**Application**

**for the implementation of a scientific, scientific and technical program within the framework of program-targeted financing**

**The application consists of the following parts:**

1) Abstract;

2) Explanatory note;

3) Calculation of the requested financing.

1. **Abstract**

In order to improve the quality of work of domestic specialists in the field of digital forensics, the project will develop new methods and approaches for gaining access to password-protected devices and their data. This project is focused on improving digital forensics by developing new methods to access password-protected devices and extract critical data. The main goal is to create practical techniques for bypassing security measures like PIN codes, graphical patterns, biometric authentication, and complex passwords. Another key aspect is decrypting data from messaging apps, which often contain essential information for forensic investigations. Alongside this, the project will explore ways to retrieve information from encrypted backups, cloud storage, and system settings, particularly in Android devices.

Beyond developing new methods, the project will turn these techniques into an open-source software solution. This software will go through real-world testing to fine-tune its capabilities before full deployment. The final product will be a software-hardware system designed to support forensic specialists in their investigations. It will include tools for accessing locked devices, adapters to connect to different hardware, programmers to gain administrative rights on Android without erasing data, and a high-performance server to process forensic data efficiently.

Modern mobile platforms, especially iOS and Android, have strong encryption systems in place to protect user data. The two most common encryption models—File-Based Encryption (FBE) and Full-Disk Encryption (FDE)—offer strong security but also create challenges for forensic analysis, particularly when encryption keys are inaccessible. Hybrid storage solutions, like Semi-Adoptable Storage, add another layer of complexity by combining different file systems and encryption techniques, making forensic data retrieval even harder.

To overcome these challenges, the project will integrate artificial intelligence (AI) with traditional forensic methods to improve password recovery and data decryption. AI techniques will be used alongside binary exploitation, brute-force attacks, and dictionary-based approaches that analyze user behavior patterns. This combination will allow forensic specialists to bypass security systems more efficiently, reducing the time and resources required for investigations. If a user’s previous login-password pair is available, AI models can analyze their password creation habits and predict possible variations, making it easier to gain access. When all else fails, the chip-off method will be used, allowing direct extraction of data from a device’s internal storage.

Beyond technical development, the project will also look at vulnerabilities in data protection systems. Understanding encryption algorithms, key generation methods, and key storage techniques will be crucial in identifying weaknesses that can be used in forensic research. The project will also examine how encryption keys are stored, such as in the /data/misc/vold directory on Android, and work on secure methods to bypass access restrictions when needed.

The project will be structured into different modules, each focusing on a specific area: various device types, operating system characteristics, authentication methods (passwords, patterns, biometrics), and tools for analyzing both local and cloud-based data. Every aspect of the project will comply with legal regulations on digital forensics, data privacy, and investigative technology. A major goal is to automate processes as much as possible, minimizing manual effort while improving accuracy and speed in forensic work.

This initiative aligns with Kazakhstan’s national priorities, as outlined in the Presidential Addresses of 2018 and 2021. By advancing AI, big data, and cybersecurity, the project supports key goals of the CyberShield-2 Concept (2022–2027), which is focused on strengthening national cybersecurity infrastructure. The solutions developed in this project will significantly enhance the capabilities of law enforcement and security agencies, helping them tackle cybercrime more effectively.

In addition to improving security, the project carries broader social and economic benefits. Strengthening cybersecurity measures will help reduce financial losses caused by cyber threats, while also driving growth in Kazakhstan’s IT sector. The creation of advanced forensic tools will lead to more job opportunities for AI and cybersecurity professionals, fostering innovation in digital forensics.

By establishing Kazakhstan as a leader in forensic research and cybersecurity, this project will help boost the country’s global reputation in the field. Strengthening digital forensics expertise will build greater trust in national institutions and encourage international collaboration in security and investigative technologies. Additionally, the scientific and technical advancements from this initiative will serve as a foundation for future research, positioning Kazakhstan as a hub for expertise in digital security.

Ultimately, this project will provide forensic specialists with powerful tools to analyze encrypted data, bypass authentication systems, and streamline digital investigations. AI-powered automation will not only improve accuracy but also reduce the time required for solving complex cases. By tackling the major technical challenges in digital forensics, this initiative will contribute to national security, enhance cybersecurity defenses, and drive further innovation in forensic investigation methods.

**2. Explanatory Note**

**1. General information**

1.1. The name of the topic of the scientific, scientific and technical program. *Development of innovative digital forensics technology for the study of locked electronic and digital devices*

1.2. The name of the priority and specialized scientific field.

*7 National security and defense, biological safety*

1.3. The field and type of research.

*2 Applied scientific research*

2.1 Ensuring information security

*2.4 Countering terrorism and extremism*

*2.5 Ensuring the activities of special government agencies*

1.4. The number of the selected technical assignment is *112*

1.5. A strategically important state task for which the program has been developed.

In accordance with the instruction of the Prime Minister of the Republic of Kazakhstan dated June 16, 2021 No. 19-1/34770бп//21-27-7.39 қбп, a Concept for the development of the digital ecosystem for 2022-2027 ("Cybershield-2") was developed. Within the framework of this concept, special attention is paid to the development of a highly adaptive and integrated public information security management system in the field of informatization and communications of the national ICI.

For the effective implementation of this task, it is critically important to create conditions for countering cybercrime, including continuous professional development of personnel in specialized departments, expansion of the arsenal of technical means for recording and forensic studies of "digital" evidence.

*The provisions of the strategic and program documents implemented within the framework of the project:*

- The Message of the President of the Republic of Kazakhstan to the people dated October 5, 2018, dedicated to improving the well-being of Kazakhstanis: income growth and improving the quality of life. The sixth priority is the development of innovative and service industries. Special attention should be paid to key areas of the "economy of the future," including alternative energy, new materials, biomedicine, big data analysis, the Internet of things, artificial intelligence, blockchain technologies, and other promising areas.;

- Decree of the President of the Republic of Kazakhstan dated February 15, 2018 No. 636 "On approval of the National Development Plan of the Republic of Kazakhstan until 2025 and invalidation of certain decrees of the President of the Republic of Kazakhstan". National priority 7. Strengthening national security;

- The Message of the President of the Republic of Kazakhstan to the people dated September 1, 2021, "Unity of the people and systemic reforms are a solid foundation for the country's prosperity." As part of the first issue, "Economic development in the post-pandemic period," it was noted that strengthening the defense capability and increasing the responsiveness to threats should become priorities at the state level. The President stressed the need to prepare for external shocks and unfavorable development scenarios. Solving these and other tasks requires a complete "digital reboot" of the public sector.;

- Resolution of the Government of the Republic of Kazakhstan dated December 20, 2016 No. 832 "On approval of uniform requirements in the field of information and communication technologies and information security";

- ST RK ISO/IEC 27037-2022 "Information technology. Methods and means of ensuring security. Guidelines for the identification, collection, receipt and storage of digital certificates";

- ST RK ISO/IEC 15408-2-2017 "Information Technology. Methods and means of ensuring security. Criteria for assessing information technology security. Part 2. Functional safety requirements".

1.6. The place of implementation of the program. *Astana IT University LLP*

1.7. Estimated start and end date of the program, its duration in months. *05/01/2025 - 12/31/2027, 32 months.*

1.8. The applicant organization of the program. *Astana IT University LLP*

1.9. Program executors (specify the names of all entities involved in the implementation of the program). *Astana IT University LLP*

1.10. The requested amount of program-specific financing (for the entire duration of the program and by year, in thousands of tenge). **900,000** thousand tenge, including by year: for 2025 – **300,000** thousand tenge, for 2026 – **300,000** thousand tenge, for 2027 – **300,000** thousand tenge.

1.11. **Keywords:** *digital forensics, information security, forensic investigation, locked electronic digital devices, password-protected electronic digital devices, "digital" evidence, artificial intelligence, encryption, decryption, cryptology, password bypass, brute force, hashing.*

**2. The general concept of the program**.

**2.1. Introductory part**

The modern world is characterized by a rapid growth in the number of mobile device users, which makes their security a critical task. Kazakhstan follows this global trend, where Samsung, Xiaomi and Oppo, which run on Android OS, remain the leading smartphone brands. This demonstrates the deep integration of mobile technologies into everyday life. However, in parallel with this, there has been a sharp increase in cyber attacks.In the second quarter of 2024, cyberattacks in CIS countries increased 2.6 times compared to 2023. In Kazakhstan, 65% of attacks involve malware, and 53% use social engineering, making government agencies, financial institutions, and media the most vulnerable sectors.

In response to these challenges, the proposed project aims to develop domestic solutions in the field of digital forensics and mobile security, reducing dependence on imported technologies. Its main goal is to develop a domestic solution in the field of digital and mobile forensics, which will reduce dependence on imported technologies and increase the efficiency of data analysis in mobile forensics. By integrating cryptographic techniques, binary exploitation, artificial intelligence, and social engineering, the project seeks to optimize data analysis, enhance digital investigations, and strengthen cybersecurity.

The result will be a universal hardware-software package compatible with Android, Windows, and specialized digital devices. This system will not only improve the efficiency of forensic specialists but also support domestic research in cybersecurity and strengthen the protection of citizens' rights in Kazakhstan.

**2.2. The goal of the program**

**The goal of the program:** *to develop technology for digital forensic analysis of locked electronic devices*, enabling law enforcement to access password-protected data without damage or loss. The solution will automate bypassing password verification, ensuring full access to files, backups, apps, messengers, Android system settings, and cloud storage. This will enhance forensic investigations by providing accurate, high-value evidence while maintaining data integrity. The technology is designed to support national security efforts by enabling efficient forensic research on encrypted devices, ensuring compliance with investigative standards and improving the effectiveness of digital forensics.

**2.3. Program objectives**

To achieve this goal, the following tasks must be solved:

*a)* *Review and analysis of similar solutions, technologies and methods used in the forensic investigation of password-protected electronic and digital devices based on the iOS and Android operating systems*. This will allow the team to identify current scientific and technical gaps and clarify directions for the creation of new methods and technologies. It is also important to study the legal aspects of not only the legislation of the Republic of Kazakhstan, but also the international experience in personal data protection and restrictions on the use of such technologies for purposes not regulated by the legislative system;

*b)* *Create universal methods to overcome security systems and gain access to information on password-protected electronic and digital devices in the framework of law enforcement and national security.* In other words, methods will be developed to ensure access to information on devices protected by passwords, graphic keys, PIN codes and biometric authentication. To implement such methods, artificial intelligence algorithms will be used to find patterns in the formation of password rules by a specific user and predict the possible password structure. Creating adaptive password sorting rules based on the device usage context. Social engineering will also allow to obtain advanced user data, which will help you create a password search algorithm based on a predefined dictionary of the most popular keywords. The disadvantages and potential vulnerability points in Windows and Android will also be studied, and it is possible to integrate the developed methods to overcome specific protection systems implemented in operating systems.;

c) *To study the algorithms for the functioning of encryption and decryption systems implemented in the Android mobile operating system.* A detailed analysis of encryption algorithms and key components of Android systems, the most popular AES-256 algorithms and their implementation in Android file systems such as dm-crypt, storage of encryption keys in the /data/misc/vold directory and methods of their extraction, as well as features of hybrid storage systems, including Semi-Adoptable Storage, will be conducted;

d) *Developing Methods for Accessing Protected Data.* Techniques will be created for accessing password-protected backups, mobile applications, messengers, cloud services, and Android system settings. The project will include decryption tools for encrypted backups and solutions for extracting data from WhatsApp, Telegram, and Signal. Specialized methods for analyzing data stored in cloud services will also be developed.e) Implement a function in the form of executable code that provides administrative access to the Android file system while preserving user data. Executable code will be created that provides administrative access to the Android file system without damaging user data. It will be necessary to circumvent security restrictions, extract hidden or encrypted data, and ensure the integrity of the source data in the framework of forensic research.;

f) *Executable code will be developed to grant administrative access to Android’s file system while maintaining data integrity.* This function will bypass security measures, extract encrypted or hidden data, and ensure that the original file structure remains intact for forensic use.

g) Conduct pilot tests, data collection and analysis to capture the actual technical and functional characteristics of the prototype and make adjustments if necessary. The APK will be tested on real devices to evaluate its functionality, which will help evaluate the effectiveness of the prototype. As part of the pilot tests, data will be collected on technical characteristics, task completion time, and accuracy levels, which will help identify problems in the prototype to adjust and improve performance.;

j) Develop methodological documentation on the use of the prototype. At the final stage of the study, instructions and guidelines will be created for the use of all PAK modules. The documentation will include a setup and operation manual, practical recommendations for digital forensics specialists, as well as a description of application scenarios in law enforcement agencies and other structures.

By structuring these elements into an integrated forensic system, the project will enhance investigative capabilities, improve forensic efficiency, and contribute to stronger national cybersecurity infrastructure.

Measurable indicators according to the approved methodology for determining the level of technological readiness (TRL) of scientific organizations and research universities, and their developments - at the application stage, the TRL level corresponds to 2. Upon completion of the project, the level of technical readiness is planned to reach 4.

**3. Scientific novelty and significance of the program**

The modern world is characterized by a rapid growth in the number of users of smartphones and other mobile devices, which makes the task of ensuring their safety more and more urgent. Kazakhstan follows this global trend, where Samsung, Xiaomi and Oppo, which run on Android OS, remain the most popular smartphone brands [1] (Figure 1). These data confirm the active penetration of mobile technologies into everyday life.

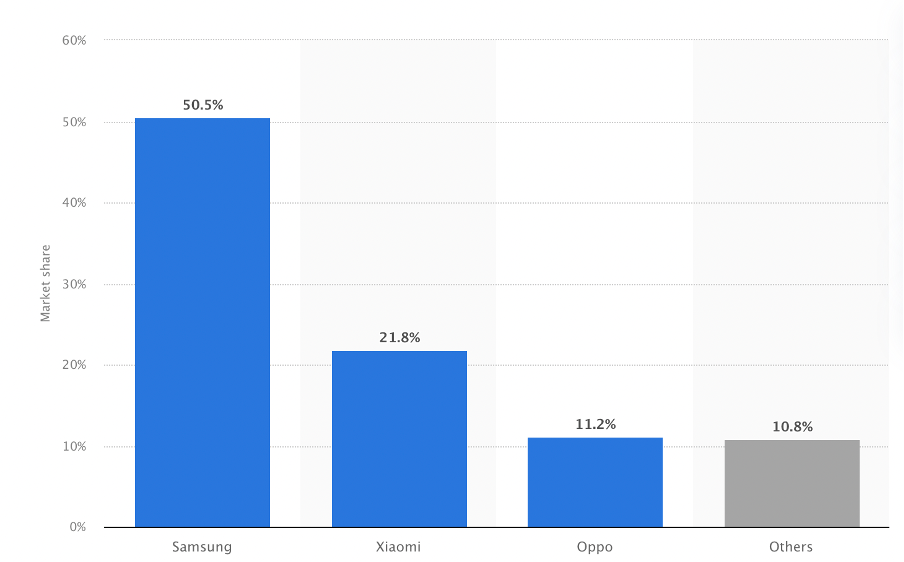


Figure 1. Smartphone sales market share in Kazakhstan in 2024 by brand

At the same time, the number of cyber attacks is growing. In the CIS countries, in the second quarter of 2024, their number increased 2.6 times compared to the same period in 2023 [2]. In Kazakhstan, 65% of attacks were related to malware, and in 53% of cases, social engineering methods were used. The main targets of attacks are government agencies (12%), financial organizations (12%), as well as the media (19%), which highlights the vulnerability of critical sectors [3].

One of the key authentication methods is passwords, which have more than half a century of history [1]. Modern research shows that when creating a password, users follow certain habits and patterns that can be used to gain access to their data. One of the most popular methods of password "strengthening" is using a capital letter at the beginning, adding numbers at the end, and using characters like "@" instead of "a", which open up the possibility for targeted password selection [2].

One of the main aspects is that users follow certain patterns when creating passwords. These include adding simple sequences (like "123"), as well as using personal information such as date of birth, names of loved ones, which makes passwords more predictable [4]. It is important to note that such information about a person can be found on social networks or professional websites [1].

Global research has suggested different approaches for working with passwords. These include dictionaries based on data from leaks, methods for estimating password complexity, and algorithms based on Markov chains [3]. At the same time, these methods often ignore contextual information that plays a key role in creating passwords and are not able to effectively cope with intelligent attacks [5]. At the same time, by using contextual information such as personal data, interests, and user habits, the password selection process is significantly accelerated [6].

In Kazakhstan, the topic of digital forensics is actively developing within the framework of the state program "Cybershield-2", which is aimed at improving national information security. However, there is no focus on integrating artificial intelligence and context analysis techniques for password cracking and data decryption. At the same time, this method opens up new opportunities for innovation in this field.

The novelty of the program lies in the development of a universal software and hardware complex that includes contextual analysis, artificial intelligence, and social engineering. This approach accelerates the process of data decryption, as well as adapts methods to suit the needs of a particular user, who will take into account cultural and behavioral factors. For example, research shows that users in different countries may have different approaches to creating a password. Passwords based on phone numbers may be popular in some regions, while passwords based on names are popular in others. These features will be taken into account in the proposed SHC, which will become a universal tool for working with locked devices.

The program being developed is aimed at solving the tasks outlined in the state concept "Cybershield-2" (2022-2027), which emphasizes the need to create a highly adaptive and integrated information security management system. That is why special attention is being paid to improving the skills of specialists in the field of digital forensics, as well as developing tools to gain access to certain users' data to counter crime. In addition, the program responds to the challenges outlined in the Message of the President of the Republic of Kazakhstan, such as the development of innovative technologies, which include artificial intelligence, big data analysis, which will help protect the national infrastructure.

The proposed program will focus on developing methods for data decryption, password circumvention, and effectively solving the tasks of extracting and analyzing digital evidence, which is especially important for investigating cybercrimes and ensuring national security. The package will be able to automate the processes of forensic investigations, which subsequently reduces the time and resources needed to access encrypted data.

At the national level, the program is able to strengthen Kazakhstan's position in the field of information security by providing the country with advanced tools to counter cyber threats. As a result, there may be an increase in confidence in government institutions, demonstrating Kazakhstan's commitment to international standards in the field of digital forensics.

In the international arena, the results of the program can be used to strengthen ties with foreign partners in the field of digital forensics. The development of unique solutions based on artificial intelligence, in turn, will help Kazakhstan to take a leading position in this field.

The use of the above-mentioned innovative approaches will create a scientific and technical foundation for future developments. The program encourages the use of modern technologies such as machine learning and big data analysis methods in practical activities, thereby accelerating the development of related scientific disciplines.

Considering the impact of the socio–economic effect, several points can be noted at once. In relation to the social effect:

There will be a professional development of specialists in the field of digital forensics, which will create new workers. Jobs in the innovation sector. In addition, the use of the proposed technologies increases the chances of solving particularly important crimes, strengthening the security of citizens.

Economic sector: The introduction of automated solutions helps to significantly reduce the costs allocated for forensic research, increasing the efficiency of law enforcement agencies. Also, the development of new technologies increases the potential for commercialization and export, which will bring revenues to the country's economy.

Modern digital devices, such as smartphones, tablets, and so on, represent the most important sources of evidence necessary for the successful completion of investigations. However, complex data protection mechanisms such as PIN codes, graphic keys, biometrics, and File and disk encryption (File-Based Encryption, Full-Disk Encryption) [7] create significant barriers for law enforcement agencies. This makes the task of securely accessing device data without losing its integrity critically important for digital forensics.

The scientific and technological significance of the program lies in overcoming these barriers by creating unique and innovative methods. The development of the package will provide specialists with universal tools for unlocking devices and extracting data, while maintaining a balance between security and efficiency. In addition, the program is particularly relevant in the context of Kazakhstan's strategic objectives, such as strengthening information security and ensuring technological sovereignty. National law enforcement agencies are facing an increasing number of crimes where devices contain critical data. However, dependence on imported solutions, which are not always adapted to local requirements, limits their capabilities and increases the time and financial costs of conducting investigations.

The development of the program allows solving several key tasks:

* To provide access to secure devices using methods that take into account modern authentication technologies such as PIN codes, graphic keys and biometrics.
* Develop methods of physical access to devices, including chip-off, which is especially important for devices that are completely blocked by existing methods.
* Create automated tools for data extraction and decryption, which will significantly speed up the information processing process.

Current data shows that Kazakhstan recorded more than 223 million cyberattack attempts in 2023 alone, including 133.5 million attacks on local executive bodies and 47.7 million attacks on government agencies. These figures demonstrate that devices are becoming a key tool for coordinating and implementing cybercrimes. In addition, 93% of mobile devices are connected to corporate networks, which makes them an important object of analysis [8].

Criminals' devices may contain not only data about crimes committed, but also information that helps prevent further threats. Quick access to this data is not only a matter of investigation, but also of preventing new threats.

Mobile security incidents also have serious economic consequences. 79% of organizations have experienced such incidents, and in 52% of large companies, losses from data leaks exceeded $500,000 per year [9]. The development of local solutions will not only reduce the damage caused by cybercrimes, but also reduce the cost of using foreign technologies. It also creates the potential for commercialization of developments and their export, which can strengthen Kazakhstan's position in the international market.

The program lays the foundation for further growth in the field of digital forensics. For example, technologies developed within the framework of the program can be adapted for other types of devices and integrated with artificial intelligence tools for automatic analysis of extracted data. These solutions will allow Kazakhstan to become a regional leader in the field of digital forensics, strengthening the country's position in international cooperation.

Thus, the proposed program responds not only to urgent scientific and technological challenges, but also contributes to strengthening Kazakhstan's information security, improving the effectiveness of investigations and creating economic advantages. Its implementation will strengthen the country's sovereignty in the field of high technologies and create conditions for a new stage in the development of digital forensics.

Today, working with secure mobile devices is one of the most difficult tasks in digital forensics. The developed program offers unique solutions that can eliminate many existing limitations. One of the key advantages of the program is a hybrid approach that combines physical access to devices, user behavior analysis, and the use of artificial intelligence to create more efficient decryption methods. This will reduce the time of investigations and increase their accuracy, which is especially important in cases involving threats to national security or complex cybercrimes.

Existing global digital forensics tools such as Cellebrite UFED, GrayKey, Oxygen Forensic Detective, and XRY have already proven themselves to be powerful data extraction tools. [10], [13], [14]. However, they have limitations that make them less effective.

*Cellebrite UFED*

* *Advantages:* It supports physical and logical data extraction, decodes protected data, and offers a user-friendly interface for analysis.
* *Disadvantages:* High cost, difficult to master for less experienced users.
* *Comparison:* The program being developed will be more affordable and focused on automating processes to speed up work.

*Oxygen Forensic Detective*

* + *Advantages:* Data collection from clouds and IoT devices, powerful analytical tools such as time line analysis and geolocation.
  + *Disadvantages:* Steep learning curve and difficult to use for beginners.
  + *Comparison:* The program will include adapted algorithms for data analysis on devices popular in Kazakhstan, such as Android (49% of users).

*GrayKey*

* + *Advantages:* Effective for unlocking iOS devices, including iOS 18.
  + *Disadvantages:* Limited access (only for law enforcement agencies), high cost ($15,000 per annual license).
  + *Comparison:* The program will focus on working with a wider range of devices, including Android, which are prevalent in Kazakhstan.

*XRY*

* + *Advantages:* Reliable data extraction, support for many mobile platforms, and creation of reports for litigation.
  + *Disadvantages:* Updates are often required to work with new OS versions.
  + *Comparison:* The program will include adaptive algorithms to ensure long-term compatibility.

Global experience shows that the key to successfully solving the tasks of digital forensics is a combination of high technologies and adaptation to specific conditions. For example:

* In the United States, *GrayKey's* tools have helped solve several major cases related to terrorism and drug trafficking, thanks to the ability to unlock modern iOS devices [13].
* *Cellebrite UFED* has been successfully used in international investigations, including cases of cyber fraud and data leaks.
* *Oxygen Forensic Detective* has proven its effectiveness in corporate investigations such as cases of industrial espionage and information leaks.

However, the cost of these solutions, their complexity and lack of localization make them less accessible to Kazakhstan.

The proposed program integrates the world's best practices such as physical data extraction (chip-off), analysis of user habits and automation of data analysis [15]. At the same time, it adapts to the specifics of our country:

* Takes into account legal requirements and local conditions.
* Optimized for popular devices, including Android.
* Provides tools available to law enforcement agencies with limited budgets.

The development of the program not only solves local problems, but also strengthens Kazakhstan's position in the field of digital forensics. It provides a more cost-effective, efficient and adaptive solution, which is especially important in the face of growing cyber threats.

Modern digital forensics tools such as *Cellebrite UFED, GrayKey, Oxygen Forensic Detective, and XRY* perform key data extraction tasks, but have a number of limitations. In contrast, the program being developed offers innovative approaches that make it unique. Unlike existing solutions that focus on brute-force or standard dictionaries, the proposed program will integrate password analysis methods that take into account the cultural and behavioral aspects of users [11]. For example, studies show that passwords of people from Central Asia often use names, dates, and simple numeric sequences [12]. This will allow you to create more accurate dictionaries for decryption. The program will create opportunities for accessing devices not only through software methods, but also using physical chip analysis (chip-off). This approach will allow you to work with devices that are completely blocked by software, which is extremely important for complex investigations.

