

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

**Студенттер мен жас ғалымдардың
«GYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ**

**СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«GYLYM JÁNE BILIM - 2024»**

**PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«GYLYM JÁNE BILIM - 2024»**

**2024
Астана**

УДК 001

ББК 72

G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докторанттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001

ББК 72

G99

ISBN 978-601-7697-07-5

**©Л.Н. Гумилев атындағы Еуразия
ұлттық университеті, 2024**

INFORMATION SECURITY IS A KEY COMPONENT OF NATIONAL SECURITY

Berikbosynova Diana

dberikbosynova0@gmail.com

Master degree student of the Faculty of International Relations,
L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
Supervisor – B. Somzhurek

In the course of modern globalization, attacks on information and communication technologies are considered as threats to the direct national security of the state, and their identification and regulation is a national priority.

In general, we can look at information security from two sides. The first is cybersecurity in the field of IT, protection against hacker attacks, ensuring personal confidential data of citizens, etc. The second is the problem of repelling various ideological information attacks on the information front from the outside and from the inside, the formation of a competent and cold-blooded consciousness among citizens. The problem of security in the IT field. This industry is an urgent problem that has worried ordinary developing countries, starting with the most advanced countries of the world. The state is also interested in the protection of personal data of citizens and, having nailed this by law, serves to ensure information security through the relevant structures.

According to statistics, in January 2021, more than 25.5 thousand cyber attacks were committed, which is 2.8% higher than in January 2020. Most of the cyber attacks occurred through malicious software on computers [7].

Thanks to the acquisition of IT technologies, cyber attacks are most often directed at government agencies and banks, as well as the infrastructure of the Kazakh internet. Attacks on the credit financial system, in turn, lead to a decrease in the economic situation of the state. For example, the National Bank attributes to the main risks in this area the losses of customers, individual financial organizations, violations of the operational reliability and continuity of the provision of financial services, violations of the systemic crisis.

The agency for regulation and development of the financial market reported that in 2021, about 2 billion dollars were robbed from two Kazakhstani banks, as well as anonymous transactions on more than 250 payment cards.

By October 2022, there were 44.3 million payment cards in circulation - 45% more than in the same period (30.6 million) for 2021. Such growth is the highest in recent years. The most common are debit cards, the share of which is 76.5%, credit cards-20.0%. At the same time, over the past nine months, 8.3 thousand cases of internet fraud were registered-52.8% more than in the corresponding period last year. Over the past three years, the frequency of such crimes has doubled [10].

Today, the most valuable asset of any organization is information, and information and communication technologies are at the heart of all business processes. However, Kazakhstan's informatization and internet infrastructure are often subjected to hacker attacks. According to The Information Security Department of the National Security Committee, cyber attacks are aimed at both government agencies and private citizens of Kazakhstan.

On September 25, Kazakhtelecom registered massive DDoS attacks on a number of sites of Kazakhstan's information resources. Newtimes.kz, toppress.kz, Kazakh language sn.kz problems were also noted in the work of a number of media outlets, such as the site and Radio Liberty.

Local internet operators also have problems. On September 28, Kazakhstanis began to complain about communication problems at Tele2, Kcell and Beeline. The operators had already stated that "the failures are not on our part, but at the global level." Such hacker attacks were attributed by the president

of the Republic of Kazakhstan Kassym-Jomart Tokayev to the upcoming elections of the head of state, which will be held on November 20 [8].

Several documents have been adopted in the country to prevent possible threats and problems of informatization. The Republic of Kazakhstan adopted the main legislative acts "on state secrets", "on Informatization", resolutions of the government of the Republic of Kazakhstan "on approval of uniform requirements in the field of Information and communication technologies and information security", "on approval of the concept of cybersecurity ("cyber shield of Kazakhstan")".

At the same time, the main strategic document on ensuring information security is the Law No. 527-IV of January 6, 2012 "on national security of the Republic of Kazakhstan".

In accordance with Article 4, "Information Security is the state of protection of the information space of the Republic of Kazakhstan from real and potential threats in the field of information, as well as the rights and interests of a person and citizen, society and the state, ensuring sustainable development and information independence of the country". Article 23 provides for the Prevention of information dependence of Kazakhstan, prevention of information isolation and isolation from other states, organizations and individuals, prevention of information isolation of the President, Parliament, government and forces ensuring national security of the Republic of Kazakhstan, detection and violation of mechanisms of hidden information influence in the process of formulating and making state decisions, undermining national security, , in particular, it is noted that priority will be given to the creation and strengthening of a national system for ensuring information security of the most important objects of State Electronic Information Resources, Information Systems, Information and communication infrastructure [3].

The main political and legal act in the country, which defines the principles and main directions of information security development, is the concept of "Cyber Shield of Kazakhstan", developed within the framework of the address of the president of the Republic of Kazakhstan "Third Modernization of Kazakhstan: Global Competitiveness" and the strategy "Kazakhstan-2050" for Kazakhstan's entry into the top 30 most developed countries of the world. The concept defines the main directions of implementation of state policy in the field of protection of Electronic Information Resources, Information Systems and telecommunications networks, ensuring the safe use of information and communication technologies [4] , [5].

