INTERNATIONAL EXPERIENCE OF THE EU COUNTRIES AND KAZAKHSTAN IN ADDRESSING CYBERSECURITY ISSUES

Makpal JEKEBAYEVA * *candidate of philosophical sciences, associate professor of Kazakh-Russian medical university, Almaty, Kazakhstan, makpal.jekebayeva@mail.ru, ORCID ID: https://orcid.org/ 0000-0001-7771-8828*

Yerzhan CHONGAROV *candidate of philosophical sciences, associate professor of Kazakh-Russian medical university, Almaty, Kazakhstan, yerzhanalemkulov@gmail.com, ORCID ID: https://orcid.org/0009-0009-9435-7345*

Namig MAMMADOV *PhD in History, Azerbaijan National Academy of sciences, Baku, Azerbaijan, mammadov.namig@yahoo.com, ORCID ID: https://orcid.org/0000-0003-4356-6111*

Дата поступления рукописи в редакцию: 30/09/2025
Доработано: 11/12/2025
Принято: 12/12/2025

DOI: 10.52123/1994-2370-2025-1663
УДК 35.078
МРНТИ 14.35.06

Annotation. The article is devoted to the problems of developing a system for assessing security against social engineering attacks. The purpose of the article is to study and analyze methods of protection against sociotechnical attacks and to develop a system for assessing security against social engineering attacks. The article describes techniques for collecting information from open sources, communication modeling, and profiling, basic principles of social engineering and the application of social engineering. Effective protection tools against social engineering have also been investigated and the process of developing a phishing simulator to counteract social engineering through phishing has been step-by-step reviewed. The article examines awareness-raising and learning is one of the key methods for assessing and effectively protecting against social engineering, and discusses effective methods of protecting against social engineering. The article also summarizes the results of the research, analysis and development of the system, as well as describes further steps to develop this area. The introduction of an effective cybersecurity training system will significantly increase the level of security and reduce the risk of data leakage, which is a key step to ensure information security.
Keywords: Security Operations Center, Artificial Intelligence, cyber range, digital society, cybersecurity, social engineering, sociotechnical attacks, cybercrime.

Аңдатпа. Мақала әлеуметтік-техникалық шабуылдардан қорғауды бағалау жүйесін әзірлеу проблемасына арналған. Бұл мақаланың мақсаты әлеуметтік-техникалық шабуылдардан қорғау әдістерін зерттеу және талдау және әлеуметтік инженерлік шабуылдардан қорғауды бағалау жүйесін әзірлеу болып табылады. Мақалада ашық көздерден ақпарат жинау әдістері, коммуникацияны модельдеу, профайлинг, әлеуметтік инженерияның негізгі принциптері және әлеуметтік инженерияны қолдану сипатталған. Сондай-ақ, әлеуметтік инженериядан қорғаудың тиімді құралдары зерттеліп, даму процесі кезең-кезеңімен қарастырылды, фишинг тренажері фишинг арқылы әлеуметтік инженерияға қарсы тұру. Мақалада хабардарлық пен оқытуды арттыру-бағалаудың негізгі әдістерінің бірі және әлеуметтік инженериядан тиімді қорғаныс ретінде зерттеліп, әлеуметтік инженериядан қорғаудың тиімді әдістері егжей-тегжейлі қарастырылған. Сонымен қоса мақалада жүйені зерттеу, талдау және әзірлеу қорытындылары шығарылды, сондай-ақ осы бағытты дамыту бойынша одан әрі қадамдар сипатталды. Тиімді киберқауіпсіздік бойынша оқыту жүйесін енгізу қауіпсіздік деңгейін айтарлықтай арттырады және деректердің бұзылу қаупін азайтады, бұл ақпараттық қауіпсіздікті қамтамасыз етудің негізгі қадамы болып табылады.
Түйін сөздер: Қауіпсіздік операциялық орталығы, жасанды интеллект, киберполигон, цифрлық қоғам, киберқауіпсіздік, әлеуметтік инженерия, әлеуметтік-техникалық шабуылдар, киберқылмыс.

Аннотация. Статья посвящена проблеме разработки системы оценки защиты от социально-технических атак. Целью данной статьи является изучение и анализ методов защиты от социально-технических атак и разработка системы оценки защиты от социально-инженерных атак. В статье описаны методы сбора информации из открытых источников, моделирование коммуникации, профилирование, основные принципы социальной инженерии и применение социальной инженерии. Также были изучены эффективные средства защиты от социальной инженерии, а процесс разработки был поэтапным, симулятор фишинга противодействие социальной инженерии с помощью фишинга. В статье изучается повышение осведомленности и обучения как один из основных методов оценки и эффективной защиты от социальной инженерии, а также подробно рассматриваются эффективные методы защиты от социальной инженерии. Также в статье были подведены итоги исследования, анализа и разработки системы, а также описаны дальнейшие шаги по развитию данного направления. Внедрение эффективной системы обучения кибербезопасности значительно повысит уровень безопасности и снизит риск утечки данных, что является ключевым шагом в обеспечении информационной безопасности..