The proposed program is very important for development, as there is a growing trend in the number of complex cybercrimes, where online access to data is very important, and new challenges related to IoT devices must be taken into account. In 2023, more than 223 million cyberattack attempts were registered in Kazakhstan, including 133.5 million attacks on local executive authorities[8]. This indicates the need to create more effective tools for extracting data from devices that are used in such attacks. Plus, in addition to the standard smartphones, there are also smart devices that can also contain critical information. Imported solutions are not targeted at these types of devices. While the program integrates approaches for working with IoT devices. Investing in the development of a local solution allows Kazakhstan to minimize its dependence on foreign technologies.

The implementation of the program will create new opportunities for training specialists in the field of digital forensics. The local production of technologies will reduce the costs of law enforcement agencies, as well as create the potential for exporting the program to the international market. The proposed program is unique in that it solves problems that are currently unattainable using existing global solutions. Its implementation will not only provide significant economic and social benefits, but also strengthen Kazakhstan's position as a leader in the field of digital forensics. This is an investment in the long-term sustainability and independence of the country, which are impossible when using exclusively imported solutions.

Modern digital forensics of mobile devices is at an advanced level of development due to the integration of sophisticated technologies that allow data extraction, analysis and presentation of the results in a legally relevant form. However, the development of this area is uneven, and the existing solutions, although they have significant advantages, cannot fully meet the needs of specific markets such as Kazakhstan.

The key aspects are listed in Table 10 below.

**Table 10** Key aspects of the state-of-the-art technology

|  |  |  |  |
| --- | --- | --- | --- |
| **Aspect** | **Current State** | **Disadvantages** | **Potential improvements** |
| **Data Extraction Technologies** | Modern tools offer physical, file, and logical extraction of data from devices. Physical extraction provides full access to the device's memory, including deleted files. | 1. Difficulties in extracting data from devices with new encryption methods (for example, Full Disk Encryption).  2. Limitations in working with Android, which dominates in Kazakhstan. | Development of extraction methods that take into account both physical access (chip-off) and the use of intelligent data analysis methods such as AI models. |
| **Decryption and data analysis** | Existing tools can recover deleted messages, multimedia and application files, as well as work with encrypted data | Most solutions require significant computing resources to analyze encrypted data.  High complexity of processing data protected by TPM or other hardware modules. | Integration of hybrid approaches, including social engineering to identify possible keys and passwords, as well as machine learning to speed up the analysis process. |
| **Working with mobile devices** | Modern systems support tens of thousands of device models. For example, Cellebrite UFED works with over 31,000 devices, including legacy models. | High cost of commercial solutions (for example, GrayKey and Cellebrite UFED).  Limited support for low-cost Android devices, which make up a significant part of the Kazakhstan market.  Limitations in the support of devices with unique regional firmware. | Local adaptation for dominant platforms such as Android, and integration of support for low-cost device models popular in Kazakhstan.  Integration of modern technologies |
| |  | | --- | | **Integration of modern technologies** | | Using AI and ML to build timelines, recover deleted data, and visualize connections between objects. | AI and ML are not yet sufficiently integrated into data analysis processes.  They are ineffective when working with large amounts of encrypted data without prior access. | Active implementation of machine learning for predicting user behavior (for example, analyzing password sequences) and automating decryption. |

The proposed hardware and software package is focused on eliminating current shortcomings and realizing opportunities that have not yet been fully disclosed by existing solutions.

The proposed project is a natural development of previous research in the field of digital forensics aimed at data extraction, recovery and analysis. Previously developed technologies laid the foundation for working with damaged devices and analyzing data, but had limited capabilities and depended on imported solutions. The new project aims to eliminate these limitations by combining modern methods of artificial intelligence, neural networks and data processing technologies in a single software and hardware complex. This solution is adapted to the realities and challenges of Kazakhstan, taking into account local features and requirements. Thus, the project not only continues the achievements of past research, but also raises them to a new level, providing effective tools for digital forensics that will strengthen national security and give impetus to the further development of science and technology.

**4. Research Methods and Ethical Issues**

The program includes the development of solutions to deal with various scenarios encountered in forensic practice, in order to extract and analyze data from password-protected devices and their backup. To solve these problems, it is expected to use technology, artificial intelligence, social engineering, brute force, searching for vulnerabilities in operating systems using the binary exploitation method to automate and optimize the work of methods for bypassing passwords of password-protected devices and decrypting extracted application data (mainly instant messengers).

The methods and technologies being developed under the program cover five key scenarios:

- brute force numerical and symbolic-digital passwords, as well as PIN codes. A classic cryptographic method with a known set of combinations depending on the length of the password, the success of which directly depends on the production capacity of the speed of computing operations of the server. Rules are used that prioritize checking the lightest and most common passwords, which minimizes time and allows you to efficiently extract data when there is a limited amount of initial information;

- drawing up a rule for generating a password for a specific user, based on additional data obtained from analyzing his other devices and the mandatory presence of his previous logins and passwords. The AI ​​model will make it possible to determine the rule for creating passwords by the user and will significantly reduce the time for further analysis and selection of passwords for electronic digital devices;

- to access backup copies, it is more logical to use password brute force and analysis of additional data that may be associated with the user of the device, which allows you to restore information while maintaining its integrity in a shorter time;

- after successfully unlocking the device, based on the received password, data is analyzed using AI models and methods to select passwords for mobile applications, instant messengers, cloud storage and other services, allowing additional information to be extracted;

- in the case of a forensic investigation of a locked electronic digital device, a chip-off method will be developed to provide administrative rights to the Android file system while preserving user data. A similar approach is used for secure access DVRs, allowing full data access and analysis for later use.

These scenarios cover the main tasks that arise when working with locked and password-protected devices, and ensure the program's versatility and adaptability for various situations.

Scientific research as a whole is focused on solving key scientific and applied problems in the field of digital forensics related to the analysis of mobile device protection mechanisms and the development of methods for circumventing them as part of legal investigations of digital forensics. The main scientific questions and hypotheses of the program include the following areas of research:

- *A study of hashing and encryption methods used to hide access passwords to secure mobile devices.* To begin with, an analysis of hashing algorithms (for example, SHA, PBKDF2, bcrypt, scrypt) used to store passwords on mobile devices will be carried out, then the stability of encryption methods and the possibility of breaking them will be assessed using the computing power of modern GPUs and FPGAs and the equipment that is already planned for purchase within the project. Next, the team will begin developing methods for optimized password selection using artificial intelligence and social engineering.

*- Analysis of encryption algorithms for authentication data in various versions of Android and iOS OS*. To begin with, we will study all possible mechanisms for protecting user accounts used in different versions of mobile operating systems, as well as the features of encrypting passwords and authentication tokens directly in Android and iOS.  Binary code analysis will be aimed at identifying possible vulnerabilities associated with changes in security algorithms in new OS updates. Identify weaknesses in the security mechanisms used by the OS to prevent unauthorized access. Methods for exploiting vulnerabilities will be studied, including attacks on bootloaders, bypassing file system encryption, and attacks through vulnerable APIs.

- *Research on the implementation of authentication methods in mobile devices.* A comparative analysis of authentication mechanisms (passwords, PIN codes, graphic keys, biometrics) will be carried out. The features of biometric security, such as fingerprint, face, and iris recognition, are also studied in detail. Only after this the team will begin to develop methods for bypassing and selecting authentication data based on the vulnerabilities of identification systems.

- *Research into additional security mechanisms for smartphones (for example, blocking after several unsuccessful password attempts).* A detailed analysis of various password guessing protection strategies implemented in modern smartphones is necessary, since incorrectly entered passwords will lead to complete blocking of devices, which is not acceptable in forensic research. But if, nevertheless, the device is locked, then studying the possibilities of bypassing such mechanisms, including hardware attacks and data recovery from the device’s memory, will help in retrieving user data from the OS file system. Perhaps the team is developing accelerated hacking methods that take into account the features of blocking algorithms.

- *Research of cloud solutions and their structure that provide backup storage functionality.* To begin with, it will be produced analysis of the architecture of cloud services (Google Drive, iCloud, OneDrive) in the context of storing backup copies of mobile devices, data transfer protocols between the device and the cloud were studied, vulnerabilities and methods for recovering deleted data from backups were identified.

- *Research on methods for bypassing the protection of mobile applications and instant messengers using binary exploitation.* It is necessary to analyze the cryptographic algorithms used in instant messengers (WhatsApp, Telegram, Signal), as well as possible attacks on correspondence encryption algorithms. And the use of binary analysis techniques to find vulnerabilities and extract encrypted data.

- *Research of algorithms for automatic decryption of authentication data.* Research and development of methods for automatically decrypting passwords and authentication tokens based on cryptographic methods, using attacks based on machine learning and neural networks to compile a user dictionary and determine the rules for generating passwords, and analyzing the protection of file systems used by mobile operating systems will be carried out.

- *Development of an optimized mathematical method for decrypting authentication data using machine learning. Selection of passwords using analysis of patterns in the creation of previous passwords. For this purpose, artificial intelligence is used, which analyzes the login history and generates forecasts. Implementation includes several key steps:* pInitially, data is collected and stored. For this purpose, user names, passwords, resource name, time of login attempt and geolocation are recorded. All this data is stored in a vector database for efficient storage and processing. Additionally, synthetic data is created to improve the model and increase the amount of information. Then pre-processing and data analysis are performed. At this stage, the data is cleared of null values, duplicates and anomalies. They are brought into a single format, after which they are analyzed and visualized in the form of graphs, charts and correlation tables. The next step involves creating a list of similar passwords. Patterns such as letter substitutions, case changes, and the addition of prefixes and suffixes are analyzed. Based on these factors, as well as security standards (NIST 800-53, ISO 27001), new passwords are generated. Next, they are ranked by the probability of a successful match, taking into account probabilistic and heuristic assessments. For a more accurate selection, an NLP model is created that is trained on the collected data. It is tested for correctness and ability to generate passwords similar to real ones. The model is then evaluated taking into account the accuracy, speed of generation, and variety of passwords generated. If necessary, the algorithm is refined and the model is retrained. It then extracts valuable information from passwords using NER (Named Entity Recognition) and regular expression techniques. This allows you to find names, dates, addresses and identify certain patterns in user behavior. Then the vector database is installed and configured. The collected data, generated passwords and security standards are loaded into it. Mechanisms for quick access to information are optimized, and integration of the database with the model is ensured. After this, the database is connected to the trained NLP algorithm. Testing of data transfer between the model and the storage is carried out, which makes it possible to verify the correctness of their interaction. At the final stage, the system undergoes final testing. The quality of generated passwords, the speed of request processing and the compatibility of system components are checked. If deficiencies are found, the necessary corrections are made. The result is an intelligent system capable of generating passwords based on analysis of patterns and user login history. It provides high accuracy, security and speeds up the password guessing process, making the system a powerful tool in the field of cybersecurity.

- *Development of a password guessing method using artificial intelligence based on data collected using social engineering methods*. The main goal is to develop a digital forensics tool that takes into account current password standards. First, user data is collected and generated. To do this, open sources are analyzed, including social networks, public web resources and databases. Based on the collected information, a correlation list of potential passwords is generated, taking into account the user's name, important dates, interests and frequently used words. To increase the volume of data, synthetic records are created that simulate possible entry scenarios. Next, the data is cleaned and normalized. All collected information is checked for duplicates, empty values, and incorrect formats. Then the information is brought into a single form: text data is converted to lowercase letters, redundant information is removed, formats for dates and other values ​​are standardized. After this, the process of generating a list of passwords begins. The most likely modifications are analyzed, such as replacing letters with symbols, mixing cases, and adding standard prefixes and suffixes. Passwords are generated taking into account international security standards (NIST 800-53, ISO 27001), after which they are ranked by likelihood of use based on statistical analysis. The next step is to train an NLP model to generate passwords. Using natural language processing algorithms, the model is trained on collected data, including the user's password history and personal information. Its accuracy is verified by assessing the realism of the generated passwords. After training the model, it is evaluated and optimized. Key indicators such as prediction accuracy, password diversity, and password generation speed are analyzed. If necessary, the model is modified or retrained. If the results remain unsatisfactory, the previous steps are returned to make corrections. Then the integration of Internet scraping tools and APIs is carried out. This allows you to automate the process of collecting data from social networks and other resources. A system is created that automatically retrieves, stores and updates information, minimizing manual labor. The next stage involves extracting key data using NER (Named Entity Recognition) algorithms and regular expressions. This helps identify names, dates, addresses and other significant elements that may be useful for further operation of the model. After this, the vector database is configured. Collected user data, generated passwords and security standards are loaded into it. The integration of the database with the model is configured, ensuring the relevance and update of knowledge. At the final stage, the system is tested and finalized. All key components are tested - from data collection and password generation to the speed and accuracy of the system. If deficiencies are identified, corrections are made and the previous stages are finalized. The result is an intelligent digital forensics system capable of generating personalized passwords based on socially engineered data. This takes into account current safety standards, ensuring high efficiency and accuracy of forecasting.

 - *Development of a method for safely removing the memory chip of a mobile device.* Study of existing methods of physical data extraction (chip-off, JTAG, ISP). Development of new techniques for safely removing information from memory chips without damaging them. Assessing the possibility of recovering deleted data at a low level. All of these areas of research are aimed at creating a universal domestic solution for digital forensics, which allows you to effectively analyze protected mobile devices, extract data and conduct forensic examinations in laboratory and field conditions.

To create a forensic system for examining locked electronic digital devices, you first need to implement a module for bypassing device authentication protection, which consists of the following tasks:

* Implementation of password search methods;
* Search and exploitation of existing vulnerabilities in authentication systems using binary exploitation methods;
* Development of a mathematical model of algorithms for generating authentication data using artificial intelligence technologies;
* Creating a method for automatically determining which password encryption methods are used.

**A brief description of the most important experiments**

1. **Experiments on the implementation of methods of brute force passwords.** Investigation of the effectiveness of various password brute force authentication techniques, including brute force, dictionary attacks and their hybrids. First, you need to assemble a test set of devices with different operating systems and security levels (smartphones, laptops, servers), and configure devices with preset passwords of varying length and complexity (numeric, alphanumeric, and passwords with special characters). Conducting a brute-force password brute-force attack involves a complete search of all possible password combinations. Conducting a dictionary attack involves using a list of passwords prepared in advance. Verification of hybrid methods: using basic dictionaries, but with slightly modified passwords (with the addition of numbers, special characters, and case changes). It is also necessary to measure the time spent trying the password, depending on its length, complexity and method of attack, as well as the success rate of the test of each technique. Based on the results of this experiment, it is necessary to develop recommendations on which method to perform password sorting.
2. **Experiments on finding and exploiting vulnerabilities in authentication systems.**

* Detection and exploitation of vulnerabilities in hardware authentication mechanisms of models through the use of binary analysis methods. First, you need to select trial devices and software for analysis, and collect data on known vulnerabilities in login systems (CVE databases, security reports). Static analysis of binary files used in the authentication process will help identify security threats. It is also necessary to check the vulnerabilities found using a real example.
* Data analysis. It is necessary to describe the results of the attacks. Based on the results of the attacks performed, assess the severity of the vulnerabilities identified during the analysis process. It is necessary to confirm that the system can be hacked through an available vulnerability.

1. **Development and testing of a mathematical model for generating authentication data.** It is necessary to create a model that allows you to predict the most likely passwords, which allows you to attack passwords more efficiently and quickly. Collect large data on passwords from open sources (for example, from leaked databases), classify passwords by length, structure, and characters included in the code. Develop a model architecture, such as machine learning methods, and train models based on accumulated data, which will allow you to create lists of the most likely passwords. Based on the results of these studies, experiments will be conducted to create an effective password generation model.
2. **Creating a method for automatically detecting the password encryption methods used.** Creating an algorithm that makes it possible to automatically find the type of encryption used for passwords by analyzing the encoded data. The study of known encryption methods (MD5, SHA-256, bcrypt, PBKDF2 and others).

Creating a group of trial data with known hashing methods.

* **Algorithm development:**

Creating a way to study the structure of hashes by their size, appearance, and special features.

Development of a classifier for finding encryption methods.

* **Testing:**

Using a custom-made method to hashes generated using different schemes.

Determining the accuracy and speed of finding encryption methods.

* **Data analysis:**

Identification of cases when the method gives incorrect results.

Improvement of the system based on the received data..

* **Expected result:**

An automated tool that can find hashing algorithms for passwords with great accuracy.

Recommendations for its use in forensic systems.

**Description of the research methods**

The following research methods are used to obtain the desired result and solve the program's tasks. Each of them is justified in terms of their usefulness, connection with the purpose and main objectives of the program, as well as their joint synergies.:

1. **Methods of brute force passwords.** The use of automatic methods for password selection, including methods of brute force, dictionary attacks and hybrid types. These methods allow access to the devices in case other ways of circumventing authentication protection are not available. Password brute force is directly related to the task of developing an authentication bypass module, providing basic functionality.
2. **Search for and exploit vulnerabilities in authentication systems.** The use of static and dynamic software analysis to find weaknesses in authentication mechanisms and create exploits to exploit them. This method helps you get past device protection without the need for a full password test, which makes the process faster. The discovered weaknesses can be used to further automate the hacking process. The method is strongly related to the task of automatically finding encryption methods and studying the data structure, complementing other workarounds.
3. **Development of a mathematical model for generating authentication data.** Using machine learning technologies and analyzing large datasets to create a model that can predict likely passwords based on statistics. Artificial intelligence makes it possible to greatly reduce the amount of data to analyze, making the selection process smarter and more efficient. The model of creating authentic data is mixed with the tasks of selecting passwords, changing or adding them in difficult cases. The connection with other methods is seen in the possibility of using the found weaknesses to refine the model settings and increase its accuracy.
4. **Methods for analyzing and determining the password encryption methods used.** Studying the shape of hashes and using the method of finding encryption methods to automatically search for the technologies used to protect them. It gives you a chance to find the best tactics to get past defenses, including applying weaknesses and tweaking your running methods. This method is the basis for a quick system check and it is crucial for the correct configuration of all other methods. It mixes with other possible methods, showing data to improve the search methods and password creation model.

The key selection methods and the numerical data creation scheme help each other. If one method does not work, another is taken, which affects the improvement of the system's confidence. The search for weaknesses makes the way for faster and less resource-intensive security bypasses, which in turn can be refined through the automatic detection of encryption methods. Automatic identification of encryption methods is a link, giving basic information for all other methods, which includes password selection and vulnerability analysis. These techniques make up one common simple method, where the results of any method (for example, vulnerability detection) are immediately applied.I am used to adjust others (for example, the selection of iteration parameters).

Each of the methods described here plays an important role in achieving the program's goal. Their connection and the order of use provide a high-quality solution to problems, along with the creation of a forensic system for the study of blocked electronic and digital devices. This approach allows you to achieve high accuracy, speed and reliability of the entire system.

**Methods of collecting primary information**

1. Physical access to the device:

* Unlocking broken smartphones and tablets in order to save information using special equipment (JTAG, Chip-Off, ISP).
* Getting a dump of the device with the possibility of conducting an examination of the data.

1. Logical analysis:

* Extract information from the device via USB, Wi-Fi, Bluetooth using third-party programs.
* Scan ports for active protocols and vulnerabilities.

1. Monitoring of system processes:

* Examination of system logs, logs and temporary files.
* Using sniffers to intercept data at the network connection level.

1. Study of documentation and source code:

* Study of device documentation.
* Reverse engineering of firmware and applications.

**5. Research group and program management**

During the implementation of this project, the members of the research group will be divided into several groups: binary exploitation analysts, reverse engineers, cryptographers, digital forensics engineers, software (module) developers and design engineers for the development and assembly of the hardware of the agroindustrial complex.

At all stages of the project, collaboration between all members of the research team will be governed by clearly defined roles, and they are complementary. Each role is responsible for completing one of the parts of the project, and the level of involvement will vary at certain stages of the project depending on the tasks being solved, as well as determined by the instructions of the project supervisor.

The area of responsibility of each of the roles is to perform the following tasks:

*Binary exploitation analysts and reverse engineers are the people who are responsible for:*

* researching existing scientific methods and software products that perform the tasks stated in this application, namely bypassing Android OS security systems.
* Investigation of security vulnerabilities in different versions of the operating systems under study (Windows, Android, iOS).
* Development of an algorithm for bypassing the protection of mobile applications and messengers using binary exploitation techniques.
* Research of protection systems for IoT devices, and existing vulnerabilities in collective networks of connected devices.
* Exploring the functions of Android and iOS smartphones that implement additional smartphone protection measures (locking the device indefinitely with multiple incorrect passwords entered).

*Cryptographers:*

1. Research of algorithms and methods of automatic decryption of encrypted authentication data used in the studied systems.
2. Research of algorithms for the functioning of encryption and decryption systems implemented in the Android mobile operating system.
3. Development of a method for automatic decryption of encrypted authentication data used in the studied systems.
4. Development of a method for decrypting extracted data related to mobile applications, messengers and cloud services.
5. Development of a method for decrypting extracted data from cloud services that implement backup storage functionality.

*Developers of the software part of the agro-industrial complex:*

* Implement a function in the form of executable code that provides administrative access to the Android file system while preserving user data.
* Development of a module for decrypting extracted data related to mobile applications, messengers and cloud services
* Development of a module for protecting mobile applications and messengers using binary exploitation techniques
* Development of code for decrypting extracted data from cloud services that implement backup storage functionality
* Development of a software module for extracting data from cloud services that implement backup storage functionality
* Development of modules for accessing password-protected backups, mobile applications, messengers, cloud services, and system settings of the Android operating system
* The development of the software part of the agro-industrial complex, embodies in the code algorithms and methods developed by binary exploitation analysts, reverse engineers, cryptographers and digital forensics engineers.
* Ensuring the interaction of software with the hardware components of the complex, creating user interfaces and proxy services for interaction between various components of the system.
* Test coverage of all software modules, debugging of the code and elimination of all bugs in the software that were discovered during the testing phase.
* Improve the efficiency and speed of the software, as well as regularly update the software to improve functionality and security.
* Create detailed documentation on the development and use of the software, which facilitates further work and support, as well as train end users and provide support on the use of the software.

*Design engineers for the development and assembly of the hardware of the agro-industrial complex:*

* Develop a prototype.
* Conduct pilot tests, data collection and analysis to capture the actual technical and functional characteristics of the prototype and make adjustments if necessary.
* Develop methodological documentation on the use of the prototype.
* Study of implemented solutions for the analysis of digital evidence using artificial intelligence methods (if any).
* Analysis of current processes and methods of digital forensics to identify existing deficiencies, followed by a proposal to eliminate it in the project.
* Develop a method to extract data from corrupted, encrypted, or recovered files.
* Development of a method for checking files for integrity.
* The use of artificial intelligence to automate and improve data analysis processes, detect relationships and patterns that may indicate the interaction of several people with each other, as well as to search for various information on a given query.
* Implementation of advanced algorithms to improve the accuracy and speed of data analysis using artificial intelligence techniques that significantly reduce the time spent researching digital evidence.
* Ensuring the integration of the developed algorithms and methods with the hardware and software complex.
* Collaborate with teams of software developers, cybersecurity specialists, and forensic experts to create a holistic solution.
* Development of algorithms that can be easily updated in the future to accommodate new types of threats and technologies.

1. **Hikmetov Askar Kusupbekovich** is an Academician of the National Academy of Sciences of the Higher School of the Republic of Kazakhstan. At the same time, he is a Corresponding Member of the National Engineering Academy of the Republic of Kazakhstan. He received his PhD in Physics and Mathematics with a PhD thesis on "Modeling turbulent flows in a stratified environment", specialty 05.13.18 -mathematical modeling, numerical methods and software package. He is the rector of Astana IT University LLP. He actively conducts research activities in the field of applied computer science, turbulence theory, mathematical modeling and organization of high-performance computing. He has more than 70 scientific publications on the problems of turbulence modeling and the development of information systems for solving various applied problems, of which more than 10 works have been published in highly rated scientific journals. He actively participates in various prestigious national and foreign scientific conferences.

2. **Rzayeva Leyla Gummetovna** – in 2016 she received a PhD in Automation and Control from L.N. Gumilyov ENU, Astana, Kazakhstan (QS World Rank 355). He works as an Assistant Professor and Acting Director of the Department of Intelligent Systems and Cybersecurity at Astana IT University (Astana, Kazakhstan). Leyla Rzayeva has published more than 40 national/international scientific articles. Her interests include control systems and industrial automation, cybersecurity, ML, DL and design of control systems in conditions of increased robustness, as well as design of neural networks and applications of artificial intelligent systems in predictive analytics and data analysis. She is the author and co-author of a significant number of scientific papers and active participants in many conferences. Member of the IEEE SIST-2024 Program Committee at Astana IT University and IEEE ICAIC-2024 at the University of Houston, Texas, USA. She is the General Chair of the RTCSE-2025 Conference at the University of Hawaii, USA. She delivered the keynote address at the IEEE International Conference on AI in Cybersecurity (ICAIC), February 7-9, 2024, at the University of Houston, USA. She delivered a keynote speech as an invited speaker at the Muti International Thematic Conference on Engineering and Science, as well as in April 2024 at the UAE Academic Center of Bath Spa University of Great Britain and at the 10th International Conference on Green Computing and Engineering Technologies (ICGCET®), and was also invited to the 10th International Conference on Green Computing and Engineering Technologies (ICGCET®) September 18-19, 2024 at Sea Cliff Resort, Zanzibar.

