UDC 004.056.5 **DOI 10.52167/1609-1817-2025-136-1-269-280**

A.K. Shaikhanova[1], D.B. Tyulemissova[1], E.E. Atanbaev[2], K.M. Ayapbergenov[2]
[1]L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
[2]LLC "WebTotem", Astana, Kazakhstan
E-mail: shaikhanova_ak@enu.kz

REVIEW OF EXISTING ADVANCED INNOVATIVE TECHNOLOGIES FOR THE DEVELOPMENT OF SECURE MOBILE COMMUNICATION MEANS, CRYPTO SMARTPHONES, AND SECURE MOBILE APPLICATIONS

Abstract. In the context of the rapid growth of security threats to mobile devices, information protection becomes a critically important task. The article is an overview of modern advanced technologies used for the development of secure mobile communication devices and crypto-smartphones. A bibliometric analysis was conducted using the Bibliometrix tool. The main principles for organizing secure communication have been classified. Innovative approaches are being considered to ensure data integrity and confidentiality. The latest achievements in the field of mobile communication security are also being analyzed. During the research, an informational and patent search for inventions in the field of mobile communication protection was conducted, and a comparative analysis of the advantages and limitations was carried out. The analysis conducted showed that some decisions create a false sense of security, as they propose the adoption of unconventional methods that do not align with well-established and widely accepted safety recommendations.

The article describes the main crypto smartphones, each possessing unique characteristics and designed for specific user needs based on their functional capabilities. The provided examples of successful implementations and research demonstrate the significance of innovative solutions for enhancing the security of mobile communications and protecting personal data in the context of the modern digital world.

Keywords. Secure mobile communication, crypto smartphone, cyber threat, crypto-secured environment, microarchitecture, data protection.

Introduction.

Mobile devices and electronic communication tools of governments and state agencies, especially in the context of international diplomatic, military, and human rights missions, are constantly subjected to surveillance, recording, and attacks on stored and transmitted data using spyware [1]. Faced with such challenges, national governments, state and commercial companies alike are compelled to use specialized mobile communication means to protect against cyberattacks, which must ensure guaranteed security and reliability—regardless of whether they are operated in their own country or abroad, in major cities around the world or in remote areas with poor network coverage and low performance.

The idea of the research is based on the results of analyzing existing threats to the security of mobile and special communications, as well as the shortcomings of current solutions in the field of secure communications [2-4]. Preliminary studies have shown that many existing secure channels and devices are either limited in functionality or do not provide an adequate level of protection against complex cyber threats [5-7], while also requiring significant infrastructure for setup at usage locations and separate support for deploying new temporary infrastructure in cases of user travel within secure networks.

This study examines the main areas of existing scientific research conducted worldwide and in the Republic of Kazakhstan on the development of mobile communication protection means.

The aim of this research is to investigate and analyze existing solutions for the development of secure mobile communication tools, crypto smartphones, along with a description of their functionality.

Materials and Methods.

The main hypothesis of the research is the implementation of a review that allows for the identification of the key methods and principles in the development of secure mobile communication tools, crypto smartphones, and secure mobile applications.

For the implementation of the scientific research, methods of studying and analyzing scientific and methodological literature were applied, along with information and patent searches related to the research problem, as well as approaches based on interdisciplinarity. A tool was used to conduct a comprehensive bibliometric analysis in accordance with the Bibliometrix scientific mapping workflow. The search for theoretical sources was conducted using the scientific resources of the international database Web of Science.

At the initial stage of the research presented in this article, a bibliometric analysis was conducted for a comprehensive study of the problem, in accordance with the workflow of scientific mapping using the Bibliometrix tool. Bibliometrix identifies leading scholars in the field and analyzes the connections between research groups from different countries. Information on data sources was collected using the bibliographic database of scientific articles Web of Science.

As a result of the extended search, 4,038 publications were found that were released in the last three years, from 2021 to 2024. This search was conducted to analyze current trends and approaches to the development of secure mobile communication, crypto smartphones, and secure mobile applications based on programmable logic integrated circuits (PLICs) and microarchitectures.

The first illustration (Fig. 1) shows the number of scientific publications in the field of research on secure mobile devices based on programmable logic integrated circuits and microarchitectures from 2021 to 2024. There has been a steady increase in the number of publications from 2020 to 2022, indicating the importance and relevance of issues related to the development of secure mobile devices. These issues encompass aspects such as the application of PLICs, methods for securing voice communication, audio steganography, and others.