* *Corresponding author: M. Jekebayeva, makpal.jekebayeva@mail.ru*

Ключевые слова: Операционный центр безопасности, искусственный интеллект, киберполигон, цифровое общество, кибербезопасность, социальная инженерия, социально-технические атаки, киберпреступность.

Introduction

In today's digital world, where information technology permeates all areas of life, cybersecurity is becoming one of the most pressing and significant international issues. The relevance of cybersecurity issues in the world and in Kazakhstan today is beyond doubt. Hacker attacks, identity theft, and the spread of malware all pose a threat not only to financial institutions and large corporations, but also to every Internet user.

Cybercrime has become an international problem that requires joint efforts on the part of states, organizations, and society as a whole. This has led to the need to develop a training platform for information security specialists. This platform is called a cyber range – a model environment that allows cyberattack and cyber defense scenarios to be practiced safely. It is similar to a military training ground, but is used in the field of cybersecurity (Hednegi, 2021).

Threats in this area can be divided into three categories:

1. Cybercrime – includes actions by individuals or groups aimed at obtaining financial gain or damaging information systems.
2. Cyberattacks – most often have political motives and are related to the collection of confidential data.
3. Cyberterrorism – aimed at destabilizing electronic systems in order to create panic or fear (kaspersky-carbanak, 2025).

Social engineering, types and techniques

To solve problems related to cybersecurity in Kazakhstan, it is planned to develop proposals aimed at creating a culture of cybersecurity and increasing the level of information security in the SOC analytics system using an AI Agent.

The main difference of this work is the implementation of recommendations and strategies to increase the level of digital security, as well as the creation of a training platform for SOC analysts using an AI agent. Among the most common cybersecurity threats, malware occupies a special place — software created by cybercriminals to hack or damage legitimate users' computers. In some cases, fraudsters commit financial crimes using the gullibility and low level of digital literacy of citizens: they gain access to personal data and fraudulently transfer funds from victims' bank accounts. There are many types of SI, which are based on the peculiarities of human decision-making. Types of SI – phishing, vishing, SMiSHing, pretexting, Trojan horse, fishing “on the bait”, the reverse side of SI, road apple, etc. All types of SI are dangerous, it is necessary to be aware of what SI is and how it functions. It is necessary to learn and master the skills of recognizing key mechanisms. In this section, I will briefly describe the types of SI (Yazan, & Reema, 2024).

Pretexting is an action that is carried out according to a pre-written script (pretext). This type of attack is usually carried out over the phone. More often than not, this technique involves more than just lying and requires some preliminary research, such as finding out the employee's name, position, bonus systems, projects they work on, family circumstances, etc., in order to gain the victim's trust.

Qui pro quo: The attacker calls the company and pretends to be a technical support employee, asking about any technical issues with the devices or system. If there are any issues, the attacker enters commands that allow them to launch malicious software or force the download of malware (Salal, 2023).

The aim of the article is to develop an educational programmer that promotes political and ethical digital literacy among young people, teenagers, students and users of other age groups in the field of cybersecurity and countering cyberbullying in a digital society.

The main idea of the article is to identify the level of awareness and attitude of young people towards cybersecurity issues, to study their perceptions of the risks of the digital environment, methods of protection and the importance of safe behavior in the online space. The project involves developing recommendations and strategies to improve digital security, as well as creating a training platform for young people called Cyber Polygon.

How can cybercrime, cyberattacks, cyberterrorism and malicious activity control computer systems? First, it is necessary to know some common methods that can compromise cybersecurity. For example: deleterious malware and spyware.

Ransomware is malicious software that locks a device or encrypts its contents, demanding money from victims. Operators of paid malware promise to restore access to the infected device or data. Malware, adware, and botnets block user files and data, which can be deleted if the payment is not made. Finally, effective combating of cyber threats requires active international cooperation. This includes the development of international standards and regulations, joint training and education, as well as educating young people and the public about the dangers of cybersecurity by sharing experiences and best practices between different countries by blocking fraudsters (Iubuzova, & Myrzaş, 2024).

Literature review

EU Cybersecurity Discourse: The academic and policy discourse surrounding EU cybersecurity consistently addresses several key themes: Legislative Alignment: This encompasses how EU directives, such as NIS2, are incorporated into the national strategies and governance structures of various member states. Risk Management Structures: It covers the frameworks for managing risks and incidents mandated by EU legislation and how these are put into practice at the national level. Challenges in Application: Research also highlights difficulties in achieving compliance and effective implementation. These include disparities in how member states adopt NIS2 provisions, limitations in institutional capabilities, and obstacles specific to certain sectors.

Kazakhstan's Cybersecurity Journey: Kazakhstan has been actively enhancing its cybersecurity posture through national initiatives and legal measures: National Digitalization and Defense Plans: Kazakhstan's overarching cybersecurity strategy, often referred to as "Cyber Shield Kazakhstan," sets out goals for safeguarding digital assets. However, there is continuous deliberation regarding the modernization and refinement of its legal architecture to counter emerging threats. Academic Exploration of Cybersecurity Law: Domestic legal research provides valuable perspectives on categorizing cyber threats and the complexities of law enforcement and legal oversight within Kazakhstan's specific environment. Comprehensive Security Assessments: Scholarly work also investigates cybersecurity within wider digital governance and risk management frameworks, including strategic risk evaluations and proposals for bolstering institutional capacity.

