

Biometrics in the Process of Concluding and Registering Real Estate Transactions: Limits of Acceptability, Guarantees of Subject Rights, and Standards of Protection against Digital Fraud

Roman Sergeevich Aleshin

Independent Researcher, Krasnodar Krai, Slavyansk-on-Kuban, RUSSIAN FEDERATION

Date of Submission: 09-10-2022

Date of Acceptance: 30-10-2022

Date of Publication: 31-10-2022

ABSTRACT

The introduction of biometric identification into real estate transactions creates a fundamentally new configuration of legal relations, in which the technical reliability of verification conflicts with constitutional guarantees of privacy and the legal certainty of civil transactions. The purpose of this article is to examine the legal limits of biometric identification in concluding and registering real estate transactions, analyze the system of guarantees of the rights of biometric data subjects, and develop recommendations for improving protection mechanisms against digital fraud. The methodology consists of a comparative legal analysis, a systematic literature review, and a content analysis of regulatory documents. The study identified systemic gaps in Russian legislation and proposed a proprietary model of biometric verification for state real estate registration, as well as a conceptual framework for legal regulation. The results are of interest to practicing lawyers, notaries, Rosreestr officials, and developers of state information systems in the real estate sector.

Keywords- biometric identification, real estate transactions, state registration, personal data, digital fraud, anti-spoofing, legal guarantees for entities, remote notarization, Rosreestr.

I. INTRODUCTION

The rapid digitalization of property transactions has brought renewed attention to the problem of verifying the identities of parties to real estate transactions. This category of transactions is particularly sensitive because it involves substantial property values and often produces legal consequences that cannot readily be reversed. According to Rosreestr, approximately 6.8 million purchase and sale agreements and other real estate transactions were registered in 2022, more than 34% of which were submitted electronically [1]. At the same time, the Bank of Russia reported a sustained increase in fraud involving forged documents in transactional activities. In 2021, such offenses accounted for 12.4% of all economic crimes, while the aggregate losses exceeded RUB 4.6 billion [2]. These figures suggest that traditional methods of identifying transaction participants no longer provide an adequate level of protection for property rights.

Legislative interest in biometrics as a means of identity verification was reflected in the adoption of Federal Law No. 572-FZ of December 29, 2022, "On the Identification and/or Authentication of Individuals Using Biometric Personal Data," which substantially reformed the architecture of the Unified Biometric System (UBS). Nevertheless, the application of biometric technologies in the real estate sector gives rise to several legal conflicts. Questions concerning informed consent, the permissible limits of biometric-data processing, technical anti-spoofing standards, and the civil-law consequences of a transaction completed through a compromised biometric session remain without an unequivocal legislative answer. These circumstances reveal a significant scholarly gap in the legal framework governing the use of biometric technologies in property transactions.

At the international level, the regulation of biometrics is being actively developed within the framework of the EU AI Act [3] and ISO/IEC 30107-3:2023, which establishes methods for detecting attacks against biometric systems [4]. The subject has also received considerable attention in academic literature. W. Yang et al. [5], for instance, identify multifactor biometric authentication as an optimal model for high-risk legal contexts. Within Russian legal scholarship, biometrics has primarily been examined from the perspective of personal-data protection, notably in the work of A. I. Savelyev [6]. Its application to the registration of rights in real estate, however, remains a largely unexplored area.

The purpose of the study is to develop a conceptual foundation for the legal regulation of biometric verification in the execution and state registration of real estate transactions in the Russian Federation, taking into account foreign experience and applicable technical standards.

The scientific novelty of the study lies in the proposed synthesis of a technical and legal model of biometric verification adapted to the mechanism of state registration of real estate transactions. The model accounts for the

permissible limits of data processing, safeguards protecting data subjects' rights, and standards intended to prevent digital attacks.

The research hypothesis holds that integrating biometric verification into the mechanism for the state registration of real estate transactions may improve the reliability of identity verification and reduce the incidence of fraud, provided that a special legal regime is established. Such a regime should include strict technical anti-spoofing standards, a mechanism for generating a single-use biometric token, and independent auditing of the UBS.

II. MATERIALS AND METHODS

The study is based on a set of complementary research methods that provide a multilevel analysis of the subject matter.