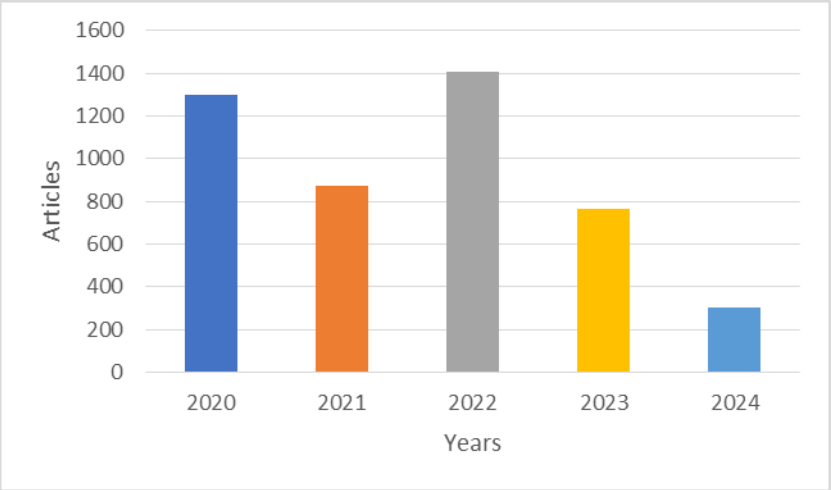

Figure 1 - The number of articles in the field of creating devices based on PLICs in the media for the period from 2021 to 2024

To search for literature from 2021 to 2024, the Web of Science database was used with the following keywords: device development, programmable logic device, cryptographically secure environment, microarchitecture, cryptographic protection, cryptophone, audio, voice. These keywords helped to form the clusters shown in Figure 2.

The results of the analysis conducted using the Bibliometrix tool provide insight into the current state and directions of research in the field of developing devices based on programmable logic integrated circuits and microarchitectures. As shown in Figure 2, researchers' main focus is on microarchitecture, logic gates, and microprocessors.

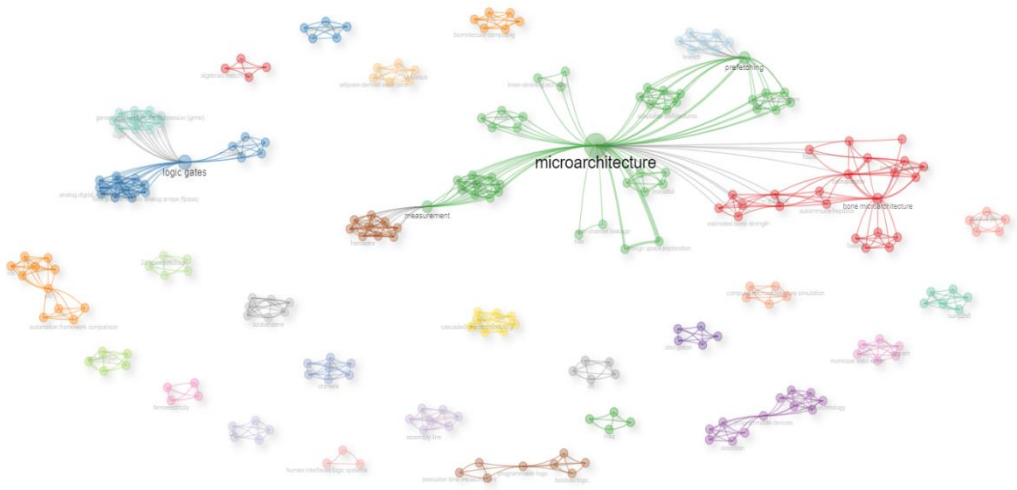

Figure 2 - Network for clustering keyword analysis

Each point on the chart represents an individual publication, and the names of the most prominent authors are also displayed on the graph.

Figure 3 shows the range of words that are most commonly found in quotes.