Contrasting and Area-Specific Viewpoints

Cross-National Legal Examination: Certain assessments contrast Kazakhstan's cybersecurity policies with those of the European Union and other nations, pointing out disparities in the advancement of regulations, the strength of organizational structures, and the focus of strategic objectives. For instance, Kazakhstan's approach to cybersecurity is frequently contrasted with the legal structures found in the EU and the United States.

Geographic Area Research: External research (such as that from the e-Governance Academy and EU collaborators) depicts Kazakhstan as a frontrunner in Central Asia regarding its institutional frameworks, national strategies like Cyber Shield, CERT/SOC networks, and its efforts in international collaboration.

Global Partnerships: Kazakhstan participates in both one-on-one and multi-nation collaborations, including initiatives within the Shanghai Cooperation Organisation (SCO), underscoring its involvement in international discussions on cybersecurity policy.

Both the EU and Kazakhstan acknowledge prevalent themes in scholarly works and practical applications:

Requirement for Aligned Legal Structures: The necessity for national and supra-national legislation to address shortcomings in managing cyber risks and to clearly define accountability.

Legal Integration: Leveraging the NIS2 framework and its underlying principles to guide modifications to national cybersecurity legislation and reporting benchmarks.

Strategic Alignment: Establishing more robust systems for incident reporting, risk evaluation, and inter-agency coordination, mirroring the standardized approaches adopted within the EU.

Kazakhstan's published materials and policies demonstrate active engagement with cybersecurity challenges, though there remains scope for further development, especially in aligning its laws with international standards and reinforcing its institutional capacities.

Methodology

This study is based on a combination of qualitative and quantitative methods, following a mixed methods research approach, which enables a comprehensive examination of the phenomenon of the smart city and urban environment comfort (Myrzaş, 2024). The research was conducted in several stages, each with specific objectives and corresponding data collection and analysis methods. The most important task of the modern world is to ensure security in an online environment where people are dependent on information technology.

Artificial intelligence (AI) is a field of computer science that focuses on creating systems capable of mimicking human cognitive functions such as learning, problem solving, and decision making. Today, from schoolchildren to adults, everyone actively uses AI services. The development of an intelligent artificial intelligence agent to automate the work of analysts at Cybersecurity Centers (SOC) in Kazakhstan is one of the most important urgent tasks of society. «Cybersecurity" includes not only data protection, but also the prevention of cyber attacks, ensuring confidentiality, integrity and availability of information. This scientific article discusses the development of cyber defense, which is aimed at improving cybersecurity, which covers aspects such as protecting personal data, preventing phishing attacks, fraud and malware, the safe use of social networks and protection against cyber espionage. Cybersecurity is an important area related to the protection of information and data from unauthorized access, use and destruction. The relevance of the problem of cybersecurity in the world and Kazakhstan today is not controversial (Jekebayeva, 2023).

The purpose of this article is to explore the study of SOC analytics using an artificial intelligence (AI) agent (SOC analytics AI Agent). This is due to the fact that people often face cyber threats and scammers because they do not have enough information about cybersecurity and personal data protection.

The article is aimed at studying the AI agent, as it will analyze event logs, identify anomalies, propose incident hypotheses, accelerate classification and prioritization, reduce response time to cyber threats, and reduce the burden on specialists. The solution will increase the effectiveness of cyber defense of government and corporate information systems, form domestic AI competencies for cybersecurity, and reduce the shortage of SOC analysts (Jekebayeva, 2023).

Taking into account the definition of the level of information security in society, the problems related to cybersecurity in Kazakhstan, and the development of effective solutions and proposals based on foreign experience that form political and ethical digital literacy among youth, adolescents, students and users of other age groups in the field of cybersecurity and countering cyberbullying in a digital society, the relevance of the implementation of this.

Results

Cybercrime has become an international problem that requires joint efforts on the part of States, organizations and society as a whole. In addition, effective measures will be proposed to improve data protection and cyber protection of society. Here are some examples of cybercrime. One of the cybercrimes of the century is Carbanak. A Russian hacker group has learned how to hack into banking systems.

Since 2013, the attacks of the criminals have been more than 100 banks in 40 countries, including USA, Russia, Germany and Ukraine. In total, they stole $1.2 billion during their existence and this is the "largest digital robbery" in history. To gain access to the internal infrastructure of the bank's network and systems, the attackers used targeted phishing mailings with malicious attachments. A backdoor program was installed on the bank employee's PC to gain control over the employee's PC (Jekebayeva, Iztaeva, Anassova, and Manapbayev, 2023).

Figure 1. – Carbanak cyber gang hacking scheme (https://www.kaspersky.ru/blog/billion-dollar-apt-carbanak/6950/).

