UDC 004.93'12

МРНТИ 20.53.19

Esmagametova G.K.1\*, B. Zhadamba1, K.K.Saginbayeva1, A.N.Ismukanova2

1Mongolian University of Science and Technology, Mongolia,

2Kokshetau University Sh.Ualikhanov, Kazakhstan

\*(e-mail: [Gal.Esm@mail.ru](mailto:Gal.Esm@mail.ru))

**Analysis of existing approaches to biometric authentication**

**Abstract**

*Main problem*: Research and analysis of methods for presentation models of biometric data, creation of algorithms for biometric verification and identification of a person based on modern models for describing and analyzing biometric authentication of a person. The most widely used in biometric identification are the following human parameters: features of facial geometry, fingerprints, geometry of the palm of the hands, retina and iris eyes, voice characteristics, signature features and keyboard underline. Biometric authentication is one of the most promising areas for the development of information system user authentication technologies.

*Purpose:* The main purpose of information system user authentication is to reduce information system security threats, namely the threat of information confidentiality violation, the threat of information integrity violation, the threat of system operability violation. Threats can be caused by different ways of violations. The most common type of violation is unauthorized access. The user authentication procedure allows checking whether the presented identifier belongs to the access subject and confirming its authenticity, i.e. checking whether the given subject is who he claims to be.

As applied to automatic identification systems, biometric systems are understood as systems and methods based on the use of any specific characteristics of the human body to determine or authenticate. Biometrics is a science based on the description and measurement of body characteristics of living organisms. The identification and authentication of our identity has become a staple in today's society, ensuring secure interaction by preventing fraud and crime.

*Methods:* Biometrics has two authentication methods:

* Verification, verification based on a biometric parameter and a unique identifier that distinguishes a particular person (for example, an identification number), that is, this method is based on a combination of authentication methods.
* Identification, unlike verification, is based only on biometric criteria. In this case, the measured parameters are compared with all entries in the database of registered users, not one of them is selected, but based on some identifier.

*Results and their significance:* It is difficult to draw an unambiguous conclusion about which of the modern methods of biometric authentication or combined methods is the most effective. Authentication methods based on the measurement of human biometric parameters provide almost 100% identification, solving the problems of losing passwords and personal identifiers, which leads to suspicions of detecting security threats to information disclosure systems.

*Keywords:* cryptography, information security, biometrics, authentication, biometric system, biometric authentication, biometric identification, statistical methods, statistical methods.

**Introduction**

Authentication is a procedure in which a user proves who he is to himself. Many confusions are common because different systems define authentication differently (for example, banking and legal systems).

Biometrics is a science based on the description and measurement of body characteristics of living organisms.

As applied to automatic identification systems, biometric systems are understood as systems and methods based on the use of any specific characteristics of the human body to determine or authenticate [10].

Our life is full of situations when it is necessary to prove who we are. Such cases are full of both personal and professional spheres.

It is easy to enumerate a wide range of areas that require fast, reliable and convenient user authentication: access to a personal computer or smartphone, access to e-mail, banking operations, opening doors and starting a car engine, controlling access to premises, crossing state borders, and in general any interaction with government authorities require identification [1].

Thus, the identification and authentication of our identity has become a staple in today's society, ensuring secure interaction by preventing fraud and crime.

Biometric identification is often referred to as pure or actual authentication, because it is not virtual, but rather a biometric sign (identifier) ​​is used in relation to a person.

**Materials and methods**

A feature of biometric identification will be the large size of the biometric database: each of the biometric samples must be compared with all records in the database (1: n comparison or "one to one"). For application in real life, such a system requires a high speed of comparison of biometric features.

Example:

The number of employees of even a large enterprise ranges from several hundred to several thousand. Take, for example, a headcount of 10,000 people. So the size of the database (using one fingerprint per person) is 10,000 fingerprints. When applying a fingerprint to the reader, the system makes a 1:10,000 comparison. This is very small for modern systems. Therefore, all access control or time attendance systems operate in the biometric identification mode.