3**. Imanberdi Abilkair Yerboluly** - Master's Degree in Software Engineering (Bauman Moscow State Technical University). He has about 7 years of experience in the manufacturing sector in the areas of malware research and computer forensics. He is the head of the Malware Research Laboratory of JSC State Technical Service, where he leads a team of virus analysts. He is also a senior lecturer at the Cybersecurity Department of Astana IT University LLP, where he teaches courses in virus analytics and computer forensics. At the request of the Ministry of Defense of the Republic of Kazakhstan, he worked as a member of the working group as a leader (head of the group, Doctor of Technical Sciences, Professor S.K. Atanov) on the development of a prototype of a domestic UAV. The project developed software and mathematical support for an unmanned aerial vehicle stabilization system based on the use of a Kalman filter, an unmanned aerial vehicle navigation system, and an intelligent energy management system for a mobile facility. As a result, these methods were successfully implemented into the project, and the following implementation acts were obtained:

1) The act of introducing software and mathematical support for the stabilization system of an unmanned aerial vehicle based on the use of a Kalman filter. Ministry of Defense of the Republic of Kazakhstan National Defense University named after the First President of the Republic of Kazakhstan. 01.02.2017. Astana, Kazakhstan.

2) The act of introducing software and hardware for the navigation system of an unmanned aerial vehicle. Ministry of Defense of the Republic of Kazakhstan National Defense University named after the First President of the Republic of Kazakhstan. 01.02.2017. Astana, Kazakhstan.

3) The act of implementing software and hardware for an intelligent energy management system for a mobile facility. Ministry of Defense of the Republic of Kazakhstan National Defense University named after the First President of the Republic of Kazakhstan. 01.02.2017. Astana, Kazakhstan.

As a result of his scientific work, he developed a system and an intellectual program for controlling unmanned aerial vehicles, for which intellectual property rights were obtained.:

1) A system for smoothing raw data to stabilize the movement of a mobile object. 11.04.2017. №670. IS 007957

2) A program for intelligent decision-making on choosing the trajectory of a mobile system using the search for the optimal path on a graph. 11.04.2017. №668. IS 007912

He has 4 scientific publications in software development in domestic and foreign journals.

He has professional international certificates in the field of information security:

1) Certified Ethical Hacker (CEH), EC-Council

2) EC-Council Certified Security Analyst (ECSA)

4. **Myrzatai Ali Altynbayuli** - Master of Technical Sciences.He has defended the degree of Doctor of Philosophy (PhD) in the specialty "6D070200 - Automation and Control" at the L.N. Gumilyov Eurasian National University, currently awaiting the award of this degree. Has experience working with algorithms and machine learning.

5. **Olzhas Balkybekuly Konakbayev** holds a Master's degree in Automation and Control (L.N. Gumilyov Eurasian National University). I have many years of experience in the manufacturing sector, namely manufacturing, installation, repair, automation, and development of industrial weighing equipment. He worked with low-current automation systems, analog and digital load cells. More than 15 successfully completed automation projects of industrial weighing equipment from scratch throughout Kazakhstan. At the moment, I have completed my doctoral studies and after defending my dissertation in the near future, I will receive a PhD degree in Automation and Control. I work as a senior lecturer at Astana IT University**.**

**6** **Tazhibayeva Perizat Shalgynbaykyzy -** Bachelor's degree in "6B06301 - Cybersecurity“ Astana IT University. Currently, he is a master's student in the "7M06106 Secure Software Engineering" program at Astana IT University.

**7. Grigoriev Timur** - He opened an Internet-oriented bank specializing in “6B06301 - Cyberspace". I went to the editorial office at the request of "7M06106 Evgeny bezopasny". I'm currently working on a PCF project. General information - python, Django, Fastcgi, SQL, WEB

8. **Baibusinov, Azamat Sansizbaevich -** Information Security Specialist (Academy of the Federal Security Service, Russian Federation), Master of Technical Sciences in 15et.

He developed software for collecting electronic and digital documents with a Windows-based computer system "Protocol 4Win". He wrote a book on digital forensics "Computer Forensics. Digital evidence collection" (LAP Lambert Academic Publishing, 2019, ISBN: 978-620-0-45594-9).

He developed methodological recommendations on "Forensic investigation of computer technology and mobile device environments."

Scientific publications and copyrights:

1) Article "Development of a module for protecting data on optical media (CD-R) from unauthorized copying", Levin V.A., Baibusinov A.S. ("Modern problems of informatization in the analysis and synthesis of technological and software-telecommunication systems", Don State Technical University, Voronezh, 2008, issue 13, p.368-369);

2) Article "Software development for the forensic examination of the Windows registry", Zhantlesov J.H., Baibusinov A.S. ("Actual problems of science", Satbayev University, Almaty, 2018, issue 1, pp.102-103), https://doi.org/10.31643/2018.018;

3) Article "Features of the forensic examination of the Windows 8.1 (x64) registry", Baibusinov A.S. ("Actual problems of science", Satbayev University, Almaty, 2018, issue 1, pp.138-142), https://doi.org/10.31643/2018.028;

4) Software for collecting electronic and digital documents from computer systems based on Windows OS "Protocol 4Win", (certificate of registration of computer software No. 684 dated November 26, 2018);

5) The book "Computer Forensics. Digital evidence collection" (LAP Lambert Academic Publishing, 2019, ISBN: 978-620-0-45594-9).

9. **Niyazaliev Kuandyk Altayuli,** specialist in the field of digital forensics, master of Technical Science in the field of Radio Engineering, Electronics and telecommunications (Kazakh National University is. Al-Farabi, Almaty).

Senior officer in / Ch 01068. experience of work in the field of digital forensics on the study and evaluation of data sources and mobile devices, as well as analysis of data sources for more than 6 years. More than 5 years have passed since the development of the program. Also, experience in scientific projects in experimental and theoretical physics (Almaty) and preparatory activities at the Department of the native body and non-native physics of the physical and Technical Faculty of kaznu is. Al-Farabi (Almaty).

"Developed methodological recommendations" "Forensic Research of computer technologies and mobile devices""."

Scientific publications and author's practices:

1) Article "experimental study of the transition of a cluster of Fitzhew-Nagumo neurons from a "dormant" state to a "shattering" mode under the influence of noise", Journal of the evolution of the open system. - Almaty, 2015. - Vol. 1, VIP.17. - p. 50-53;

2)" comparative analysis of the production of OpenMP and CUDA on the example of the introduction of Fourier transform", Kazakhstan. Physics series. №2 (61). 2017.

10. **Kurmangali Elzhas Sergalievich,** specialist in digital forensics, Bachelor's degree in Computer Engineering and Software Engineering (Bolashak University, Kyzylorda).

Military officer 01068. More than 2 years of experience in the field of digital forensics in unlocking, extracting and restoring data from storage devices and mobile devices, as well as analyzing extracted data. He has been working in software development for more than 5 years.

He developed methodological recommendations on "Forensic investigation of computer technology and mobile devices".

He has developed and holds the copyright for the mobile application of the KARVA marketplace. He was accelerated in the technopark of IT startups “Astana Hub” with this mobile application. Copyright and certificates have been obtained from Astana Hub:

1. Copyright certificate of the KARVA mobile application marketplace.

2. Certificate of completion of the "Startup School" course from Astana Hub, 2021.

3. Acceleration Certificate (KARVA Startup) from Astana Hub 2021.

The Juzim mobile application, AISuret and ArBat software, as well as a web application for criminologists are currently under development.

In addition, certificates are available.:

1. "CISCO IoT Introduction to the Comprehensive Internet", 2018.

2. "CISCO ITE-R Computer equipment maintenance and Repair", 2018.

3. "Application development for iOS" (02/07/2023-07/31/2023) from the STEP Computer Academy.

**11.** **Shayakhmetov Madi Arsenovich** - An information security engineer with a background in cybersecurity, as well as current specialization in secure software development, confirm a deep understanding of current threats and protection methods. His experience in cryptography, digital forensics and web application security allows him to effectively solve problems related to information security. He also participated in the project "BR24993232"Development of innovative technologies.

**12.** **Daniel Pugolovkin** has a master's degree. He Is An Information Security Engineer. He has experience in cryptography, digital forensics, and web application security.

13.**Mohsen Guizani** - Full Professor, received a Bachelor of Science degree. (with honors) and M.S. degrees in Electrical Engineering and Graduate studies. and a PhD. Degrees in Computer Engineering from Syracuse University, New York, in 1984, 1986, 1987, and 1990, respectively. He is currently a professor at the Department of Computer Science and Engineering at Qatar University. He is the author/co-author of nine books and more than 450 publications in peer-reviewed journals and conferences. His research interests include wireless communications and mobile computing, smart grids, cloud computing, and security.

**14.** **Satybaldina Dina Zhagyparovna**, Candidate of Physico-Mathematical Sciences, PhD, Associate Professor, specialty 05.13.00 - Computer Science, Computer Engineering and Management. She led a project on the topic "Development of models and algorithms for processing and transferring sensory data in the production of multitasking gas analytical systems."She investigated the electrical characteristics and sensitivity characteristics of 8 metal-oxide sensors of a gas analyzer obtained from a partner for the presence of vapors of model analytes in the air at different concentrations of their vapors in the air and different operating temperatures of the sensors.Implemented procedures for digitizing analog experimental data, saving the results in numerical format inside a text file.

**15.** **Yerbol Tolevkanovich Nurdauletov** holds a Bachelor's degree in Computer Science (International University of Information Technology). I have many years of manufacturing experience in the field of cybersecurity. In particular, he worked as the chief analyst at KZ-CERT and the Malware Research Laboratory of JSC GTS. The main focus of the work was the analysis of malicious code. He also helped the team of digital criminologists and tret-hunters. He completed the courses “digital forensics“, ”advanced reverse engineering“ from Kaspersky Lab and ”Methods of detecting and countering computer attacks in networks" from MEPHI.

**16.** **Amirov, Yersultan Yerbolovich**, holds a bachelor's degree.He is a digital forensics engineer.

**17.** **Kozhakhmet Zhaksylyk,** Master of Information Systems.He has 10 years of experience in software development. He is a instructor at Astana IT University. He is instructor of software testing and quality assurance services.

**18. Zhansaya Alim kyzy Bizhanova, Master of Technical Sciences.**

In 2016-2017, while working as a doctor of the sanitary and epidemiological service in the zonal virological laboratory of the National Center for Expertise Branch of the Committee for Consumer Protection of the Ministry of National Economy of the Republic of Kazakhstan, in addition to her main work, she assisted in the public procurement of laboratory kits for DNA isolation and PCR.

• PCF project: A new device for early detection and diagnosis of new threats of viral diseases

• PCF Project: Validating a Minimally Invasive Tissue Sampling Procedure as a New Paradigm for obtaining Reliable Mortality Statistics for Assigning Cause of Death: Experience from Kazakhstan

• \* AXEL and TYRO3 signaling pathways as therapeutic targets in bladder cancer: preclinical study"/AXL and TYRO3 signaling pathways as therapeutic targets in bladder cancer: preclinical studies

**19.Vacancy 1**

**20.Vacancy 2**

**Information about the main publications of the supervisor:**

1. Mikhailov, P., Ualiyev, Z., Kabdoldina, A., Smailov, N., Khikmetov, A., & Malikova, F. (2021). Multifunctional fiber-optic sensors for space infrastructure. *Eastern-European Journal of Enterprise Technologies*, *5*(5), 113.<https://doi.org/10.15587/1729-4061.2021.242995> CiteScore 2.0 (for 2021); Percentile – 46, Q3
2. Kabdoldina, A., Ualiyev, Z., Smailov, N., Malikova, F., Oralkanova, K., Baktybayev, M., ... & Bazarb, L. (2022). DEVELOPMENT OF THE DESIGN AND TECHNOLOGY FOR MANUFACTURING A COMBINED FIBER-OPTIC SENSOR USED FOR EXTREME OPERATING CONDITIONS. *Eastern-European Journal of Enterprise Technologies*, *119*(5). [https://doi.org/](https://doi.org/10.15587/1729-4061.2021.242995)10.15587/1729-4061.2022.266359, CiteScore 2.0 (for 2022); Percentile – 45, Q3
3. Kabdoldina, A., Ualiyev, Z., Ibrayev, S., Jamalov, N., Ibrayeva, A., Tuleshov, Y., Analiyeva, A., Arinova, D., Khikmetov, A., & Uaissov, B. (2023). The use of technologies for stabilizing the electrophysical characteristics of sensor structures used in the development and manufacture of measuring transducers. Eastern-European Journal of Enterprise Technologies, 1(5 (121), 6–16. <https://doi.org/10.15587/1729-4061.2023.274686>, CiteScore 2.0 (for 2022); Percentile – 45, Q3
4. Issakhov, A., Borsikbayeva, A., Abylkassymova, A., Issakhov, A., & Khikmetov, A. (2023). Numerical modeling of the dam-break flood over natural rivers on movable beds. *International Journal of Nonlinear Sciences and Numerical Simulation*, *24*(5), 1659-1681. [https://doi.org/](https://doi.org/10.15587/1729-4061.2023.274686)[10.15587/1729-4061.2023.274686](http://dx.doi.org/10.15587/1729-4061.2023.274686), CiteScore 2.8 (for 2023); Percentile – 60, Q3
5. Tynymbaev A.B. Baisholanova K.S., Mambetov S.T. (2024). Application of logistic regression to detect attacks on financial monitoring. Bulletin of NIA RK No. 3 (93) 2024, pp. 245-255.<https://doi.org/10.47533/2024.1606-146X.64> (List of editions of KOKSNVO: Mathematical sciences, information and communication technologies)
6. Mambetov, S. T., Begimbaeva, E. E., Khikmetov, A. K., Zoldasbaev, S. K., & Kazbekova, G. N. (2023). SENTIMENT ANALYSIS OF HACKING INTERNET FORUMS. Vestnik KazNPU named after Abaya, Series "Physico-mathematical sciences", 84(4), 162-172.<https://doi.org/10.51889/2959-5894.2023.84.4.016> (List of editions of KOKSNVO: Information and communication technologies)
7. Mambetov S.T., Begimbaeva E.E., Joldasbaev S.K. (2023). Development of an algorithm for obtaining data from thematic Internet resources. Bulletin of the National Engineering Academy of the Republic of Kazakhstan. 2023. No. 2 (88), pp. 58-71.<https://doi.org/10.47533/2023.1606-146X.6> (List of editions of KOKSNVO: Mathematical sciences, information and communication technologies)
8. Khikmetov, A. K., Karuna, O. L., & Karzhaubaev, K. K. (2013). DEVELOPMENT OF LINUX APPLICATIONS ADAPTED FOR KAZAKHSTAN AS A STEP IN THE CREATION OF A HIGH-TECH ECONOMY OF THE RK. Vestnik EKSTU im. D. Serikbaeva and Computational Technologies SB RAS, Ust-Kamenogorsk, 2013 - P.221-225. [https://kazneb.kz/ru/bookView/view?brId=1163719&simple=true#](https://kazneb.kz/ru/bookView/view?brId=1163719&simple=true)
9. Khikmetov, A. K., Karzhaubaev, K. K., & Isakhov, A. A. (2013). CREATION OF A LINUX OS INSTALLER WITH KAZAKH LANGUAGE SUPPORT. Vestnik EKSTU im. D. Serikbaeva and Computational Technologies SB RAS, Ust-Kamenogorsk, 2013 - P.218-221. [https://kazneb.kz/ru/bookView/view?brId=1163719&simple=true#](https://kazneb.kz/ru/bookView/view?brId=1163719&simple=true)
10. Kolesnikova, K., Lukianov, D., Khikmetov, A., Alpysbayev, K., Mukhamedyeva, A., & Dauletbek, Y. (2024). Using Model-Based Systems Engineering Tools in Software Development. *Procedia Computer Science*, *241*, 470-475.<https://doi.org/10.1016/j.procs.2024.08.066> H-Index:132 in Computer Science (miscellaneous)

**Information about the research group's publications:**

1. Pandey, B., Pandey, P., Kulmuratova, A., & Rzayeva, L. (2024). Efficient usage of web forensics, disk forensics and email forensics in successful investigation of cyber crime. *International Journal of Information Technology*, *16*(6), 3815-3824. https://doi.org/10.1007/s41870-024-02014-6 **(Percentile 84th)**
2. Tendikov, N., Rzayeva, L., Saoud, B., Shayea, I., Azmi, M. H., Myrzatay, A., & Alnakhli, M. (2024). Security Information Event Management data acquisition and analysis methods with machine learning principles. *Results in Engineering*, *22*, 102254.   
   https://doi.org/10.1016/j.rineng.2024.102254 **(Percentile 82th)**
3. Ahmed, A. A., Hasan, M. K., Alqahtani, A., Islam, S., Pandey, B., Rzayeva, L., ... & Alqahtani, N. (2024). Deep Learning Based Side-Channel Attack Detection for Mobile Devices Security in 5G Networks. *Tsinghua Science and Technology*, *30*(3), 1012-1026.  https://doi.org/10.26599/TST.2024.9010123.
4. Rzayeva, L., Myrzatay, A., Abitova, G., Sarinova, A., Kulniyazova, K., Saoud, B., & Shayea, I. (2023). Enhancing LAN Failure Predictions with Decision Trees and SVMs: Methodology and Implementation. *Electronics*, *12*(18), 3950. https://doi.org/10.3390/electronics12183950 **(Percentile 64th)**
5. Myrzatay, A., Rzayeva, L., Bandini, S., Shayea, I., Saoud, B., Çolak, I., & Kayisli, K. (2024). Predicting LAN Switch Failures: An Integrated Approach with DES and Machine Learning Techniques (RF/LR/DT/SVM). *Results in Engineering*, 102356. https://doi.org/10.1016/j.rineng.2024.102356 **(Percentile 82th)**
6. Ahmed, A. A., Hasan, M. K., Aman, A. H., Safie, N., Islam, S., Ahmed, F. R. A., ... & Rzayeva, L. (2024). Review on hybrid deep learning models for enhancing encryption techniques against side channel attacks. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3431218 **(Percentile 87th)**
7. Shingissov, D., Seilov, S., Goikhman, V., Sokolov, N., Akhmetova, Z., Uskenbayeva, G., & Rzayeva, L. (2022). Study of the Process of Packet Arrival at a Multiservice Node. *Symmetry*, *14*(4), 752.   
   https://doi.org/10.3390/sym14040752 (**Percentile 78th**)
8. Imanberdi, A., Lira, L., Aitolkyn, K., Leila, R., Abitova, G., Aigerim, B., ... & Assem, B. (2023). Assessment of the main features of the model of dissemination of information in social networks. *International Journal of Electrical & Computer Engineering (2088-8708)*, *13*(6).   
   https://doi.org/10.11591/ijece.v13i6.pp6729-6736 (**Percentile 66th** )
9. Slyamkhanov, A., Bozbayev, Z., Alzhanova, A., Pan, A., Ramazan, T., & Rzayeva, L. (2023, October). Usage of Machine Learning in DDOS Attack Detection. In *2023 10th International Conference on Wireless Networks and Mobile Communications (WINCOM)* (pp. 1-6). IEEE.  
   https://doi.org/10.1109/WINCOM59760.2023.10322885
10. Sarinova, A., Rzayeva, L., Tendikov, N., & Shayea, I. (2023, October). Simple Implementation of Terrain Classification Models via Fully Convolutional Neural Networks. In *2023 10th International Conference on Wireless Networks and Mobile Communications (WINCOM)* (pp. 1-6). IEEE.  
    https://doi.org/10.1109/WINCOM59760.2023.10323012
11. Maralbayev, A., Omar, G. S., Abdulayeva, M., Rzayeva, L., Kalybek, G., & Rakhym, E. (2023, October). New Algorithm of Weak Password Detection. In *2023 10th International Conference on Wireless Networks and Mobile Communications (WINCOM)* (pp. 1-6). IEEE.  
    https://doi.org/10.1109/WINCOM59760.2023.10323000
12. Kara, M. Ü., Benlakehal, M. E., Shayea, I., Tussupov, A., & Rzayeva, L. (2024, May). Data Caching in Edge Computing: A Survey. In *2024 IEEE 4th International Conference on Smart Information Systems and Technologies (SIST)* (pp. 433-439). IEEE.  
    https://doi.org/10.1109/SIST61555.2024.10629324
13. Saoud, B., Shayea, I., Rzayeva, L., & Tussupov, A. (2024, May). Community structure detection in complex network based on MST and modularity. In *2024 IEEE 4th International Conference on Smart Information Systems and Technologies (SIST)* (pp. 526-529). IEEE.  
    https://doi.org/10.1109/WINCOM59760.2023.10323000
14. Er, F., Shayea, I., Saoud, B., Rzayeva, L., & Alibek, A. (2024, February). Machine Learning and Deep Learning Algorithms in Times Series Analysis. In *2024 IEEE International Conference on Big Data & Machine Learning (ICBDML)* (pp. 251-256). IEEE.  
    https://doi.org/10.1109/ICBDML60909.2024.10577333
15. Dael, F. A., Amran, M. A., Shayea, I., & Rzayeva, L. (2024, February). Performance Evaluation of Routing Protocols in Vehicular Ad-Hoc Networks for Highway Scenarios. In *2024 IEEE International Conference on Big Data & Machine Learning (ICBDML)* (pp. 257-264). IEEE.  
    https://doi.org/10.1109/ICBDML60909.2024.10577327
16. Zor, E., Taskiran, Y., Dael, F. A., Shayea, I., Rzayeva, L., & Syzdykova, Z. (2024, February). AirWave: Enhancing UAV Connectivity in Cellular Networks through an Integrated Simulation Framework. In *2024 IEEE International Conference on Big Data & Machine Learning (ICBDML)* (pp. 295-302). IEEE.  
    https://doi.org/10.1109/ICBDML60909.2024.10577299
17. Singh, A. K., Jain, T. K., Pandey, P., & Rzayeva, L. (2024, February). LVCMOS Based Low Power Implementation of DES Encryption Algorithm on 28nm FPGA. In *2024 3rd International conference on Power Electronics and IoT Applications in Renewable Energy and its Control (PARC)* (pp. 383-386). IEEE.  
    https://doi.org/10.1109/PARC59193.2024.10486400
18. Pandey, P., Singh, A. K., Kumar, K., Gohel, H., Rzayeva, L., & Pandey, B. (2024, May). HSTL IO Standards Based Low Power Implementation of Elliptic Curve Cryptography (ECC) on FPGA. In *2024 IEEE 4th International Conference on Smart Information Systems and Technologies (SIST)* (pp. 261-265). IEEE.  
    https://doi.org/10.1109/SIST61555.2024.10629505
19. Abasi, A. K., Aloqaily, M., & Guizani, M. (2025). 6G mmWave Security Advancements through Federated Learning and Differential Privacy. IEEE Transactions on Network and Service Management, 1.   
    https://doi.org/10.1109/tnsm.2025.3528235 **(Percentile 86th)**
20. Hijazi, N. M., Aloqaily, M., & Guizani, M. (2024). Collaborative IoT learning with secure peer-to-peer federated approach. Computer Communications, 228, 107948. https://doi.org/10.1016/j.comcom.2024.107948 **(Percentile 95th)**
21. Shan, C., Zeng, J., Liu, H., Chen, C., Du, X., &Guizani, M. (2024). TDOcc: Exploit machine learning and big data in multi-view 3D occupancy prediction. Future Generation Computer Systems, 164, 107583.   
    https://doi.org/10.1016/j.future.2024.107583 **(Percentile 98th)**
22. Shafiq, M., Tian, ​​Z., Bashir, A. K., Du, X., & Guizani, M. (2020). CORRAUC: A malicious Bot-IoT traffic detection method in IoT network using Machine-Learning techniques. IEEE Internet of Things Journal, 8(5), 3242–3254. https://doi.org/10.1109/jiot.2020.3002255 **(Percentile 97th)**
23. Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. IEEE Communications Surveys & Tutorials, 22(3), 1646–1685. https://doi.org/10.1109/comst.2020.2988293 **(Percentile 99th)**
24. Khan, S., Gani, A., Wahab, A. W. A., Abdelaziz, A., Ko, K., Khan, M. K., & Guizani, M. (2016). Software-Defined Network Forensics: motivation, potential locations, requirements, and challenges. IEEE Network, 30(6), 6–13. https://doi.org/10.1109/mnet.2016.1600051nm **(Percentile 98th)**
25. Liu, X., Fu, X., Du, X., Luo, B., &Guizani, M. (2022). Machine Learning-Based Non-Intrusive Digital Forensic Service for smart homes. IEEE Transactions on Network and Service Management, 20(2), 945–960.   
    https://doi.org/10.1109/tnsm.2022.3224863 **(Percentile 86th)**
26. Ren, G., Wu, J., Li, G., Li, S., &Guizani, M. (2022). Protecting intellectual property with reliable availability of learning models in AI-Based cybersecurity services. IEEE Transactions on Dependable and Secure Computing, 21(2), 600–617.   
    https://doi.org/10.1109/tdsc.2022.3222972 **(Percentile 90th)**
27. He, D., Chan, S., & Guizani, M. (2017). Cyber security analysis and protection of wireless sensor networks for smart grid monitoring. IEEE Wireless Communications, 24(6), 98–103.   
    https://doi.org/10.1109/mwc.2017.1600283wc **(Percentile 99th)**
28. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE communications surveys & tutorials, 17(4), 2347-2376.  
    https://doi.org/10.1109/COMST.2015.2444095 **(Percentile 99th)**
29. Ge, X., Cheng, H.,Guizani, M., & Han, T. (2014). 5G wireless backhaul networks: challenges and research advances. IEEE network, 28(6), 6-11.   
    https://doi.org/10.1109/MNET.2014.6963798 **(Percentile 98th)**
30. Singh, J., Wazid, M., Das, A. K., Chamola, V., & Guizani, M. (2022). Machine learning security attacks and defense approaches for emerging cyber physical applications: A comprehensive survey. Computer Communications, 192, 316–331.   
    https://doi.org/10.1016/j.comcom.2022.06.012 **(Percentile 95th)**

