Research Inventy: International Journal of Engineering And Science
Vol.15, Issue 9 (September 2025), PP 49-54
Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com

Imei Registration Under Conditions Of Mass 5g Deployment: Problems And Solutions

[1]Dilmurod Davronbekov, [2]Jamshid Isroilov
[1] Department of technologies of Mobile communication Tashkent University of Information Technologies named after Muhammad al-Khwarizmi 108, Amir Temur street, Tashkent, Uzbekistan.
[2] Department of technologies of Mobile communication Tashkent University of Information Technologies named after Muhammad al-Khwarizmi 108, Amir Temur street, Tashkent, Uzbekistan.
Corresponding Author: Jamshid Isroilov, email: jamshidisroilov@gmail.com

Abstract: *The article presents an analysis of the development of the IMEI and IMEISV structures, considers their functions under conditions of mass deployment of multi-mode and multi-frequency terminals, and also identifies the main technical problems: limited format, overload of national and international databases, vulnerability to cloning, integration difficulties with eSIM/iSIM and mass IoT connections. Particular attention is paid to scalability and security issues under conditions of exponential growth in the number of connected devices. Possible solution directions are proposed: expansion of the IMEI structure, introduction of next-generation digital identifiers (IoT-ID, UCI), use of cryptographic protection, modernization of the EIR/CEIR database architecture using distributed and blockchain technologies, as well as the application of machine learning for automatic anomaly detection.*

Keywords: IMEI, IMEISV, Type Allocation Code (TAC), Software Version Number (SVN), EIR/CEIR, eSIM/iSIM, IoT-ID, Unified Communication Identifier (UCI), cryptographic protection, blockchain, 5G NR, 6G, Non-Terrestrial Networks (NTN).

Keywords: *Ibuprofen, derivatives, Phaseolus vulgaris, Callosobruchus maculatus, Mortality.*

Date of Submission: 15-09-2025 Date of acceptance: 30-09-2025

I. INTRODUCTION

The International Mobile Equipment Identity (IMEI) has undergone profound evolution from a simple mechanism of device accounting in GSM networks to a key element of the infrastructure of global 4G/5G networks. Historically, IMEI registration performed the function of device authenticity control in GSM/UMTS/LTE networks and supported the operation of the Equipment Identity Register (EIR) and the Centralized Equipment Identity Register (CEIR) [1]. However, with the transition to 5G and the mass spread of eSIM/iSIM, multi-frequency terminals, as well as IoT devices, traditional registration approaches faced a number of limitations [2]. Among the most acute problems are the scalability of national and global IMEI databases, vulnerability to identifier cloning, imperfection of registration procedures in countries with different legal systems, as well as the absence of cryptographic protection of the identifier.

Despite the fact that in a number of states (India, Turkey, Uzbekistan, Nigeria, etc.) laws on mandatory IMEI registration have been introduced, at the global level the issue of unifying procedures and ensuring compatibility of national registers with GSMA international databases remains open. Additional difficulties are created by the integration of devices with virtual profiles (eSIM/iSIM), where the traditional binding to a physical SIM card loses its significance, and the role of IMEI as an anchor identifier increases.

Thus, the need to rethink IMEI registration procedures under conditions of mass 5G deployment is a relevant research task. Existing scientific publications focus mainly on the technical aspects of identification and cryptographic protection of mobile devices, however they insufficiently reveal the issues of scalability, legal regulation, and global harmonization of IMEI registration..

II. MATERIALS AND METHODOLOGY

2.1 Evolution of IMEI and its registration (from 2G to 5G)

IMEI (International Mobile Equipment Identity) was first introduced in second-generation (GSM) networks in the early 1990s as a 15-digit identifier of mobile equipment. Its structure included TAC (Type Approval Code), FAC (Final Assembly Code), SNR (Serial Number), and check digit (CD). The main goal was to ensure unique device identification, prevent the use of stolen terminals, and support national and operator EIR (Equipment Identity Register) databases [3].

With the growth in the number of manufacturers and models of phones, as well as the appearance of updatable software, the IMEI format in third-generation (3G) networks was expanded to IMEISV (International Mobile Equipment Identity and Software Version). A field SVN (Software Version Number, 2 digits) was added. This made it possible to take into account software versions and eSIM profile increases, as well as block devices with vulnerable software [4].