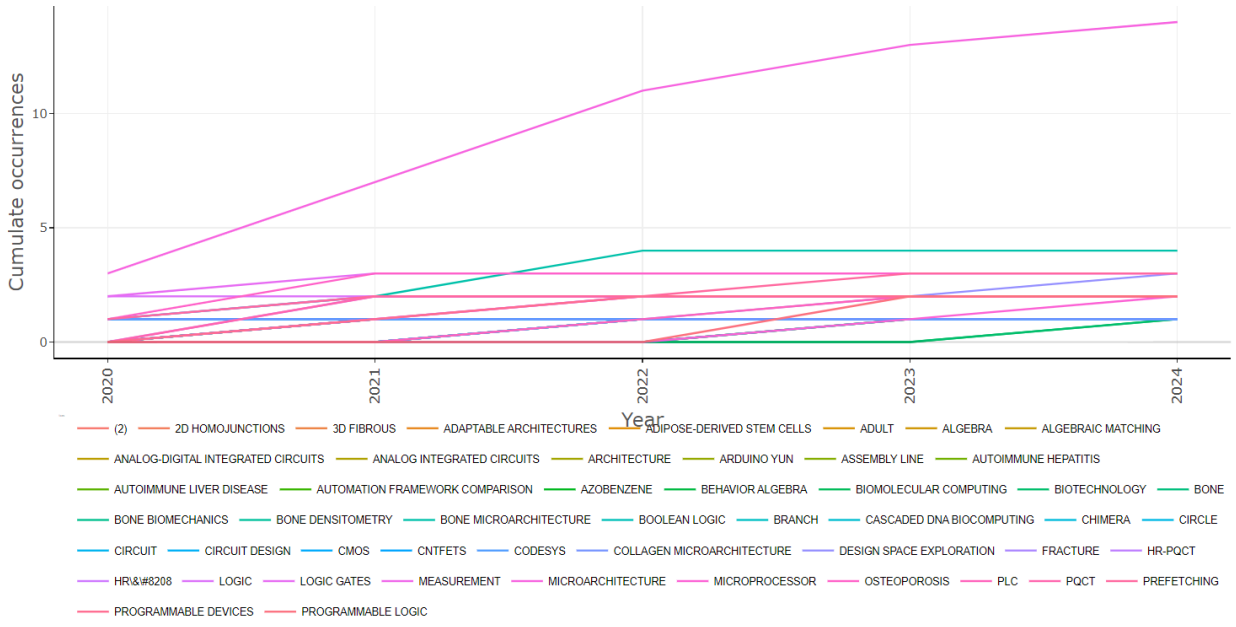

Figure 3 - Words that are most commonly found in quotes

The Bibliometrix software was used to identify keywords by analyzing the most frequently cited terms. The graph shows a timeline demonstrating the periods of highest citation for each keyword from 2021 to 2024. It is clearly evident that "microarchitecture" is the most dominant keyword, as it has been mentioned the most frequently and for the longest duration. Similar conclusions can be drawn regarding other words shown in Figure 3.

The data analysis in Figure 4 allows us to highlight contemporary popular terms such as "architecture," "critical path analysis," and "design space."

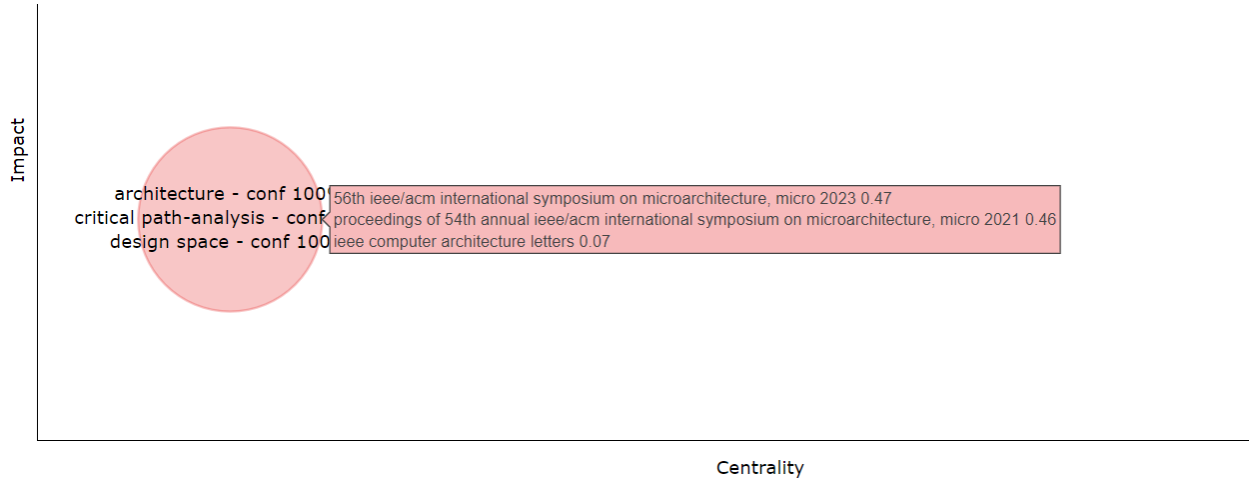

Figure 4 - Clustering by linking keywords with works

From the latest quotes of key terms, we can identify scientific trends and directions in the development of this issue.

Figure 5 shows the most frequently cited scientific works highlighted by the keyword analysis tool.

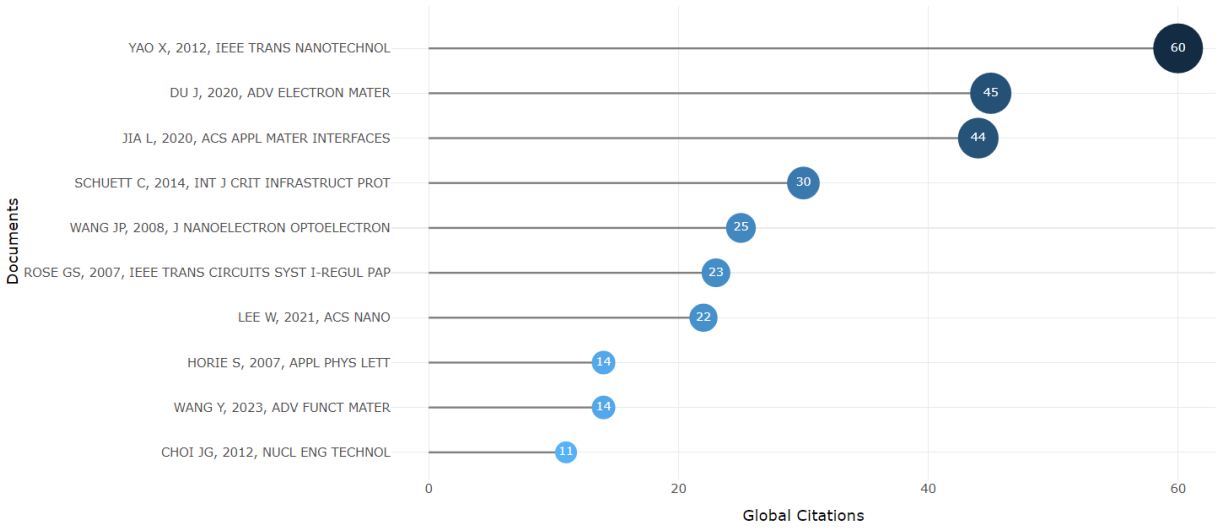

Figure 5 - Most cited documents worldwide

From the perspective of scientific development, international cooperation in researching a specific problem is crucial. The joint efforts of countries, scientific institutions, and researchers contribute not only to progress in this field but also to the development of related scientific disciplines.