**Table 1**– Composition of the research group for scientific research, including foreign scientists, young scientists (postdoctoral students, doctoral, master's and undergraduate students)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No. | SNF (if exists), education, degree, academic title | Main place of work, position | H-index, ResearcherID, ORCID, Scopus Author ID (if available) | Role in the project or program and nature of the work performed | Brief rationale for participation |
| 1 | Khikmetov Askar Kusupbekovich, Candidate of Physical and Mathematical Sciences, Associate Professor | Chairman of the Board – Rector of Astana IT University LLP | h index = 3, ResearcherIDIEM-5232-2023, https://orcid.org/0000-0002-3045-7592, https://www.scopus.com/authid/detail.uri?authorId=56741480900 | **Scientific director of the project**  *Project management:*  1. Setting project goals;  2.Distribution of functional responsibilities of project participants;  3.Organization and coordination of the work of performers in all areas and types of program activities;  4. Prompt response to risks;  5. Monitoring the progress of project stages;  6. Adjusting assignments;  7. Analysis of the scientific results obtained;  8. Preparation and formation of WoS, Scopus, monographs, patents, reporting materials in international peer-reviewed publications;  9. Preparation and formation of documents for filing for patents and intellectual property rights;  10. Problem formulation experimental work;  11.  Development of proposals and recommendations;  12. The process of transferring and presenting research results to the customer.  13.  Obtaining a patent and monograph | Is an expert in mathematical modeling, which is one of the key factors in the implementation of the development of methods for accessing password-protected backups, mobile applications, instant messengers, cloud services and system settings of the Android operating system. When implementing this task, it is planned to use AI models, NER models, to study the social engineering of the object. The participant's competencies will be useful in defining their own AI model, for the most accurate selection of possibly correct options. |
| 2 | **Rzayeva Leila Gummetovna,**Doctor of Philosophy PhD in Automation and Control | Limited Liability Partnership "Astana IT University", Deputy Director of the Department of Intelligent Systems and Cybersecurity, Associate Professor | h-index -4, ResearcherID - https://www.researchgate.net/profile/Rzayeva-Leila,  ORCID - 0000-0002-3382-4685,  Scopus Author ID - 57218901417 | Responsible executor, Data analyst and system integrator, cryptographer, VNS   1. Research of algorithms and methods for automatic decryption of encrypted authentication data used in the systems under study.   Research of algorithms of functioning of encryption and decryption systems implemented in the Android mobile operating system.   1. Research of existing scientific methods and software products that perform the tasks stated in this application, namely bypassing the Android OS security systems. 2. Research of vulnerabilities of security systems in different versions of the operating systems under study (Windows, Android, IOS). 3. Implementation of advanced algorithms to improve the accuracy and speed of data analysis, using artificial intelligence methods that significantly reduce the time of examination of digital evidence. 4. Ensuring the integration of developed algorithms and methods with the hardware and software complex. 5. Obtaining a patent and monograph | Has 16 years of experience in the implementation and maintenance of automated production lines and the implementation of SAP S4/Hana modules MM, WM, PM.  Area of ​​responsibility: development, implementation and technical support of an information system for optimizing production processes.  **Scientific and pedagogical activity since 2010:**  Since 2010, he has experience in teaching undergraduate, graduate and doctoral students in specialized disciplines of the educational programs "Automation and Control", "Telecommunications", "Cybersecurity", "Smart Technologies". Supervisor of more than 100 undergraduate students, more than 20 masters and 2 PhD students. The main direction of scientific research is the development of optimal, adaptive and robust control systems, the use of artificial intelligence in various technological and technical processes, programming microcontrollers, development of embedded control systems, information security, smart technologies and IoT.  Most of the research is aimed specifically at solving the problems of the industrial sector. He has experience in managing scientific research on the development of automatic detection of hidden networks from USB devices (work in a research laboratory during a scientific internship in the USA), as well as participation in projects on the application of machine learning algorithms and the creation of neural networks to improve the efficiency of thermal production processes (copper production) and pattern recognition of hyperspectral aerospace images and predictive analytics, as well as the development of methods for increasing the stability of the aircraft control system by order of the Ministry of Defense of the Republic of Kazakhstan (under the supervision of Professor Beisenbi M.A.).  The following research areas have been published:  - 15 articles cited in Scopus (Q1-Q3) and Web of Science,  - more than 50 publications in foreign journals and magazines recommended by the Committee for Quality Assurance in Education of the Ministry of Education of the Republic of Kazakhstan.  Head of the targeted funding project BR24993232 "Development of innovative technologies for conducting digital forensic research using intelligent software and hardware systems" |
| 3 | Imanberdi Abilkair Erboluly, Master | Limited Liability Partnership "Astana IT University", Senior Lecturer, CTF Trainer | https://www.researchgate.net/profile/Abilkair-Imanberdi,0009-0005-6144-2392,000000000 | Reverse - engineer, cryptographer   1. Development of an algorithm for bypassing the protection of mobile applications and instant messengers using binary exploitation techniques. 2. Research of IoT device security systems and existing vulnerabilities in collective networks of connected devices. 3. Development of a method for automatic decryption of encrypted authentication data used in the systems under study. 4. Development of a method for decrypting extracted data related to mobile applications, messengers and cloud services. 5. Development of a method for decrypting extracted data from cloud services that implement the functionality of a backup storage. 6. Obtaining a patent and monograph | Has about 8 years of experience in the manufacturing sector in the areas of malware research and computer forensics. Manages a team of virus analysts at JSC GTS. Is a CTF trainer at Astana IT University LLP.  At the request of the Ministry of Defense of the Republic of Kazakhstan, he worked as a co-leader in the working group (the group leader is Doctor of Technical Sciences, Professor S.K. Atanov) on the development of a prototype of a domestic UAV. The project developed software and mathematical support for the unmanned aerial vehicle stabilization system based on the use of the Kalman filter, a navigation system for the unmanned aerial vehicle, and an intelligent energy management system for the mobile object. As a result, these methods were successfully implemented in the project, and implementation certificates were received.  **Intellectual Property Rights:**  1) Raw data smoothing system for stabilizing the motion of a mobile object. 11.04.2017. No. 670. IS 007957  2) A program for intelligent decision-making on the choice of the trajectory of a mobile system using the search for the optimal path on a graph. 11.04.2017. No. 668. IS 007912  Has 4 scientific publications on software development in domestic and foreign journals.  **International professional certificates:**  1) Certified Ethical Hacker (CEH), EC-Council  2) EC-Council Certified Security Analyst (ECSA) |
| 4 | Myrzatay Ali Altynbayuly, Master of Technical Sciences | Limited Liability Partnership "Astana IT University", Project Manager | h - index = 3  ORCID: 0000-0002-5339-2437 | Machine Learning Algorithm Engineer, CNN   1. Study of implemented solutions for digital evidence analysis using artificial intelligence methods (if any). 2. Analysis of current digital forensics processes and methods to identify existing deficiencies, followed by a proposal for their elimination in the project.   Using artificial intelligence to automate and improve data analysis processes, discover relationships and patterns that may indicate interactions between multiple individuals, and search for various information based on a given request. | He defended his PhD degree in the specialty "6D070200 - Automation and Control" at the L.N. Gumilyov Eurasian National University, and is currently awaiting the award of this degree. He has significant experience in working with algorithms and machine learning methods, which allows him to apply modern approaches in the field of algorithmic research. He is an expert in the field of algorithm development and analysis. He has published scientific papers in international journals indexed in the Scopus database, with high quality indicators (Q1 and Q2 percentile). He has 13 published scientific articles |
| 5 | **Konakbaev Olzhas Balkybekuly**, Master of Engineering Sciences in the field of “Automation and Control” | Astana IT University Limited Liability Partnership, Senior Lecturer, Department of Intelligent Systems and Cybersecurity | ORCID 0009-0002-9156-4858 | Hardware Technology Specialist, Lab Assistant |  |
| 6 | Tazhibaeva Perizat Shalgynbaykyzy  Bachelor of Science in Cyber ​​Security | Limited Liability Partnership "Astana IT University", Master's student"7M06106 Secure Software Engineering" | ORCID: 0009-0009-1566-636X,000 | Information security engineer   1. Conducting an analysis of existing technological solutions for processing digital evidence in order to identify potential vulnerabilities and assess the associated risks. 2. Development and implementation of information security measures, including the use of cryptographic methods, implementation of access control systems and monitoring settings to ensure the confidentiality, integrity and availability of data. 3. Conducting an audit of the project's information systems to assess their compliance with regulatory requirements and standards. | Received a bachelor's degree in 2024 in the specialty "6B06301 - Cybersecurity". Currently studying for a master's degree in the specialty "7M06106 Secure Software Engineering".  Has good skills necessary to conduct analysis of existing methods.  Has good knowledge required for an information security specialist.  Existing education in cybersecurity, as well as current specialization in secure software development, confirm a deep understanding of current threats and methods of protection. Experience in cryptography, digital forensics and web application security allows you to effectively solve problems related to ensuring information security. |
| 7 | Shayakhmetov Madi Arsenovich  Bachelor of Science in Cyber ​​Security | Limited Liability Partnership "Astana IT University", Master's student"7M06106 Secure Software Engineering" |  | Information security engineer   1. Development of a method for automatic decryption of encrypted authentication data used in the systems under study. 2. Development of a method for decrypting extracted data related to mobile applications, messengers and cloud services. 3. Development of a method for decrypting extracted data from cloud services that implement the functionality of a backup storage. | Possesses the necessary knowledge and skills that make him a valuable participant in the project. Education in the field of cybersecurity, as well as current specialization in secure software development, confirm a deep understanding of current threats and protection methods. Experience in cryptography, digital forensics and web application security allows him to effectively solve problems related to ensuring information security. He also participated in the project "BR24993232 "Development of innovative technologies for conducting digital forensic research using intelligent software and hardware systems" as a junior researcher, which indicates his practical experience in the field of digital forensic research. |
| 8 | **Timur Grigoryev, Master** |  | ORCID: 8987-6756-57 | Information security engineer, Laboratory assistant  1. Research of algorithms for the functioning of encryption and decryption systems implemented in the Android mobile operating system.  2. Research of cloud solutions and their structure that implement the functionality of backup storage.  3.Development of a method for automatic decryption of encrypted authentication data used in the systems under study | is an information security specialist and developer of AI models to optimize the tasks of ensuring the protection of personal data and has excellent knowledge of data encryption and decryption methods; |
| 9 | **Niyazaliev Kuandyk Altayuly,** | Military unit 01068, Researcher | Web of Science ResearcherID: AGX-8506-2022,0000-0002-3928-5248 | Research of cloud solutions and their structures that implement the functionality of backup storage.  Research of algorithms and methods for bypassing the protection of mobile applications and instant messengers using binary exploitation techniques.  To create universal methods for overcoming security systems and gaining access to information on password-protected electronic digital devices within the framework of law enforcement and national security  Development of a method for automatic decryption of encrypted authentication data used in the systems under study  Implement a function in the form of executable code that provides administrative rights to the Android file system while preserving user data | Isa specialist in digital forensicshas the knowledge, skills and abilities to solve the following tasks |
| 10 | **Kurmangali Elzhas Sergaliuly** |  |  | Digital Forensics Engineer  1. Development of instructions for searching for vulnerabilities in security systems in different versions of the operating systems under study  2.Development of a method for decrypting extracted data related to mobile applications, messengers and cloud services  3. Develop methodological documentation for the use of the prototype | is valid  a digital forensics specialist of the National Security Committee and can clearly describe current problems in this area, contribute to the development of methods and testing of results, provide expert assessment and recommendations for improving the developed PAC |
| 11 | **Pogolovkin Daniil** |  | Scopus Author ID: 77113355 | Information security engineer  1.Research of algorithms and methods for bypassing the protection of mobile applications and instant messengers using binary exploitation techniques.  2.Development of a method for automatic decryption of encrypted authentication data used in the systems under study  3. Implement a function in the form of executable code that provides administrative rights to the Android file system while preserving user data | is an information security specialist and a developer of AI models to optimize the tasks of ensuring the protection of personal data and has excellent knowledge of data encryption and decryption methods; |
| 12 | **Mohsen Guizani** |  | h index = 106 https://www.scopus.com/authid/detail.uri?authorId=7004750176 ResearcherIDD-9103-2018 | Foreign scientific consultant  1. Research of algorithms for the functioning of encryption and decryption systems implemented in the Android mobile operating system.  2. Research into the implementation of the main authentication methods used in mobile phones and tablets  3. To create universal methods for overcoming security systems and gaining access to information on password-protected electronic digital devices within the framework of law enforcement activities and ensuring national security  4.Development of a method for automatic decryption of encrypted authentication data used in the systems under study  5. Implement a function in the form of executable code that provides administrative rights to the Android file system while preserving user data  6. Development of a software module for extracting data from cloud services, implementing the functionality of a backup storage | a professor with many years of experience, his research interests focus on computer networks, cybersecurity, wireless and sensor networks, and cloud computing. In his research, he pays special attention to the issues of protecting cloud technologies and intelligent networks, considering them in the context of computer security, which will significantly facilitate the team's work on developing algorithms and methods that solve the main goal of the study; |
| 13 | **Satybaldina Dina Zhagyparovna** | Non-profit joint-stock company "L.N. Gumilyov Eurasian National University", director of the Research Institute of Information Security and Cryptology | ORCID:0000-0003-0291-4685  ResearcherID:P-1120-2014  Scopus Author ID:  57193740669 | 1.Research of vulnerabilities of security systems in different versions of the studied operating systems (Windows, Android, IOS)  2. Research of algorithms and methods for bypassing the protection of mobile applications and instant messengers using binary exploitation techniques.  3. To create universal methods for overcoming security systems and gaining access to information on password-protected electronic digital devices within the framework of law enforcement activities and ensuring national security  4.Development of a method for automatic decryption of encrypted authentication data used in the systems under study  5.Development of a method for bypassing the protection of mobile applications and instant messengers using binary exploitation techniques  6.Development of a software module for decrypting extracted data related to mobile applications, messengers and cloud services | has many years of experience in the field of modeling a cryptographic system for backup storage of confidential data in secure servers and the use of artificial intelligence methods to ensure cybersecurity of cellular networks, for many years headed the Department of Information Security at the L.N. Gumilyov Eurasian National University, and is currently the founder and head of the Research Institute of Information Security and Cryptology at the L.N. Gumilyov Eurasian National University. Has established herself as one of the best experts in data encryption and decryption. This project requires her strongest competence in decrypting files extracted from mobile devices; |
| 14 | **Nurdauletov Erbol Tolevkanovich** |  |  | Binary Exploitation Analyst, Cryptographer  1. Research into the implementation of the main authentication methods used in mobile phones and tablets.  2. To create universal methods for overcoming security systems and gaining access to information on password-protected electronic digital devices within the framework of law enforcement activities and ensuring national security  3.Development of code for decrypting extracted data from cloud services that implement backup functionalitystorages | is a binary exploitation analyst at JSC GTS. His competencies will be necessary to solve the main tasks of searching for authentication bypass methods in the OS code |
| 15 | **Amirov Ersultan Erbolovich** | military unit 01068, military |  | Executor  Digital Forensics Engineer  1. Review and analysis of similar solutions, technologies and methods used in forensic examination of password-protected digital electronic devices based on iOS and Android operating systems.  2. To create universal methods for overcoming security systems and gaining access to information on password-protected electronic digital devices within the framework of law enforcement activities and ensuring national security |  |
| 16 |  |  |  |  |  |
| 17 | **Kozhakhmet Zhaksylyk** |  |  | Software Engineer  1.Research of cloud solutions and their structures that implement the functionality of backup storage.  2.Creating an artificial intelligence model to automatically determine the rules for generating user authentication data  3.Creating an artificial intelligence model for password guessing using a dictionary from the results of social engineering research  4.Development of a software module for decrypting extracted data related to mobile applications, messengers and cloud services  5.Development of code for decrypting extracted data from cloud services implementing backup storage functionality | is a teacher at Astana IT University. Has experience in developing client-server and mobile applications. His skills will be applied in implementing tasks related to software development and its integration into the hardware of the APCS; |
| 18 | **Bizhanova Zhansaya Alimkyzy** |  |  | Project Manager  1. Monitoring the execution of tasks  2.Organizing meetings on the project  3. Meeting minutes  4. Receiving feedback from the customer | is an experienced project manager. During the project implementation, he will communicate between all employees, monitor the completion of tasks, and receive feedback from the customer. |
| 19 | **Vacancy** |  |  | Executor Binary Exploitation Analyst, Cryptographer |  |
| 20 | **Vacancy** |  | Accountant/lawyer/economist/buyer | Executor Accountant/Lawyer/Economist/buyer |  |

**6. Research environment**.

In connection with this task, the following list of researchers was formed:

**Justification of each performer's participation in the program based on their role, background and contribution to the achievement of the program's goal**

In connection with this task, the following list of researchers was formed:

**- A.K. Hikmetov** is the chief researcher, an expert in mathematical modeling, which is one of the key factors in the development of methods for accessing password-protected backups, mobile applications, messengers, cloud services and system settings of the Android operating system. When implementing this task, it is planned to use AI models, NER models, to study the social engineering of the facility. The participant's competencies will be useful in determining their own AI model, for the most accurate selection of possible correct options.;

**- Rzayeva L.G.** - executive officer, data analyst and system integrator, cryptographer, VNS. The competencies of this participant in the areas of data analysis, modeling, optimization and automation of processes by industry, engineering, development of AI models for solving various tasks, cryptography and authentication methods will be useful in implementing universal methods to overcome security systems and gain access to information on password-protected electronic and digital devices within the framework of law enforcement and ensuring national security;

**- Imanberdi A.E.** - has experience in implementing his own solutions for the tasks of the Ministry of Defense of the Republic of Kazakhstan and has professional international certificates in the field of information security, during which he acquired the skills necessary to implement tasks related to the study of algorithms for the functioning of encryption and decryption systems implemented in the Android mobile operating system and the development of methods for accessing password-protected backups, mobile applications, messengers, cloud services, and system settings of the Android operating system;

**- Myrzatai A.A**. is engaged in research on machine learning algorithms. His competencies are aimed at solving the following tasks: the study of implemented solutions for the analysis of digital evidence using artificial intelligence methods and the development of AI models to compile an optimized user's "dictionary" based on data from a given person's social networks.;

**- Konakbaev O.B.** is a specialist in hardware technologies and has the competence to solve the problems of developing the hardware of the PAK, integrating software into it, conducting pilot tests and developing methodological documentation on the use of a prototype of the agro-industrial complex.;

**- Tazhibayeva P.S., Grigoriev T., Pogolovkin D. and Shayakhmetov M.A.** are experts in the field of information security and developers of AI models in order to optimize the tasks of ensuring personal data protection and have excellent knowledge of data encryption and decryption methods.;

- **Baibusinov A.S., Niyazaliev K.A., Kurmangali E.S. and Amirov E.E.** are current specialists in digital forensics of the National Security Committee and can clearly describe current problems in this area, contribute to the development of methods and testing results, provide expert assessment and recommendations for improving the developed software;

- **Mohsen Guizani** is a professor with many years of experience, his research interests are focused on computer networks, cybersecurity, wireless and sensor networks, as well as cloud computing. In his research, he pays special attention to the protection of cloud technologies and intelligent networks, considering them in the context of computer security, which will greatly facilitate the team's work on developing algorithms and methods that solve the main purpose of the research.;

- **Satybaldina D.J.** has many years of experience in the field of modeling a cryptographic system for backup storage of confidential data in secure servers and the use of artificial intelligence methods to ensure cybersecurity of cellular communication networks. For many years, she headed the Department of Information Security at the L.N.Gumilyov ENU. Currently, she is the founder and head of the Information Security Research Institute and Cryptology at the L.N.Gumilyov ENU. She has established herself as one of the best experts in data encryption and decryption. In this project, her strongest competence is needed to decrypt files extracted from mobile devices.;

-**E. Nurdauletov** is an analyst for the binary operation of JSC GTS. His competencies will be necessary to solve the main tasks of finding methods for circumventing authentication in the OS code.;

- **Kozhakhmet J.** is a lecturer at Astana IT University. Has experience in developing client-server and mobile applications. His skills will be applied in the implementation of tasks related to software development and its integration into the hardware of the agro-industrial complex.;

**- Bizhanova J.A**. is an experienced project manager. During the implementation of the project, he will communicate between all employees, monitor the completion of tasks, and receive feedback from the customer.

The project also requires the support of specialists such as an economist, lawyer, buyer and accountant.

For the successful implementation of the program, the CyberTech Research Center and the Digital Forensic laboratory are being created on the basis of Astana IT University LLP, which ensures effective interaction between performers, coordination of their work and prompt decision-making.

The Digital Forensic Laboratory has a wide material and technical base that contributes to the effective implementation of cybersecurity programs. The center is equipped with modern devices for digital data analysis, tools for soldering and repairing microchips, as well as equipment for testing networks and communication devices.

Specialized equipment for working with data carriers plays a key role in the work of the laboratory. A set of adapters and adapters provides connection of hard and solid-state drives of various formats, including SATA, mSATA and M.2. Due to the possibility of full hardware write lock, data remains unchanged during their extraction and analysis. This hardware is compatible with popular operating systems, including Windows, macOS and Linux, which expands its applicability. In addition, ROG Strix SCAR 18 laptops are used, which provide sufficient computing power for complex analytical tasks.

The laboratory pays special attention to data extraction methods, including the physical "Chip-off" method. This approach allows you to work with damaged devices by soldering memory chips and restoring data even with significant damage. Soldering stations and auxiliary tools, including thermal sensors, scrapers, and chip holders, are used to perform such tasks. Additionally, specialized software is used for memory decoding and dump analysis.

The laboratory is also equipped with high-performance servers such as Supermicro and X13DEG-QT-P, which are used for storing and processing large amounts of data. These systems support graphical and video tasks, including machine learning and video analysis. Ubiquiti and D-Link switches are used to manage the network infrastructure, providing stable connectivity and high throughput.

FPGA-based FPGA boards, including Xilinx Artix-7 and Zynq-7000, are used for tasks related to programmable logic. These devices enable the development and testing of complex digital systems. Programmers such as Z3X Easy-JTAG and Medusa PRO II are also used to restore memory chips and processors in mobile devices.

Tools for repairing and modifying electronic devices are an important component of the laboratory. These include SUGON soldering stations, Soptop microscopes for detailed component analysis, and 3D printers for prototyping. Together, they create the conditions for performing complex engineering tasks.

In addition, the laboratory is equipped with devices for testing and calibrating mobile phones, such as JCID adapters and Aixun charging pads. This equipment is used to repair, restore, and test mobile devices, including Apple devices.

Thus, the material and technical base of the Digital Forensic laboratory allows performing a wide range of tasks: from data analysis and recovery to the development and testing of complex digital systems. It meets modern requirements in the field of computer expertise, providing opportunities for any kind of research.