On the other side of the pole, there are validation systems that typically only do one comparison in a 1:1 mode. That is, the presented biometric mark is compared to one biometric mark in the database. That is, the system answers the question to whom you give yourself.

We often use this term, despite its importance, confusion often arises, since the definitions of the term are different in different systems, for example, in banking and legal systems.

Accordingly, we will give definitions of these terms for biometric systems.

Authentication (from English - authentication) - a procedure for verifying that the identifier provided by them belongs to the subject of access. The simplest example of authentication is the confirmation of a user's identity by comparing the entered login with a password in a database of previously identified users. In this example, authentication is the process of comparing passwords, which then grants access or denial, and the ID is just login.

Authentication methods can be grouped into three main categories called authentication factors: what the person knows, what the user knows, or what the person is.



Figure 1 - Authentication factors

Biometrics has two authentication methods:

1. Verification, verification based on a biometric parameter and a unique identifier that distinguishes a particular person (for example, an identification number), that is, this method is based on a combination of authentication methods.

2. Identification, unlike verification, is based only on biometric criteria. In this case, the measured parameters are compared with all entries in the database of registered users, not one of them is selected, but based on some identifier.

Each authentication factor includes a number of elements used to authenticate or verify identity, down to access, approval of a transaction request, signing a document, delegation of authority to others, and so on.

1. Knowledge factors are what the user knows and remembers, such as password, PIN, security question answer, etc.

2. Sign factors are our part, such as fingerprint, signature, voice, etc.

3. Ownership factors are factors such as user ID, mobile phone, physical key, etc.

When comparing biometric authentication with other types of authentication, one should pay attention to their strengths and weaknesses.

Authentication based on knowledge factors such as the use of a password or pattern. Using a password is technically easy to implement both in software and on any specialized devices. But with the same discount, the password can be cracked like spyware or a computer virus that can be downloaded from the Internet to the user's devices. And when it comes to devices (such as a PIN reader), you can simply view the password. All this does not prevent the Old Believers from frequently using PIN code readers in access control systems.

In general, biometric authentication systems are divided into two main types according to the principle of operation: static and dynamic.

Static (physiological characteristics)

* Fingerprints or papillary lines
* The iris of the eye (iris)
* The retina of the eye (retina)
* Vein pattern
* Face
* Hand geometry
* Heartbeat
* DNA
* Multimodal identification

Dynamic (behavioral characteristics)

* Dynamics of handwriting and signature
* Heartbeat
* Rhythm of voice and speech
* Action recognition
* The speed and features of working on a computer keyboard (or typing a code on a coded panel)
* Behavior

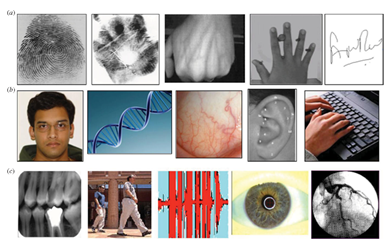


Figure 2 - Static and dynamic authentication

Statistical Methods

Static biometric images include a fingerprint, palm geometry, iris (iris), retina, 3D "image" of a face or skull, DNA (deoxyribonucleic acid), and more. Most of the existing authentication technologies based on the parameters of these images have a low percentage of erroneous decisions. For example, the results of building the main chain using PBC, and then recognizing the subject are known:

* FAR - False Acceptance Rate - the probability of false identification of a user that is not in the database.
* FRR-False Rejection Rate - the probability of refusing to identify a user in the database.

Table 1 - Static Methods Far and FRR

|  |  |  |
| --- | --- | --- |
| Biometric identification method | Transmittance, FAR | False rejection rate, FRR |
| Vein pattern | 0.0008% | 0.01% |
| Iris | 0.00001% | 0.016% |
| 3D face recognition | 0.0005% | 0.1% |
| Retina | 0.0001% | 0.4% |
| Fingerprint | 0.001% | 0.6% |
| 2D face recognition | 0.1% | 2.5% |

Fingerprint detection

Despite the long history of the use of fingerprints in forensics, the detailed principles of the formation of papillary patterns have become known relatively recently. To put it simply, the formation of a papillary pattern affects the conditions for the formation of DNA and spermatozoa. Therefore, even identical twins have similar fingerprints. Fingerprints appear in the first three months of pregnancy [7].

