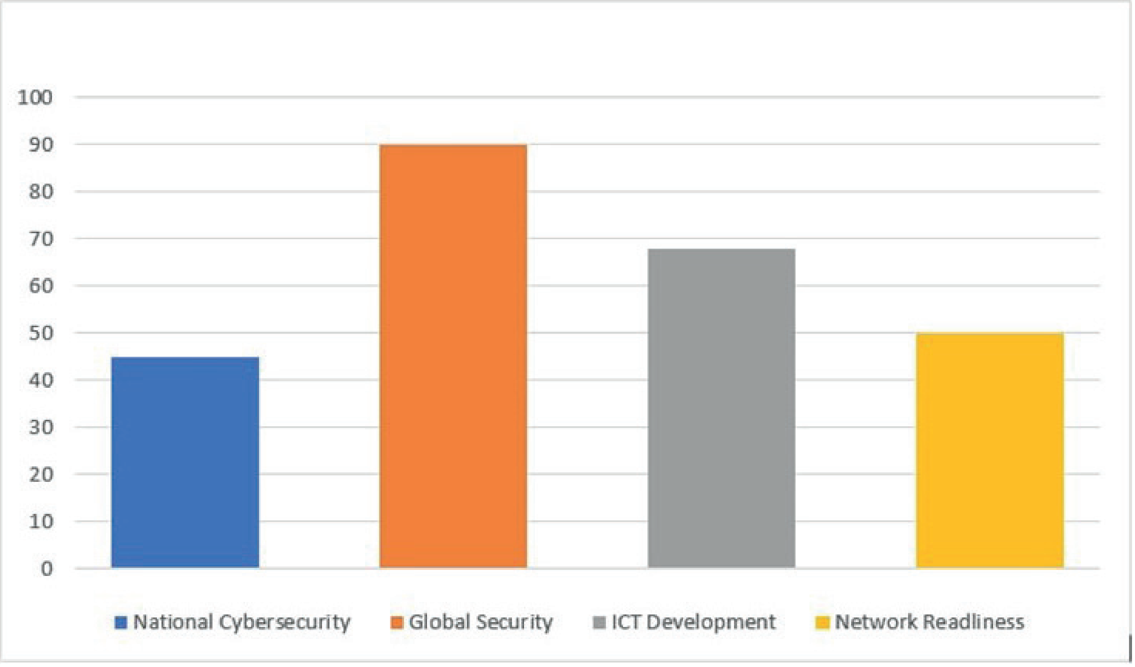

Figure 1 - Percentage of completion of the national Cybersecurity Index

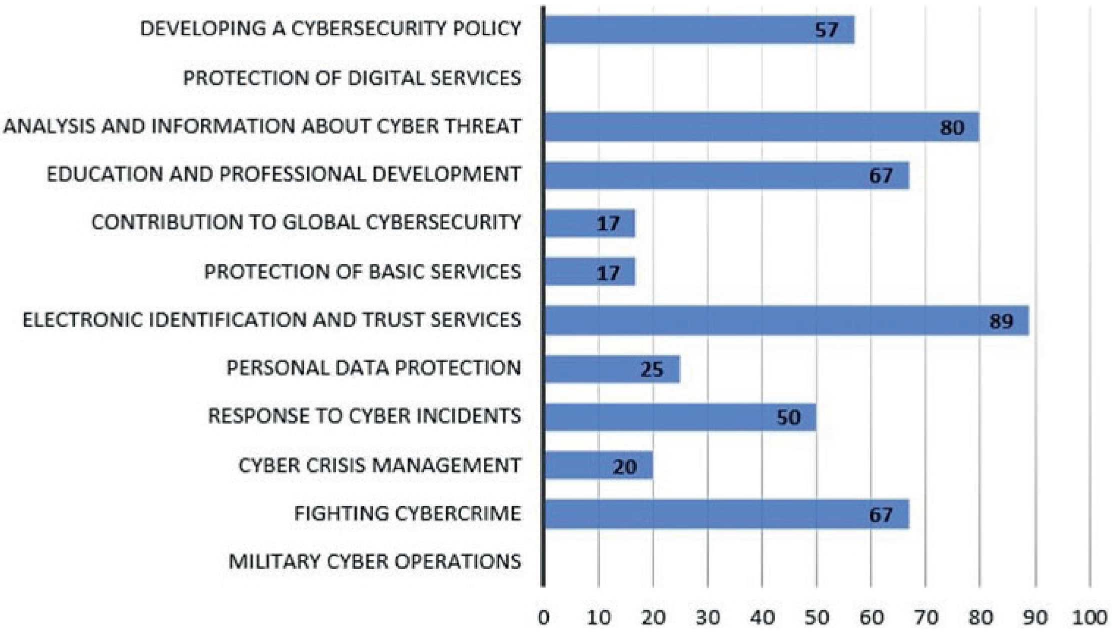

Figure 2 - Percentage of NCSI completion

"Within the framework of the program "Cyber Defense of Kazakhstan", the state has identified 336 critical cybersecurity facilities, including state institutions, banks and industrial companies, attacks on which may have a national or interstate effect. As of now, testing laboratories have been set up in the country to study malicious code, the National Information Security Coordination Center has been launched. There is also a Private Computer Incident Response Service (CERT) and 7 operational centers for information protection (COMI). The number of grants in this specialty for future specialists has been increased. It is also planned to endow the Information Security Committee with functions to protect personal data, conduct audits and verify the owners of information systems. This will help to improve the situation in the field of information security and personal data protection.

Analysts note the country's successes in the legal sphere. In particular, it is noted that Kazakhstan has uniform requirements in the field of information and communication technologies and information security. The Digitization Initiative attaches increasing importance to an effective cybersecurity strategy. Over the past two years, fundamental conceptual approaches to the development of the country's cybersecurity sphere have been developed in the country. The cybersecurity concept "Cyber Defense of Kazakhstan" has been developed and approved, as well as a number of legislative acts and industry contracts. In addition, testing laboratories have been established to study malicious code, a national information security coordination center has been established, the number of scholarships in this area has been increased, etc. [9, p. 32-34].

Over the past few years, Kazakhstan has developed basic conceptual approaches to the development of the country's cybersecurity sphere. One of the important events is the approval of the Cyber Shield concept of Kazakhstan. The purpose of the concept is to achieve and maintain the level of protection of electronic information resources, information systems and ICT infrastructure from external and internal threats, ensuring the sustainable development of the Republic of Kazakhstan in the conditions of global competition. The implementation of the Cybersecurity Concept "Cyber Shield of Kazakhstan" by 2022 is expected to yield the following results:

− the number of retrained specialists in the field of information security in 2022 will reach 800 people;

− a 50% increase in the share of domestic software products in the field of computerization and communications used in the public and quasi-public sectors in 2022 compared to the base period of 2017;