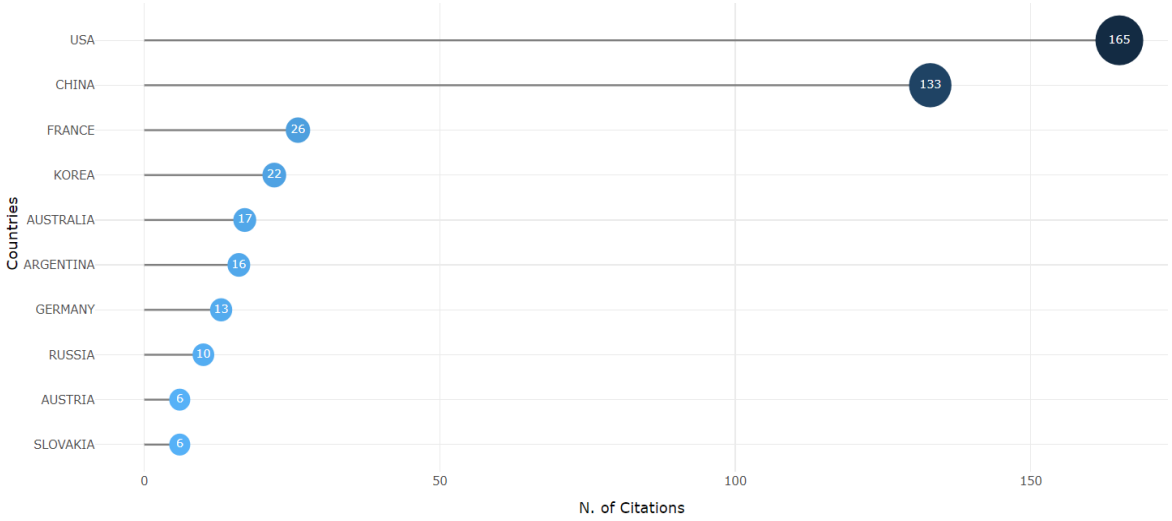

Figure 6 - The number of quotes by a representative of the country

Figure 6 illustrates the activity of countries in citing works related to the research and development of devices based on programmable logic devices. The graph shows that the most cited publications on image encryption were presented by researchers from the USA (165 citations) and China (133 citations). Researchers from France (26 citations), Korea (22 citations), Australia (17 citations), and Argentina (16 citations) also demonstrated high activity.

Results and Discussion.

A literature review of previous scientific studies conducted worldwide and in the Republic of Kazakhstan has shown that currently, three main principles are used for organizing secure communication:

1) Scramblers, or devices that encrypt speech throughout the communication line, are effective for protection against basic interception devices. They mainly consist of a set of additional equipment that must be present at both ends of the conversation, which poses no problems in stationary applications. However, in the context of business trips, it requires carrying extra equipment and personnel to operate it;

2) Cryptophones [11-15], or smartphones with special software installed for cryptographic protection of calls, are mainly implemented based on a regular smartphone using a modified operating system based on Android and/or utilizing special programs;

3) The use of secure messengers and End-to-End encryption programs [1, 16-22] is the simplest method, and at the same time, the most unreliable.

These solutions, to varying degrees of effectiveness, allow for communication with other network subscribers, but they leave vectors of attack when deviating from the conditions of using a specific type of equipment. For example, when there is a requirement for communication through a secure communication channel during a business trip, it is necessary to deploy a special channel. In this case, the device connected to the channel must either be exclusively for use with that setup, or it can be the same mobile phone that is primarily used in an unsecured environment. This limits the mobility of use. Devices, encryption algorithms, and channels are often used for several years and require not only maintenance costs but also expenses for monitoring and vulnerability detection, while there is no guarantee that the devices have not been compromised some time ago, leading to a continuous transmission of critical data to the attacker. To avoid such incidents, it is necessary to frequently change the equipment or update the keys more often. But even this won't protect against malware on the user's device.

Analysis of decisions using additional devices and applications. During the research, an intensive information and patent search was conducted [23-29], and a comparative analysis of

the advantages and limitations of existing modern solutions used in mobile communication protection was carried out (Table 1).

Selected inventions based on the use of additional hardware devices. We have identified three types of such devices:

1) A headset or a specialized device that connects between the headset and the mobile phone;

2) Protected element (SE) in the form of a microSD implementation or a trusted execution environment (TEE);

3) Specialized mobile phone.

It is important to note that the list of solutions that was analyzed is not exhaustive. The products chosen for presentation are those that are representative and have relatively good documentation.