Identification by vein pattern

The venous picture is inherent in every person, including Gemini. Since the veins are under the skin, they cannot be faked, which allows you to reliably authenticate using the False Acceptance Rate value - the probability of falsely identifying a user that is not in the database is up to 0.00008%.

The definition of the vessels of the finger or palm by drawing (Vein Recognition-English) is based on obtaining a sample when photographing the outer or inner side of the hand or finger with an infrared camera. An infrared camera is used to scan a finger or hand. The image is visible due to the hemoglobin war (the dye absorbs the infrared radiation of the blood and is visible from the vein in the chamber. The software, based on the obtained data, creates a digital accumulation.

Root or root recognition is typically performed on the palm or finger of the user.

The high level of security and non-contact recognition make core recognition suitable for most applications requiring very high security.

The only thing that limits the scope is the size and cost of the scanners. Scanners are quite difficult to penetrate most mobile devices, but are ideal for use in access control systems. Over time, these are venous imaging scanners that replace fingerprint scanners.

Identification, which also includes 1:n pattern identification, can take significant time, especially if there are many biometric patterns in the database. This is due to the high requirements for sample processing, as root samples are very complex.

One of the decisive advantages of venous sample identification is the difficulty of unauthorized removal of the sample.

Recognition reliability is comparable to iris identification, although the equipment is much cheaper. Now it is being actively studied and implemented in the ACS.

Face ID

Face recognition uses various expressions to create a unique digital model that are used together. Examples of facial features that can be used for identification are the shape of the nose or the distance between the eyes. In total, more than 80 different signs are used [13]

Retinal Identification

The first biometric eye scanning systems (Retinal scan) were retinal scanners, which appeared in 1985. The retina remains unchanged from birth to death, and only some chronic diseases can change it [5].

Instead, a retinal scan is performed with infrared light, which detects a capillary pattern and uses it for detection.

While retinal scanning provides high security, the technology has many disadvantages that have led to limited commercial use:

* Slow identification process
* High price

Retinal scanning has been used by organizations such as the FBI, NASA and the CIA for (1:N) detection in high security environments.

Definition of the iris

The process of iris identification (Iris Recognition) begins with obtaining a detailed image of the human eye. They try to make an image for further analysis in high quality, but this is not necessary. The iris is such an unusual parameter that even a fuzzy image gives a confident result. To do this, use a monochrome CCD-camera with soft illumination, sensitive to infrared radiation. They usually consist of several photographs because the pupil is sensitive to light and constantly changes its size [6].

Table 2 - Advantages and disadvantages of the iris method

|  |  |
| --- | --- |
| Advantages of the method | Disadvantages of the method |
| No need to contact the scanning device | Do not expose the scanner to sunlight |
| High Confidence | The method is less studied compared to other statistical methods of biometrics |

The backlight is invisible to the naked eye and takes multiple shots in seconds. Then select one or more of the received photos and proceed to segmentation.

Heart rate authentication

Heart rate detection is one of the most important biometric technologies today. The heartbeat is a special character of a person, such as fingerprints, retina or venous pattern. One of the advantages of biometric identification by heart rate: high accuracy, high difficulty in obtaining fakes and standards, analysis of the physical condition of the recipient.

Recently, heart rate authentication was only in the list of promising solutions for biometric identification, today we have ready-made solutions for commercial use. The heart rate of a person is characterized by many measurable parameters - frequency, rhythm, filling, voltage, amplitude of oscillations, impulse speed.

One of the benefits of heart rate is:

* Impossibility of use in the absence of the recipient

That is, if you lose or forget the bracelet, no one but you will be able to use it.

* Cannot be used after death

Monitoring the physical condition of the recipient for the purpose of identification is secondary, but there are many uses beyond identification, monitoring the biological condition is necessary.

DNA identification

DNA analysis (DNA Biometrics - English) is an increasingly common biometric identification technology and is often used in forensics and healthcare.