**Material and technical base (Astana IT University):**

|  |  |  |
| --- | --- | --- |
| **№** | **Name** | **What is used for** |
| 1 | Server (Supermicro server chassis CSE-745BAC-R1K23B) | high-performance server for data processing and information storage |
| 2 | Сервер (X13 4U 4GPU, X13DEG-QT-P, 749TS-RNT1S) | GPU-enabled server for resource-intensive computing |
| 3 | Switch (Ubiquiti UniFi Switch PRO 48) | a managed switch for connecting to a local network |
| 4 | Switchboard (D-Link, DGS-1210-28P/FL1A) | PoE-enabled switch for network infrastructure |
| 5 | FPGA Board (Arty-7 A7-100T) | FPGA board for prototyping digital circuits |
| 6 | FPGA Board (Arty z7 20 (10)) | FPGA board with integrated ARM processor for embedded system development |
| 7 | Programmer (Z3X Easy-JTAG Plus Full Set) | a tool for working with memory chips and data recovery |
| 8 | FPGA Board (Genesys 2 Kintex-7 FPGA) | high-performance FPGA platform for digital device development |
| 9 | FPGA Board (Genesys ZU-5EV (ZU-3EG)) | FPGA board for working with video and audio signals |
| 10 | Programmer (Medusa PRO II Box) | flash memory recovery and programming device |
| 11 | USB cable (O.MG cable) | special USB cable with data transfer functions |
| 12 | Router (WIFI PINEAPPLE) | device for testing wireless networks for reliability |
| 13 | Portable Multifunction Device (USB RUBBER DUCKY) | keyboard simulation to automate attacks |
| 14 | O.MG UNBLOCKER | a device for bypassing blocking in networks |
| 15 | LAN TURTLE | a tool for network traffic interception and security testing |
| 16 | Bus Pirate v3.6a | a debugging device for interacting with various digital interfaces |
| 17 | HackRF One | software-defined radio receiver for signal analysis |
| 18 | Alfa Network Awus036Nha | high-frequency Wi-Fi adapter for testing the continuity of wireless networks |
| 19 | Pwnagotchi | an autonomous device for analyzing and attacking Wi-Fi networks |
| 20 | DSTIKE Deauther Watch V4S | a device for testing the security of a Wi-Fi network |
| 21 | Chameleon mini | RFID card analyzer and emulator |
| 22 | Ubertooth One | Bluetooth traffic analysis device |
| 23 | Hunter cat | compact equipment for wireless network auditing |
| 24 | USBKill V4 Kit | a tool for testing the health of USB ports |
| 25 | Server cabinet (Ship VE series) | secure server software storage |
| 26 | 3D Printer (CreatBot D600 Pro) | The furnace of prototypes and models |
| 27 | Microscope (Soptop 9 Microscope) | inspection of microcircuits and soldering |
| 28 | Soldering Station (SUGON T3602) | a tool for mounting electronic components |
| 29 | Hair Dryer (Sugon 8650 Hot Air Gun) | a tool for dismantling components on boards |
| 30 | Power Supply (RF-3005Pro DC Power Supply) | laboratory power supply for working with electronics |
| 31 | Screwdriver (Qianli Flyfish 2D Screwdriver) | precision screwdriver for electronics repair |
| 32 | Motherboard Holder (2UUL THE ONE JIG) | fixing the boards during the repair |
| 33 | Tin (60G Kailiwei Sealing Paste) | soldering paste for mounting components |
| 34 | Knife (Luowei K1 CPU Knife) | a tool for working with processors |
| 35 | Clamp (2UUL BH02 MINI JIG) | a lock for precise work with electronics |
| 36 | Tweezer (RELIFE RT-15D Ultra lightweight Precision tweezer) | precision tool for working with small components |
| 37 | Tweezer (RELIFE RT-11D Ultra lightweight Precision tweezer) | a similar tool for precision work |
| 38 | Flux (Amtech 559 Flux) | soldering enhancement tool |
| 39 | Scraper (TE-04 Scraper Phone Kailiwei 3 in1) | surface cleaning tool |
| 40 | Knifes (RELIFE RL - 050 Professional Opening Tools) | a set of tools for opening equipment |
| 41 | Glue (RELIFE T7000 Black) | adhesive for electronics repair |
| 42 | Programs (JCID V1S Pro Programs) | data recovery device |
| 43 | Adapter (JCID V1S 7-11 Pro Max Truetone adapter) | a tool for working with displays |
| 44 | Adapter (JCID V1S 12-14 Truetone adapter) | a similar tool for new models |
| 45 | Charging Panel (Aixun Dp20 Desktop Smart Fast Charger) | fast charging for devices |
| 46 | Interactive Display (Samsung Flip WM55R) | digital visualization panel |
| 47 | Soldering furnace (Reflow Oven RK320 "ProtoFlow S4") | heat treatment of boards |
| 48 | Mobile phones (Used Android phone) | digital forensics testing |
| 49 | Laboratory table | workplace of specialists |
| 50 | Laboratory cabinet | storage of tools |
| 51 | Server Cabinet (SHIP 601S.6615.24.100) | secure server software storage |
| 52 | Office printer (Epson L6490) | office printer for printing documents |
| 53 | Laptops (MacBook Pro 16.2" Apple M3 Max) | high-performance laptop for data analysis |
| 54 | A set of adapters and adapters | a set for connecting and locking recording drives |

The developed software and hardware complex (SHC) is the only domestic solution for conducting research in the field of digital forensics. It provides specialists with the opportunity to work both in the laboratory and directly at the scene of an accident.

The following tools are used as the customer's material base:

* R-Studio;
* Disk Drill;
* Mobile Forensics Expert Plus;
* UFED Cellebrite;
* Oxygen Detective;
* Passware Kit Ultimate;
* DVR Examiner.

At the testing stage, the developed APK will be used for comparative analysis with existing solutions. The tests will be conducted on two APCs with the same source device, which will allow an objective assessment of the effectiveness of the proposed approach.

1. **Justification of the requested financing**

The successful implementation of the project requires an integrated approach involving specialists from various scientific and practical fields, such as mathematics, statistics, big data analysis, cryptography, computer and electronic engineering, automated and automated systems, software development, and information security.

Given that a significant part of the work is aimed at solving problems related to constantly updated technologies, participation in events dedicated to the presentation of new technologies and solutions becomes an integral part of the research process. Attending international conferences will not only allow us to get an objective assessment of our results, but also to get acquainted with the developments of colleagues from other countries.

Publication of the results in scientific journals also plays a key role, since peer review and citation of the work by scientists from other countries provides a qualified assessment of the relevance and significance of the research. This is an important stage in the testing of the scientific component of the project.

For the successful implementation of the project, technical support is also necessary, including the study of methods of working with the hardware. In this regard, the cost item for the purchase of laboratory equipment is included in the calculations.

Since the project involves teamwork involving a large number of researchers, laboratory research, software development and other work, the cost of renting, operating and maintaining equipment and machinery is also an important factor in achieving the goals.

Summary calculation of the program (budget) according to table 2.

**Table 2** – Summary cost estimate for the requested amount

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Name of the expense item | The amount of financing, thousand tenge | | | |
| Total | Year 2025  (first year) | Year 2026  (second year) | Year 2027  (third year) |
| 1. | Remuneration (including taxes and other mandatory payments to the budget) | 387 475,040 | 99 059,360 | 143 591,040 | 144 824,640 |
| 2. | Business trips | 59 702,892 | 15 311,797 | 19 588,509 | 24 802,586 |
| 3 | Scientific and organizational support, other services and works | 65 957,267 | 39 494,900 | 18 322,847 | 8 139,520 |
| 4. | Purchase of materials (for individuals and legal entities), purchase of equipment and/or software (for legal entities) | 314 864,801 | 146 133,943 | 82 497,604 | 86 233,254 |
| 5. | Rental costs, operating costs of equipment and machinery used for the implementation of research | 72 000,000 | - | 36 000,000 | 36 000,000 |
| Total | | 900 000,000 | 300 000,000 | 300 000,000 | 300 000,000 |

At least 17 full-time and 4 part-time specialists will participate in the project.

3 vacancies were left for the positions of "Binary Exploitation Analyst, Cryptographer", "Cloud Technology Engineer" and "The Project office".

Table 3 – Wages (including taxes and other mandatory payments to the budget).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№** | **Full name** | **Position** | **Salary tenge** | | | | | | | | | | | | | |
| **1st year** | | | | **2nd year** | | | | | **3rd year** | | | | **Total (group.6×group.10×group.14)** |
| **Employment (full / part-time)** | **Monthly salary, tenge** | **Number of working months** | **Total (group.3×group.4×group.5)** | **Employment (full / part-time)** | **Monthly salary, tenge** | **Number** | **Total (group.3×group.4×group.5)** | **Employment (full / incomplete)** | | **Monthly salary, tenge** | **Number** | **Total (group.3×group.4×group.5)** |  |
| 1 |  | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | | 12 | 13 | 14 | **15** |
| ***1*** |  | ***Main Personnel of the Research Group*** | | | X | ***77 040 000*** |  |  | X | ***110 160 000*** |  | |  | X | ***110 160 000*** | ***297 360 000*** |
| 1.1 | Khikmetov Askar Kusupbekovich | Scientific Supervisor | **1** | **990 000** | **8** | **7 920 000** | **1** | **990 000** | **12** | **11 880 000** | **1** | | **990 000** | **12** | **11 880 000** | **31 680 000** |
| 1.2 | Rzayeva Leila Gummetovna | Responsible executive, Data Analyst and system integrator, Cryptographer, LRA | **1** | **900 000** | **8** | **7 200 000** | **1** | **900 000** | **12** | **10 800 000** | **1** | | **900 000** | **12** | **10 800 000** | **28 800 000** |
| 1.3 | Imanberdi Abilkair Yerboluly | Reverse engineer, cryptographer | **1** | **900 000** | **8** | **7 200 000** | **1** | **900 000** | **12** | **10 800 000** | **1** | | **900 000** | **12** | **10 800 000** | **28 800 000** |
| 1.4 | Nurdauletov Yerbol Tolevkanovich | Binary Exploitation Analyst, Cryptographic | 1 | **500 000** | 8 | 4 000 000 | 1 | **500 000** | 12 | 6 000 000 | 1 | | **500 000** | 12 | 6 000 000 | **16 000 000** |
| 1.5 | Myrzatay Ali | Machine Learning Algorithm Engineer, ORA | 1 | **500 000** | 8 | 4 000 000 | 1 | **500 000** | 12 | 6 000 000 | 1 | | **500 000** | 12 | 6 000 000 | **16 000 000** |
| 1.6 | Vacancy 1 | Binary Exploitation Analyst, Cryptographic | 1 | **500 000** | 8 | 4 000 000 | 1 | **500 000** | 12 | 6 000 000 | 1 | | **500 000** | 12 | 6 000 000 | **16 000 000** |
| 1.7 | Mohsen Guizani | Foreign scientific consultant | 1 | **600 000** | 8 | 4 800 000 | 1 | **600 000** | 12 | 7 200 000 | 1 | | **600 000** | 12 | 7 200 000 | 19 200 000 |
| 1.8 | Vacancy 2 | Cloud Technology Engineer | 1 | **600 000** | 8 | 4 800 000 | 1 | **600 000** | 12 | 7 200 000 | 1 | | **600 000** | 12 | 7 200 000 | 19 200 000 |
| 1.9 | Tazhibayeva Perizat | Information Security Engineer, RA | 1 | **380 000** | 8 | 3 040 000 | 1 | **380 000** | 12 | 4 560 000 | 1 | | **380 000** | 12 | 4 560 000 | **12 160 000** |
| 1.10 | Konakbayev Olzhas | Design Engineer | 1 | **500 000** | 8 | 4 000 000 | 1 | **500 000** | 12 | 6 000 000 | 1 | | **500 000** | 12 | 6 000 000 | **16 000 000** |
| 1.11 | Grigoryev Timur | Information Security Engineer, Laboratory Assistant, RA | 1 | **400 000** | 8 | 3 200 000 | 1 | **400 000** | 12 | 4 800 000 | 1 | | **400 000** | 12 | 4 800 000 | **12 800 000** |
| 1.12 | Kozhakhmetov Zhaksylyk | Software Engineer, RA | 1 | **300 000** | 8 | 2 400 000 | 1 | **300 000** | 12 | 3 600 000 | 1 | | **300 000** | 12 | 3 600 000 | **9 600 000** |
| 1.13 | Satybaldina Dina Zhagyparovna | Cryptographer, LRA | 1 | **900 000** | 8 | 7 200 000 | 1 | **900 000** | 12 | 10 800 000 | 1 | | **900 000** | 12 | 10 800 000 | **28 800 000** |
| 1.14 | Baibusinov A.S. | Digital Forensics Engineer | 0,5 | **450 000** | 8 | 1 800 000 | 0,25 | **450 000** | 12 | 1 350 000 | 0,25 | | **450 000** | 12 | 1 350 000 | **4 500 000** |
| 1.15 | Amirov E.E. | Digital Forensics Engineer | 0,5 | **450 000** | 8 | 1 800 000 | 0,25 | **450 000** | 12 | 1 350 000 | 0,25 | | **450 000** | 12 | 1 350 000 | **4 500 000** |
| 1.16 | Niyazaliev Kuandyk Altayuli | Digital Forensics Engineer | 0,5 | **450 000** | 8 | 1 800 000 | 0,25 | **450 000** | 12 | 1 350 000 | 0,25 | | **450 000** | 12 | 1 350 000 | **4 500 000** |
| 1.17 | Kurmangali Yelzhas | Digital Forensics Engineer | 0,5 | **450 000** | 8 | 1 800 000 | 0,25 | **450 000** | 12 | 1 350 000 | 0,25 | | **450 000** | 12 | 1 350 000 | **4 500 000** |
| 1.18 | Shayakhmetov Madi | Information Security Engineer, RA | 1 | **380 000** | 8 | 3 040 000 | 1 | **380 000** | 12 | 4 560 000 | 1 | | **380 000** | 12 | 4 560 000 | **12 160 000** |
| 1.19 | Pogolovkin Daniil | Information Security Engineer, RA | 1 | **380 000** | 8 | 3 040 000 | 1 | **380 000** | 12 | 4 560 000 | 1 | | **380 000** | 12 | 4 560 000 | **12 160 000** |
| ***2*** |  | ***Additional staff*** | | | X | ***8 800 000*** |  |  | X | ***13 200 000*** |  | |  | X | ***13 200 000*** | ***35 200 000*** |
| 2.1 | Bizhanova Zhansaya | Project Manager | 1 | **500 000** | 8 | 4 000 000 | 1 | **500 000** | 12 | 6 000 000 | 1 | | **500 000** | 12 | 6 000 000 | **16 000 000** |
| 2.2 | Project office | Accountant/lawyer/economist/buyer | 1 | 600 000 | 8 | 4 800 000 | 1 | 600 000 | 12 | 7 200 000 | 1 | | 600 000 | 12 | 7 200 000 | **19 200 000** |
| **3** |  | **Total salary fund (gr.1+gr.2)** | **X** | **X** | **X** | **85 840 000** | **X** | **X** | **X** | **123 360 000** | **X** | | **X** | **X** | **123 360 000** | **332 560 000** |
| **4** |  | **Taxes and other mandatory payments to the budget, (total gr.4.1+ gr.4.2+ gr.4.3)** | X | X | X | **13 219 360** | X | X | X | **20 231 040** | X | | X | X | **21 464 640** | **54 915 040** |
| 4.1. |  | Calculation of social tax expenses | X | X | X | 4 635 360 | X | X | X | 6 661 440 | X | | X | X | 6 661 440 | **17 958 240** |
| 4.2. |  | Calculation of expenses for the payment of social contributions to the State Social Insurance Fund | X | X | X | 3 862 800 | X | X | X | 5 551 200 | X | | X | X | 5 551 200 | **14 965 200** |
| 4.3. |  | Deductions for compulsory health insurance | X | X | X | 2 575 200 | X | X | X | 3 700 800 | X | | X | X | 3 700 800 | **9 976 800** |
| 4.1. |  | Mandatory employer pension contributions | X | X | X | 2 146 000 | X | X | X | 4 317 600 | X | | X | X | 5 551 200 | **12 014 800** |
| **Total (gr.3+ gr.4)** | | | X | X | X | **99 059 360** | X | X | X | **143 591 040** | X | | X | X | **144 824 640** | **387 475 040** |

Table 4 - Business trips

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | Destination (country, city, name of settlement) | Reimbursement rate for daily expenses per person (2 x monthly calculation index) (tenge) | Norm of expenses for renting residential premises per day per 1 person (tenge) | Average annual number of people/days for calculating daily expenses (person/days) | Average annual number of people/days to calculate the cost of renting residential premises (persons/days) | Average annual number of seconded people (persons) | Average cost of one round trip (tenge) | Amount of expenses (thousand tenge) (gr. 3 x gr. 5 + gr. 4 x gr. 6 + gr. 7 x gr. 8)/1000 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 1. | **2025 (1st year) total** | | | | | |  | **15 311, 797** |
|  |
| 1.1. | Chania, Crete, Greece (IEEE CSR 2025) August 4-6 | 44 000 | 101 750 | 28 | 16 | 4 | 823 620 | 6 154,480 |  |
| 1.2. | Salt Lake City, USA -July 24-31 | 53 100 | 138 060 | 42 | 27 | 3 | 1 066 499 | 9 157,317 |  |
| 2. | **2026 (2nd year) total** | | | | | |  | **19 588, 509** |  |
|  |
| 2.1. | Taipei, Taiwan, September 10-12 | 42 480 | 53 100 | 30 | 20 | 5 | 1 121 481 | 7 943,805 |  |
| 2.2. | Canada, Toronto August 18-31 | 53 100 | 79 650 | 56 | 52 | 4 | 1 132 326 | 11 644,704 |  |
| 3. | **2027 (3rd year) total** | | | | |  |  | **24 802, 586** |  |
|  |
| 3.1. | Canada, Toronto APRIL 1-10 | 53 100 | 79 650 | 52 | 40 | 4 | 1 258 769 | 10 982,276 |  |
| 3.2. | Defcon, Las Vegas, USA AUGUST 7-10 | 53 100 | 138 060 | 70 | 25 | 5 | 1 330 362 | 13 820,310 |  |
|  |  |  |  |  |  |  |  |  |  |
| **Total** (gr. 1 + gr. 2 + gr. 3) | | | | | | |  | **59 702,892** |  |

Table 4 “Planned business trips” reflects the list of foreign trips necessary for the implementation of the project, including participation in international conferences, internships and scientific events. Business trips are planned for 2025–2027 and include trips to Greece (IEEE CSR 2025), USA (Salt Lake City, Las Vegas, Defcon), Taiwan, Canada (Toronto). Teams are composed of researchers involved in the project, taking into account the optimal number of participants to achieve scientific goals. Business trips provide presentation of research results, exchange of experience and advanced training of specialists, which contributes to the successful implementation of the project. A total of 25 people will take part in international business trips, and the total budget for these trips will be 59,702,892 tenge.

Participation in conferences, exhibitions, scientific seminars

1. Participation in the IEEE International Conference on Cyber ​​Security and Resilience (IEEE CSR) (http://ieee-csr.org/) is an important part of scientific and research activities aimed at studying and implementing advanced cybersecurity techniques. The conference provides a unique opportunity to get acquainted with the latest scientific developments, innovative solutions and best practices in the field of protecting digital systems.

The relevance and significance of participation is due to the fact that IEEE CSR is one of the leading international conferences covering key aspects of cyber resilience, including:

• Detection and prevention of cyber threats,

• Methods for protecting critical systems,

• Cryptographic technologies and their applications,

• Artificial intelligence in the field of information security,

• Attacks and defense mechanisms in communication networks.

Participation in the conference will allow you to gain access to the latest research, establish cooperation with international colleagues and present the results of your own scientific work on the world stage.

2. Participation in the Digital Forensics Summit 2025 (https://www.sans.org/cyber-security-training-events/digital-forensics-summit-2025/), organized by the SANS Institute, is a key event for digital forensics and cybersecurity professionals. The summit offers a unique opportunity to explore modern techniques for investigating cyber attacks, analyzing malware and recovering data after incidents.

The relevance and significance of participation is due to the fact that digital forensics plays a decisive role in identifying attacks, collecting evidence and ensuring the security of information systems. And the SANS summit is dedicated to key areas affecting this research:

• Modern methods of digital forensic analysis,

• Investigation of cybersecurity incidents,

• Memory, network traffic and malware analysis techniques,

• Automation of digital forensics processes,

• Practical cases of investigating complex attacks.

Participation in the event will allow you to study new technologies and methods, as well as establish interaction with international experts and researchers in this field.

The requested funds are necessary to cover the following expenses:

Registration fee - includes access to all scientific sections, plenary sessions and publication of an article in the conference collection.

Transport costs – flight to the conference venue and transfer within the city.

Accommodation – accommodation in a hotel near the conference venue.

Daily expenses – food and transportation expenses during the stay.

All calculated data are based on the cost of tickets and accommodation obtained from open sources, such as www.aviata.kz (air tickets) and www.booking.com (hotel).

Participation in IEEE CSR 2025, Defcon (USA) and internship at the SANS Institute is critical to improve the scientific level of the research group, exchange experience with international experts and present the results on the global stage. The IEEE CSR 2025 (International Conference on Cyber ​​Security and Resilience) conference is dedicated to current challenges in cybersecurity and digital forensics, which corresponds to the key areas of the project. Attending Defcon, one of the largest hacker conferences, will allow the team to learn best practices for identifying vulnerabilities and testing security systems. An internship at the SANS Institute will provide access to the world's leading practitioners in the field of digital investigations and cyber defense, which will contribute to the development of the team's competencies.

**Table 5** – Scientific and organizational support, other services and work

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Designation | A unit of measurement | Quantity, units | Cost per unit, tenge | Total cost, tenge (gr.4 × gr.5) |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 2025 (1st year), total |  |  |  | 39 494 900,00 |
| 1.1. | Registration fee for participation in the conference at IEEE CSR 2025 | article | 2 | 866 250,00 | 1 732 500,00 |
| 1.2. | Registration fee for internship at SANS Institute | article and certificate of participation | 4 | 4 565 600,00 | 18 262 400,00 |
| 1.3. | Organization of CTF and Hackathon competitions | competition service | 1 | 3 500 000,00 | 3 500 000,00 |
| 1.4. | A service for collecting and annotating a data set and further synthetically generating data for training AI models. | Providing data collection services | 2 | 5 000 000,00 | 10 000 000,00 |
| 1.5. | Service for implementation, configuration and maintenance of vector database software and monitoring tools aimed at optimizing the operation of machine learning models and ensuring their performance. | Service for implementation, configuration and maintenance of software | 1,00 | 6 000 000,00 | 6 000 000,00 |
| 2 | 2026 (2nd year), total |  |  |  | 18 322 847,00 |
| 2.1. | Payment for publication in the scientific journal IEEE Access | article | 3 | 1 101 825,00 | 3 305 475,00 |
| 2.2. | Payment for publication in NAS RK | article | 3 | 40 000,00 | 120 000,00 |
| 2.3. | Organization of CTF and Hackathon competitions | competition service | 2 | 3 500 000,00 | 7 000 000,00 |
| 2.4. | Service for “Source code analysis” of developed software modules for implementation | service | 1 | 7 897 372,00 | 7 897 372,00 |
| 3 | 2027 (3rd year), total | X | X |  | 8 139 520,00 |
| 3.1. | Registration fee for participation in the Defcon conference, Las Vegas, USA | article | 4 | 254 880,00 | 1 019 520,00 |
| 3.2. | Payment for publication in NAS RK | article | 3 | 40 000,00 | 120 000,00 |
| 3.3. | Organization of CTF and Hackathon competitions | competition service | 2 | 3 500 000,00 | 7 000 000,00 |
| Total (column 1 + group 2 + group 3), tenge | | X | X |  | 65 957 267,00 |

Publishing our articles in IEEE Access and COKNVO journals provides several key benefits that align with our program goals and enhance our professional reputation. IEEE Access® is a multidisciplinary, fully electronic, archival, practice-oriented, open access (OA) journal that continuously publishes original research and development in all areas of interest to IEEE. IEEE Access publishes articles of high interest to readers that are original, technically correct, and clear. The magazine provides a high level of credibility and recognition for our work. Publication here means that our research has been thoroughly peer-reviewed and meets high scientific standards.

Confirmation links:

1. https://journals.nauka-nanrk.kz/physics-mathematics/payment 40,000 tenge;

2. https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6287639 866,250.00 tenge

Also included in the expense item are cost items for services:

• for collection and annotation of the data set and further synthetic generation of data for training AI models - a total of 10,000,000 tenge

• for implementation, configuration and maintenance of vector database software and monitoring tools aimed at optimizing the operation of machine learning models and ensuring their performance – 6,000,000 tenge

• for “Source code analysis” of developed software modules for implementation - 7,897,372 tenge

CTF and Hackathon organization

As part of this project, it is planned to hold large CTFs and Hackathons for technical students. These activities will include challenges developed within the project, with the goal of shaping the next generation of researchers and generating creative solutions. As a result, it is planned to involve these students in the project.

Organizational and promotional materials:

● The banner will be used to advertise events, which will attract more participants and increase awareness of the project.

● The bags will be used to distribute promotional materials and swag to participants to help promote the event.

● Stickers with the project logo for distribution among participants and spectators; badges for members to create an atmosphere of unity and professionalism.

Materials for participants and organizers:

● Badges for identifying participants and organizers at events.

● Pens with logo for participants and organizers.

● Notebooks for participants to take notes and notes during events.

Cash awards for winners to motivate participants for high achievements.

Organize coffee breaks for participants and organizers to maintain high energy levels and networking.

T-shirts with logo for participants and organizers.

The total amount for holding one competition is 3,500,000 tenge, a total of 5 are planned for three years (a total of 17,500,000 tenge), which covers all the necessary expenses for the successful implementation of the project’s activities. This includes organizing the CTF and Hackathon, providing necessary materials to participants and organizers, and providing all logistical and operational needs.