Table 1 - Comparative analysis of solutions in the field of mobile communication security

Patent number and title	**Functionality**	**Advantages**	**Restrictions**
WO2019/097511 PCT/IL2018/051228 CELLULAR PHONE SECURITY PACK METHOD AND APPARATUS	It provides highly secure voice and data encryption features using slightly modified mobile phones and a mechanically attached protective block.	A secure mobile phone with an attached security package based on a cryptographic module.	The only available access for this phone to data is the encrypted data transmission between the private cloud and the phone. Other 3G/4G services are unavailable (regular voice calls, SMS, etc.).
US 10,277,730 BI SMARTPHONE LOCK BOX SYSTEM	A locking box system for smartphones that is used to track and record when and how long a mobile computing device is locked or secured in a container (locking box), without access to the owner of the mobile computing device.	It includes a method for using a blocking system for connected smartphones; the system can provide a report on the accumulated time spent without distractions or without using the smartphone.	The smartphone locking system is used solely to help the owner of the mobile device disconnect from it and devote time and attention to other tasks.
US 2014/0201807 Al SYSTEMS AND METHODS FOR ENFORCING SECURITY IN MOBILE COMPUTING	The described methods and systems relate to enhancing the security of a device by configuring one or more software functions in the trusted zone of the processor using object firewalls, inter-process communication mechanisms, and/or policy engines.	The inter-process communication mechanism and the inter-process communication bus ensure secure inter-process communication between inter-process communication applications within the trusted zone and inter-process communication applications outside the trusted zone.	There is no assessment of the proposed methods and system in the context of a real testing platform.

US 2016/0203326 Al SECURING DATA GATHERING DEVICES OF A PERSONAL COMPUTING DEVICE WHILE PERFORMING SENSITIVE DATA GATHERINGACTIVITIES TO PREVENT THE MISAPPROPRIATION OF PERSONAL USER DATA GATHERED THEREWITH	The functional library ensures the security of personal computer data collection devices on behalf of a secure application program, in order to provide a safer computing session during which actions are taken to collect confidential data using any of these data collection devices.	Exclusive access is achieved by obtaining access to each of the predefined sets and then blocking that access throughout the computing session or, at the very least, until the completion of sensitive data collection operations conducted during that computing session.	There is a lack of security assessment for basic processors from both a software and hardware perspective.
EP 2 699 033 A1 MOBILE COMMUNICATION DEVICE WITH AN INSECURE APPLICATION STORAGE AND A SECURE DATA STORAGE.	A mobile communication device, wherein the communication device comprises at least one unsecured application data storage and at least one secure data storage, with the key stored in the secure storage.	Access to protected memory is blocked by security logic if the specified number of failed authentications is exceeded. The possibility of successfully executing a brute force attack to determine the key is excluded.	It has unprotected application data storage.
WO 2019/088875 A1 SECURE SMARTPHONE	A modular smartphone with protection against unauthorized access to audio information coming from the microphone.	The smartphone's design allows for the physical disconnection of the microphone from the main module.	The additional module must be equipped with an extra battery to power the main module.
3038420 DEVICE AND METHOD FOR CRYPTOGRAPHIC DATA PROCESSING	A device for cryptographic data processing, including a graphics processor. It is used when it is necessary to perform cryptographic processing using a graphics processor.	A cryptographic processing device in which the secure element and the graphics processor are designed to interact only in a secure operating mode.	The security of the basic processor was overlooked.

The analysis of useful models presented in Table 1 showed that some solutions create a false sense of security, as they propose the adoption of unconventional methods that do not align with well-established and widely accepted safety recommendations. In order to draw well-founded conclusions about the performance and safety level of each solution, a common testing platform and detailed documentation are necessary.

One of the most successful solutions can be attributed to the useful model of patent WO 2019/088875 A1. SECURE SMARTPHONE [28]. The utility model relates to smartphone construction, specifically to modular smartphones with protection against unauthorized access to audio information coming from the microphone. In the proposed technical solution, this is achieved by the fact that the smartphone's design allows for the physical disconnection of the

microphone from the main module. Thus, WO2019/088875 proposes to create a smartphone consisting of two modules: a main module that contains all the essential components of the smartphone, ensuring its operation, and an additional removable module that houses the microphone. (fig. 7-9).

In Figure 7, there is an overall view of the additional removable module, where: 6 - additional removable module 7 - connector of the additional removable module for connection to the main module 8 - microphone of the additional removable module.

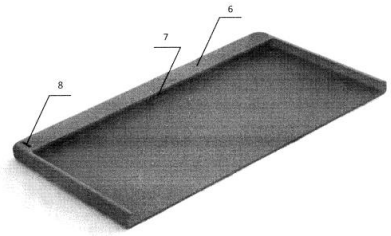

Figure 7 - General view of the additional removable module

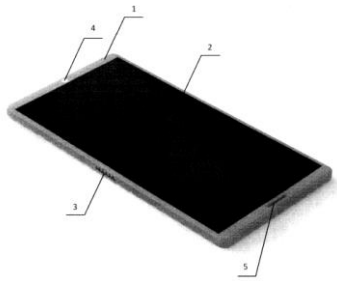

Figure 8 - Overall view of the main module with an additional detachable module connected to it

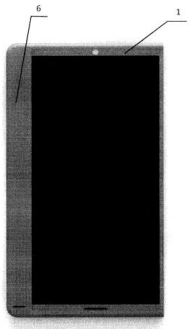

Figure 9 - Overall view of the main module with an additional detachable module connected to it

Figure 8 shows an overall view of the main module with an additional removable module connected to it (the modules are used together as a single device).