− the share of IT systems of state bodies, non-state information systems integrated with state IT systems of critical ICT infrastructure facilities associated with information security monitoring centers should be 80% in 2021 and 100% in 2022 [10, p. 16-20].

Conclusion. In general, cybersecurity is the most important area of the IT industry. There are a number of professional certification opportunities for training and gaining experience in the field of cybersecurity. Although billions of dollars are spent on cybersecurity every year, no computer or network is protected from attacks and can be considered completely secure. All devices and IT facilities must be protected from intrusion, unauthorized use and vandalism. In addition, information technology users should be protected from asset theft, extortion, identity theft, loss of privacy and confidentiality of personal information, malicious damage, equipment damage, hacking of business processes and cybercriminals in general. The public should be protected from acts of cyberterrorism, such as compromise or loss of the power grid.

In conclusion, it is shown that strengthening cybersecurity is an essential condition for maintaining peace in the country. And the rapid development of the security market is directly determined by the rapid development and use of technological innovations, as well as the toughening requirements to the protected data security. Thus, it can be assumed that the set goals have been achieved. A lot of new, interesting and useful developments have taken place. The knowledge gained will be useful to all of us in life. The stronger the dependence of society on computer systems becomes, the greater is the vulnerability of Kazakhstan and other countries to all types of cybercriminals. You have to think about security today, tomorrow may be too late.

REFERENCES

1. What is cybersecurity and why is it important? (multipassword.com)
2. T.A. Tereshchenko. Cybersecurity: Problems and Solutions / Natural Sciences and Humanities Research №24(2), 2019. – 63- 65p.
3. Malik, T. N. Cybersecurity: problems and prospects / T. N. Malik. - Text : direct // Young scientist. — 2021. — № 7 (349). — Pp. 10-12.
4. Yablochkin A.S., Koshkin A.P. - Modern directions of research in the field of information security strategies // National security / nota bene. – 2019. – № 5. – 34- 42c.
5. Cybersecurity Trends 2021 | Kaspersky Lab (kaspersky.ru)
6. Cybersecurity and information security (spravochnick.ru)
7. NCSI: Kazakhstan (ega.ee)
8. How Kazakhstan's Cybersecurity is developing | Strategy2050.kz
9. Lim V.B. Development of information security in Kazakhstan//Science, Technology and education, 2020 - 32-34s.
10. Biekenov N. A. Some problems of cybersecurity in the Republic of Kazakhstan // Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan No. 1 (33) 2014 - 16-20s.

Мубаракова С.Р., Аманжолова С.Т., Ускенбаева Р.К.