**Table 6** – Purchase of materials, equipment and (or) software (for legal entities)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Designation** | **A unit of measurement** | **Quantity, units** | **Cost per unit, tenge** | **Total cost, tenge (gr.4 × gr.5)** |
| 1 | 2 | 3 | 4 | 5 | 6 |
| **1** | **2025 (1st year), total** |  |  |  | **146 133 943,00** |
| 1.1. | 1x Server SuperMicro SYS-421GE-TNRT  2x P4X-EMR6530-SRN5C-XCC  16x MEM-DR532MD-ER48  1x AOC-S3916L-H16IR-32DD-O  2x HDS-25T0-480G0-L2-TXD-NON-007  4x HDS-25T0-007T6-L2-TXD-NON-007  1x BTR-CVPM05 | Thing | 1 | 20200000 | 20 200 000,00 |
| 1.2. | Video card NVIDIA H100 NVL GPU 94GB PCI 5.0 | Thing | 4 | 30000000 | 120 000 000,00 |
| 1.3. | KEHUA rack-mount UPS,  KR6000L-J+, 6kVA + Battery pack  for UPS KEHUA, KR6000L-J+ for 15  minutes | Thing | 1 | 1800000 | 1 800 000,00 |
| 1.4. | Cabinet SHIP, 601S.8242.24.100, 124 series,  19'' 42U, 800\*1200\*2000 mm, W\*D\*H | Thing | 1 | 420000 | 420 000,00 |
| 1.5. | Used mobile phones on Android OS | Thing | 20 | 164297,15 | 3 285 943,00 |
| 1.6. | Switch with Ubiquiti Layer 3 switch  (48) GbE RJ45 ports and (4) 10G SFP+  ports. | Thing | 1 | 428000 | 428 000,00 |
| **2** | **2026 (2nd year), total** |  |  |  | **82 497 604,00** |
| 2.1. | 1x Server SuperMicro SYS-421GE-TNRT  2x P4X-EMR6530-SRN5C-XCC  16x MEM-DR532MD-ER48  1x AOC-S3916L-H16IR-32DD-O  2x HDS-25T0-480G0-L2-TXD-NON-007  4x HDS-25T0-007T6-L2-TXD-NON-007  1x BTR-CVPM05 | Thing | 1 | 20200000 | 20 200 000,00 |
| 2.2. | Video card NVIDIA H100 NVL GPU 94GB PCI 5.0 | Thing | 1 | 30000000 | 30 000 000,00 |
| 2.3. | KEHUA rack-mount UPS,  KR6000L-J+, 6kVA + Battery pack  for UPS KEHUA, KR6000L-J+ for 15  minutes | Thing | 1 | 1800000 | 1 800 000,00 |
| 2.4. | Cabinet SHIP, 601S.8242.24.100, 124 series,  19'' 42U, 800\*1200\*2000 mm, W\*D\*H | Thing | 1 | 420000 | 420 000,00 |
| 2.5. | Switch with Ubiquiti Layer 3 switch  (48) GbE RJ45 ports and (4) 10G SFP+  ports. | Thing | 1 | 428000 | 428 000,00 |
| 2.6. | Server CHECK TALINO KA-Ultra Server 32 HDDs, 20TBHDDs640TB RAW Space | Thing | 1 | 19816720 | 19 816 720,00 |
| 2.7. | Mac Forensics (Tallino) | Thing | 1 | 9 832 884,00 | 9 832 884,00 |
|  | **2027 (3rd year), total** |  |  |  | **86 233 254,00** |
| 3.1. | Video card NVIDIA H100 NVL GPU 94GB PCI 5.0 | Thing | 2 | 30000000 | 60 000 000,00 |
| 3.2. | Cyber ​​polygon | Thing | 1 | 26 233 254,00 | 26 233 254,00 |
|  | Total (column 1 + group 2 + group 3), tenge |  |  |  | **314 864 801,00** |

Purchase of materials, equipment and (or) software (for legal entities)

To implement a project related to computer forensics, a high-performance server infrastructure and related equipment are required. The system will be based on the SuperMicro SYS-421GE-TNRT server with P4X-EMR6530 processors and MEM-DR532MD RAM, which will provide computing power for analyzing large volumes of data. Storage based on NVMe disks (HDS-25T0) will allow you to process data with minimal delays, and the use of NVIDIA H100 NVL GPU will provide performance for machine learning and analysis tasks.

For stable power supply to the system, a KEHUA KR6000L-J+ UPS with a battery pack is provided, which will prevent data loss during failures. The SHIP 124 Series server cabinet will provide compact and secure storage of equipment, and the Ubiquiti Layer 3 switch will improve network connectivity with high-speed ports.

All components are selected to ensure reliability, performance and extensibility, which are critical to the success of the scientific tasks and data analysis of the project. In total, over three years it is planned to spend 314,864,801.00 tenge.

Server and components:

• SuperMicro SYS-421GE-TNRT Server: Selected due to its high scalability, allowing you to add additional processors and graphics accelerators to speed up the brute force process.

• P4X-EMR6530-SRN5C-XCC processors: Provide high performance for parallel computations required to brute force large numbers of password combinations.

• Memory MEM-DR532MD-ER48: Sufficient RAM will allow you to store large password dictionaries and intermediate calculation results in memory, speeding up the process.

• Network card AOC-S3916L-H16IR-32DD-O: Provides high speed data transfer between the server and other devices, which is important when working with large amounts of data.

• Disks: Allows you to store source data, password dictionaries, as well as brute force results. It is recommended to use high-speed SSD drives to speed up read and write operations.

NVIDIA H100 NVL GPU 94GB PCI 5.0: The GPU is ideal for accelerating floating point calculations, which are often used in brute force algorithms. It allows you to process multiple tasks in parallel, significantly increasing the speed of password retrieval

UPS KEHUA KR6000L-J+: Will ensure uninterrupted operation of the system during power outages, which is especially important during long-term brute force processes.

SHIP cabinet: Protects equipment from dust, overheating and mechanical damage.

Ubiquiti Switch: Provides a reliable network connection between the server and other devices.

Mac Forensics (Tallino) is a set of hardware and software optimized for digital forensics on Apple devices.

As part of the project, it is planned to acquire a cyber polygon —a specialized testing complex(polygon) designed for simulating cyberattacks, analyzing network vulnerabilities, and testing digital forensics methods. This cyber polygon will enable the study of locked electronic-digital devices in conditions close to real-world scenarios, the development and testing of new data processing algorithms, and the improvement of strategies for detecting and preventing cyber threats.

The cyber polygon is a physical model with emulated infrastructures across various sectors, including energy, transportation, finance, government institutions, and industrial facilities. It is equipped with controllers, sensors, and management systems, allowing for experiments in cybersecurity, malware analysis, and data recovery. The implementation of this complex will provide a secure testing environment for training specialists and validating advanced digital forensics technologies.

The use of the cyber polygon in the project will not only enhance the efficiency of research but also create a platform for training and upskilling cybersecurity professionals. The development and testing of new methods for analyzing digital storage devices under real-world threat conditions will contribute to improving the security of digital infrastructure and the advancement of innovative solutions for investigating cybersecurity incidents.

**Table 7** – Rental costs, operating costs of equipment and machinery used to carry out research

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №  n/p | Designation | A unit of measurement | Unit price, tenge | Quantity, units | Total, tenge  (gr.4 x gr.5) |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 1. | 2025 (1st year), total |  |  |  | **0** |
| 1.1. | Renting office space for long-term computing processes | month | 3 000 000 | 0 | 0 |
| 2. | 2026 (2nd year), total | X | X |  | **36 000 000** |
| 2.1. | Renting office space for long-term computing processes | month | 3 000 000 | 12 | 36 000 000 |
| 3. | 2027 (3rd year), total | X | X |  | **36 000 000** |
| 3.1. | Renting office space for long-term computing processes | month | 3 000 000 | 12 | 36 000 000 |
| Total (gr.1 + gr.2 + gr.3) | | X | X |  | **72 000 000** |

Operating costs of equipment and machinery used to implement research for 2025-2027 include the rental of office space for long-term computing processes. Such premises will be rented from 2026 for 24 months and a total cost of 72,000,000 tenge. The need for such costs is due to ensuring the fault tolerance of long-term computing operations by the server infrastructure to solve the scientific and practical problems assigned to the project. In case of failures, computational operations will be carried out again to level out potential errors and random operations. These premises will provide uninterrupted power and the necessary climate zone to maintain the server infrastructure in optimal working condition.

**8. Program implementation plan**

The project aims to develop and implement advanced digital forensics techniques that ensure efficient extraction, decryption and analysis of data from secure electronic devices. The focus is on mobile devices, DVRs, cloud services, and other digital media.

The work will explore existing encryption methods, identify vulnerabilities, and develop tools for data analysis and recovery. The project covers the development of both software and hardware solutions, as well as the creation of a scientific and methodological base.

The project will consist of the main stages, as shown in the Gantt chart.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Year** | **2025** | | | | **2026** | | | | **2027** | | | | |
| **Project Phases** | **Phase 1** | | | | **Phase 2** | | | | **Phase 3** | | | | |
| **Quarter** | **Q1** | **Q2** | **Q3** | **Q4** | **Q1** | **Q2** | **Q3** | **Q4** | **Q1** | **Q2** | **Q3** | **Q4** |
| Analysis of existing solutions |  |  |  |  |  |  |  |  |  |  |  |  |
| Review and analysis, purchase of necessary equipment |  |  |  |  |  |  |  |  |  |  |  |  |
| Research of existing algorithms and development of theoretical models |  |  |  |  |  |  |  |  |  |  |  |  |
| Development of software and hardware solutions |  |  |  |  |  |  |  |  |  |  |  |  |
| Testing and optimization |  |  |  |  |  |  |  |  |  |  |  |  |
| Data monitoring and analysis |  |  |  |  |  |  |  |  |  |  |  |  |
| Interacting and cooperation |  |  |  |  |  |  |  |  |  |  |  |  |
| Risk management and quality assurance |  |  |  |  |  |  |  |  |  |  |  |  |
| Intellectual property management |  |  |  |  |  |  |  |  |  |  |  |  |
| Presentation of the final result and delivery of all development on the project |  |  |  |  |  |  |  |  |  |  |  |  |

More detailed planning of work on the implementation of specific research and engineering tasks is presented in Table 8.

**Table 8** - Implementation work plan

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №  n/p | We  of tasks and measures for their implementation | Period of execution | | Expected results of the project (in terms of tasks and activities), form of completion |
| Start  (month) | Finish  (month) |  |
| 2025 year | | | | |
| 1 | Review and analysis of similar solutions, technologies, and methods used in the forensic investigation of password-protected electronic and digital devices based on the iOS and Android operating systems. | 05.2025 | 12.2025 | An analysis of existing solutions and technologies for the forensic examination of electronic and digital devices protected by a password will be carried out. Completion form: an analytical report containing a comparative analysis of solutions. |
| 1.1 | Research of algorithms for the functioning of encryption and decryption systems implemented in the Android mobile operating system. | 05.2025 | 12.2024 | An analysis of encryption and decryption algorithms in Android will be conducted. Completion form: a report with a technical description of the protection mechanisms. |
| 1.2 | Research of the implementation of basic authentication methods used in mobile phones and tablets. | 05.2025 | 12.2024 | Authentication mechanisms in mobile devices will be studied. Completion form: an analytical report with a classification of authentication methods. |
| 1.3 | Research into the vulnerabilities of security systems in different versions of the studied operating systems (Windows, Android, IOS) | 05.2025 | 12.2024 | An analysis of vulnerabilities in the protection systems of various versions of operating systems will be conducted. Completion form: a report with identified vulnerabilities and proposed protection measures. |
| 1.4 | Research of the functions of smartphones based on Android and IOS, implementing additional measures of protection of smartphones (blocking the device for an indefinite period of time if several incorrect passwords are entered). | 05.2025 | 12.2025 | An analysis of additional protection mechanisms for smartphones will be performed. Completion form: a report with a detailed description of the protection mechanisms. |
| 1.5 | Research of cloud solutions and their structures that implement the functionality of backup storage. | 05.2025 | 12.2025 | The architecture of cloud storage and its protection mechanisms will be studied. Completion form: technical report with analysis and recommendations. |
| 1.6 | Research of algorithms and methods for bypassing the protection of mobile applications and instant messengers using binary exploitation techniques. | 05.2025 | 12.2025 | An analysis of binary exploitation methods to bypass mobile application protection will be conducted. Completion form: technical report with identified methods and protection proposals. |
| 1.7 | Research of algorithms and methods for automatic decryption of encrypted authentication data used in the systems under study. | 05.2025 | 12.2025 | The process of automatic decryption of authentication data will be studied. Completion form: analytical report describing possible approaches. |
| 2 | Creating an artificial intelligence model for automatically determining the rules for generating user authentication data | 05.2025 | 12.2025 | An artificial intelligence model will be created to automatically determine the rules for generating user authentication data. |
| 2026 year | | | | |
| 3 | To create universal methods for overcoming security systems and gaining access to information on password-protected electronic digital devices within the framework of law enforcement and national security | 01.2026 | 12.2026 | A set of universal methods will be developed that will allow for the effective bypass of protective mechanisms of electronic digital devices, including mobile phones, tablets and other gadgets. Completion form: Preparation of methodological recommendations for law enforcement agencies, development of tools for automated analysis and testing of methods on various versions of operating systems. |
| 3.1 | Development of instructions for searching for vulnerabilities in security systems in different versions of the operating systems under study | 01.2026 | 12.2026 | A detailed instruction will be prepared, including modern methods of searching for vulnerabilities in Windows and Android security systems. Completion form: Development of methodological materials containing a classification of vulnerabilities, a description of possible attacks and recommendations for their use in forensic practice. |
| 3.2 | Development of a method for automatic decryption of encrypted authentication data used in the systems under study | 01.2026 | 12.2026 | An automatic decryption method will be created that allows encrypted credentials to be restored without direct interaction with the user. Completion form: Preparation of a report with the algorithms of the method, its practical implementation in the form of a software module and recommendations for use in investigative activities. |
| 4 | Building a dictionary-based password guessing AI model from social engineering research | 01.2026 | 12.2026 | An artificial intelligence model of password guessing will be created using a dictionary from the results of social engineering research. |
| 5 | Develop methods for accessing password-protected backups, mobile applications, instant messengers, cloud services, and system settings of the Android operating system. | 01.2026 | 12.2026 | Methods will be developed that will allow for efficient extraction of data from protected backups and applications, even when the encryption system is enabled. Completion form: Creation of instructions for using the methods, development of software tools and their testing on various device models. |
| 5.1 | Development of a method for decrypting extracted data related to mobile applications, messengers and cloud services | 01.2026 | 12.2026 | A method for decrypting data extracted from mobile applications and cloud services will be developed and tested. Completion form: Preparation of a detailed report on the method, its practical application and the results of testing on real data. |
| 5.2 | Developing a method to bypass protection of mobile applications and messengers using binary exploitation techniques | 01.2026 | 12.2026 | New methods of bypassing the protection mechanisms of mobile applications and messengers using binary analysis techniques will be researched and implemented. Completion form: Creation of an experimental prototype, a detailed report with attack examples, analysis of possible countermeasures and application scenarios within the framework of forensics. |
| 5.3 | Development of a method for decrypting extracted data from cloud services that implement the functionality of a backup storage | 01.2026 | 12.2026 | The data storage mechanisms in cloud services will be investigated and a method for their decryption will be developed. Completion form: Preparation of an analytical report, creation of a working decryption algorithm and its testing on real cloud storages. |
| 5.4 | Development of a method for extracting data from cloud services that implement the functionality of a backup storage | 01.2026 | 12.2026 | A method for efficient extraction of data from cloud storage, including encrypted files and backups, will be created. Completion form: Development of a prototype software tool, description of the methodology and its testing on common cloud platforms. |
| 5.5 | Developing methods for accessing password-protected backups, mobile applications, instant messengers, cloud services, and system settings of the Android operating system | 01.2026 | 12.2026 | Effective methods will be developed to gain access to protected backups, mobile applications, cloud services and Android system settings, bypassing standard authentication mechanisms. Completion form: Preparation of methodological recommendations, development of a test software solution and its testing on various versions of Android. |
| 6 | Preparation and submission of scientific articles on the developed methods of automatic decryption of encrypted authentication data used in the studied systems and the results of the work of the artificial intelligence model of password selection using the dictionary of social engineering | 01.2026 | 12.2026 | Three articles will be published in journals recommended by the SAHEQAC |
| 7 | Preparation and submission of scientific articles on the developed methods of access to password-protected backups, mobile applications, messengers, cloud services and system settings of the Android operating system | 01.2026 | 12.2026 | **Two** articles will be published in peer-reviewed scientific journals in the scientific field of the program, included in the 1st (first), 2nd (second) and/or 3rd (third) quartile of impact factor in the Web of Science database and/or having a CiteScore percentile in the Scopus database of at least 50 (fifty). |
| 8 | Application for intellectual property rights and submission of materials | 01.2026 | 12.2026 | **Two** intellectual property objects (patent; for applications in the field of information technology - copyright certificate) registered at the National Institute of Intellectual Property of the Republic of Kazakhstan will be obtained. |
| 9 | Hardware development of the Software Hardware Complex | 01.2026 | 12.2026 | Engineering and design work will be carried out to develop modules that ensure the implementation of the developed methods. Completion form: a prototype package with a functional and logical diagram of the interaction of all hardware components. |
| 2027 year | | | | |
| 10 | Implement a function in the form of executable code that provides administrative rights to the Android file system while preserving user data. | 01.2027 | 11.2027 | An executable code will be developed to obtain administrative privileges without losing user data. Completion form: software module with documentation. |
| 10.1 | Develop a prototype | 01.2027 | 11.2027 | A prototype of a solution for forensic analysis of protected devices will be created. Completion form: demo sample with documentation. |
| 10.2 | Development of a software module for decrypting extracted data related to mobile applications, messengers and cloud services | 01.2027 | 11.2027 | A software module for automatic data decryption will be created. Completion form: software and user manual. |
| 10.3 | Development of a software module for protecting mobile applications and instant messengers using binary exploitation techniques | 01.2027 | 11.2027 | A security module will be created to prevent binary attacks. Completion form: software module with technical documentation. |
| 10.4 | Developing code for decrypting extracted data from cloud services that implement backup storage functionality | 01.2027 | 11.2027 | A software tool will be created for automatic decryption of data obtained from cloud services. Completion form: Testing the tool on various cloud platforms, preparing methodological recommendations for its use. |
| 10.5 | Development of a software module for extracting data from cloud services, implementing the functionality of a backup storage | 01.2027 | 11.2027 | A specialized software module will be created for automated extraction of information from cloud storage, including encrypted data. Completion form: Preparation of technical documentation, testing on popular cloud platforms and creation of instructions for use in the field of digital forensics. |
| 10.6 | Development of software modules for access to password-protected backups, mobile applications, messengers, cloud services and system settings of the Android operating system | 01.2027 | 11.2027 | A set of software modules will be developed that will allow access to password-protected data in mobile devices and cloud services, as well as analyze them. Completion form: Development of a prototype of the software package, its testing on various versions of Android, and preparation of methodological materials for law enforcement agencies. |
| 10.7 | Conduct pilot tests, collect and analyze data to record the actual technical and functional characteristics of the prototype and make adjustments if necessary | 01.2027 | 11.2027 | The prototype will be tested and adjusted. Completion form: Testing and performance analysis report. |
| 11 | Design and submission of monograph materials | 01.2027 | 11.2027 | **One** monograph will be published in foreign and (or) Kazakhstani publishing houses recommended by the Academic Council and (or) the scientific and technical council of the applicant's organization. |
| 12 | Preparation and submission of scientific articles on the developed methods of decryption of extracted data related to mobile applications, messengers and cloud services and protection of mobile applications and messengers using binary exploitation techniques | 01.2027 | 11.2027 | **Three** articles will be published in journals recommended by the SAHEQAC |
| 13 | Develop methodological documentation for the use of a prototype | 01.2027 | 11.2027 | A guide to using the developed solution will be compiled. Completion form: methodological documentation. |
| 14 | Preparation and submission of scientific articles on all developed methods | 01.2027 | 11.2027 | **One** articles will be published in peer-reviewed scientific journals in the scientific field of the program, included in the 1st (first), 2nd (second) and/or 3rd (third) quartile of impact factor in the Web of Science database and/or having a CiteScore percentile in the Scopus database of at least 50 (fifty). |

**Stage 1.** Analysis of existing solutions in the field of digital forensics

The first stage analyzes existing technologies in the field of digital forensics, including encryption methods, data storage systems, and authentication mechanisms. Special attention is paid to the study of cryptographic algorithms, principles of operation of encryption systems on mobile devices and in cloud services. At the same time, possible vulnerabilities and methods of their exploitation are being analyzed, including ways to circumvent protection, attacks on passwords and decryption mechanisms for encrypted data. The results of this stage will allow us to identify promising areas for further development and set the vector of work at the next stages of the project.

**Stage 2.** Development of software and hardware solutions

As part of the second stage, software and hardware tools are being developed for the forensic analysis of secure devices and cloud services. The software part includes the creation of secure data decryption algorithms, password selection tools, and methods for bypassing standard security mechanisms. The hardware is developing devices that allow access to data from locked mobile phones, tablets, and other digital media without damaging information. The completion of the stage involves the initial testing of solutions on various device models and operating systems.

**Stage 3.** Testing and optimization

At the third stage, a comprehensive health check of the developed solutions is carried out. During testing, decryption algorithms, password selection, and security circumvention methods are analyzed, and their accuracy, performance, and resilience to various attack scenarios are evaluated. Hardware solutions are tested for compatibility with different models of mobile devices, and the correctness of data extraction is checked without violating their integrity. Based on the data obtained, software and hardware tools are optimized, algorithms are adjusted, and identified deficiencies are eliminated.

**Stage 4.** Preparation of documentation and scientific publications

During this stage, instructions on how to use the developed solutions, methodological recommendations and technical documentation are created. Manuals for specialists in the field of digital forensics are being prepared, describing in detail how to work with the created tools. In parallel, scientific articles on the developed methods of data analysis are being prepared and published in peer-reviewed scientific journals. This stage plays a key role in the formation of a scientific base for the further development of the project and the dissemination of acquired knowledge in the professional community.

**Stage 5.** Patenting and intellectual property protection

At this stage, patents for the created technologies are being registered, as well as copyright applications are being filed. The patenting procedure includes the protection of both software algorithms and hardware solutions, which allows for the legal protection of developments and their further commercialization. Work is underway to formalize intellectual property and define strategies for using the developments obtained for research and commercial purposes.

**Stage 6.** Implementation of the developed solutions

The sixth stage is devoted to the integration of the developed tools into practical activities. The solutions are being adapted for use in law enforcement agencies, expert laboratories, and commercial organizations involved in information security. Training programs for specialists are being created, test trials and refinement of software tools are being organized, taking into account the practical needs of users. In parallel, work is underway to develop interfaces for the convenience of specialists and integration with existing forensic systems.

**Stage 7.** Technology support and further development

The final stage of the project includes long-term support of the developed solutions, their updating and adaptation to new challenges. Current threats are being analyzed, data analysis and decryption methods are being improved, and software updates are being developed. In parallel, user support is provided, consultations and recommendations on the use of tools are provided. Work is underway to improve existing algorithms and create new models for more effective forensic examination of digital data.

The project covers the entire development cycle, from basic research to practical implementation and implementation in various fields. Such an integrated approach will not only create effective tools for digital forensics, but also ensure their relevance and relevance in the long term.

**9. Expected program results**

According to the results of the program, the following results should be obtained::

- a review and analysis of similar solutions, technologies, and methods used in the forensic investigation of password-protected electronic and digital devices based on the iOS and Android operating systems has been performed;

- universal methods have been created to overcome security systems and gain access to information on password-protected electronic and digital devices within the framework of law enforcement and national security;

- algorithms for the functioning of encryption and decryption systems implemented in the Android mobile operating system have been studied;

- methods of access to password-protected backups, mobile applications, messengers, cloud services and system settings of the Android operating system have been developed;

- implemented a function in the form of executable code that ensures obtaining administrative rights to the Android file system while preserving user data;

- a prototype has been developed;

- pilot tests, data collection and analysis were carried out to record the actual technical and functional characteristics of the prototype and make adjustments if necessary.;

- methodological documentation on the use of the prototype has been developed;

**As a result of the implementation of the program, the following should be published:**

1) at least 3 (three) articles and (or) reviews in peer-reviewed scientific publications in the scientific field of the program, included in the 1st (first), 2nd (second) and (or) 3rd (third) quartile of the impact factor in the Web of Science database and (or) having a percentile of CiteScore has at least 50 (fifty) in the Scopus database.

2) at least 5 (five) articles in the journals recommended by the COKNVO.

3) at least 1 (one) monograph or textbook in foreign and (or) Kazakhstani publishing houses recommended by the academic council and (or) the scientific and technical council of the applicant's organization;

4) at least 2 (two) objects of intellectual property (patent; for applications in the field of information technology - copyright certificate) registered at the National Institute of Intellectual Property of the Republic of Kazakhstan.

The end result:

Scientific and technical effect: as a result of the implementation of the scientific and technical program, innovative technologies should appear in the form of software complexes for the study of locked electronic and digital devices, including using artificial intelligence methods in separate modules.

The scientific effect is expressed in the creation of new methods and algorithms for automatically bypassing the protection of authentication of operating systems based on the search for vulnerabilities using binary exploitation methods.

The economic effect of the implementation of this project is due to the creation and development of domestic technical means, which will reduce costs compared to the purchase of foreign analogues.

The social effect is expressed in increasing the level of technological sovereignty by reducing dependence on technologies from foreign manufacturers. In this regard, increasing the level of protection of the interests of society, the state and cyberspace of the country, as well as the prevention and investigation of high-tech cyber threats, which is an integral part of national security.

The impact of expected results on the development of the main scientific field and related fields of science and technology. The main key advantage of the project being developed will be an optimized approach to carrying out work on the search and research of existing features.

Based on the results of testing and implementation of methods and algorithms, a number of scientific papers will be published in national and international journals and presented at conferences, scientific symposiums and master classes, which can serve as the basis for many other scientific papers both in the field of information security and information technology sciences. In addition to all of the above, within the framework of this project, it is planned to hold CTF for students of technical specialties, with the formulation of tasks solved in the project in order to generate a new generation of researchers in this field and possibly obtain new creative solutions. Also, students, undergraduates and doctoral students of Kazakhstani universities will definitely participate in the project to form a school of digital forensics to solve problems in favor of the interests of the state. In the future, the stages of launching a number of laboratories and research centers may be considered.

**Scientific, technical and design documentation**

As part of the creation of a system for the study of blocked electronic and digital devices, including methods using artificial intelligence, technical and methodological documentation will be developed regarding the functionality, assembly, launch, user recommendations and possible failures with answers for their elimination.

The documentation will contain:

* A description of how the system works, and how the project components work with each other, as well as the technologies used.
* Technical requirements for the hardware and software required for the operation of the system.
* Instructions on how to install and start using the system, as well as step-by-step instructions for using key functions.
* Tips on using and researching the system, including applying System Access to Artificial Intelligence.
* A list of known problems with the system, their description, and detailed instructions on how to identify and fix them.
* Security measures that will be necessary to ensure that data is not copied and that we do not use data in accordance with the policy.
* Ideas on how to use this project to fix client devices and file systems with different diagnoses.

