SHORTCOMINGS OF EXISTING IDENTIFICATION AND AUTHENTICATION METHODS

Umbetaliev Bekmurza Maxsudovich,
Assistant teacher at the University of innovation technologies
E-mail: bekumbetaliev@yandex.com

Annotatsiya: Maqolada foydalanuvchilarni identifikatsiya va autentifikatsiya qilishning zamonaviy usullari hamda ularning axborot xavfsizligidagi ahamiyati tahlil qilingan. Bilim, egalik va biometrik belgilar asosidagi yondashuvlar tasniflangan. Mavjud kamchiliklar ko‘rsatilgan va ishonchlilikni oshirish uchun ko‘p omilli yondashuv taklif etilgan. Muallifning ilmiy hissasi autentifikatsiya tizimlarini takomillashtirish bo‘yicha amaliy tavsiyalar ishlab chiqishda namoyon bo‘ladi.

Kalit so‘zlar: identifikatsiya, autentifikatsiya, parol, smart-karta, token, biometrika, xavfsizlik, zaifliklar, inson omili, axborotni himoya qilish.

Аннотация: В статье рассмотрены современные методы идентификации и аутентификации пользователей, а также их значение для информационной безопасности. Представлена классификация по признакам знания, владения и биометрии. Отмечены недостатки существующих подходов и предложена комбинированная модель, повышающая надежность и защиту. Научный вклад автора заключается в формировании практических рекомендаций по совершенствованию систем аутентификации.

Ключевые слова: идентификация, аутентификация, пароль, смарт-карта, токен, биометрия, безопасность, уязвимости, человеческий фактор, защита информации.

Abstract: The article analyzes modern methods of user identification and authentication, emphasizing their importance for information security. It classifies approaches based on knowledge, possession, and biometrics. The study highlights existing weaknesses and proposes a combined, multi-factor model to enhance reliability and protection. The author’s contribution lies in developing practical recommendations for improving authentication systems.

Keywords: identification, authentication, password, smart card, token, biometrics, security, vulnerabilities, human factor, information protection.

Introduction

Identification and authentication are fundamental components of information security systems, ensuring that access to digital resources is granted only to legitimate users. With the rapid advancement of information technologies and the increasing sophistication of cyberattacks, traditional authentication methods such as passwords and PIN codes have become highly vulnerable to

ISSN 3030-3907

various forms of compromise. As a result, the need for more secure and reliable identification mechanisms has become critical.

Modern identification methods are generally classified into three main categories: knowledge-based, possession-based, and biometric-based systems. Each approach has distinct characteristics, advantages, and limitations. Knowledge-based methods rely on information known by the user, such as passwords, but they are susceptible to human error, password reuse, and phishing attacks. Possession-based methods, such as smart cards or tokens, offer higher security but can be lost, stolen, or shared, compromising system integrity.

In contrast, biometric identification has emerged as a more secure and convenient alternative. By relying on unique physiological and behavioral traits such as fingerprints, iris patterns, or voice characteristics, biometric systems provide strong resistance to impersonation and unauthorized access. However, they also introduce challenges related to data privacy, accuracy, environmental sensitivity, and implementation cost.

This study aims to analyze and compare existing identification and authentication methods, focusing on their reliability, accuracy, and resistance to forgery. Special attention is given to biometric technologies, as they represent a rapidly developing direction in information security, providing enhanced protection while reducing the influence of the human factor.

LITERATURE REVIEW

This section analyzes the sources used in the study related to user identification and authentication. In modern information systems, the identification process serves as a key component in ensuring information security by verifying a user's identity.

Development of identification methods.

Dobryakova G. E. [1] analyzed the main problems of identification in information systems and emphasized the importance of minimizing the negative influence of the human factor during authentication. Pham Z. T. [2] examined the implementation of modern identification systems in Vietnam's national information infrastructure and highlighted their role in strengthening national security.

Biometric technologies.