Unlike the aforementioned identification technologies, DNA identification not only reduces costs, but also makes our lives easier and safer.

Benefits of DNA identification:

* DNA is the only biometric technology that allows relatives to be identified from an undefined DNA pattern.
* Like fingerprints, DNA is one of the biometric characteristics of a person that criminals leave at the crime scene.
* DNA testing is a relatively mature and dynamic technology that is widely used and familiar to the general public.
* Rapid DNA identification devices enable sequencing in as little as 90 minutes
* Many DNA results can be easily stored in a database, allowing data to be collected and quickly searched using automated tools.

Multimodal biometric identification

Biometric identification methods can be combined with each other - multimodal identification significantly increases the security of an object, since the number of possible errors inherent in biometric systems is reduced.

For example, an iris reader can read an iris from a single source, and can also read an iris from two sources.

Dynamic Methods

The most studied dynamic biometric images include: keyboard handwriting, features of handwritten password and signature reproduction, running characteristics, voices, the nature of working with a computer mouse, head tremor parameters, face and neck thermograms. In addition, no additional hardware is required to register the keyboard, handwritten passwords and signatures, and voice. However, voice images can be easily intercepted by recording them on a simple voice recorder (mobile phone), which reduces the trust in the voice password. When using user-set voice passwords, the learning and authentication processes must be carried out in a secure environment.

Behavioral biometrics

Whatever we do, it has a unique signature. How exactly you hold your smartphone, swipe, tap, type, scroll and move the mouse, creating a unique combination of parameters, a kind of digital handwriting. Some banks use this technology (behavioral biometrics) for additional verification of users. This is convenient - nothing is required from the user, he always does it, and the system does not have anything special in its actions. By deviations from the usual behavior, it can be assumed that the user is not the one who manifests himself.

Voice biometrics

The use of human voice biometrics is more complex and interesting than the use of most biometric features. The classical voice identification technology cannot be the main violin here, a separate one is a much more interesting direction of voice recognition [8].

The voice recognition method determines the personality of a person by a combination of specific characteristics of the voice. The algorithms analyze the main features by which a decision is made about the personality of the speaker: the voice eye, the resonant frequency of the speech pathways and their attenuation, as well as the dynamics of articulation control.

Gait

For example, the definition of a hike or the definition of a pedestrian has been carried out for decades without much progress - until now. Recent advances in precision have been made possible by a graceful discovery of something viable in behavior. Earlier this year, researchers at the University of Manchester achieved an accuracy of 99.3%, according to an article published in the journal Imaging and Machine Intelligence Operations (TPAMI). The system analyzes people's steps using gender sensors, and getting that final percentage of accuracy is often a challenge.

As you know, there are no systems that provide one hundred percent protection against leakage, hackers were able to penetrate objects that are separated from the outside world.

When using biometric data for authentication, the violation of biometric databases becomes especially important. The thing is that biometric tags do not change, that is, a stolen (hacked) sign cannot be replaced as a hacked password.

In this sense, the password will be an advantage over biometrics, since passwords can be replaced with new ones when hacked, and human biometric symbols do not change, so it is very convenient to identify them.

Starting with the face and voice, they are almost impossible to hide in the modern world, and ending with fingerprints and fragments of his biomaterial DNA fragment, which leaves a person in the places of his presence. We leave all this data in the process of life to the things around us and can collect them secretly from the carrier.

Of course, there are biometric signs in which it is impossible to collect a latent venous sample of a finger or hand, retina.

The likelihood of falsification does not depend on the type of biometric feature, but on the technology used to read this feature.

Table 3 - Static Methods Far and FRR

|  |  |
| --- | --- |
| Biometric reader | Probability of forgery |
| 3D fingerprint reader | Not possible |
| Multispectral Fingerprint Reader | Not possible |
| Further fingerprints, optical devices | Possible |
| Iris | Possible |
| Face recognition 2D | Possible |
| 3D face recognition | Possible |
| Photo of veins | Not possible |
| Retina | Not possible |

Natural limits

If password authentication requires an exact match between two alphanumeric strings, the biometric authentication system relies on the degree of similarity between the two biometric samples, while the individual biometric samples obtained during registration and authentication are rarely identical, a biometric the system can create two types of authentication errors.