The further transition of networks to LTE (4G) was accompanied by exponential growth in the number of devices and frequency bands, strengthening the importance of IMEISV as a universal identifier for multi-mode devices (GSM/UMTS/LTE), integration of IMEI into national and international databases (CEIR, GSMA IMEI DB).

The problem of IMEI cloning and forgery became widespread, which forced many countries to introduce laws on mandatory IMEI registration (India, Turkey, Ukraine, Uzbekistan, etc.).

In fifth-generation (5G NR) networks, IMEISV retained the previous structure (TAC + SNR + SVN), however the conditions of its application changed [5]:

- support for multi-frequency (FR1, FR2) and multi-mode (2G/3G/4G/5G in one device);
- integration with eSIM and iSIM, where IMEI performs the role of the anchor device identifier;
- growth of the importance of centralized international IMEI databases;
- the need to strengthen security (cryptographic protection is still absent).

Table 1 provides a comparison of the IMEI/IMEISV structure in networks from 2G to 5G.

Table 1- Comparison of IMEI/IMEISV structure (2G–5G)

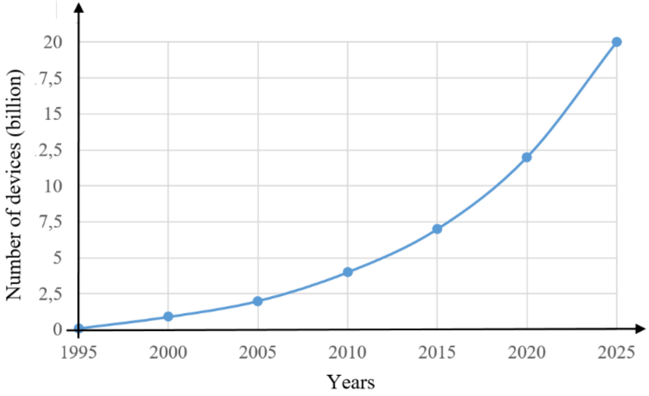
№	Поле	2G (GSM)	3G (UMTS)	4G (LTE)	5G (NR)
1	TAC (Type Allocation Code)	6 digits	8 digits	8 digits	8 digits
2	FAC (Final Assembly Code)	2 digits	–	–	–
3	SNR (Serial Number)	6 digits	6 digits	6 digits	6 digits
4	CD (Check Digit)	1 digit	–	–	–
5	SVN (Software Version Number)	–	2 digits	2 digits	2 digits + eSIM/iSIM support

Table 1 shows the evolution of the structure of the international equipment identifier: from the classical IMEI format in GSM (TAC, FAC, SNR, CD) to IMEISV in UMTS/LTE/5G, supplemented by the SVN field. In 5G the IMEISV format is preserved, but the role of additional identifiers (eSIM/iSIM), as well as the need for future expansion for IoT integration, increases.

2.2. Mass deployment of 5G and IMEI registration challenges

Fifth-generation (5G NR) networks are characterized not only by increased throughput and support for new services (eMBB, URLLC, mMTC), but also by exponential growth in the number of connected devices, which poses new challenges in the field of their accounting, identification, and registration. According to ITU and GSMA forecasts, by 2030 the number of active connections will exceed 25–30 billion (Figure 1), with a significant part of them functioning in multi-band and multi-mode networks, supporting both traditional terrestrial infrastructure and satellite segments (NTN — Non-Terrestrial Networks), with more than 60% being IoT devices. Each of them requires a unique identifier, which significantly increases the load on national and global IMEI databases [6].

Figure 1. Growth of the number of devices with IMEI registration (1995–2025).



The traditional architecture of the Equipment Identity Register (EIR) and Central Equipment Identity Register (CEIR) was designed to account for millions, but not billions of devices. The mass deployment of 5G led to the following challenges:

- the need for constant expansion of storage volumes;
- difficulties in synchronizing national and international databases;
- increase in response time when checking IMEI under peak loads;
- the need for automated management of “black” and “white” device lists.

One of the main challenges is the problem of IMEI cloning (Figure 2) [7]. Despite the presence of centralized registers, cases of terminals using duplicate identifiers are recorded in 5G networks. The main risks are undermining trust in authentication systems, illegal use of network resources, and the impossibility of correct law enforcement (for example, in lawful interception).