The comparative legal method was employed to examine and compare regulatory models governing biometric identification in real estate transactions in Russia, Germany, Estonia, the United States, and the United Arab Emirates. The comparison was conducted according to several criteria: the applicable legal framework, the permissibility of biometric use, the mechanism for obtaining the data subject's consent, and the authority responsible for state registration.

The systematic literature review covered publications indexed in Scopus, Web of Science, and the Russian Science Citation Index. The search was conducted using the following key phrases: "biometric authentication real estate," "digital identity land registry," "deepfake fraud property transaction," and "biometrics in real estate transactions." From an initial pool of more than 380 publications, 20 sources meeting the criteria of relevance and scholarly verifiability were selected.

The content analysis of technical and regulatory documentation included an examination of Federal Law No. 152-FZ, Federal Law No. 572-FZ, Federal Law No. 218-FZ, ISO/IEC 30107-3, GOST R 52633, Rosreestr regulations, and the technical specifications of the UBS. This method made it possible to identify existing regulatory gaps and determine the technical requirements applicable to a biometric-verification system.

The case-study method was used to analyze the implementation of biometric technologies in the registration systems of Estonia, particularly X-Road and Maa-amet, and the United Arab Emirates, represented by the Dubai Land Department. The findings provided a basis for developing specific recommendations applicable to the Russian legal system.

III. RESULTS AND DISCUSSION

A quantitative assessment of the penetration of biometric technologies into property transactions constitutes the starting point of the analysis. For a clearer presentation of the statistical trends, the graph below illustrates the relationship between the proportion of biometrically verified transactions and the number of detected cases of digital fraud from 2019 to 2022, together with a forecast for 2023. The calculations are based on aggregated data provided by Rosreestr [1], the Bank of Russia [2], and Deloitte's analytical report on digital identity [7].

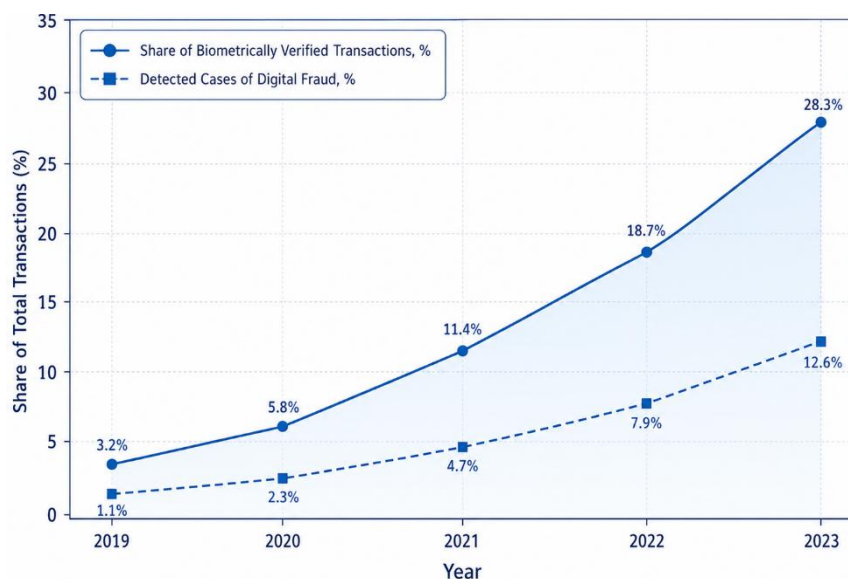


Fig. 1. Dynamics of the use of biometrics in real estate transactions in Russia (compiled by the author based on [1, 2, 7]).

The graph reveals a paradoxical pattern: the growing share of biometrically verified transactions is accompanied by an even more rapid increase in detected cases of digital fraud, from 1.1% to 12.6%. This trend does not indicate the inherent ineffectiveness of biometric technologies. Rather, it may be explained by an “attractive-target effect”: as biometric data acquire greater economic and legal value, offenders gradually shift from conventional document forgery toward attacks directed against biometric systems. This conclusion is consistent with the findings of F. Abdullakutty et al. [8], who established that first-generation biometric systems lacking anti-spoofing protection were vulnerable to presentation and replay attacks in 34–67% of the tested attack vectors.