Table 4 - Authentication errors

|  |  |
| --- | --- |
| Authentication errors | Content |
| False mismatch | * Two biometric samples of the same person appear at low germination, and the system refuses to accept them as the same, that is, it cannot identify them. * A false mismatch results in a denial of service for the legitimate user. |
| false match | * Two biometric samples of different people appear when they have a high similarity and the System declares them incorrectly matched. * A false match leads to an impostor attack. Such an attack is also called a zero-force attack because it does not require the attacker to use a special hacking system. |

**Conclusion**

This article explores the methods and means of existing approaches to authentication and information protection and existing approaches to authentication based on biometric features. Structural methods of data protection are stated. It is impossible to make an unambiguous conclusion about which of the modern methods of biometric authentication or combined methods is the most effective for a particular commercial method by calculating the ratio of price and reliability. Obviously, for most commercial applications, the use of complex mixed systems does not seem logical.

**THE LIST OF SOURCES**

1. Спиридонов И.Н., Биометрические технологии в комплексных автоматизированных системах безопасности государства / Вестник МГТУ. Н.Э. Баумана. Серия: приборостроение, 2011, 2, 3-10.

2. Смит Р.Э., Аутентификация: от паролей к открытым ключам, Издательство «Вильямс», (2002). 432 с.

3. Комаров А.Е., Современные методы аутентификации: токен и все о нем / Телекоммуникации и транспорт, 2008, 6, 13–16.

4. Кухарев Г.А., Алгоритмы двумерного анализа главных компонент для задач распознавания изображений лиц, Н. Л. Щеголева // Компьютерная оптика, 2010, 34, 4, 545–551.

5. Ушмаев О.С., Биометрическая идентификация по радужной оболочке: современное состояние и перспективы / График-кон, 2011, 192-194.

6. К. Нгуен, Фукс К., Р. Джиллела, Распознавание радужной оболочки на большом расстоянии: опрос / распознавание образов, 2017- Том. 72.—С. 123–143.

7. Ю. Сюй, З. Фан, М. Куи, Метод разреженного представления бимодальной биометрии и эксперименты по распознаванию отпечатков пальцев // Нейрокомпьютинг, 2013, 164–171.

8. Матвеев Ю.Н., Технологии биометрической идентификации человека по голосу и другим модальностям / Вестник МГТУ им. Н.Э. Баумана. сер. Инструментарий, 2012, 3, 46–61.

9. Шомакер, Л., Идентификация и проверка писателя // Успехи биометрии, 2008, 247–264.

10. Лысак, А.Б., Идентификация и аутентификация личности: обзор основных биометрических методов проверки подлинности пользователя компьютерных систем / Математические структуры и моделирование, 2012, 26, 124–134.

11. Ли С.З. , Справочник по распознаванию лиц, Springer, 2005, 395 стр.

12. Джейн, А.К., Справочник по биометрии / А.К. Джейн, П. Флинн, А. Росс.— Спрингер, 2008.

13. Кухарев Г.А., Кухарев Е.И. Каменская, Ю.Н. Матвеев, Н.Л. Щеголева (). Методы обработки и распознавания изображений лиц в задачах биометрии [Текст] 2013, 387 с.