It should be noted that the shortage of personnel in the IT sector in Kazakhstan is quite high. This was announced at a Government Meeting by the minister of digital development, innovation and aerospace industry Bagdat Musin. It was noted that the main focus is on strengthening the Institute of state control in the field of information security, focusing on research work in this area. Earlier, President Kassym-Jomart Tokayev said that by 2025 Kazakhstan will train at least 100 thousand highly qualified IT specialists [9].

Information security is the most important area that forms the national security of any state. Especially as internet communication develops, the relevance of Information Security is increasing. Examples of this are cybersecurity, which is becoming increasingly important around the world today, unauthorized possession of personal data of citizens through hacking on the internet platform and its use for various negative purposes, various ideological contradictions in the information sphere, attempts to manipulate consciousness

In conclusion, realizing the complexity and responsibility of this problem, an integrated approach is needed to solve it at the state level. Cybersecurity is a complex transnational problem that requires international cooperation to ensure the Internet. To effectively counter these threats, we need a multi-level cybersecurity system that protects our citizens and government institutions.

Studying the scale of the threat of cyber threats and cybercrime, it is necessary to strive to prevent cyber attacks rather than eliminate their consequences based on the methods of the leading countries of the world.

Literature

1. Gafner V.V. Information security: Textbook - Moscow, 2017.
2. Gromov Yu.Yu. Information security and information protection: Textbook - Art. Oskol: TNT, 2017. 384 b.
Bubnov A.A., Przhegorlinsky V.N., Savinkin O.A. Akparattyk kauipsizdik negizderi. - Moscow State University 2016. - 180 b.
3. Kazakhstan Republikasynyn ulttyk kauipsizdigi turaly - "Adilet" AKZH (zan.kz)
4. Resolution of the Government of the Republic of Kazakhstan dated June 30, 2017 No. 407 "On approval of the Concept of Cybersecurity (Cybersecurity of Kazakhstan)" // adilet.zan.kz/rus/docs/P1700000407 .
5. "Kazakhstan Ushinshi zhangyru: zhahandyk basekege kabilettilik" - "Adilet" AKZH (zan.kz)
6. Akparattandyr turaly - "Adilet" AKZH (zan.kz)
7. More than 25 thousand cases of cyber attacks were recorded in the Republic of Kazakhstan in 2021 — The Village Kazakhstan. – [Electronic resource]. Access mode: the-village-kz.com
8. "In the saddest case, this will lead to a massive blackout." Who is behind the cyber attacks on Kazakhstan on the eve of the presidential elections. – [Electronic resource]. Access mode: mediazona.ca
9. There is a shortage of IT specialists in Kazakhstan - Capital. – [Electronic resource]. Access mode: kapital.kz
10. Cyber attacks in the banking sector of Kazakhstan have doubled in a year. – [Electronic resource]. Access mode: NewTimes.kz

УДК 327

ЭНЕРГЕТИЧЕСКАЯ БЕЗОПАСНОСТЬ РЕСПУБЛИКИ КАЗАХСТАН В КОНТЕКСТЕ СОВРЕМЕННЫХ ГЕОПОЛИТИЧЕСКИХ РЕАЛИИ

Біржанұлы Сұлтан

Sultan_2002@mail.ru

студент факультета международных отношений

ЕНУ им. Л.Н. Гумилева, Астана, Казахстан

Научный руководитель – Г.М. Какенова

Глобальное развитие XXI века тесно взаимосвязанно с энергетической составляющей экономического роста субъектов международной политики. В условиях геополитической нестабильности государства проектируют и реализуют национальные стратегии и в сфере энергетической безопасности. Республика Казахстан, как обладатель большого ресурсно-энергетического потенциала, не является исключением. Проводя энергетическую политику, Казахстан учитывает и актуальные проблемные составляющие, которые остро влияют на энергетическую безопасность. В целом, для понимания сути энергетической безопасности стоит остановиться на контексте данного понятия. Энергетическую безопасность научные сотрудники Международной школы бизнеса РГУ нефти и газа имени И.М. Губкина Тургумбаева А.К. и Кульмамирова М.С. определяют как один из главных компонентов национальной безопасности государства. Данный термин приобрел особую значимость после нефтяного кризиса и скачка цен на энергоресурсы в 1970-1980-х гг. XX века. Сам термин «energy security» чуть раньше, в 1940-х г. в США. Политологи и юристы связывали данный термин с интенсивным развитием экономики штатов после Второй мировой войны и огромным спросом на энергоносители [1].

П. Робертс определяет энергетическую безопасность как уверенность в том, что энергия будет иметься в распоряжении в том количестве и того качества, которые необходимы при данных экономических условиях. Подчеркивается, что энергетическая безопасность есть «возможность