Notably, the sharpest increase in fraudulent attempts was recorded in 2021–2022. Chronologically, this period coincided with the widespread availability of deepfake-generation technologies and the simultaneous expansion of the range of public services accessible through the Unified Biometric System. This concurrence confirms the systemic nature of the problem and its inseparable connection with the quality of the technical standards governing identity verification.

Understanding the position of the Russian model within the international regulatory landscape requires a comparative analysis of the legal approaches applied to biometrics in the registration of rights in real estate. Table 1 systematizes the principal characteristics of five jurisdictions that differ in the maturity of their regulatory frameworks and levels of technological readiness.

Table 1. Comparative analysis of the regulation of biometric identification in real estate transactions (compiled by the author based on [3, 9, 10, 11, 12]).

Country/Jurisdiction	Legal Framework	Permissibility of Remote Biometric Identification	Mandatory Consent	Registration Authority
Russia	Federal Law No. 152-FZ, Federal Law No. 572-FZ, Civil Code of the Russian Federation	Partial; remote biometric identification is permitted with consent	Yes	Rosreestr / Unified Biometric System
Germany	GDPR, BGB, GBO	Permitted in the presence of a notary	Yes	Grundbuchamt
Estonia	ID-card Act, X-Road	Full implementation within the e-Residency framework	No; used by default	Maa-amet
United States, selected states	BIPA in Illinois, CCPA	Limited	Yes; explicit consent	County Recorder
United Arab Emirates	Federal Decree-Law No. 45 of 2021	Broad application within Smart Dubai	No; public-registry model	Dubai Land Department

The data presented in Table 1 permit the identification of three fundamentally different regulatory models. The first may be characterized as the “enabling model,” represented by Estonia and the United Arab Emirates. Under this approach, biometrics function as a basic infrastructural component of public administration, while procedural barriers for the data subject are minimized. A biometric profile is created during the individual’s initial interaction with a public authority and subsequently operates as a default identification instrument.

The second, or “consent-based model,” prevails in Russia, Germany, and several U.S. states. It is founded upon the principle of informed consent and treats biometric identification as an additional and optional instrument rather than as a mandatory component of public infrastructure. The third, “mixed model,” is characteristic of federal systems in which the applicable rules differ at the subfederal level, as illustrated by the United States. Within this classification, the Russian framework is generally aligned with the second model. Nevertheless, it is distinguished by the insufficient technical specification of the verification standards applicable to real estate registration.

The experience of Estonia is of particular relevance to Russian legal and administrative practice. More than 98% of real estate transactions in Estonia are reportedly completed electronically through digital identification based on the national ID card [9]. A central element of the Estonian system is the “once-only” principle. Biometric and identity-related data are collected once and may subsequently be reused without requiring renewed consent for each transaction. This arrangement reduces transaction costs while preserving the legal protection afforded to the data subject.

On the basis of the comparative findings and the systemic gaps identified in Russian legislation, a phased model of biometric verification has been developed for incorporation into the state registration mechanism governing real estate transactions.

The initial identification stage, comprising Stages 1 and 2, establishes a legally significant correspondence between the biometric data and the passport information contained in the Unified Biometric System. During the collection of biometric data at Stage 3, a fundamental distinction must be drawn between “live” data obtained through liveness detection and previously stored biometric templates. The use of an archived template should be permitted only when its continued relevance and authenticity have been confirmed in accordance with ISO/IEC 30107-3 [4].

The risk-assessment stage, designated as Stage 5, involves the automated application of an anti-spoofing algorithm. Its results are recorded in the biometric-session log and subsequently become part of the evidentiary record in the event that the transaction is contested.

The legal significance of the notarization stage, identified as Stage 6, lies in the fact that a notary acting pursuant to Article 44.2 of the Fundamental Principles of Legislation of the Russian Federation on Notaries makes a decision regarding the performance of a notarial act on the basis of the final biometric-session protocol rather than solely through visual contact with the individual concerned. This arrangement creates a need to establish a formal procedure under which the notary verifies the algorithmic conclusion and to define the allocation of liability in cases involving system error.

The introduction of a “biometric extract” from the Unified State Register of Real Estate at Stage 8 would provide an additional evidentiary safeguard. Such a document would contain a marker identifying the verification method applied during the transaction. In subsequent litigation, this information would allow a court to reconstruct the complete sequence of events and determine the point at which a possible compromise of the biometric session occurred.