**REFERENCES**

1. Spiridonov, I.N. (2011). Biometric technologies in integrated automated security systems of the state [Text] / I.N. Spiridonov // Bulletin of the Moscow State Technical University. N.E. Bauman. Series: instrument making, 2, 3-10.
2. Smith (2002). R.E. Authentication: from passwords to public keys [Text] / R.E. Smith. - M .: Publishing house "Williams", 432 p.
3. Komarov, A.E. (2008). Modern authentication methods: a token and that's all about it [Text] / A.E. Komarov // Telecommunications and transport, 6, 13–16.
4. Kukharev, G. A. (2010). Algorithms for two-dimensional principal component analysis for face image recognition problems [Text] / G. A. Kukharev, N. L. Shchegoleva // Computer Optics, 34, 4, 545–551.
5. Ushmaev, O.S. (2011). Biometric identification by the iris of the eye: current state and prospects [Text] / O.S. Ushmaev // Graphic-con'2011, 192-194.
6. K. Nguen, Fookes C., R. Jillela (2017). Long range iris recognition: A survey [Text] / Pattern recognition. -. - Vol. 72.—P. 123–143.
7. Y. Xu, Z. Fan, M. Qui (2013). A sparce representation method of bimodal biometrics and palmprint recognition experiments [Text] / [et al.] // Neurocomputing, 164–171.
8. Matveev, Yu.N. (2012). Technologies of biometric identification of a person by voice and other modalities [Text] / Bulletin of MSTU im. N.E. Bauman. Ser. Instrumentation, 3, 46–61.
9. Schomaker, L. (2008). Writer identification and verification [Text] / L. Schomaker // Advances in biometrics, 247–264.
10. Lysak, A.B. (2012). Identification and authentication of a person: a review of the main biometric methods for verifying the authenticity of a user of computer systems [Text] / A.B. Lysak // Mathematical structures and modeling, 26, 124–134.
11. Li, SZ (2005). Handbook of Face Recognition [Text] / SZ Li, AK Jain.— Springer, 395 p.
12. Jain, AK (2008) Handbook of biometrics [Text] / AK Jain, P. Flynn, A. Ross.— Springer.
13. G. A. Kukharev, E.I. Kamenskaya, Yu.N. Matveev, N.L. Shchegolev (2013). Methods of processing and recognition of images of faces in biometrics problems [Text] , 387 p.

**Есмағамбетова Г.Қ.1\*, Б.Жадамбаа1, Қ.Қ.Сағынбаева1, А.Н.Исмұқанова2**

1Моңғолия ғылым және технология университеті, Моңғолия

2Көкшетау университеті Ш.Уәлиханов, Қазақстан

**Биометриялық аутентификацияның қолданыстағы тәсілдерін талдау**

Мақалада адамның биометриялық аутентификациясын сипаттау мен талдаудың заманауи үлгілері негізінде биометриялық деректер модельдерін ұсыну, биометриялық верификация алгоритмдерін құру және тұлғаны сәйкестендіру әдістері зерттеледі және талданады. Биометриялық сәйкестендіруде адамның келесі параметрлері кеңінен қолданылады: бет геометриясының ерекшеліктері, саусақ іздері, алақанның геометриясы, көз торы мен ирис, дауыс сипаттамалары, қолтаңба ерекшеліктері және пернетақта астын сызу. Биометриялық аутентификация ақпараттық жүйені пайдаланушылардың аутентификация технологияларын дамытудың ең перспективалы бағыттарының бірі болып табылады.

Мақсаты: Ақпараттық жүйені пайдаланушының аутентификациясының негізгі мақсаты – ақпараттық жүйе қауіпсіздігінің қатерлерін, атап айтқанда, ақпараттың құпиялылығын бұзу қаупін, ақпараттың тұтастығын бұзу қаупін, жүйенің жұмыс қабілеттілігін бұзу қаупін азайту. Қауіптер әртүрлі жолдармен бұзушылықтар арқылы туындауы мүмкін. Бұзушылықтың ең көп тараған түрі – рұқсатсыз кіру. Пайдаланушыны аутентификациялау процедурасы ұсынылған идентификатор қол жеткізу субъектісіне жататынын тексеруге және оның түпнұсқалығын растауға мүмкіндік береді, яғни. субъектінің ол кім екенін тексеріңіз.

Автоматты сәйкестендіру жүйелеріне келетін болсақ, биометриялық жүйелер деп сәйкестендіру немесе аутентификация үшін адам ағзасының кез келген ерекше сипаттамаларын пайдалануға негізделген жүйелер мен әдістер түсініледі. Биометрия – тірі ағзалардың дене ерекшеліктерін сипаттауға және өлшеуге негізделген ғылым. Біздің жеке басын сәйкестендіру және аутентификациялау алаяқтық пен қылмыстың алдын алу арқылы қауіпсіз өзара әрекеттесуді қамтамасыз ететін заманауи қоғамның негізгі элементтерінің біріне айналды.