Figure 2. Problems with IMEI cloning.

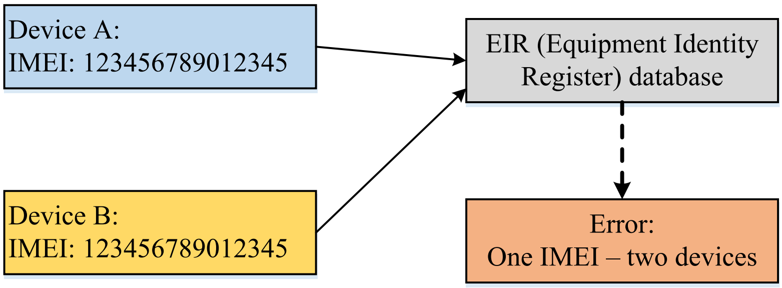


Figure 2 shows a situation where two different devices use the same IMEI. When accessing the EIR database, an identification error occurs, which undermines the reliability of equipment control systems, makes accurate terminal authentication impossible, and increases the risks of illegal use of network resources [8].

The appearance of embedded SIM (eSIM) and integrated SIM (iSIM) changed the nature of user binding to the device. If earlier IMSI (SIM card) and IMEI (terminal) formed the “subscriber–device” link, then with SIM virtualization, the IMEI as the anchor of physical equipment acquires the main significance. However, eSIM/iSIM complicate the registration procedure, since profiles can change dynamically, the risk of substitution or use of uncertified devices with a valid eSIM profile increases [9].

Another separate issue is regional and legal aspects. In a number of countries, laws on mandatory IMEI registration in national databases are in force. However, at the global level there is no single regulation, which leads to such problems as fragmentation of systems (different countries use uncoordinated database formats), data exchange gaps between national registers and the GSMA IMEI DB, differences in legal regimes (from strict control (with mandatory blocking of uncertified devices) to minimal regulation).

The absence of cryptographic protection is also an issue requiring solutions. IMEI and IMEISV remain open digital identifiers. Under 5G conditions, this creates such threats as [10]:

- falsification of numbers using firmware and software;
- mass cloning in illegal workshops;
- impossibility of fully guaranteeing uniqueness.

Thus, the mass deployment of 5G has intensified challenges related to IMEI registration: scalability, security, legal regulation, and integration with eSIM/iSIM. These problems require a systemic solution [11].

Among the main technical problems of IMEI identifier registration in 5G networks are the limitations of the IMEISV structure, the scalability of IMEI databases, and the mass nature of IoT devices.

1) Limitations of the IMEISV structure

The IMEISV format, including TAC (8 digits) + SNR (6 digits) + SVN (2 digits), historically ensured uniqueness and identification of equipment. However, under 5G conditions this format encounters a number of limitations:

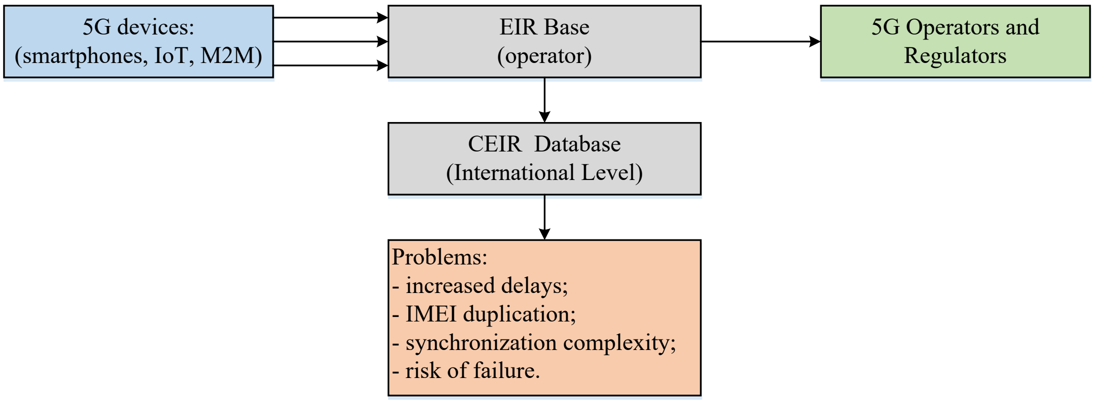
- limited SVN length (only 2 digits), which allows a maximum of 100 software versions;
- fixed length of the identifier (16 digits), which becomes a bottleneck with the growth in the number of devices and the complexity of their functions;
- absence of special fields for identifying IoT terminals, multi-module devices, and integrated chipsets.