Қазіргі әлемдегі кибер қауіпсіздіктің өзектілігі

Андатпа. Бұл мақалада бүгінгі күннің ең өзекті мәселелерінің бірі: қазіргі әлемдегі киберқауіпсіздіктің өзектілігі талқыланады. Мақалада киберқауіпсіздік туралы негізгі фактілер талқыланады. Сондай-ақ киберқауіпсіздікті дамытудың тұжырымдамасы мен тарихи аспектісі қарастырылды. Бұған қоса Қазақстандағы киберқауіпсіздіктің қазіргі жағдайы сараланды. Бұл мақаланың өзектілігі қазіргі қоғам үшін киберқауіпсіздік туралы нақты ақпарат беруінде. Мақаланың негізгі мақсаты – қазіргі әлемдегі киберқауіпсіздіктің өзектілігін талдау. Осыған байланысты мақалада сіз қазіргі заманның кибершабуылдары мен киберқауіпсіздігі туралы өзекті деректерді таба аласыз.

Кілт сөздер: Киберқауіпсіздік, Ақпараттық технологиялар, Кибершабуылдар, Киберқылмыс.

Мубаракова С.Р., Аманжолова С.Т., Ускенбаева Р.К.

Актуальность кибербезопасности в современном мире

Аннотация. В данной статье рассматривается один из наиболее актуальных вопросов сегодняшнего дня: актуальность кибербезопасности в современном мире. В статье рассматриваются основные факты о кибербезопасности. Также были рассмотрены концепция и исторический аспект развития кибербезопасности. После этого было проанализировано текущее состояние кибербезопасности в Казахстане. Актуальность данной статьи заключается в том, что она предоставляет четкую информацию о кибербезопасности для современного общества. Основной целью статьи является анализ актуальности кибербезопасности в современном мире. В связи с этим в статье вы можете ознакомиться с актуальными данными о кибератаках и кибербезопасности нашего времени.

Ключевые слова: Кибербезопасность, Информационные Технологии, Кибератаки, Киберпреступность.

Авторлар туралы мәліметтер:

Мубаракова Салтанат Рахатқызы, «Компьютерлік инженерия және ақпараттық қауіпсіздік» кафедрасының до кторанты, Халықаралық ақ параттық технологиялар ун иверситеті, Манас көш. 8, Алматы, Қазақстан. OR CID: 0000-0002-2394-881X.

Аманжолова Сауле Токсановна, «Компьютерлік инженерия және ақпараттық қауіпсіздік» кафедрасының ассистент-профессоры, техника ғылымдарының кандидаты, Халықаралық ақпараттық технологиялар университеті, Манас көш. 8, Алматы, Қазақстан. ORCID: 0000-0002-6779-9393.

Ускенбаева Раиса Кабиевна, «Компьютерлік инженерия және ақпараттық қауіпсіздік» кафедрасының профессоры, техника ғылымдарының докторы, Халықаралық ақпараттық технологиялар университеті, Манас көш. 8, Алматы, Қазақстан. ORCID: 0000-0002-8499-2101.

Сведения об авторах:

Мубаракова Салтанат Рахаткызы, докторант кафедры «Компьютерная инженерия и информационная безопасность», Международный университет информационных технологий, ORCID: 0000-0002-2394-881X.

Аманжолова Сауле Токсановна, кандидат технических наук, ассистент-профессор кафедры «Компьютерная инженерия и информационная безопасность», Международный университет информационных технологий, ORCID: 0000-0002-6779-9393.

Ускенбаева Раиса Кабиевна, доктор технических наук, профессор кафедры «Компьютерная инженерия и информационная безопасность», Международный университет информационных технологий, ORCID: 0000-0002-8499-2101.

About the authors:

Saltanat R. Mubarakova, Doctoral student, Department of Computer Engineering and Information Security, International Information Technology University, ORCID: 0000-0002-2394-881X.

Saule T. Amanzholova, Candidate of Technical Sciences, Assistant–Professor, Department of Computer Engineering and Information Security, International Information Technology University, ORCID: 0000-0002-6779-9393.

Raissa K. Uskenbayeva, Doctor of Technical Sciences, Professor, Department of Computer Engineering and Information Security, International Information Technology University, ORCID: 0000-0002-8499-2101.

INTERNATIONAL JOURNAL OF INFORMATION AND
COMMUNICATION TECHNOLOGIES

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И
КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ
КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

Ответственный за выпуск	Есбергенов Досым Бектенович
Редакторы	Медведев Евгений Юрьевич
Компьютерная верстка и дизайн	Жадыранова Гульнур Даутбековна

Редакция журнала не несет ответственности за
недостоверные сведения в статье и
неточную информацию по цитируемой литературе

Подписано в печать 15.12.2021 г.
Тираж 500 экз. Формат 60х84 1/16. Бумага тип.
Уч.-изд.л. 6.5. Заказ №170

Издание Международный университет информационных технологий
Издательский центр КБТУ, Алматы, ул. Толе би, 59