After gaining control of the bank employee's PC, cybercriminals used it as a reference point: they explored and analyzed the internal infrastructure of the bank's network, infected other PCs and devices, and identified the most key infrastructures and important agro-industrial complex and IP systems that could be used to gain access to the infrastructure of financial systems.

The next stage included the study of the infrastructure of information systems used by the bank in financial transactions, and for this purpose key loggers and video screen recording were used.

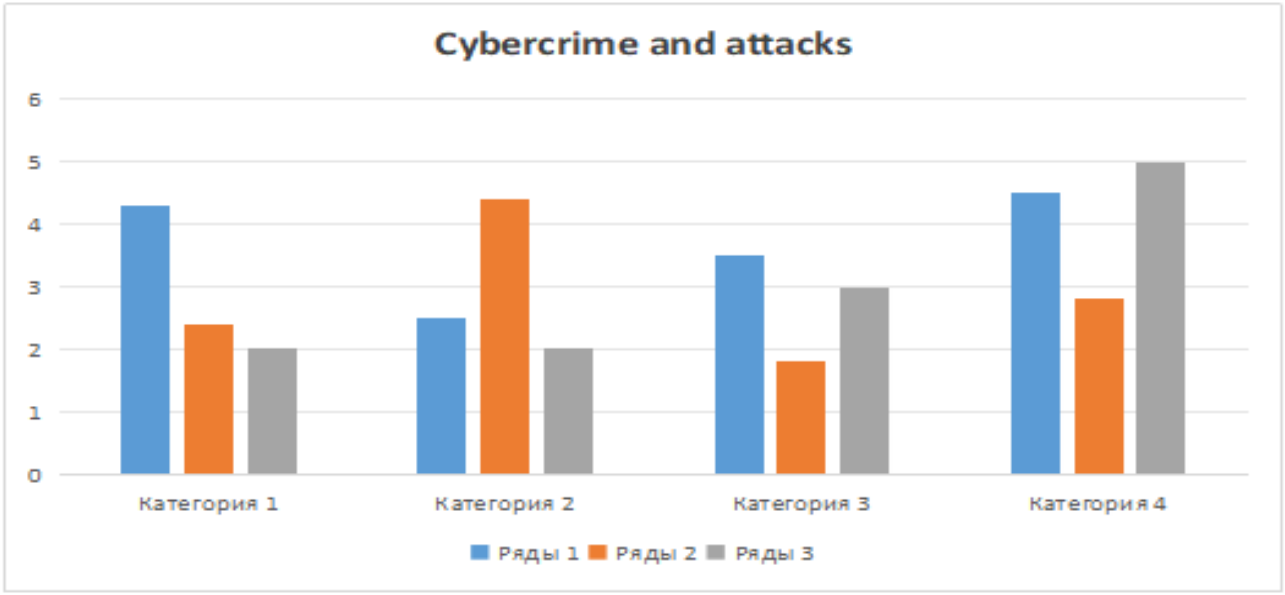
At the final stage, Carbanak's attackers withdrew large amounts of money from the bank in the most convenient ways for each specific situation. They used transfers through the SWIFT banking system, created fake checking accounts of this bank and cash withdrawal through ATMs. There are a lot of cybercrimes in the 21st century and the damage from them is enormous. For example, Russian hackers destroyed a nuclear plant in Iran using the Stuxnet virus, which is now considered scarier than a bomb. In this attack, the attacker used C, namely the road apple type. The attackers planted a flash drive and began infecting different hosts. However, the Iranians kept the computers that control the nuclear facilities disconnected from the network. Stuxnet could only be distributed over flash drives. Antiviruses could not detect the virus in any way. Thus, an attacker using a virus was able to hack into the plant's system and speed up the processes, as a result, the nuclear plant was destroyed (Alimseitova, Adranova, Akhmetov, Lakhno, Zhilkishbayeva, and Smirnov, 2020).

SI research and analysis. Analyzing the cases of the SI attack, we discovered the general attack pattern, implementation mechanisms, and tools that the attackers use. The analysis process is called the "SI pyramid". Collecting data from open sources is the foundation, the foundation of the work of a C specialist. This stage requires significant time resources when planning an attack on a victim, as well as creative approaches when collecting information, therefore it occupies a primary and important role in the SI pyramid. Developing a legend. Based on previously collected data from open sources, the next logical step would be to create a target and a reason or scenario for carrying out an attack by XI. This part of the SI specialist's job should be based on previously collected information. Possible changes and necessary additions to the initial SI attack plan become obvious, and it is also necessary to consider what additional tools and requisites will be needed. Fraudsters often use open social media to find information about people, learning about their jobs, fields of work, status, social standing, travel history, and so on. Therefore, it's crucial to keep personal information secret; this helps prevent scammers from snooping. For example, if I search for information about myself on Google, it returns all my information.