Figure 9 shows an overall view of the main module with an additional removable module connected to it (the modules are used together as a single device).

The proposed design allows the smartphone to operate in safe mode and full-function mode.

The authors of the utility model guarantee the user that while using the smartphone in safe mode, there will be no eavesdropping, as the additional removable module with the microphone is physically separated from the main module. However, it is important to note that the additional module must be equipped with an extra battery to power the main module.

Crypto smartphones. There are already many solutions in the world for protecting mobile communication, each with its unique features and designed for specific user needs. For example, smartphones like the BlackPhone and BlackPhone 2 from Silent Circle are equipped with a specialized operating system that supports end-to-end encryption. This allows users to ensure a high level of protection for transmitted data and voice messages.

The Siemens S35 Top-Sec, HC-2413, and STEALTHPHONE use additional devices, such as encryption headsets or built-in microphone encryptors, to protect audio signals transmitted over GSM. These devices encrypt the voice before it is sent, thereby ensuring the confidentiality of the conversations [31].

The ELCRODAT 6-2 system and Tiger 7401 represent more complex solutions used in military and government sectors, where the highest level of information protection is required. These devices guarantee the protection of voice data from malicious actions and information interception [32].

SiMKo 3 also offers comprehensive solutions for encrypting calls and messages, using the L4Re microkernel, which replaces commercial software as a virtualization layer and allows two operating systems to run simultaneously and in real time.

These diverse approaches demonstrate that mobile communication security can be implemented at many levels, from simple hardware disconnection of the microphone and camera to complex encryption systems using modern cryptographic technologies. It is important to choose a solution that best meets the specific requirements and operating conditions in a particular country or industry.

Conclusion.

As part of this research, advanced innovative technologies for the development of secure mobile communication tools, crypto smartphones, and secure mobile applications were analyzed. It is extremely important to not only tackle the challenges of the present but also to prepare in advance for potential complex cyber threats. The use of cloud technologies and virtualization inevitably increases the attack surface, leading to a high dependence on secure software and hardware.

International experience shows that the implementation of comprehensive secure mobile solutions significantly reduces the risks of data leaks and cyberattacks. Examples of successful implementations include secure communication devices for government agencies and military units in the United States and European Union countries, which confirms the demand and effectiveness of such solutions.

The conducted research shows that there is a need to develop a domestic integrated solution that includes hardware protection using a secure bootloader and a modified operating system capable of providing a high level of protection against all types of known attacks. This will contribute not only to enhancing information security but also to improving device performance, thanks to the optimization of software for the user's specific tasks.

Financing. This research has been/was/is funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. BR249014/02240)

REFERENCES

[1] Johansen, C., Mujaj, A., Arshad, H., & Noll, J. The snowden phone: a comparative survey of secure instant messaging mobile applications //Security and Communication Networks. – 2021. – V. 2021. – Pp. 1-30.

[2] Ferrag, M. A., Maglaras, L., Argyriou, A., Kosmanos, D., & Janicke, H. Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes //Journal of Network and Computer Applications. – 2018. – V. 101. – Pp. 55-82.

[3] Salahdine, F., Han, T., & Zhang, N. Security in 5G and beyond recent advances and future challenges //Security and Privacy. – 2023. – V. 6. – № 1. – Paper. e271.

[4] Nguyen, V. L., Lin, P. C., Cheng, B. C., Hwang, R. H., & Lin, Y. D. Security and privacy for 6G: A survey on prospective technologies and challenges //IEEE Communications Surveys & Tutorials. – 2021. – V. 23. – № 4. – Pp. 2384-2428.

[5] Sivaprakash, S., Anbazhagu, U. V., Perumal, I., Kumar, V. V., Mahesh, T. R., & Guluwadi, S. Analysis and attack detection in GSM mobile network with an intelligent jammer using ANFIS classifier //IEEE Access. – 2023. – V. 11. – Pp. 118962-118972.

[6] Gustov V., Levina A. Electromagnetic Fields as a Sign of Side-Channel Attacks in GSM Module //2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS). – IEEE, 2021. – Pp. 1-5.

[7] Bakare B. I., Ekolama S. M. Preventing man-in-the-middle (MITM) attack of GSM calls //European Journal of Electrical Engineering and Computer Science. – 2021. – V. 5. – № 4. – Pp. 63-68.

[8] Raheema A. M., Sadkhan S. B., Satar S. M. A. Performance enhancement of speech scrambling techniques based on many chaotic signals //2020 International Conference on Computer Science and Software Engineering (CSASE). – IEEE, 2020. – Pp. 308-313.

[9] Zghair H. K., Mehdi S. A., Sadkhan S. B. Speech scrambler based on discrete cosine transform and novel seven-dimension hyper chaotic system //Journal of physics: conference series. – IOP Publishing, 2021. – V. 1804. – № 1. – Paper. 012048.