The documentation will help users prepare for work and will focus on preventing errors related to the operation of the system.

**10. Bibliography**

1. A. Kanta, I. Coisel and M. Scanlon, "A Novel Dictionary Generation Methodology for Contextual-Based Password Cracking," in *IEEE Access*, vol. 10, pp. 59178-59188, 2022, doi: 10.1109/ACCESS.2022.3179701.
2. N. Balasubramaniam, J. Dhalia Sweetlin and R. Anirudh, "Distributed Parallelized Password Cracking Framework for Enhanced Cybersecurity using Authentication Codes," *2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, Chennai, India, 2024, pp. 1-6, doi: 10.1109/ACCAI61061.2024.10601823.
3. N. Tihanyi, T. Bisztray, B. Borsos and S. Raveau, "Privacy-Preserving Password Cracking: How a Third Party Can Crack Our Password Hash Without Learning the Hash Value or the Cleartext," in *IEEE Transactions on Information Forensics and Security*, flight. 19, pp. 2981-2996, 2024, doi: 10.1109/TIFS.2024.3356162.
4. H. Yin and L. Ni, "Optimization of WinRAR Password Cracking Algorithm Based on Heterogeneous Computing," *2021 IEEE 21st International Conference on Communication Technology (ICCT)*, Tianjin, China, 2021, pp. 892-896, doi: 10.1109/ICCT52962.2021.9658021.
5. Q. Ding, Z. Zhang, S. Li and P. Liu, "Energy-Efficient RAR3 Password Recovery with Dual-Granularity Data Path Strategy," 2019 IEEE International Symposium on Circuits and Systems (ISCAS), 2019, pp. 1- 5, doi: 10.1109/ISCAS.2019.8702713.
6. A. Kanta, I. Coisel, and M. Scanlon, ‘‘A survey exploring open source intelligence for smarter password cracking,’’ Forensic Sci. Int., Digit. Invest., vol. 35, Dec. 2020, Art. no. 301075.
7. A. Kanta, I. Coisel, and M. Scanlon, ‘‘PCWQ: A framework for evaluating password cracking wordlist quality,’’ in Proc. 12th EAI Int. Conf. Digit. Forensics Cyber Crime (ICDFC). Singapore: Springer, Dec. 2021, pp. 1–18.
8. D. Omirgazy, «Kazakhstan Registers Significant Attempts of Cyber-Attacks in 2023»,<https://astanatimes.com/2024/01/kazakhstan-registers-significant-attempts-of-cyber-attacks-in-2023/>
9. Password Manager and Vault 2021 Annual Report: Usage, Awareness, and Market Size. [Online]. Available: https://www.security. org/digital-safety/password-manager-annual-report/
10. O. Parhad and V. Naik, "Comparative analysis of Data Extraction for Qualcomm based android devices," *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Delhi, India, 2023, pp. 1-7, doi: 10.1109/ICCCNT56998.2023.10307241.
11. O. Parhad and V. Naik, "Comparative analysis of Data Extraction for Qualcomm based android devices," *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Delhi, India, 2023, pp. 1-7, doi: 10.1109/ICCCNT56998.2023.10307241.
12. M. AlSabah, G. Oligeri, and R. Riley, ‘‘Your culture is in your password: An analysis of a demographically-diverse password dataset,’’ Comput. Secur., vol. 77, pp. 427–441, Aug. 2018.
13. F. Lorenzo, J. T. McDonald, T. R. Andel, W. B. Glisson and S. Russ, "Evaluating Side Channel Resilience in iPhone 5c Unlock Scenarios," *2019 SoutheastCon*, Huntsville, AL, USA, 2019, pp. 1-7, doi: 10.1109/SoutheastCon42311.2019.9020529.
14. Sutikno, Tole & Busthomi, Iqbal. (2024). Capabilities of cellebrite universal forensics extraction device in mobile device forensics. Computer Science and Information Technologies. 5. 254-264. 10.11591/csit.v5i3.p254-264.
15. S. Singh, A. Chavekar, S. Mane and F. Kazi, "Exploring Chip-Off Firmware Extraction Techniques and Challenges: Case Studies in Smart Plugs," *2023 IEEE International Carnahan Conference on Security Technology (ICCST)*, Pune, India, 2023, pp. 1-6, doi: 10.1109/ICCST59048.2023.10726849.

Application: 1) a plan for the partner's contribution to the implementation of the program, similar to table 9 (for applied scientific research).

3. Calculation of the requested financing The part "Calculation of the requested financing" is drawn up in the form of tables 2-7, justifying the calculation of the amount requested for the implementation of the financing program, which are filled in the information system of the center of expertise. Explanations to the calculations are provided in section 7 "Justification of the requested financing" in the "Explanatory Note" part.

Table 1 - Composition of the research group for scientific research, including foreign scientists, young scientists (postdoctoral students, doctoral, master's and undergraduate students)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №  n/p | Full name (if available), education, degree, academic title | Main place of work, position | H-index, ResearcherID, ORCID, Scopus Author ID (if available) | Role in the project or program and nature of the work performed | Brief rationale for participation |
| 1 | Khikmetov Askar Kusupbekovich, Candidate of Physical and Mathematical Sciences, Associate Professor | Chairman of the Board - Rector of Astana IT University LLP | h index = 3, ResearcherIDIEM-5232-2023, https://orcid.org/0000-0002-3045-7592, https://www.scopus.com/authid/detail.uri?authorId=56741480900 | Scientific director of the project  Project management and management:  1.   Setting project goals;  2.   Distribution of functional responsibilities of project participants;  3.   Organization and coordination of the work of performers in all areas and types of program activities;  4.   Prompt response to risks;  5.   Monitoring the progress of project stages;  6.   Adjustment of tasks;  7.   Analysis of the obtained scientific results;  8.   Preparation and formation of articles in international peer-reviewed publications WoS, Scopus, monographs, patents, reporting materials;  9.   Preparation and formation of documents for filing for patents and intellectual property rights;  10. Formulation of the problem; experimental work;  11. Development of proposals and recommendations;  12. The process of transferring and presenting research results to the customer.  Obtaining a patent and monograph | He is an expert in mathematical modeling, which is one of the key factors in the implementation of the development of methods for accessing password-protected backups, mobile applications, instant messengers, cloud services and system settings of the Android operating system. When implementing this task, it is planned to use AI models, NER models, to study the social engineering of an object. The participant’s competencies will be useful in determining your own AI model, for the most accurate selection of the most correct options. |
| 2 | Rzaeva Leila Gummetovna, Doctor of Philosophy PhD in the field of “Automation and Control” | Limited Liability Partnership "Astana IT University", Deputy Director of the Department of Intelligent Systems and Cybersecurity, Associate Professor | h-index -4, ResearcherID - https://www.researchgate.net/profile/Rzayeva-Leila,  ORCID - 0000-0002-3382-4685,    Scopus Author ID - 57218901417 | Responsible executive, Data analyst and system integrator, cryptographer, VNS  Research of algorithms and methods for automatic decryption of encrypted authentication data used in the systems under study.  Study of algorithms for the functioning of encryption and decryption systems implemented in the Android mobile operating system.  Research of existing scientific methods and software products that perform the tasks stated in this application, namely bypassing Android OS security systems.  Research of security system vulnerabilities in different versions of the operating systems under study (Windows, Android, IOS).  Implementation of advanced algorithms to improve the accuracy and speed of data analysis, using artificial intelligence methods that significantly reduce the time of researching digital evidence.  Ensuring the integration of developed algorithms and methods with the hardware and software complex.  Obtaining a patent and monograph | Has 16 years of experience in implementing and maintaining automated production lines and implementing SAP S4/Hana modules MM, WM, PM.  Area of ​​responsibility - development, implementation and technical support of an information system to optimize production processes.  Scientific and pedagogical activities since 2010:  Since 2010, he has experience teaching undergraduate, graduate and doctoral students in specialized disciplines of the educational programs “Automation and Control”, “Telecommunications”, “Cyber ​​Security”, “Smart Technologies”. Supervisor of more than 100 undergraduate students, more than 20 masters and 2 PhDs.  The main direction of scientific research is the development of optimal, adaptive and robust control systems, the use of artificial intelligence in various technological and technical processes, programming microcontrollers, development of embedded control systems, information security, smart technologies and IoT.  Most of the research is aimed specifically at solving problems in the industrial sector. Has experience in leading scientific research on the development of automatic detection of hidden networks from USB devices (working in a research laboratory during a scientific internship in the USA), as well as participating in projects on the use of machine learning algorithms and the creation of neural networks to improve the efficiency of thermal production processes (copper production) and pattern recognition of hyperspectral aerospace images and predictive analytics, as well as the development of methods for increasing the stability of the aircraft control system commissioned by the Ministry of Defense of the Republic of Kazakhstan (under the leadership of Professor Beisenby M.A.).  The following publications have been published in the following areas of research:  - 15 articles cited in Scopus (Q1-Q3) and Web of Science,  - more than 50 publications in foreign journals and journals recommended by the Committee for Quality Assurance in Education of the Ministry of Education of the Republic of Kazakhstan.  Head of the targeted funding project BR24993232 “Development of innovative technologies for conducting digital forensic research using intelligent software and hardware systems” |
| 3 | Imanberdi Abilkair Yerboluly, Master | Limited Liability Partnership "Astana IT University", Senior Lecturer, CTF Trainer | https://www.researchgate.net/profile/Abilkair-Imanberdi,0009-0005-6144-2392,000000000 | Reverse - engineer, cryptographer  Development of an algorithm for bypassing the protection of mobile applications and instant messengers using binary exploitation techniques.  Research of IoT device protection systems and existing vulnerabilities in collective networks of connected devices.  Development of a method for automatically decrypting encrypted authentication data used in the systems under study.  Development of a method for decrypting extracted data related to mobile applications, instant messengers and cloud services.  Development of a method for decrypting extracted data from cloud services that implement the functionality of backup storage.  Obtaining a patent and monograph | He has about 8 years of experience in the manufacturing sector in the areas of malware research and computer forensics. Manages a team of virus analysts at JSC GTS. He is a CTF trainer at Astana IT University LLP.  At the request of the Ministry of Defense of the Republic of Kazakhstan, he worked as part of a working group as a co-leader (group leader, Doctor of Technical Sciences, Professor S.K. Atanov) on the development of a prototype of a domestic UAV. The project included the development of software and mathematical support for a stabilization system for an unmanned aerial vehicle based on the use of a Kalman filter, a navigation system for an unmanned aerial vehicle, and an intelligent system for managing the energy resources of a mobile object. As a result, these methods were successfully implemented into the project, and implementation certificates were obtained.  Intellectual Property Rights:  1) Raw data smoothing system to stabilize the movement of a mobile object. 04/11/2017. No. 670. IS 007957  2) A program for intelligent decision-making on choosing the trajectory of a mobile system using a search for the optimal path on the graph. 04/11/2017. No. 668. IS 007912  Has 4 scientific publications in software development in domestic and foreign journals.  International professional certificates:  1) Certified Ethical Hacker (CEH), EC-Council  2) EC-Council Certified Security Analyst (ECSA) |
| 4 | Myrzatay Ali Altynbayly, , master of technical sciences | Limited Liability Partnership "Astana IT University", Project Manager | h - index = 3  ORCID: 0000-0002-5339-2437 | Machine learning algorithm engineer, CNN  Study of implemented solutions for analyzing digital evidence using artificial intelligence methods (if they exist).  Analysis of current digital forensics processes and methods to identify existing deficiencies, followed by proposals for eliminating them in the project.  Using artificial intelligence to automate and improve the processes of data analysis, detect relationships and patterns that may indicate the interaction of several individuals with each other, as well as to search for various information for a given request. | He defended his Doctor of Philosophy (PhD) degree in the specialty “6D070200 – Automation and Control” at the Eurasian National University named after L.N. Gumilyov, it is currently expected that he will be awarded this degree. He has significant experience working with algorithms and machine learning methods, which allows him to apply modern approaches in the field of algorithmic research. He is an expert in the development and analysis of algorithms. He has published scientific works in international journals indexed in the Scopus database, with high quality scores (Q1 and Q2 percentile). Has 13 published scientific articles |
| 5 | Konakbaev Olzhas Balkybekuly, Master of Technical Sciences in the field of “Automation and Control” | Limited Liability Partnership "Astana IT University", Senior Lecturer of the Department of Intelligent Systems and Cybersecurity | ORCID 0009-0002-9156-4858 | Hardware Technology Specialist, Laboratory Assistant |  |
| 6 | Tajibaeva Perizat Shalgynbaykyzy  Bachelor in Cybersecurity | Limited Liability Partnership "Astana IT University", master's student "7M06106 Security Software Engineering" | ORCID: 0009-0009-1566-636X,000 | Information Security Engineer  Conducting an analysis of existing technological solutions for processing digital evidence in order to identify potential vulnerabilities and assess the risks associated with them.  Development and implementation of information security measures, including the use of cryptographic methods, implementation of access control systems and configuration of monitoring to ensure confidentiality, integrity and availability of data.  Conducting an audit of project information systems to assess their compliance with regulatory requirements and standards. | Received her bachelor's degree in 2024 with a major in “6B06301 - Cybersecurity”. Currently studying for a master's degree in the specialty "7M06106 Security Software Engineering".  Has good skills necessary to analyze existing methods.  Has good knowledge necessary for an information security specialist.  Existing education in the field of cybersecurity, as well as current specialization in secure software development, confirms a deep understanding of current threats and protection methods. Experience in cryptography, digital forensics and web application security allows you to effectively solve problems related to information security. |
| 7 | Madi Arsenovich Shayakhmetov  Bachelor in Cybersecurity | Limited Liability Partnership "Astana IT University", master's student "7M06106 Security Software Engineering" |  | Information Security Engineer  Development of a method for automatically decrypting encrypted authentication data used in the systems under study.  Development of a method for decrypting extracted data related to mobile applications, instant messengers and cloud services.  Development of a method for decrypting extracted data from cloud services that implement the functionality of backup storage. | Has the necessary knowledge and skills that make him a valuable participant in the project. Education in cybersecurity, as well as current specialization in secure software development, confirms a deep understanding of current threats and protection methods. Experience in cryptography, digital forensics and web application security allows him to effectively solve problems related to information security. He also took part in the project “BR24993232 “Development of innovative technologies for conducting digital forensic research using intelligent software and hardware systems” as a junior researcher, which indicates his practical experience in the field of digital forensic research. |
| 8 | Grigoriev Timur, master's degree |  | ORCID: 8987-6756-57 | Information Security Engineer, Laboratory Assistant  1. Research of algorithms for the functioning of encryption and decryption systems implemented in the Android mobile operating system.  2. Research of cloud solutions and their structures that implement the functionality of backup storage.  3. Development of a method for automatically decrypting encrypted authentication data used in the systems under study | is a specialist in the field of information security and developers of AI models in order to optimize the tasks of ensuring the protection of personal data and have excellent knowledge of data encryption and decryption methods; |
| 9 | Niyazaliyev Kuandyk Altayuly, Master, junior researcher | Military unit 01068, Researcher | Web of Science ResearcherID: AGX-8506-2022,0000-0002-3928-5248 | Research of cloud solutions and their structures that implement the functionality of backup storage.  Research of algorithms and methods for bypassing the protection of mobile applications and instant messengers using binary exploitation techniques.  Create universal methods to overcome security systems and gain access to information on password-protected electronic digital devices as part of law enforcement and national security  Development of a method for automatically decrypting encrypted authentication data used in the systems under study  Implement a function in the form of executable code that provides administrative rights to the Android file system while preserving user data | He is a specialist in the field of digital forensics and has the knowledge and skills to solve the following problems |
| 10 | Kurmangali Elzhas Sergalyuly, bachelor |  |  | Digital Forensics Engineer  1. Development of instructions for searching for security system vulnerabilities in different versions of the operating systems under study  2.Development of a method for decrypting extracted data related to mobile applications, instant messengers and cloud services  3.Develop methodological documentation for the use of a prototype | is valid  digital forensics specialist of the KNB and can clearly describe current problems in this area, contribute to the development of methods and testing results, provide expert assessment and recommendations for improving the developed software system |
| 11 | Pogolovkin Daniil, Master |  | Scopus Author ID : 77113355 | Information Security Engineer  1. Research of algorithms and methods for bypassing the protection of mobile applications and instant messengers using binary exploitation techniques.  2. Development of a method for automatically decrypting encrypted authentication data used in the systems under study  3. Implement a function in the form of executable code that provides administrative rights to the Android file system while saving user data | is an information security specialist and a developer of AI models in order to optimize the tasks of ensuring the protection of personal data and have excellent knowledge of data encryption and decryption methods; |
| 12 | Mohsen Guizani,  Professor |  | h index = 106 https://www.scopus.com/authid/detail.uri?authorId=7004750176 ResearcherIDD-9103-2018 | Foreign scientific consultant  1. Study of algorithms for the functioning of encryption and decryption systems implemented in the Android mobile operating system.  2. Research on the implementation of the main authentication methods used in mobile phones and tablets  3.Create universal methods for overcoming security systems and gaining access to information on password-protected electronic digital devices as part of law enforcement and national security  4. Development of a method for automatically decrypting encrypted authentication data used in the systems under study  5. Implement a function in the form of executable code that provides administrative rights to the Android file system while saving user data  6.Development of a software module for retrieving data from cloud services, implementing the functionality of backup storage | A professor with many years of experience, his research interests focus on computer networks, cybersecurity, wireless and sensor networks, and cloud computing. In his research, he pays special attention to the issues of protecting cloud technologies and smart networks, considering them in the context of computer security, which will significantly facilitate the team’s work on developing algorithms and methods that solve the main goal of the research; |
| 13 | Satybaldina Dina Zhagyparovna, Candidate of Physical and Mathematical Sciences, PhD, Associate Professor in the specialty 05.13.00 - Informatics, computer technology and management | Non-profit joint-stock company "Eurasian National University named after L.N. Gumilyov", director of the Research Institute of Information Security and Cryptology | ORCID:0000-0003-0291-4685  ResearcherID: P-1120-2014  Scopus Author ID:  57193740669 | 1. Research of security system vulnerabilities in different versions of the operating systems under study (Windows, Android, IOS)  2. Research of algorithms and methods for bypassing the protection of mobile applications and instant messengers using binary exploitation techniques.  3.Create universal methods for overcoming security systems and gaining access to information on password-protected electronic digital devices as part of law enforcement and national security  4. Development of a method for automatically decrypting encrypted authentication data used in the systems under study  5.Development of a method for bypassing the protection of mobile applications and instant messengers using binary exploitation techniques  6. Development of a software module for decrypting extracted data related to mobile applications, instant messengers and cloud services | has many years of experience in the field of modeling a cryptographic system for backup storage of confidential data in secure servers and the use of artificial intelligence methods to ensure cybersecurity of cellular communication networks, for many years she headed the Department of Information Security at L.N. Gumilyov ENU, and is currently the founder and head of the Research Institute of Information Security and Cryptology at L.N. Gumilyov ENU. She has established herself as one of the best experts in data encryption and decryption. This project requires her strongest competency in decrypting files extracted from mobile devices; |
| 14 | Nurdauletov Yerbol Tolevkanovich |  |  | Binary Exploitation Analyst, Cryptographer  1. Research on the implementation of the main authentication methods used in mobile phones and tablets.  2. Create universal methods for overcoming security systems and gaining access to information on password-protected electronic digital devices as part of law enforcement and national security  3.Development of code for decrypting extracted data from cloud services, implementing the functionality of backup storage | is an analyst for binary operation of GTS JSC. His competencies will be necessary to solve the main problems of finding authentication bypass methods in OS code |
| 15 | Amirov Ersultan Erbolovich, bachelor | military unit 01068, military |  | Executor  Digital Forensics Engineer  1. Review and analysis of similar solutions, technologies and methods used in the forensic investigation of password-protected electronic digital devices based on the iOS and Android operating systems.  2. Create universal methods for overcoming security systems and gaining access to information on password-protected electronic digital devices as part of law enforcement and national security |  |
| 16 |  |  |  |  |  |
| 17 | Kozhakhmet Zhaksylyk, Master of Information Systems |  |  | Software engineer  1. Research of cloud solutions and their structures that implement the functionality of backup storage.  2.Creation of an artificial intelligence model to automatically determine the rules for generating user authentication data  3.Creating an artificial intelligence model for password guessing using a dictionary from the results of social engineering research  4. Development of a software module for decrypting extracted data related to mobile applications, instant messengers and cloud services  5.Development of code for decrypting extracted data from cloud services, implementing the functionality of backup storage | is a teacher at Astana IT University. Has experience in developing client server and mobile applications. His skills will be applied in the implementation of tasks related to software development and its integration into the hardware of the agro-industrial complex; |
| 18 | Bizhanova Zhansaya Alimkyzy, Master of Technical Sciences |  |  | Project manager  1. Monitoring the completion of tasks  2.Organization of meetings on the project  3. Recording of meetings  4.Receiving feedback from the customer | is an experienced project manager. During the implementation of the project, he will communicate between all employees, monitor the completion of tasks, and receive feedback from the customer. |
| 19 | Vacancy |  |  | Executor Binary Exploitation Analyst, Cryptographer |  |
| 20 | Vacancy |  | Accountant/lawyer/economist/purchaser | Executor Accountant/lawyer/economist/purchaser |  |

Table 2 - Consolidated cost estimate for the requested amount

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Name of expense item | Amount of financing, thousand tenge | | | |
| Total | 2025  (1st year) | 2026  (2nd year) | 2027  (3rd year) |
| 1. | Wages (including taxes and other obligatory payments to the budget) | 387 475,040 | 99 059,360 | 143 591,040 | 144 824,640 |
| 2. | Business trips | 59 702,892 | 15 311,797 | 19 588,509 | 24 802,586 |
| 3 | Scientific and organizational support, other services and work | 65 957,267 | 39 494,900 | 18 322,847 | 8 139,520 |
| 4. | Purchase of materials (for individuals and legal entities), purchase of equipment and (or) software (for legal entities) | 314 864,801 | 146 133,943 | 82 497,604 | 86 233,254 |
| 5. | Rental costs, operating costs of equipment and machinery used to carry out research | 72 000,000 | - | 36 000,000 | 36 000,000 |
| Total | | 900 000,000 | 300 000,000 | 300 000,000 | 300 000,000 |