DIAGRAM № 1: Cybersecurity Approaches — EU vs. Kazakhstan

INTERNATIONAL CYBERSECURITY MODELS	
EU COUNTRIES	**KAZAKHSTAN**
Legal framework	Legal framework
GDPR	Law “On Informat’
NIS	Cybersecurity Concept
Institutional	Institutional
ENISA	National Security
CSIRTs Network	Committee
Technical Measures	Technical Measures
Standardization	National CERT
5G security	Critical Infra. Prot
Cyber drills	Gov. SOC Centers
International cooperation	International cooperation
NATO CCDCOE	CSTO, SCO, ITU
EU–US Dialogue	Bilateral EU projects
EU Cyber Act	UN cyber negotiations
Note: The table was compiled by the authors	

DiAGRAM № 1: Cybersecurity Approaches — EU vs. Kazakhstan



The next stage is the process of carrying out the SI attack. This is where the real actions of a social engineer begin. After completing all the stages of preparation, you can proceed with the attack. It's important to be prepared for everything, but don't make too detailed a plan. Excessive detail of each step can create difficulties in unforeseen situations. It is recommended to draw up a general action plan that will allow you to maintain creative freedom.

Report. Few people like to write reports, especially technical specialists. However, your client relies on your professional skills and knowledge to solve an important problem. A specialist should not just demonstrate his capabilities, but the ability to provide specific recommendations and an action plan to eliminate identified vulnerabilities (Lakhno, Togzhanova, Kasatkin, Kartbayev, Uskenbayeva, Alimseitova and Kashaganova, 2021).

Collecting data from open sources is the fundamental foundation of a C specialist. The initial step to a successful SI attack involves gathering available information. Mastering this skill can be difficult, but mastering this skill will allow you to collect a lot of useful information on the Internet. Data collection is a core element of all possible cyberattacks by SI. Knowing the victim's personal information makes it easier to manipulate and impersonate another person, which in turn allows you to collect more additional information about the target.

Today, there are several methods of collecting information on the Internet. One of the main

tools for collecting information are search engines such as Google, Yandex, Brave and others.

Facebook Instagram, VK and other social media profiles that have become publicly available can be accessed by the above-mentioned search engines. In addition to traditional search engines like Google, Yandex, and so on, an experienced C specialist does not limit himself to them alone.

Instagram Facebook, Youtube, Twitter, VK are some of the best sources of personal data. Personal data such as family, birthday, pet names, places of study, interests, friends, and more are often published on social networks. Having carefully studied and analyzed this data, it is possible to collect a huge database about the victim and use them to achieve the desired goal (Lakhno, Kartbayev, Malyukov, Uskenbayeva, Togzhanova, Alimseitova, Beketova, and Turgynbayeva, 2021).

Check the source of the messages. Before you trust a message, check where it came from. There are often cases when a malicious disk drive or flash drive unexpectedly appears on the desktop. Check the drive through antivirus software, do not run questionable drives. It is also important to note that you need to disable the auto-start function of the drive when connecting. In order to check for a virus, before launching.

Let's imagine another situation: the head of the department or the chief executive requested in an email to provide corporate and personal information about employees. First of all, you need to check the source of the messages. Carefully study the headers and text of the incoming letter from the supervisor; you should compare it with other previously received letters from this supervisor. Pay attention to the style, grammar, and formatting. If there are links in the email, do not rush to follow them. If the letter requests information that includes a lot of personal and corporate data, it is better to contact the supervisor directly for clarification using another source of communication, such as a phone call or a private message. This helps to verify the authenticity of the request and prevent possible phishing attacks. It is recommended to be careful when working with confidential data.

The next step in organizing protection against SI is to clarify whether it has complete information, such as: full name, IIN, code word, and so on. Usually, bank employees must know your personal information and request a verification code word before allowing changes to your account. If this doesn't happen, it's most likely scammers. Be careful and careful!

Scammers using SI often put pressure, creating urgency so that the victim cannot think carefully about what is happening. Short-term consideration of the situation can significantly reduce the likelihood of a successful attack. It is important not to rush into transmitting confidential data over the phone or clicking on links. Instead, it is recommended to verify the authenticity of the source through official communication channels, such as calling back to the official number or visiting the official website (Kartbayev, Lakhno, Malyukov, Turgynbayeva, Alimseitova, Malikova, and Kashaganova, 2022).

An important aspect in the organization of protection against SI is the use of alternative communication methods to verify the validity of requests. For example, if you receive an email from someone you supposedly know requesting a money transfer, first contact them through another channel, be it a phone call or a message, to verify the authenticity of the request. In addition, according to research, the use of multi-factor authentication and maintaining awareness of current cybersecurity threats significantly increases protection against such attacks.

It is equally important to require proof of identity, especially in the case of visits to protected sites. It is much easier for social engineers to enter a secure building if they look like legitimate visitors, for example, carrying a box or a stack of folders in their hands. It is strongly recommended to check the identity cards and supporting documents of all incoming users in order to minimize the risk of unauthorized access. Follow this rule in other similar situations. If someone requests confidential information from you, specify their name, ask clarifying questions about the manager or the organization. Then check this information on the Internet or in the directory before providing any personal or personal information (Lakhno, Alimseitova, Kalaman, Kryvoruchko, Desiatko, and Kaminskyi, 2023).