[10] Blintsov, V., Nuzhniy, S., Kasianov, Y., & Korytskyi, V. Mathematical model of the system of active protection against eavesdropping of speech information on the scrambler generator //Eureka: Physics and Engineering – 2020. – № 3. - Pp. 11-22.

[11] GSMK CryptoPhone Baseband Firewall (BBFW). Online https://www.cryptophone.de/ Accessed: May 10, 2024.

[12] Carper T.A., Miller H. Voice encryption device for securing voice communication of cellular phones, has combiner which combines rearranged block of voice data provided from selector with block of voice data to generate encrypted block of voice data // Derwent Primary Accession Number: 2020-329388. – Indexed: 2023-08-10. – Patent Number: US2020127816-A1

[13] Ivanov A.I. Cryptophone handset of fixed wired telephone set containing standard elements of negotiation processes, has main portion that contains functional elements of mobile devices configured to access and use of special mobile applications // Derwent Primary Accession Number: 2021-03352R. – Indexed: 2023-08-10. – Patent Number: RU2019116195-A.

[14] Zhang N., Hang N., Jiang R., Hu X. Voice encryption device for e.g. global system for mobile communication (GSM) mobile phone, has field programmable gate array (FPGA) module which receives voice signals to perform voice encryption based on encrypting function. // Derwent Primary Accession Number 2011:H53753**. –** Indexed: 2023-08-10. **–** Patent Number: CN102075321-A, B.

[15] Li Y., Jiang J., Zkang P., Zhang J., Gong X. Encryption and decryption device for voice communication of mobile terminal, has processing unit provided with encryption chip for encrypting or decrypting collected voice signal, and encryption and decryption key fixed in encryption chip // Derwent Primary Accession Number**:** 2019-89196R**. –** Indexed**:** 2023-08-10. **–** Patent Number: CN209526781-U.

[16] Kamarudin, N. K., Bismi, N. S., Zukri, N. H. A., Fuzi, M. F. M., & Ramle, R. Network Security Performance Analysis of Mobile Voice Over Ip Application (mVoIP): Kakao Talk, WhatsApp, Telegram and Facebook Messenger //Journal of Computing Research and Innovation. – 2020. – V. 5. – № 2. – Pp. 21-27/

[17] Dreßler P., Fischer D. and Markscheffel B. Software solutions for high-security voice and data communication for smartphones // 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014), London, UK. – 2014. – Pp. 327-332

[18] Hayati N., Suryanto Y., Ramli K. and Suryanegara M. End-to-End Voice Encryption Based on Multiple Circular Chaotic Permutation //2019 2nd International Conference on Communication Engineering and Technology (ICCET). – 2019. - Pp. 101-106.

[19] Lubkowski, P., Polak, R., Sierzputowski, R., & Laskowski, D. Assessment of voice call quality in SCIP encrypted traffic // XII Conference on Reconnaissance and Electronic Warfare Systems. - 2019. - Vol. 11055. - Pp. 115-122.

[20] Krasnowski P., Lebrun J., Martin B. A novel distortion-tolerant speech encryption scheme for secure voice communication // Speech Communication. – 2022. – V. 143.– Pp. 57-72.

[21] Seitkulov Y., Boranbayev S., Tashatov N., Davydau H., Patapovich A. Speech information security assessing in case of combined masking signals // Journal of Theoretical and Applied Information Technology. – 2020. – V. 98. – №16. - Pp. 3270-3281.

[22] C. Ntantogian, E. Veroni, G. Karopoulos, and C. Xe-nakis, “A survey of voice and communication pro-tection solutions against wiretapping,” en, Computers& Electrical Engineering, vol. 77, pp. 163–178, Jul.2019, ISSN: 00457906. DOI: 10.1016/j.compeleceng.2019.05.008.

[23] Patent WO2019/097511 PCT/IL2018/051228. Cellular phone security pack method and apparatus.

[24] Patent US 10,277,730 BI. Smartphone lock box system.

[25] Patent US 2014/0201807 Al. Systems and methods for enforcing security in mobile computing.

[26] Patent US 2016/0203326 Al. Securing data gathering devices of a personal computing device while performing sensitive data gatheringactivities to prevent the misappropriation of personal user data gathered therewith.

[27] Patent EP 2 699 033 A1. Mobile communication device with an insecure application storage and a secure data storage.

[28] Patent WO 2019/088875 A1. Secure smartfone.

[29] Patent 3038420. Device and method for cryptografic data processing.

[30] Pisaric M. Encrypted mobile phones //Archibald Reiss Days. – 2021. – V. 11.

[31] Ntantogian, C., Veroni, E., Karopoulos, G., & Xenakis, C. A survey of voice and communication protection solutions against wiretapping. //Computers & Electrical Engineering. – 2019. – V. 77. – Pp. 163-178.

[32] Belous, A., Saladukha, V., Belous, A., & Saladukha, V. Hardware trojans in electronic devices. // Viruses, Hardware and Software Trojans: Attacks and Countermeasures. – 2020. -Pp. 209-275.

[33] Danisevskis J. Accelerated secure GUI for virtualized mobile handsets. – Technische Universitaet Berlin (Germany). – 2017. – 167 p.