Әдістер: Биометрияда аутентификацияның екі әдісі бар:

• Биометриялық параметрге және нақты адамды ерекшелендіретін бірегей идентификаторға негізделген верификация, верификация (мысалы, сәйкестендіру нөмірі), яғни бұл әдіс аутентификация әдістерінің жиынтығына негізделген.

• Сәйкестендіру, верификациядан айырмашылығы, тек биометриялық критерийлерге негізделген. Бұл жағдайда өлшенген параметрлер тіркелген пайдаланушылардың деректер қорындағы барлық жазбалармен салыстырылады, олардың біреуі таңдалмайды, бірақ кейбір идентификаторға негізделеді.

Нәтижелер және олардың маңыздылығы: Биометриялық аутентификацияның заманауи әдістерінің немесе аралас әдістердің қайсысы тиімдірек екендігі туралы біржақты қорытынды жасау қиын. Адамның биометриялық параметрлерін өлшеуге негізделген аутентификация әдістері 100% дерлік сәйкестендіруді қамтамасыз етеді, құпия сөздерді және жеке идентификаторларды жоғалту мәселелерін шешеді, бұл ақпаратты ашу жүйелеріне қауіпсіздік қатерлерін анықтауға күдік туғызады.

**Есмагамбетова Г.K.1\*, Б. Жадамбаа1, K.K.Сагинбаева1, A.Н.Исмуканова2**

1 Монгольский университет науки и технологии, Монголия

2 Кокшетауский университет им. Ш.Уалиханова, Казахстан

**Анализ существующих подходов к биометрической аутентификации**

В статье исследуются и анализируются методы представления моделей биометрических данных, создание алгоритмов биометрической верификации и идентификации личности на основе современных моделей описания и анализа биометрической аутентификации личности. Наиболее широко в биометрической идентификации используются следующие параметры человека: особенности геометрии лица, отпечатки пальцев, геометрия ладоней, сетчатки и радужной оболочки глаз, характеристики голоса, особенности подписи и подчеркивание клавиатуры. Биометрическая аутентификация является одним из наиболее перспективных направлений развития технологий аутентификации пользователей информационных систем.

Назначение: Основной целью аутентификации пользователя информационной системы является снижение угроз безопасности информационной системы, а именно угрозы нарушения конфиденциальности информации, угрозы нарушения целостности информации, угрозы нарушения работоспособности системы. Угрозы могут быть вызваны различными способами нарушений. Самый распространенный вид нарушения — несанкционированный доступ. Процедура аутентификации пользователя позволяет проверить принадлежность предъявленного идентификатора субъекту доступа и подтвердить его подлинность, т.е. проверить, является ли данный субъект тем, за кого себя выдает.

Применительно к системам автоматической идентификации под биометрическими системами понимаются системы и методы, основанные на использовании каких-либо специфических характеристик человеческого тела для определения или аутентификации. Биометрия – это наука, основанная на описании и измерении характеристик тела живых организмов. Идентификация и аутентификация нашей личности стали одним из основных элементов современного общества, обеспечивая безопасное взаимодействие путем предотвращения мошенничества и преступлений.

Методы: Биометрия имеет два метода аутентификации:

• Верификация, верификация на основе биометрического параметра и уникального идентификатора, отличающего конкретного человека (например, идентификационного номера), то есть этот метод основан на сочетании методов аутентификации.

• Идентификация, в отличие от верификации, основана только на биометрических критериях. При этом измеряемые параметры сравниваются со всеми записями в базе данных зарегистрированных пользователей, выбирается не один из них, а на основе некоторого идентификатора.

Результаты и их значимость: Сложно сделать однозначный вывод о том, какой из современных методов биометрической аутентификации или комбинированных методов является наиболее эффективным. Методы аутентификации, основанные на измерении биометрических параметров человека, обеспечивают практически 100% идентификацию, решая проблемы утери паролей и персональных идентификаторов, что приводит к подозрениям в обнаружении угроз безопасности систем раскрытия информации.