Protect yourself and your devices: Device protection is a key aspect preventing a successful SI attack. According to Kaspersky's cutting-edge company, regardless of the type of device, whether it's a smartphone, phone, WiFi, IOT device, or corporate system, the basic principles of anti-SI security remain unchanged.

Kaspersky company offers the following recommendations on the organization of information security:

- update your antivirus software and operating system (OS) regularly;
- use antivirus software;
- arrange for the restriction of access rights. Restrict root rights on devices, and create restrictive measures for users on the network or PC and leave administrator rights only for some users.;
- Use unique and complex passwords. It is recommended to use different passwords for different information systems. It is recommended to use a password manager to store and create passwords;
- change passwords in a timely manner. If you suspect that your password has been compromised, change it immediately;
- Use two-factor or multi-factor authentication for the most important accounts so that they cannot be hacked with just a password.;
- use a VPN to connect to the internet securely;
- protect the Wifi network with a complex administrator password and modern encryption protocols such as WPA3;
- Use spam filters for email. Effective and reliable spam filters analyze a variety of information to recognize and block malicious emails. Spam filters usually have a blacklist of IP addresses, which is used to quickly check websites. Spam filters using AI can effectively analyze the contents of an email and, if necessary, block unwanted emails;
- conduct seminars and training programs about current cyber threats, and regularly read publications, articles, and forums about new information security threats. This will help you keep abreast of new methods of cyberattacks and significantly reduce the risk of becoming a victim of fraud.

Check the profiles and social media posts. By posting a lot of personal information online, you help attackers collect data and gain your trust by mentioning recent events that a person has shared on social media.

It is recommended to be careful when posting on social media. If you do not run a blog and can afford to block access to social media pages, then it is recommended to open access only to friends.

An important step in this direction was the recent publication of cybersecurity recommendations by the Ministry of Security. These recommendations provide valuable advice and strategies for protecting against cyberattacks and phishing, but more such publications are needed to achieve maximum effect. Regularly publishing articles, conducting seminars, organizing phishing attack simulators, and other educational events should become the norm.

Raising public awareness about cyber threats and how to prevent them is a key aspect in the fight against phishing. Training programs and simulators designed to address current threats and realities can significantly increase people's awareness and strengthen their ability to protect themselves from phishing attacks. By involving a wide range of participants in the training and awareness-raising process, a sustainable cybersecurity culture can be fostered, where everyone understands their role in protecting information.

Within the framework of this article, research and practical work were carried out, aimed at the well-known problem of information security: social engineering, effective ways to protect against them, as well as the development of a system for assessing the security of socio-technical attacks.

In the modern world, in different corporations, one of the main vulnerabilities in the information security system is the human factor. Therefore, attackers often use this factor for their own selfish purposes. After carefully studying this topic, I came to the conclusion that information security specialists and IT departments should carefully study social engineering.

The following components have been studied and analyzed in detail in the conducted research works:

- the basics of social engineering, types of social engineering, and ways to protect against social engineering attacks have been studied and analyzed;
- the literary works of Christopher Haddon and other authors on the topic of social engineering have been studied and analyzed;
- the principles of influence and manipulation have been studied;
- effective methods of protecting against social engineering have been studied and analyzed;
- the artificial intelligence used in cyber fraud has been studied and analyzed.

- the protocols of mail services and the operation of mail servers have been studied and analyzed;

- the existing methods of improving the skills of employees have been studied and analyzed using the phishing simulator: "Gophish",

"Wolfish";

Based on the results of the work carried out, the following conclusions can be drawn:

An effective way to protect against social engineering is through continuous training and raising people's awareness. To achieve good results in cybersecurity, it is necessary to conduct extensive work in collaboration with the "Committee on Information Security of the Ministry of Digital Development, Innovation, and Aerospace Industry of the Republic of Kazakhstan" and other government agencies. This includes organizing seminars, courses, and publishing articles on various cybersecurity topics (Lakhno, Malyukov, Malyukova, Akhmetov, Alimseitova, and Ogan, 2024).

Phishing simulators reduce the risk of phishing-related incidents. By practicing with phishing messages, employees can analyze and prepare for real threats. According to statistics, security professionals are also exposed to phishing emails. Therefore, continuous training is necessary.

3. Recognizing phishing messages is not enough; it is necessary to report the incident to the security department in accordance with the internal security policy.

4. It is important to continuously learn, improve, and follow the security rules and procedures.

Conclusion

Cybersecurity plays a very important, key role in the modern world. Increasing public awareness of cybersecurity issues, providing effective training tools and cybersecurity simulators will solve many problems. To do this, it is necessary to introduce various government training courses on cybersecurity for the entire population. Training programs and simulations should be fun to increase interest and effectiveness.

In conclusion, I would like to note that the modern world uses various intelligent technologies, electronic payment methods, online earning on the Internet, social networks, Internet of Things, and email services, so it is necessary to constantly train employees on cybersecurity.

Thus, the research and development conducted in this article not only highlight the importance and relevance of the topic of social engineering, but also provide practical tools for improving the level of protection and awareness among employees. The developed phishing simulators have proven to be effective and can be successfully implemented in various organizations to reduce risks and enhance overall information security. The results of the study show that cybersecurity is a complex problem that has not only technical, but also socio-ethical aspects. The scientific article provides for the development of proposals aimed at creating a culture of cybersecurity and increasing the level of information security in the SOC analytics system using an AI Agent.