Айгуль Шайханова, PhD, профессор, L.N. Gumilyov Eurasian National University, Астана, Қазақстан, aigul.shaikhanova@gmail.com

Дана Тюлемисова, докторант, L.N. Gumilyov Eurasian National University, Астана, Қазақстан, tyulemissova_db_3@enu.kz

Ернат Атанбаев, магистр, ТОО WebTotem, Астана, Қазақстан, yernat@wtotem.com

Камиль Аяпбергенов, магистр, ТОО WebTotem, Астана, Қазақстан, ayapbergenov.kamil@gmail.com

ҚАУІПСІЗ МОБИЛЬДІ БАЙЛАНЫСТАРДЫ, КРИПТО СМАРТФОНДАР МЕН ҚАУІПСІЗ МОБИЛЬДІ ҚОЛДАНБАЛАРДЫ ДАМЫТУ ҮШІН ҚОЛДАНЫЛҒАН ОЗЫҚ ИННОВАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАРҒА ШОЛУ

Аңдатпа. Мобильді құрылғылардың қауіпсіздігіне қауіп төніп тұрған кезде ақпаратты қорғау маңызды мәселеге айналып отыр. Мақалада қауіпсіз ұялы байланыс пен крипто-смартфондарды дамыту үшін қолданылатын заманауи озық технологияларға шолу жасалады. Bibliometrix құралы арқылы библиометриялық талдау жүргізілді. Қауіпсіз байланыстарды ұйымдастырудың негізгі принциптері жіктеледі. Деректер тұтастығы мен құпиялылығын қамтамасыз ету үшін инновациялық тәсілдер қарастырылады. Сондай-ақ ұялы байланыс қауіпсіздігі саласындағы соңғы жетістіктер сараланады. Зерттеу барысында ұялы байланысты қорғау саласындағы өнертабыстарға ақпараттық-патенттік іздеу жүргізіліп, артықшылықтар мен шектеулерге салыстырмалы талдау жасалды. Талдау көрсеткендей, кейбір шешімдер қабылданған және жалпы қабылданған қауіпсіздік

нұсқауларына сәйкес келметін стандартты емес әдістерді қабылдауды ұсына отырып, жалған қауіпсіздік сезімін тудырады.

Мақалада өзіндік бірегей сипаттамалары бар және олардың функционалдығы негізінде пайдаланушының нақты қажеттіліктеріне арналған негізгі криптосмартфондар сипатталған.

Сәтті енгізулер мен зерттеулердің келтірілген мысалдары заманауи цифрлық әлемде ұялы байланыстың қауіпсіздік деңгейін арттыру және жеке деректерді қорғау үшін инновациялық шешімдердің маңыздылығын көрсетеді.

Түйінді сөздер. Қауіпсіз ұялы байланыс, криптографиялық смартфон, киберқауіп, крипто-қауіпсіз орта, микроархитектура, деректерді қорғау.

Айгуль Шайханова, PhD, профессор, L.N. Gumilyov Eurasian National University, Астана, Казахстан, aigul.shaikhanova@gmail.com

Дана Тюлемисова, докторант, L.N. Gumilyov Eurasian National University, Астана, Казахстан, tyulemissova_db_3@enu.kz

Ернат Атанбаев, магистр, ТОО WebTotem, Астана, Казахстан, yernat@wtotem.com

Камиль Аяпбергенов, магистр, ТОО WebTotem, Астана, Казахстан, ayapbergenov.kamil@gmail.com

ОБЗОР СУЩЕСТВУЮЩИХ ПЕРЕДОВЫХ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ ПО РАЗРАБОТКЕ СРЕДСТВ ЗАЩИЩЕННОЙ МОБИЛЬНОЙ СВЯЗИ, КРИПТО СМАРТФОНОВ И ЗАЩИЩЕННЫХ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

Аннотация. В условиях стремительного роста угроз безопасности мобильных устройств защита информации становится критически важной задачей. Статья представляет собой обзор современных передовых технологий, применяемых для разработки защищенных мобильных средств связи и крипто-смартфонов. Произведен библиометрический анализ с использованием инструмента Bibliometrix. Классифицированы основные принципы для организации защищенной связи. Рассматриваются инновационные подходы для обеспечения целостности и конфиденциальности данных. Также анализируются последние достижения в сфере защиты мобильной связи. В ходе исследования проведен информационно-патентный поиск изобретений в сфере защиты мобильной связи и выполнен сравнительный анализ достоинств и ограничений. Проведенный анализ показал, что некоторые решения создают ложное чувство безопасности, так как предлагают принятие нестандартных методов, которые не соответствуют хорошо установленным и широко принятым рекомендациям по безопасности.

В статье описаны основные крипто смартфоны, обладающие своими уникальными характеристиками и предназначенные для определенных пользовательских потребностей на основе их функциональных возможностей.

Приведенные примеры успешных реализаций и исследований демонстрируют значимость инновационных решений для повышения уровня безопасности мобильной связи и защиты персональных данных в условиях современного цифрового мира.

Ключевые слова. Защищенная мобильная связь**,** крипто смартфон, киберугроза, крипто-защищенная среда, микроархитектура, защита данных.

****

Редакцияға түсті / Поступила в редакцию / Received 20.09.2024
Жариялауға қабылданды / Принята к публикации / Accepted 13.02.2025