A systemic assessment of digital-fraud threats affecting biometric identification requires a structured classification through which each category of threat may be correlated with specific technical and legal countermeasures. Table 2 presents an original classification developed on the basis of ISO/IEC 30107-3 [4], GOST R 52633 [13], and criminal-enforcement practice under Article 272 of the Criminal Code of the Russian Federation.

Table 2. Classification of digital fraud threats and countermeasures for biometric identification (compiled by the author based on [4, 13, 14, 15]).

Risk Category	Specific Threat	Technical Measures	Legal Measures
Technical risk	Deepfake or synthetic biometric data	ISO/IEC 30107-3 liveness detection and anti-spoofing mechanisms	Article 16 of Federal Law No. 572-FZ: prohibition on processing without verification
Technical risk	Interception of a biometric template	GOST R 52633 and TLS 1.3 channel encryption	Operator liability under Article 13.11 of the Code of Administrative Offenses of the Russian Federation
Organizational risk	Substitution of the subject during a video session	Multifactor authentication and video identification	Notarial videoconferencing protocol under Ministry of Justice Order No. 313
Legal risk	Violation of informed-consent requirements	Logging of consent issuance within the Unified Biometric System	Article 9 of Federal Law No. 152-FZ: right to withdraw consent
Systemic risk	Data breach affecting the Unified Biometric System	Database segregation and SIEM-based access auditing	Federal Law No. 187-FZ on Critical Information Infrastructure and criminal liability under Article 272 of the Criminal Code
Social risk	Social engineering or coercion	Behavioral biometrics, including stress analysis	Contesting the transaction under Article 179 of the Civil Code of the Russian Federation on transactions concluded under threat

The category of social risk merits separate consideration in the context of real estate transactions. The threat of coercion through violence or intimidation, governed by Article 179 of the Civil Code of the Russian Federation, acquires an additional dimension when biometric verification is used. An offender who physically forces an individual to complete a biometric-verification procedure may obtain consent that appears formally valid and legally documented.

As a countermeasure, the introduction of behavioral biometrics may be appropriate. Analysis of facial microexpressions, heart-rate variability captured through peripheral cameras, and speech patterns may identify signs of psychoemotional stress inconsistent with a voluntary expression of intent with an accuracy of up to 78% [16]. Such mechanisms cannot independently establish the existence of coercion. They may, however, generate a heightened-risk indicator requiring additional verification by a notary or registration authority.

For a clearer representation of the system of threats and the corresponding safeguards, the original diagram below illustrates the paired relationships between attack vectors and the instruments designed to counter them. Figure 2 provides a structured representation of these relationships.

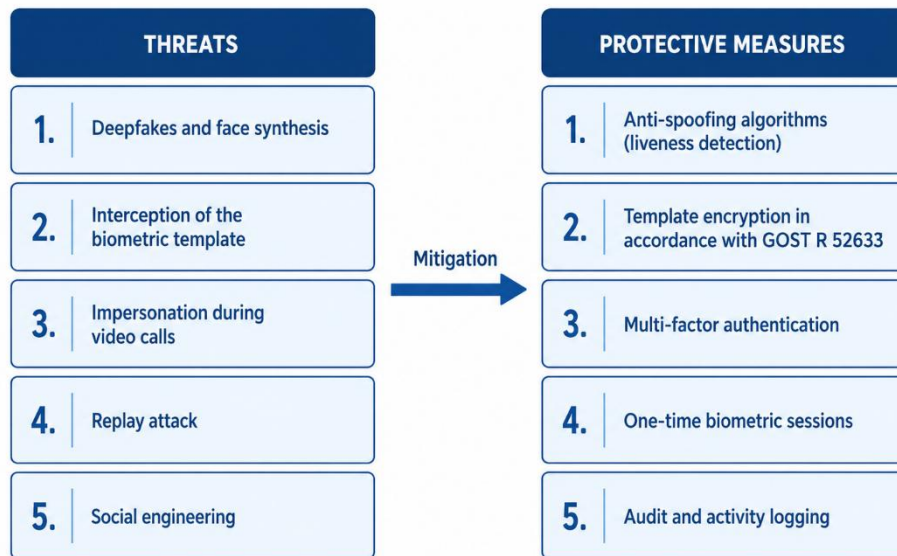


Fig. 2. The system of threats of digital fraud and countermeasures for biometric identification in real estate transactions (compiled by the author based on [4, 13, 14, 15, 16]).