References

Hednegi, K. (2021). *Unmasking the social engineer: The human element of security*. Indianapolis, IN.

Киберпреступление века: Carbanak. (2025). *Kaspersky*. https://www.kaspersky. ru/blog/billion-dollar-apt-carbanak/6950/

Защита от социального инжиниринга. (2025). *Kaspersky*. https://www.kaspersky .ru/resource-center/threats/how-to-avoid-social-engineering-attacks

Yazan, A. A., & Reema, A. (2024). Exploring the potential implication of AI-generated content in social engineering attacks. *International Journal of Computing and Digital Systems*.

Salal, A. K. (2023). *Social engineering*. MACS, St. Francis Xavier University, Canada.

Юбузова, Х. И., & Мырзаш, Б. Б. (2024, May 31). Искусственный интеллект в мошеннических схемах. *Научный прогресс: проблемы и перспективы развития*, 31–34.

Мырзаш, Б. Б. (2024). *Разработка системы оценки защищенности от социотехнических атак* (Магистерская диссертация). КазНИТУ им. К. Сатпаева.

Джекебаева, М. А. (2023). Ақпараттық қоғамдағы жеке бас бостандығына төнетін қауіптер және ақпараттық мәдениет. *5th International Symposium on Turcology Studies*, Van, Turkey.

Джекебаева, М. А. (2023). Жастар арасындағы киберқауіпсіздік: цифрлық дәуірдегі қорғаныс. *5th International Symposium on Turcology Studies*, Van, Turkey.

Jekebayeva, M. A., Iztaeva, V., Anassova, K. T., & Manapbayev, N. (2023). Cybersecurity: Importance for Kazakhstan and international experiences. *Хабаршы Абылай хан атындағы ҚазХҚжӘТУ. Серия: Халықаралық қатынастар және аймақтану*, 4(54), 80–93.

Alimseitova, Zh., Adranova, A., Akhmetov, B., Lakhno, V., Zhilkishbayeva, G., & Smirnov, O. A. (2020). Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources. *Journal of Theoretical and Applied Information Technology*, 98(21), 3334–3346.

Lakhno, V., Togzhanova, K., Kasatkin, D., Kartbayev, T., Uskenbayeva, R., Alimseitova, Zh., & Kashaganova, G. (2021). The information technologies in the tasks of planning of smart city development. *Journal of Theoretical and Applied Information Technology*, 99(14), 3645–3662.

Lakhno, V., Kartbayev, T., Malyukov, V., Uskenbayeva, R., Togzhanova, K., Alimseitova, Zh., & Beketova, G. (2021). Risk assessment of investment losses aimed at the development of smart city systems. *Journal of Theoretical and Applied Information Technology*, 99(15), 3683–3692.

Kartbayev, T., Lakhno, V., Malyukov, V., Turgynbayeva, A., Alimseitova, Zh., Malikova, G., & Kashaganova, G. (2022). Model for the decision support system during the procedure of investment projects assessment in the field of enterprise digitalization considering multifactorality. *Journal of Theoretical and Applied Information Technology*, 100(6), 1684–1692.

Lakhno, V., Alimseitova, Zh., Kalaman, Y., Kryvoruchko, O., Desiatko, A., & Kaminskyi, S. (2023). Development of an information security system based on modeling distributed computer network vulnerability indicators of an informatization object. *International Journal of Electronics and Telecommunications*, 69(3), 475–483. https://doi.org/10.24425/ijet.2023.146495

Lakhno, V., Malyukov, V., Malyukova, I., Akhmetov, B., Alimseitova, Zh., & Ogan, A. (2024). A neuro-game model for analyzing strategies in the dynamic interaction of participants of phishing attacks. *TELKOMNIKA Telecommunication Computing Electronics and Control*, 22(3), 645–656. https://doi.org/10.12928/TELKOMNIKA.v22i3.25938

References

Hednegi, K. (2021). *Unmasking the social engineer: The human element of security*. Indianapolis, IN.

Kiberprestuplenie veka: Carbanak. (n.d.). *Kaspersky*. https://www.kaspersky.ru/blog/ /billion-dollar-apt-carbanak/6950/

Zaşita ot SI. (n.d.). *Kaspersky*. https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks

Yazan, A.A., & Reema, A. (2024). Exploring the potential implication of AI-generated content in social engineering attacks. *International Journal of Computing and Digital Systems*.

Salal, A. K. (2023). *Social engineering*. MACS, St. Francis Xavier University, Canada.

İubuzova, H. İ., & Myrzaş, B. B. (2024, May 31). İskustvennyi intelekt v moşenicheskih shemah. In *Nauchnyi progres: problemy i perspektivy razvitia* (pp. 31–34). Zapadno-Sibirskii nauchnyi sentr.

Myrzaş, B. B. (2024). *Razrabotka sistemy otsenki zashishchennosti ot sotsiotehnicheskih atak* (Master's thesis). KazNITU imeni K. Satpaeva.