2) Scalability of IMEI databases

The growth in the number of devices in 5G, including smartphones, IoT modules, and M2M terminals, leads to a significant load on the Equipment Identity Register (EIR) systems. Among the main technical problems it is necessary to note the increase in response time when accessing IMEI databases, synchronization difficulties between national and international registers, and the risk of record duplication under conditions of mass IoT equipment integration.

The diagram reflects the growth of load on Equipment Identity Register (EIR) and Central Equipment Identity Register (CEIR) systems under exponential increase in the number of devices (smartphones, IoT, M2M) in fifth-generation networks (Figure 3).

Figure 3. Overload of EIR/CEIR databases under mass 5G deployment.



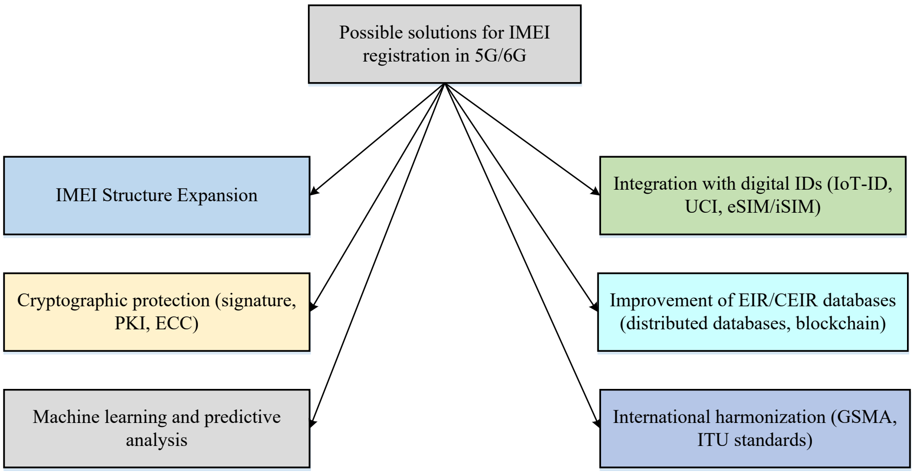
3) Mass nature of IoT devices

In 5G, IMEI began to be used not only for phones but also for numerous sensors and IoT terminals. This aggravates the following problems:

- mass registrations of billions of new devices annually;
- technical limitations of databases in storage and search of records;
- the need for new identifiers (for example, IoT-ID or UCI), which would complement IMEI.

Possible solutions and key directions for the development of the identification and accounting system of devices for IMEI registration under 5G/6G conditions are shown in Figure 4.

Figure 4. Possible solutions for IMEI registration under 5G/6G conditions.


Possible solutions for IMEI registration in 5G/6G
IMEI Structure Expansion
Cryptographic protection (signature, PKI, ECC)
Machine learning and predictive analysis
Integration with digital IDs (IoT-ID, UCI, eSIM/iSIM)
Improvement of EIR/CEIR databases (distributed databases, blockchain)
International harmonization (GSMA, ITU standards)

1) Expansion of the IMEI structure. One of the directions of development may be the increase in the length of the IMEI/IMEISV identifier [12]:

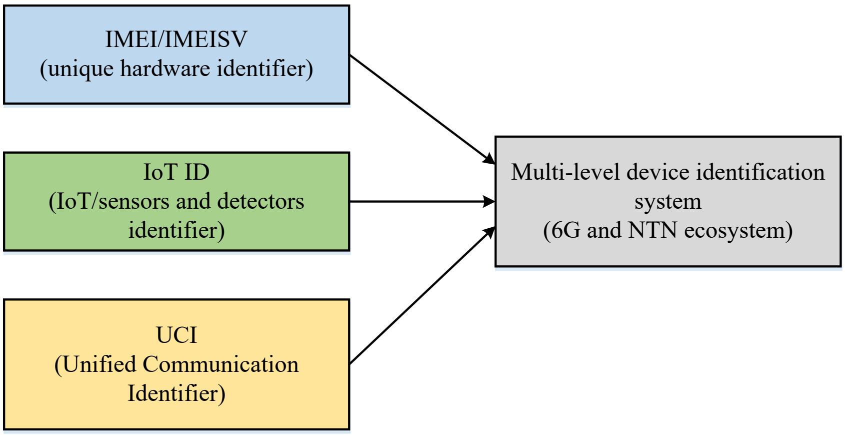
- expansion of the TAC (Type Allocation Code) field to account for the growing number of manufacturers and models;
- addition of new fields for IoT devices and embedded chipsets;
- development of the IMEI+ format, ensuring scalability in the 6G era.