The framework reveals a notable asymmetry between technical and legal instruments. Technical safeguards have been developed in considerable detail and specified in international standards, whereas legal mechanisms often remain general in nature and have not been adapted to the particular characteristics of biometric data. Article 272 of the Criminal Code of the Russian Federation, which criminalizes unlawful access to computer information, is formally applicable to the interception of a biometric template. It does not, however, contain qualifying elements that reflect the distinctive legal nature of biometric data as unique and effectively immutable personal identifiers. This legislative gap requires correction through the introduction of a specific criminal offense comparable to that established under Article 222-1 of the French Criminal Code.

The conceptual framework for regulating biometrics within the state registration mechanism for real estate transactions makes it possible to visualize the relationships among statutory provisions, technical standards, institutional participants, and the rights of data subjects. An analysis of this legal architecture provides a basis for formulating the following original recommendations for improving the existing regulatory mechanism.

First, a specialized federal law “On Biometric Identification in Real Estate Transactions” should be adopted, or a separate chapter should be incorporated into Federal Law No. 218-FZ “On State Registration of Real Estate.” The legislation should establish an exhaustive list of circumstances in which biometric verification constitutes a mandatory condition of registration, including transactions exceeding a prescribed value threshold and cross-border transactions. At the same time, the data subject should retain the right to refuse biometric verification in favor of the traditional notarized procedure [17].

Second, the institution of a “biometric token” (BT) should be introduced as a single-use, cryptographically protected identifier linked to a specific transaction. The BT would be generated during the biometric session and would record its essential parameters, including the time, location, verification method, and anti-spoofing result. The token would cease to be valid upon completion of state registration.

The data subject’s right to revoke the BT before the agreement is signed would constitute a central guarantee of the voluntary nature of the expression of intent. This mechanism addresses a gap identified in the analysis of Article 9 of Federal Law No. 152-FZ. Although the right to withdraw consent to the processing of biometric data is formally recognized, such withdrawal does not automatically suspend the corresponding registration proceedings.

Third, a Register of Biometrically Verified Transactions (RBVT) should be established as a structural component of the Unified State Register of Real Estate. The RBVT should contain the biometric-session identifier, a hash value of the biometric template without retaining the template itself in accordance with the principle of data minimization, the code and version of the anti-spoofing algorithm, the verification result, and the notary’s identification code.

The inclusion of RBVT data in an extract from the Unified State Register of Real Estate would create a verifiable chain of custody and would substantially simplify the evidentiary process when a transaction is challenged before a court.

Fourth, an anti-spoofing technical standard no lower than ISO/IEC 30107-3 Level 2 should be established as a mandatory requirement for operators providing biometric services in the real estate sector. This level should include biometric liveness verification through both active and passive liveness-detection methods. The requirement should be

incorporated into a subordinate regulatory instrument issued by Rosreestr in coordination with the Federal Service for Technical and Export Control of Russia and Roskomnadzor [18].

Table 3 presents specific measures, implementation instruments, and expected outcomes as a practical framework for applying the proposed recommendations.

Table 3. Author's recommendations for improving the legal regulation of biometrics in real estate transactions (author's development).

Area	Author's Recommendation	Implementation Instrument	Expected Effect
Regulatory framework	Adopt a specialized federal law governing biometrics in real estate transactions	Legislative initiative and Rosreestr regulations	Elimination of legal gaps
Technical standards	Introduce a national GOST profile based on ISO/IEC 30107-3 for the Unified Biometric System	Federal technical-regulation authorities and Rosstandart	Uniform anti-spoofing requirements
Rights of data subjects	Introduce a biometric token with a right of one-time revocation	Amendments to Federal Laws No. 152-FZ and No. 572-FZ	Protection against involuntary registration
Institutional mechanism	Establish the Register of Biometrically Verified Transactions	Amendments to Federal Law No. 218-FZ administered by Rosreestr	Transparency and verifiability
Law-enforcement and notarial practice	Develop a standardized biometric-session protocol for notaries	Order of the Ministry of Justice and methodological guidelines of the Federal Notarial Chamber	Standardization of the evidentiary record

Two principal limitations of the proposed methodology should nevertheless be acknowledged.