Table 3 – Wages (including taxes and other obligatory payments to the budget)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| No | Full name | Position | Salary, tenge | | | | | | | | | | | | | | | | |
| 1st year | | | | 2nd year | | | | | 3rd year | | | | | Total (gr.6+ gr.10+ gr.14) | |
| Employment (full / part-time) | Salary, tenge per month | Number of months of work | Summa (gr.3× gr.4× gr.5) | Employment (full / part-time) | Salary, tenge per month | Number of months of work | Summa (gr.7× gr.8× gr.9) | Employment (full / part-time) | | Salary, tenge per month | Number of months of work | Summa (gr.11× gr.12× gr.13) |  | |
| 1 |  | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | | 12 | 13 | 14 | 15 | |
| 1 |  | Key research team personnel | | | X | 77 040 000 |  |  | X | 110 160 000 |  | |  | X | 110 160 000 | 297 360 000 | |
| 1.1 | Hikmetov Askar Kusupbekovich | Scientific supervisor, State Tax Service | 1 | 990 000 | 8 | 7 920 000 | 1 | 990 000 | 12 | 11 880 000 | 1 | | 990 000 | 12 | 11 880 000 | 31 680 000 | |
| 1.2 | Rzaeva Leila Gummetovna | Responsible executive, Data analyst and system integrator, cryptographer, VNS | 1 | 900 000 | 8 | 7 200 000 | 1 | 900 000 | 12 | 10 800 000 | 1 | | 900 000 | 12 | 10 800 000 | 28 800 000 | |
| 1.3 | Imanberdi Abilkair Yerboluly | Reverse-engineering and cryptography | 1 | 900 000 | 8 | 7 200 000 | 1 | 900 000 | 12 | 10 800 000 | 1 | | 900 000 | 12 | 10 800 000 | 28 800 000 | |
| 1.4 | Nurdauletov Yerbol Tolevkanovich | Binary Exploitation Analyst, Cryptographer | 1 | 500 000 | 8 | 4 000 000 | 1 | 500 000 | 12 | 6 000 000 | 1 | | 500 000 | 12 | 6 000 000 | 16 000 000 | |
| 1.5 | Myrzatai Ali | Machine learning algorithm engineer, CNN | 1 | 500 000 | 8 | 4 000 000 | 1 | 500 000 | 12 | 6 000 000 | 1 | | 500 000 | 12 | 6 000 000 | 16 000 000 | |
| 1.6 | Vacancy 1 | Binary Exploitation Analyst, Cryptographer | 1 | 500 000 | 8 | 4 000 000 | 1 | 500 000 | 12 | 6 000 000 | 1 | | 500 000 | 12 | 6 000 000 | 16 000 000 | |
| 1.7 | Mohsen Guizani | Foreign scientific consultant | 1 | 600 000 | 8 | 4 800 000 | 1 | 600 000 | 12 | 7 200 000 | 1 | | 600 000 | 12 | 7 200 000 | 19 200 000 | |
| 1.8 | Vacancy 2 | Cloud Engineer | 1 | 600 000 | 8 | 4 800 000 | 1 | 600 000 | 12 | 7 200 000 | 1 | | 600 000 | 12 | 7 200 000 | 19 200 000 | |
| 1.9 | Tajibaeva Perizat | Information Security Engineer, NS | 1 | 380 000 | 8 | 3 040 000 | 1 | 380 000 | 12 | 4 560 000 | 1 | | 380 000 | 12 | 4 560 000 | 12 160 000 | |
| 1.10 | Konakbaev Olzhas Balkybekuly | Design engineer | 1 | 500 000 | 8 | 4 000 000 | 1 | 500 000 | 12 | 6 000 000 | 1 | | 500 000 | 12 | 6 000 000 | 16 000 000 | |
| 1.11 | Grigoriev Timur | Information security engineer, laboratory assistant, NS | 1 | 400 000 | 8 | 3 200 000 | 1 | 400 000 | 12 | 4 800 000 | 1 | | 400 000 | 12 | 4 800 000 | 12 800 000 | |
| 1.12 | Kojakhmet Jaksylyk | Software engineer, NS | 1 | 300 000 | 8 | 2 400 000 | 1 | 300 000 | 12 | 3 600 000 | 1 | | 300 000 | 12 | 3 600 000 | 9 600 000 | |
| 1.13 | Satybaldina Dina Zhagiparovna | Cryptographer, VNS | 1 | 900 000 | 8 | 7 200 000 | 1 | 900 000 | 12 | 10 800 000 | 1 | | 900 000 | 12 | 10 800 000 | 28 800 000 | |
| 1.14 | Baybusinov A.S. | Digital Forensics Engineer | 0,5 | 450 000 | 8 | 1 800 000 | 0,25 | 450 000 | 12 | 1 350 000 | 0,25 | | 450 000 | 12 | 1 350 000 | 4 500 000 | |
| 1.15 | Amirov E.E. | Digital Forensics Engineer | 0,5 | 450 000 | 8 | 1 800 000 | 0,25 | 450 000 | 12 | 1 350 000 | 0,25 | | 450 000 | 12 | 1 350 000 | 4 500 000 | |
| 1.16 | Niyazaliyev Kuandyk Altaiuli | Digital Forensics Engineer | 0,5 | 450 000 | 8 | 1 800 000 | 0,25 | 450 000 | 12 | 1 350 000 | 0,25 | | 450 000 | 12 | 1 350 000 | 4 500 000 | |
| 1.17 | Kurmangali Elzhas Sergalyuly | Digital Forensics Engineer | 0,5 | 450 000 | 8 | 1 800 000 | 0,25 | 450 000 | 12 | 1 350 000 | 0,25 | | 450 000 | 12 | 1 350 000 | 4 500 000 | |
| 1.18 | Shayakhmetov Madi | Information Security Engineer, NS | 1 | 380 000 | 8 | 3 040 000 | 1 | 380 000 | 12 | 4 560 000 | 1 | | 380 000 | 12 | 4 560 000 | 12 160 000 | |
| 1.19 | Pogolovkin Daniil | Information Security Engineer, NS | 1 | 380 000 | 8 | 3 040 000 | 1 | 380 000 | 12 | 4 560 000 | 1 | | 380 000 | 12 | 4 560 000 | 12 160 000 | |
| 2 |  | Additional staff | | | X | 8 800 000 |  |  | X | 13 200 000 |  | |  | X | 13 200 000 | 35 200 000 | |
| 2.1 | Bijanova Zhansaya Alimovna | Project manager | 1 | 500 000 | 8 | 4 000 000 | 1 | 500 000 | 12 | 6 000 000 | 1 | | 500 000 | 12 | 6 000 000 | 16 000 000 | |
| 2.2 | Project office | Accountant/lawyer/economist/purchaser | 1 | 600 000 | 8 | 4 800 000 | 1 | 600 000 | 12 | 7 200 000 | 1 | | 600 000 | 12 | 7 200 000 | 19 200 000 | |
| 3 |  | Total wage fund (column 1+column 2) | X | X | X | 85 840 000 | X | X | X | 123 360 000 | X | | X | X | 123 360 000 | 332 560 000 | |
| 4 |  | Taxes and other obligatory payments to the budget (total gr. 4.1 + gr. 4.2 + gr. 4.3) | X | X | X | 13 219 360 | X | X | X | 20 231 040 | X | | X | X | 21 464 640 | 54 915 040 | |
| 4.1. |  | Calculation of social tax expenses | X | X | X | 4 635 360 | X | X | X | 6 661 440 | X | | X | X | 6 661 440 | 17 958 240 | |
| 4.2. |  | Calculation of expenses for paying social contributions to the State Social Insurance Fund | X | X | X | 3 862 800 | X | X | X | 5 551 200 | X | | X | X | 5 551 200 | 14 965 200 | |
| 4.3. |  | Contributions for compulsory health insurance | X | X | X | 2 575 200 | X | X | X | 3 700 800 | X | | X | X | 3 700 800 | 9 976 800 | |
| 4.1. |  | Mandatory employer pension contributions | X | X | X | 2 146 000 | X | X | X | 4 317 600 | X | | X | X | 5 551 200 | 12 014 800 | |
| Total (group 3+ group 4) | | | X | X | X | 99 059 360 | X | X | X | 143 591 040 | X | | X | X | 144 824 640 | 387 475 040 | |

Table 4 - Business trips

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | Destination (country, city, name of settlement) | Reimbursement rate for daily expenses per person (2 x monthly calculation index) (tenge) | Norm of expenses for renting residential premises per day per 1 person (tenge) | Average annual number of people/days for calculating daily expenses (person/days) | Average annual number of people/days to calculate the cost of renting residential premises (persons/days) | Average annual number of seconded people (persons) | Average cost of one round trip (tenge) | Amount of expenses (thousand tenge) (gr. 3 x gr. 5 + gr. 4 x gr. 6 + gr. 7 x gr. 8)/1000 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 1. | 2025 (1st year) total | | | | | |  | 15 311, 797 |
|  |
| 1.1. | Chania, Crete, Greece (IEEE CSR 2025) August 4-6 | 44 000 | 101 750 | 28 | 16 | 4 | 823 620 | 6 154,480 |  |
| 1.2. | Salt Lake City, USA -July 24-31 | 53 100 | 138 060 | 42 | 27 | 3 | 1 066 499 | 9 157,317 |  |
| 2. | 2026 (2nd year) total | | | | | |  | 19 588, 509 |  |
|  |
| 2.1. | Taipei, Taiwan, September 10-12 | 42 480 | 53 100 | 30 | 20 | 5 | 1 121 481 | 7 943,805 |  |
| 2.2. | Canada, Toronto August 18-31 | 53 100 | 79 650 | 56 | 52 | 4 | 1 132 326 | 11 644,704 |  |
| 3. | 2027 (3rd year) total | | | | |  |  | 24 802, 586 |  |
|  |
| 3.1. | Canada, Toronto APRIL 1-10 | 53 100 | 79 650 | 52 | 40 | 4 | 1 258 769 | 10 982,276 |  |
| 3.2. | Defcon, Las Vegas, USA AUGUST 7-10 | 53 100 | 138 060 | 70 | 25 | 5 | 1 330 362 | 13 820,310 |  |
|  |  |  |  |  |  |  |  |  |  |
| Total (gr. 1 + gr. 2 + gr. 3) | | | | | | |  | 59 702,892 |  |

Table 5 – Scientific and organizational support, other services and work

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Designation | A unit of measurement | Quantity, units | Cost per unit, tenge | Total cost, tenge (gr.4 × gr.5) |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 2025 (1st year), total |  |  |  | 39 494 900,00 |
| 1.1. | Registration fee for participation in the conference at IEEE CSR 2025 | article | 2 | 866 250,00 | 1 732 500,00 |
| 1.2. | Registration fee for internship at SANS Institute | article and certificate of participation | 4 | 4 565 600,00 | 18 262 400,00 |
| 1.3. | Organization of CTF and Hackathon competitions | competition service | 1 | 3 500 000,00 | 3 500 000,00 |
| 1.4. | A service for collecting and annotating a data set and further synthetically generating data for training AI models. | Providing data collection services | 2 | 5 000 000,00 | 10 000 000,00 |
| 1.5. | Service for implementation, configuration and maintenance of vector database software and monitoring tools aimed at optimizing the operation of machine learning models and ensuring their performance. | Service for implementation, configuration and maintenance of software | 1,00 | 6 000 000,00 | 6 000 000,00 |
| 2 | 2026 (2nd year), total |  |  |  | 18 322 847,00 |
| 2.1. | Payment for publication in the scientific journal IEEE Access | article | 3 | 1 101 825,00 | 3 305 475,00 |
| 2.2. | Payment for publication in NAS RK | article | 3 | 40 000,00 | 120 000,00 |
| 2.3. | Organization of CTF and Hackathon competitions | competition service | 2 | 3 500 000,00 | 7 000 000,00 |
| 2.4. | Service for “Source code analysis” of developed software modules for implementation | service | 1 | 7 897 372,00 | 7 897 372,00 |
| 3 | 2027 (3rd year), total | X | X |  | 8 139 520,00 |
| 3.1. | Registration fee for participation in the Defcon conference, Las Vegas, USA | article | 4 | 254 880,00 | 1 019 520,00 |
| 3.2. | Payment for publication in NAS RK | article | 3 | 40 000,00 | 120 000,00 |
| 3.3. | Organization of CTF and Hackathon competitions | competition service | 2 | 3 500 000,00 | 7 000 000,00 |
| Total (column 1 + group 2 + group 3), tenge | | X | X |  | 65 957 267,00 |

Table 6 – Purchase of materials, equipment and (or) software (for legal entities)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Designation | A unit of measurement | Quantity, units | Cost per unit, tenge | Total cost, tenge (gr.4 × gr.5) |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 2025 (1st year), total |  |  |  | 146 133 943,00 |
| 1.1. | 1x Server SuperMicro SYS-421GE-TNRT  2x P4X-EMR6530-SRN5C-XCC  16x MEM-DR532MD-ER48  1x AOC-S3916L-H16IR-32DD-O  2x HDS-25T0-480G0-L2-TXD-NON-007  4x HDS-25T0-007T6-L2-TXD-NON-007  1x BTR-CVPM05 | Thing | 1 | 20200000 | 20 200 000,00 |
| 1.2. | Video card NVIDIA H100 NVL GPU 94GB PCI 5.0 | Thing | 4 | 30000000 | 120 000 000,00 |
| 1.3. | KEHUA rack-mount UPS,  KR6000L-J+, 6kVA + Battery pack  for UPS KEHUA, KR6000L-J+ for 15  minutes | Thing | 1 | 1800000 | 1 800 000,00 |
| 1.4. | Cabinet SHIP, 601S.8242.24.100, 124 series,  19'' 42U, 800\*1200\*2000 mm, W\*D\*H | Thing | 1 | 420000 | 420 000,00 |
| 1.5. | Used mobile phones on Android OS | Thing | 20 | 164297,15 | 3 285 943,00 |
| 1.6. | Switch with Ubiquiti Layer 3 switch  (48) GbE RJ45 ports and (4) 10G SFP+  ports. | Thing | 1 | 428000 | 428 000,00 |
| 2 | 2026 (2nd year), total |  |  |  | 82 497 604,00 |
| 2.1. | 1x Server SuperMicro SYS-421GE-TNRT  2x P4X-EMR6530-SRN5C-XCC  16x MEM-DR532MD-ER48  1x AOC-S3916L-H16IR-32DD-O  2x HDS-25T0-480G0-L2-TXD-NON-007  4x HDS-25T0-007T6-L2-TXD-NON-007  1x BTR-CVPM05 | Thing | 1 | 20200000 | 20 200 000,00 |
| 2.2. | Video card NVIDIA H100 NVL GPU 94GB PCI 5.0 | Thing | 1 | 30000000 | 30 000 000,00 |
| 2.3. | KEHUA rack-mount UPS,  KR6000L-J+, 6kVA + Battery pack  for UPS KEHUA, KR6000L-J+ for 15  minutes | Thing | 1 | 1800000 | 1 800 000,00 |
| 2.4. | Cabinet SHIP, 601S.8242.24.100, 124 series,  19'' 42U, 800\*1200\*2000 mm, W\*D\*H | Thing | 1 | 420000 | 420 000,00 |
| 2.5. | Switch with Ubiquiti Layer 3 switch  (48) GbE RJ45 ports and (4) 10G SFP+  ports. | Thing | 1 | 428000 | 428 000,00 |
| 2.6. | Server CHECK TALINO KA-Ultra Server 32 HDDs, 20TBHDDs640TB RAW Space | Thing | 1 | 19816720 | 19 816 720,00 |
| 2.7. | Mac Forensics (Tallino) | Thing | 1 | 9 832 884,00 | 9 832 884,00 |
|  | 2027 (3rd year), total |  |  |  | 86 233 254,00 |
| 3.1. | Video card NVIDIA H100 NVL GPU 94GB PCI 5.0 | Thing | 2 | 30000000 | 60 000 000,00 |
| 3.2. | Cyber ​​polygon | Thing | 1 | 26 233 254,00 | 26 233 254,00 |
|  | Total (column 1 + group 2 + group 3), tenge |  |  |  | 314 864 801,00 |

Table 7 – Rental costs, operating costs of equipment and machinery used to carry out research

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №  n/p | Designation | A unit of measurement | Unit price, tenge | Quantity, units | Total, tenge  (gr.4 × gr.5) |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 1. | 2025 (1st year), total |  |  |  | 0 |
| 1.1. | Renting office space for long-term computing processes | month | 3 000 000 | 0 | 0 |
| 2. | 2026 (2nd year), total | X | X |  | 36 000 000 |
| 2.1. | Renting office space for long-term computing processes | month | 3 000 000 | 12 | 36 000 000 |
| 3. | 2027 (3rd year), total | X | X |  | 36 000 000 |
| 3.1. | Renting office space for long-term computing processes | month | 3 000 000 | 12 | 36 000 000 |
| Total (gr.1 + gr.2 + gr.3) | | X | X |  | 72 000 000 |

Table 8 - Implementation work plan

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| №  n/p | Designation  tasks and measures for their implementation | Due date | | | | Expected results of the project (in terms of tasks and activities), form of completion |
| Start  (month) | | End  (month) | |  |
| 2025 | | | | | | | |
| 1 | Review and analysis of similar solutions, technologies and methods used in the forensic investigation of password-protected electronic digital devices based on the iOS and Android operating systems. | 05.2025 | 12.2025 | | An analysis of existing solutions and technologies for forensic investigation of password-protected electronic digital devices will be carried out. Completion Form: Analytical report containing comparative analysis of solutions. | |
| 1.1 | Study of algorithms for the functioning of encryption and decryption systems implemented in the Android mobile operating system. | 05.2025 | 12.2024 | | An analysis of encryption and decryption algorithms in Android will be carried out. Completion form: report with a technical description of the protection mechanisms. | |
| 1.2 | Research on the implementation of the main authentication methods used in mobile phones and tablets. | 05.2025 | 12.2024 | | A study of authentication mechanisms in mobile devices will be carried out. Completion form: analytical report with classification of authentication methods. | |
| 1.3 | Research of security system vulnerabilities in different versions of the operating systems under study (Windows, Android, IOS) | 05.2025 | 12.2024 | | An analysis of vulnerabilities in security systems of various versions of operating systems will be carried out. Completion form: report with identified vulnerabilities and proposed protection measures. | |
| 1.4 | Studying the functions of smartphones based on Android and IOS, which implement additional security measures for smartphones (locking the device for an indefinite period of time if several incorrect passwords are entered). | 05.2025 | 12.2025 | | An analysis of additional protection mechanisms for smartphones will be performed. Completion Form: A report detailing the defense mechanisms. | |
| 1.5 | Research of cloud solutions and their structures that implement the functionality of backup storage. | 05.2025 | 12.2025 | | The architecture of cloud storage and their protection mechanisms will be studied. Completion Form: Technical report with analysis and recommendations. | |
| 1.6 | Research of algorithms and methods for bypassing the protection of mobile applications and instant messengers using binary exploitation techniques. | 05.2025 | 12.2025 | | An analysis of binary exploitation methods will be conducted to bypass the protection of mobile applications. Completion Form: Technical report with identified methods and proposals for protection. | |
| 1.7 | Research of algorithms and methods for automatic decryption of encrypted authentication data used in the systems under study. | 05.2025 | 12.2025 | | The process of automatic decryption of authentication data will be studied. Completion Form: Analytical report describing possible approaches. | |
| 2 | Creating an artificial intelligence model to automatically determine the rules for generating user authentication data | 05.2025 | 12.2025 | | An artificial intelligence model will be created to automatically determine the rules for generating user authentication data. | |
| 2026 | | | | | | |
| 3 | Create universal methods to overcome security systems and gain access to information on password-protected electronic digital devices as part of law enforcement and national security | 01.2026 | 12.2026 | | A set of universal methods will be developed to effectively bypass the security mechanisms of electronic digital devices, including mobile phones, tablets and other gadgets. Completion form: Preparation of methodological recommendations for law enforcement agencies, development of tools for automated analysis and testing of methods on various versions of operating systems. | |
| 3.1 | Development of instructions for searching for security system vulnerabilities in different versions of the operating systems under study | 01.2026 | 12.2026 | | Detailed instructions will be prepared, including modern techniques for searching for vulnerabilities in Windows and Android security systems. Completion form: Development of methodological materials containing a classification of vulnerabilities, a description of possible attacks and recommendations for their use in forensic practice. | |
| 3.2 | Development of a method for automatically decrypting encrypted authentication data used in the systems under study | 01.2026 | 12.2026 | | An automatic decryption method will be created to recover encrypted credentials without direct user interaction. Completion form: Preparation of a report with algorithms for the method, its practical implementation in the form of a software module and recommendations for use in investigative activities. | |
| 4 | Creating an artificial intelligence model for password guessing using a dictionary from social engineering research | 01.2026 | 12.2026 | | An artificial intelligence model for password guessing will be created using a dictionary from the results of social engineering research. | |
| 5 | Develop methods for accessing password-protected backups, mobile applications, instant messengers, cloud services and system settings of the Android operating system | 01.2026 | 12.2026 | | Methods will be developed to efficiently retrieve data from secure backups and applications, even when encryption is enabled. Completion form: Creation of instructions for using methods, development of software tools and testing them on various device models. | |
| 5.1 | Development of a method for decrypting extracted data related to mobile applications, instant messengers and cloud services | 01.2026 | 12.2026 | | A method for decrypting data extracted from mobile applications and cloud services will be developed and tested. Completion Form: Preparation of a detailed report on the method, its practical application and results of testing on real data. | |
| 5.2 | Development of a method for bypassing the protection of mobile applications and instant messengers using binary exploitation techniques | 01.2026 | 12.2026 | | New methods will be researched and implemented to bypass the security mechanisms of mobile applications and instant messengers using binary analysis techniques. Completion form: Creation of an experimental prototype, a detailed report with examples of attacks, analysis of possible countermeasures and forensic application scenarios. | |
| 5.3 | Development of a method for decrypting extracted data from cloud services that implement the functionality of backup storage | 01.2026 | 12.2026 | | Mechanisms for storing data in cloud services will be investigated and a method for decrypting them will be developed. Completion form: Preparing an analytical report, creating a working decryption algorithm and testing it on real cloud storage. | |
| 5.4 | Development of a method for retrieving data from cloud services that implement the functionality of backup storage | 01.2026 | 12.2026 | | A method will be created to efficiently retrieve data from cloud storage, including encrypted files and backups. Completion form: Development of a prototype software tool, description of the methodology and its testing on common cloud platforms. | |
| 5.5 | Development of methods for accessing password-protected backups, mobile applications, instant messengers, cloud services and system settings of the Android operating system | 01.2026 | 12.2026 | | Effective methods will be developed to allow access to secure backups, mobile applications, cloud services and Android system settings, bypassing standard authentication mechanisms.  Completion form: Preparation of methodological recommendations, development of a test software solution and its testing on various versions of Android. | |
| 6 | Preparation and submission of scientific articles on developed methods for automatic decryption of encrypted authentication data used in the systems under study and the results of the artificial intelligence model of password selection using a social engineering dictionary | 01.2026 | 12.2026 | | Three articles will be published in journals recommended by COKNVO. | |
| 7 | Preparation and submission of scientific articles on developed methods for accessing password-protected backups, mobile applications, instant messengers, cloud services and system settings of the Android operating system | 01.2026 | 12.2026 | | Two articles will be published in peer-reviewed scientific publications in the scientific area of ​​the program, included in the 1st (first), 2nd (second) and (or) 3rd (third) quartile by impact factor in the Web of Science database and (or) having a CiteScore percentile in the Scopus database of at least 50 (fifty). | |
| 8 | Filling out an application for rights to intellectual property and submitting materials | 01.2026 | 12.2026 | | Two objects of intellectual property will be received (patent; for applications in the field of information technology - copyright certificate), registered with the National Institute of Intellectual Property of the Republic of Kazakhstan | |
| 9 | PAC hardware development | 01.2026 | 12.2026 | | Engineering and design work will be carried out to develop modules that ensure the implementation of the developed methods.  Completion form: prototype PAC with a functional and logical diagram of the interaction of all hardware components. | |
| 2027 | | | | | | |
| 10 | Implement a function in the form of executable code that provides administrative rights to the Android file system while preserving user data | 01.2027 | 11.2027 | | Executable code will be developed to gain administrative privileges without losing user data. Completion form: software module with documentation. | |
| 10.1 | Develop a prototype PAK | 01.2027 | 11.2027 | | A prototype solution for forensic analysis of protected devices will be created. Completion form: demonstration sample of the PAK with engineering and design documentation. | |
| 10.2 | Development of a software module for decrypting extracted data related to mobile applications, instant messengers and cloud services | 01.2027 | 11.2027 | | A software module will be created to automatically decrypt data. Completion Form: Software and User Manual. | |
| 10.3 | Development of a software module for protecting mobile applications and instant messengers using binary exploitation techniques | 01.2027 | 11.2027 | | A security module will be created to prevent binary attacks. Completion form: software module with technical documentation. | |
| 10.4 | Development of code for decrypting extracted data from cloud services, implementing the functionality of backup storage | 01.2027 | 11.2027 | | A software tool will be created designed to automatically decrypt data received from cloud services. Completion form: Testing the tool on various cloud platforms, preparing guidelines for its use. | |
| 10.5 | Development of a software module for retrieving data from cloud services, implementing the functionality of backup storage | 01.2027 | 11.2027 | | A specialized software module will be created for automated retrieval of information from cloud storage, including encrypted data. Completion form: Preparation of technical documentation, testing on popular cloud platforms and creation of instructions for use in the field of digital forensics. | |
| 10.6 | Development of software modules for access to password-protected backups, mobile applications, instant messengers, cloud services and system settings of the Android operating system | 01.2027 | 11.2027 | | A set of software modules will be developed that will allow access to password-protected data in mobile devices and cloud services, as well as their analysis. Completion form: Development of a prototype software package, testing it on various versions of Android and preparation of methodological materials for law enforcement agencies. | |
| 10.7 | Conduct pilot tests, collect and analyze data to record the actual technical and functional characteristics of the prototype and make adjustments if necessary | 01.2027 | 11.2027 | | The prototype will be tested and subsequently adjusted. Completion Form: Test and Performance Analysis Report. | |
| 11 | Design and submission of monograph materials | 01.2027 | 11.2027 | | One monograph will be published in foreign and (or) Kazakh publishing houses recommended by the scientific council and (or) scientific and technical council of the applicant’s organization | |
| 12 | Preparation and submission of scientific articles on developed methods for decrypting extracted data related to mobile applications, instant messengers and cloud services and protecting mobile applications and instant messengers using binary exploitation techniques | 01.2027 | 11.2027 | | Three articles will be published in journals recommended by COKNVO. | |
| 13 | Develop methodological documentation for using a prototype | 01.2027 | 11.2027 | | A guide to using the developed solution will be compiled. Completion form: methodological documentation. | |
| 14 | Preparation and submission of scientific articles on all developed methods | 01.2027 | 11.2027 | | One article will be published in peer-reviewed scientific publications in the scientific area of ​​the program, included in the 1st (first), 2nd (second) and (or) 3rd (third) quartile by impact factor in the Web of Science database and (or) having a percentile on CiteScore in the Scopus database of at least 50 (fifty). | |

Table 9 - Partner Contribution Plan

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №  n/p | Partner name, address, contact information | Contribution form (no more than 50 words) | Cost of deposit, thousand tenge | Date of entry  (dd.mm.yyyy) |
|
| 1 | 2 | 3 | 4 | 5 |
| 1 | TOO «tLab Technologies»  Astana city, district Almaty, Buyrat street, building 49B, +7 705 844-00-06 | Funds to provide the material and technical base for the implementation of the program.  Providing services for collecting data for analysis and experiments as part of the project. | 3 000,0 | Until 01.09.2025 |
| 2 | TOO «tLab Technologies»  g Astana, district Almaty, Buyrat street, building 49B, +7 705 844-00-06 | Funds to provide the material and technical base for the implementation of the program.  Providing services for collecting data for analysis and experiments as part of the project. | 3 000,0 | Until 01.03.2026 |
| 3 | TOO «tLab Technologies»  Astana city, district Almaty, Buyrat street, building 49B, +7 705 844-00-06 | Funds to provide the material and technical base for the implementation of the program.  Providing services for collecting data for analysis and experiments as part of the project. | 3 000,0 | Until 01.03.2027 |
|  | IN JUST 3 YEARS: |  | 9 000,0 |  |