2) Integration with digital identifiers. To increase resilience, the formation of a multi-level identification system is proposed (Figure 5):

- combination of IMEI with IoT-ID for sensors and actuators;
- integration with UCI (Unified Communication Identifier) for unification in the global ecosystem;

- binding to eSIM/iSIM profiles, which will reduce substitution risks [13].

Figure 5. Concept of multi-level identification (IMEI + IoT-ID + UCI)


IMEI/IMEISV
(unique hardware identifier)
IoT ID
(IoT/sensors and detectors identifier)
UCI
(Unified Communication Identifier)
Multi-level device identification system
(6G and NTN ecosystem)

The diagram demonstrates a possible direction for the development of device identification in the era of 6G and NTN. The traditional IMEI/IMEISV remains the basic equipment identifier, but it is supplemented by a specialized IoT-ID for mass connections of sensors and M2M terminals, as well as by the universal UCI (Unified Communication Identifier), providing global unification at the ecosystem level. The joint use of these identifiers forms a multi-level system that increases the resilience, scalability, and security of next-generation networks.

3) Introduction of cryptographic protection. To prevent IMEI cloning it is necessary to introduce methods of cryptographic verification. These may include [14]:

- digital signature embedded in IMEI at the manufacturer level;
- use of asymmetric algorithms (RSA, ECC) for authenticity confirmation;
- integration with PKI infrastructure of operators and regulators.

4) Improvement of EIR/CEIR databases. To combat overload of national and international IMEI databases it is advisable to:

- transition to distributed databases with big data architecture support;
- introduction of blockchain technologies for decentralized IMEI verification;
- development of global exchange interfaces (API) for automated control.

5) Machine learning and predictive analytics. Modern data analysis methods can be applied to detect anomalies in the IMEI database [15]:

- use of ML algorithms to detect suspicious IMEIs;
- forecasting of database overload risks;
- automatic detection of cloning attempts.

6) International harmonization of registration procedures. Solving technical problems is impossible without unification of legal and organizational approaches. In this aspect, the following directions are promising:

- creation of a single global IMEI registration standard under the auspices of GSMA and ITU;
- integration of national databases into the GSMA IMEI DB international system;
- data exchange between operators and regulators in real time.

The combined implementation of these directions can ensure the scalability, resilience, and security of the global IMEI registration system in the era of 5G and future 6G networks.

III. RESULTS AND DISCUSSIONS

The IMEI system, originally developed for controlling mobile phones in GSM networks, has undergone significant evolution and has become a fundamental element of the infrastructure of modern 4G/5G networks. The main technical problems have been identified: the limited structure of IMEISV, the increasing load on EIR/CEIR databases, vulnerability to cloning, integration difficulties with eSIM/iSIM, and the mass adoption of IoT devices. These factors create a threat to the stability and security of the global mobile ecosystem.

IV. CONCLUSION

The proposed solutions include the expansion of the IMEI format, the use of additional digital identifiers (IoT-ID, UCI), the introduction of cryptographic protection methods, modernization of databases based on distributed architectures and blockchain technologies, as well as the application of machine learning methods for predictive analysis.

It is forecasted that in the future, device registration will be based on a multi-level identification system, where IMEI will be only one of the elements. Integration with new digital identifiers and international harmonization of registration processes will be key conditions for ensuring scalability, resilience, and trust in the global mobile infrastructure of the future.

REFERENCES

[1]. ITU-T. Reliability of International Mobile Station Equipment Identity (IMEI). Technical Report QTR-RLB-IMEI. Geneva: International Telecommunication Union, 2020. – 17 p. URL: https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-CCICT-2020-PDF-E.pdf (accessed: 13.09.2025).