The first concerns the dependence of biometric-verification accuracy on the quality and representativeness of the original database of biometric templates maintained within the Unified Biometric System. As of 2022, the system reportedly contained approximately 30 million records [19], while the economically active population of Russia exceeded 75 million people. Such incomplete coverage creates a risk of unequal access to biometric registration procedures.

The second limitation is associated with differences in the accuracy of anti-spoofing and facial-recognition algorithms across demographic groups, including groups differentiated by age and ethnicity. Such disparities were documented by Grother, Ngan, and Hanaoka [20] in relation to facial-recognition systems. The findings indicate a need to develop specialized datasets for the calibration and validation of biometric systems used in the Russian Federation.

The combined results of the analysis demonstrate that the incorporation of biometrics into the mechanism of state registration of real estate transactions constitutes not merely a technological challenge but also a fundamentally legal one. Addressing this challenge requires simultaneous progress in several interconnected areas: specialization of the regulatory framework, standardization of technical requirements, expansion of safeguards protecting the rights of data subjects, and creation of institutional mechanisms capable of verifying the complete chain of events.

The proposed biometric-token mechanism and the Register of Biometrically Verified Transactions represent instruments capable of maintaining an appropriate balance among transactional security, technological efficiency, and the protection of individual rights, provided that sufficient political and institutional commitment exists for their implementation.

IV. CONCLUSION

The study supports the formulation of the following principal conclusions.

The stated research objective has been achieved. Conceptual foundations have been developed for the legal regulation of biometric verification within the mechanism of state registration of real estate transactions. These foundations include an original eight-stage verification model, a conceptual framework of the relevant legal architecture, and a classification of threats accompanied by corresponding countermeasures.

The analysis established that the existing Russian regulatory framework, including Federal Laws No. 152-FZ, No. 572-FZ, and No. 218-FZ, contains systemic gaps in several areas. These gaps concern special requirements for biometric verification in the registration of real estate; a mechanism for exercising the data subject's right to withdraw biometric consent, together with its legal consequences for pending registration proceedings; a mandatory anti-spoofing standard for operators in the real estate sector; and an evidentiary regime governing biometric sessions when a transaction is contested.

The comparative analysis of five jurisdictions confirmed that the most mature systems, particularly those of Estonia and the United Arab Emirates, are characterized by a "once-only identification" principle and the direct integration

of biometric and digital identity data into the relevant register of rights. The Russian system, by contrast, continues to operate through parallel databases that remain only weakly integrated.

The research hypothesis has been partially confirmed. Biometric technologies may improve the reliability of identity verification. Without a specialized legal regime incorporating a biometric token, the Register of Biometrically Verified Transactions, and an anti-spoofing standard corresponding to ISO/IEC 30107-3 Level 2, however, their use may generate new legal risks. In the context of irreversible property transactions, these risks may exceed those associated with traditional identity-verification procedures.

The practical significance of the study lies in the development of specific legislative and technical instruments: the biometric-token institution, the Register of Biometrically Verified Transactions, and a standardized biometric-session protocol for notaries. These instruments may be used in preparing amendments to Federal Laws No. 218-FZ and No. 572-FZ, as well as subordinate regulatory instruments issued by Rosreestr and the Ministry of Justice of the Russian Federation.

Further research should focus on the empirical validation of the proposed model through a pilot project conducted within a regional office of Rosreestr. Another promising area involves the development of a methodology for assessing the reliability, admissibility, and evidentiary value of biometric data in judicial proceedings.