Jekebayeva, M.A. (2023). Aqparattyq qoğamdağy jeke bas bostandyğyna tönetın qauıpter jäne aqparattyq mädeniet. In *5th International Symposium on Turcology Studies*, Van, Turkey.

Jekebayeva, M.A. (2023). Jastar arasındağy kiberqauıpsızdık: sıfrlyq däuırdegı qorğanys. In *5th International Symposium on Turcology Studies*, Van, Turkey.

Jekebayeva, M.A., Iztaeva, V., Anassova, K. T., & Manapbayev, N. (2023). Cybersecurity: Importance for Kazakhstan and international experiences. *Habarşysy Abylai han atyndağy QazHQjÄTU. Halyqaralyq qatynastar jäne aimaqtanu seriasy*, 4(54), 80–93.

Alimseitova, Zh., Adranova, A., Akhmetov, B., Lakhno, V., Zhilkishbayeva, G., & Smirnov, O. A. (2020). Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources. *Journal of Theoretical and Applied Information Technology*, 98(21), 3334–3346.

Lakhno, V., Togzhanova, K., Kasatkin, D., Kartbayev, T., Uskenbayeva, R., Alimseitova, Zh., & Kashaganova, G. (2021). The information technologies in the tasks of planning of smart city development. *Journal of Theoretical and Applied Information Technology*, 99(14), 3645–3662.

Lakhno, V., Kartbayev, T., Malyukov, V., Uskenbayeva, R., Togzhanova, K., Alimseitova, Zh., Beketova, G., & Turgynbayeva, A. (2021). Risk assessment of investment losses aimed at the development of smart city systems. *Journal of Theoretical and Applied Information Technology*, 99(15), 3683–3692.

Kartbayev, T., Lakhno, V., Malyukov, V., Turgynbayeva, A., Alimseitova, Zh., Malikova, G., & Kashaganova, G. (2022). Model for the decision support system during the procedure of investment projects assessment in the field of enterprise digitalization considering multifactorality. *Journal of Theoretical and Applied Information Technology*, 100(6), 1684–1692.

Lakhno, V., Alimseitova, Zh., Kalaman, Y., Kryvoruchko, O., Desiatko, A., & Kaminskyi, S. (2023). Development of an information security system based on modeling distributed computer network vulnerability indicators of an informatization object. *International Journal of Electronics and Telecommunications*, 69(3), 475–483.
https://doi.org/10.24425/ijet.2023.146495

Lakhno, V., Malyukov, V., Malyukova, I., Akhmetov, B., Alimseitova, Zh., & Ogan, A. (2024). A neuro-game model for analyzing strategies in the dynamic interaction of participants of phishing attacks. *TELKOMNIKA: Telecommunication, Computing, Electronics and Control*, 22(3), 645–656. https://doi.org/10.12928/TELKOMNIKA.v22i3.25938

ЕО ЕЛДЕРІ МЕН ҚАЗАҚСТАННЫҢ КИБЕРҚАУІПСІЗДІК МӘСЕЛЕЛЕРІН ШЕШУДЕГІ ХАЛЫҚАРАЛЫҚ ТӘЖІРИБЕСІ

Мақпал ДЖЕКЕБАЕВА*, философия ғылымдарының кандидаты, Қазақстан-Ресей медициналық университетінің қауымдастырылған профессоры, Алматы, Қазақстан, makpal.jekebayeva@mail.ru, ORCID ID: https://orcid.org/0000-0001-7771-8828*

***Ержан ЧОНГАРОВ**, философия ғылымдарының кандидаты, Қазақстан-Ресей медициналық университетінің қауымдастырылған профессоры, Алматы, Қазақстан, yerzhanalemkulov@gmail.com, ORCID ID: https://orcid.org/0009-0009-9435-7345*

***Namig MAMMADOV**, PhD, Әзірбайжан Ұлттық ғылым академиясы, Баку, Әзірбайжан, mammadov.namig@yahoo.com, ORCID ID: https://orcid.org/0000-0003-4356-6111*

МЕЖДУНАРОДНЫЙ ОПЫТ СТРАН ЕС И КАЗАХСТАН В РЕШЕНИИ ПРОБЛЕМ КИБЕРБЕЗОПАСНОСТИ

Мақпал ДЖЕКЕБАЕВА*, кандидат философских наук, ассоциированный профессор Казахстанско-Российский медицинский университет, Алматы, Казахстан, yerzhanalemkulov@gmail.com, ORCID ID: https://orcid.org/0009-0009-9435-7345*

***Ержан ЧОНГАРОВ**, кандидат философских наук, ассоциированный профессор Казахстанско-Российский медицинский университет, Алматы, Казахстан, makpal.jekebayeva@mail.ru, ORCID ID: https://orcid.org/0000-0001-7771-8828*

***Namig MAMMADOV**, PhD, Национальная академия наук Азербайджана, Баку, Азербайджан, mammadov.namig@yahoo.com, ORCID ID: https://orcid.org/0000-0003-4356-6111*