[2]. Alsunaidi S.J., Almuhaideb A.M. The Security Risks Associated With IMEIs And Security Solutions // 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS). – 2019. DOI: 10.1109/CAIS.2019.8769521 (accessed: 13.09.2025).

[3]. D.A.Davronbekov, K.P.Abdurakhmanov, M.O.Sultonova, J.D.Isroilov, A.S Kiriakidi. Identification of Mobile Devices by IMEI: Monograph. – Tashkent: TUIT, 2019. – 108 p.

[4]. El-Gohary E., Shehata A. A New Design Approach for Mobile Devices Security against IMEI Tampering and Cloning // International Journal of Innovative Research in Computer and Communication Engineering. – 2017. – Vol. 5, No. 8. – Pp. 16432–16439. (accessed: 13.09.2025).

[5]. Davronbekov D.A., Isroilov J.D. Evolution of IMEI Standards in the Context of the Transition to Multi-Frequency Wireless Communications // Raqamli iqtisodiyot Scientific Electronic Journal. – No. 12, 2025. – Pp. 208–220.

[6]. D.Davronbekov, A.Kiriakidi, D.Yelkin, J. Isroilov, M.Nurmatova. Status and Analysis of the Mobile Device Market for Creating a Unified IMEI-Based Identification Database // International Scientific Journal «Science and World». – 2018. – No. 11(63). Vol. I. – Pp. 41–42.

[7]. M.S.M.A. Notare, A.Boukerche, F.A.S. Cruz, B.G.Riso, C.B.Westphall. Security Management Against Cloning Mobile Phones // Seamless Interconnection for Universal Services. Global Telecommunications Conference. GLOBECOM'99. (Cat. No.99CH37042), Rio de Janeiro, Brazil, 1999, pp. 1969–1973, vol. 3. doi: 10.1109/GLOCOM.1999.832514 (accessed: 13.09.2025).

[8]. J.Isroilov, D.Davronbekov, Z.Khakimov, M.Abdullaev, N.Turaxodjaev. Assessment of the Reliability of the Information System for Identifying Mobile Devices by IMEI Code // TransSiberia 2023. E3S Web of Conferences 402, 03040 (2023). https://doi.org/10.1051/e3sconf/202340203040

[9]. National Institute of Standards and Technology (NIST). Guidelines for Managing the Security of Mobile Devices in the Enterprise. Special Publication 800-124r2. Gaithersburg: NIST, 2023. – 51 p. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r2.pdf (accessed: 13.09.2025).

[10]. Sh.U.Pulatov, D.A.Davronbekov, J.D.Isroilov, A.Sh.Gafurov, N.S.Turakhodjaev. Some Methods of Mobile Phone Cloning // Muhammad al-Khorazmiy avlodlari. – No. 2(20), 2022. – Pp. 156–161.

[11]. D.Davronbekov, J.Isroilov, Z.Khakimov. Architecture of Organizing IMEI Code Registration in the Database of the Information System for Mobile Device Identification // International Scientific Journal «Science and World». – 2020. – No. 10(86). – Pp. 39–43.

[12]. Shikah J. Alsunaidi, Abdullah M. Almuhaideb. Investigation of the Optimal Method for Generating and Verifying the Smartphone’s Fingerprint: A Review // Journal of King Saud University – Computer and Information Sciences. – Vol. 34, Issue 5, 2022. – Pp. 1919–1932. https://doi.org/10.1016/j.jksuci.2020.06.007 (accessed: 13.09.2025).

[13]. Chandrasekaran V., Amjad F., Sharma A., Subramanian L. Secure Mobile Identities // arXiv preprint. – 2016. – arXiv:1604.04667. URL: https://arxiv.org/abs/1604.04667 (accessed: 13.09.2025).

[14]. Khan M., Niemi V. Concealing IMSI in 5G Network Using Identity-Based Encryption // arXiv preprint. – 2017. – arXiv:1708.01868. URL: https://arxiv.org/abs/1708.01868 (accessed: 13.09.2025).

[15]. Sh.U.Pulatov, J.D.Isroilov, A.Sh.Gafurov. Mobile Phone Cloning // Republican Scientific-Technical Conference “The Role of ICT in the Innovative Development of Economic Sectors”, Proceedings. – Tashkent, 2022. – Pp. 181–184.