REFERENCES

- [1] Rosreestr. Key Results of Rosreestr's Activities in 2021 and Key Objectives for 2022. [Electronic resource]. Available at: <https://rosreestr.gov.ru/upload/iblock/6b5/6b519a3c7ab10d4ddefc9876096bdb36.pdf> (Accessed: 15 May 2022).
- [2] Bank of Russia. Key Directions for the Development of Information Security in the Credit and Financial Sector for 2019–2021. [Electronic resource]. Available at: https://www.cbr.ru/Content/Document/File/83253/onrib_2021.pdf (Accessed: 20 May 2022).
- [3] European Commission. Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. [Electronic resource]. – Access mode: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206> (access date: 06/03/2022).
- [4] ISO/IEC 19795-1:2021. Information technology - Biometric performance testing and reporting - Part 1: Principles and framework. – Geneva: International Organization for Standardization, 2021.
- [5] Yang W., Wang S., Sahri N. M., Karie N. M., Ahmed M., Valli C. Biometrics for Internet-of-Things Security: A Review // *Sensors*. – 2021. – T. 21. – No. 18. – Art. 6163. – <https://doi.org/10.3390/s21186163>.
- [6] Savel'ev A. I. Legal Framework for Personal Data Protection in the Digital Economy. – Moscow: Statut, 2022.
- [7] Deloitte. The Future of Digital Identity. [Electronic resource]. – Available at: <https://www.deloitte.com/na/en/services/risk-advisory/perspectives/the-future-of-digital-identity.html> (accessed: June 18, 2022).
- [8] Abdullakutty F., Elyan E., Johnston P. A review of state-of-the-art in face presentation attack detection: From early development to advanced deep learning and multi-modal fusion methods // *Information Fusion*. – 2021. – Vol. 75. – Pp. – <https://doi.org/10.1016/j.inffus.2021.04.015>.
- [9] Kattel R., Mergel I. Estonia's Digital Transformation: Mission Mystique and the Hiding Hand // *Great Policy Successes* / ed. P. 't Hart, M. Compton. – Oxford: Oxford University Press, 2019. – Pp. 143–160. – <https://doi.org/10.1093/oso/9780198843719.003.0008>.
- [10] Federal Ministry of Justice of Germany. Gesetz über Personalausweise und den elektronischen Identitätsnachweis. [Electronic resource]. – Available at: <https://www.gesetze-im-internet.de/pauswg/BJNR134610009.html> (Accessed: 24.06.2022).
- [11] Woodhouse T. Biometric data and privacy law: a comparative analysis of the United States, European Union, and Australia // *Computer Law & Security Review*. – 2022. – Vol. 44. – Article 105643. – <https://doi.org/10.1016/j.clsr.2021.105643>.
- [12] Dubai Land Department. DLD participates in “UAE Innovates 2022” initiative. [Electronic resource]. – Available at: <https://dubailand.gov.ae/en/news-media/dld-participates-in-uae-innovates-2022-initiative/> (Accessed: 25.07.2022).
- [13] GOST R 58624.3-2019. Information technology. Biometrics. Detection of attacks on biometric presentation. Part 3. Tests and test reports. – Moscow: Standartinform, 2019.
- [14] Medvedev I., Shadmand F., Cruz L., Gonçalves N. Towards Facial Biometrics for ID Document Validation in Mobile Devices // *Applied Sciences*. – 2021. – Vol. 11. – No. 13. – Article 6134. – <https://doi.org/10.3390/app11136134>.
- [15] Marcel S., Nixon M. S., Fierrez J., Evans N. Handbook of Biometric Anti-Spoofing: Presentation Attack Detection. – 2nd ed. – Cham: Springer, 2019. – <https://doi.org/10.1007/978-3-319-92627-8>.

-
- [16] Eglitis T., Guest R., Deravi F. Data behind mobile behavioral biometrics: a survey // IET Biometrics. – 2020. – Vol. 9. – No. 6. – Pp. 224–237. – <https://doi.org/10.1049/iet-bmt.2018.5174>.
 - [17] Federal Law of July 13, 2015 No. 218-FZ "On State Registration of Real Estate".
 - [18] Federal Law of December 29, 2020 No. 479-FZ "On Amendments to Certain Legislative Acts of the Russian Federation".
 - [19] Ministry of Digital Development, Communications and Mass Media of the Russian Federation. Unified Biometric System. [Electronic resource]. – Available at: <https://digital.gov.ru/activity/czifrovaya-identifikaciya/edinaya-biometricheskaya-sistema> (Accessed: August 11, 2022).
 - [20] Grother P., Ngan M., Hanaoka K. Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects. – Gaithersburg, MD: National Institute of Standards and Technology, 2019. – NIST Interagency Report 8280. – <https://doi.org/10.6028/NIST.IR.8280>.