Kubitovich S. N. [3] explored DNA identification as an information carrier that allows storing unique individual traits. Golubev M. N. [4] demonstrated the efficiency of using color information in face recognition algorithms and proposed neural network–based methods to increase the accuracy of biometric systems.

Global development trends.

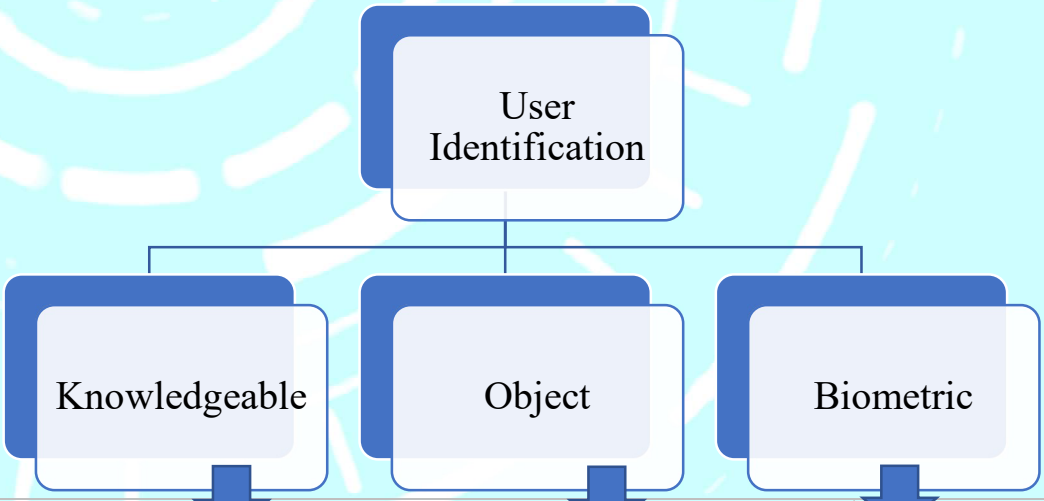
ISSN 3030-3907

According to Biometric Update [5], by 2020 the global biometrics market had reached 24.6 billion USD. This fact reflects the rapid growth of biometric authentication technologies and their rising importance in ensuring information security.

Overall, the reviewed literature indicates that identification and authentication technologies are continuously evolving toward minimizing human error, increasing accuracy, and enhancing overall system security.

RESEARCH METHODOLOGY

Identification is the process of comparing data with a specific person. Identification methods are usually classified according to the tools used. In this case, as shown in Figure 1, these methods were divided into 3 groups.



Manifestation	Password	Subject	Biometry
Identifies	By knowledge	By possession	By uniqueness
Deficiency	Low secrecy	By possession	Difficult to replace

Figure 1 - Classification of identification methods

The first method is the most common and consists in the fact that the user who has access to system resources knows that no one else knows (password, PIN, security. In most systems, identification is carried out using the username and password. When using control information, there is a risk of forgetting it or passing it on to a third party. Additionally, the effectiveness of PIN codes has been severely undermined by the emergence of counterfeit devices such as ATM keyboards, scrapers, and mini-cameras. This way, your password may be compromised. Additionally, you can easily hack accidentally chosen passwords in October (in the same recording, referring to the person's identity). Password protection is especially relevant for the distribution of social networks, where all personal information is readily available [17].

ISSN 3030-3907

The identification system implementing the group method also has its drawbacks. They use what the user has as an identity document. Examples include magnetic stripe maps and smart decks. Smart cards, tokens, or other identification elements can be stolen or deliberately transferred to someone due to non-compliance with security rules, which jeopardizes the system's security, thereby increasing the system's reliability, but without adequately eliminating the human factor.

Another important disadvantage of these methods is that they only carry out control at the beginning of work in the system and do not control the individual during work [17].

Biometric technology is based on biometrics, which represents the measurement of a specific person's behavioral or physiological characteristics. Physiological characteristics, also called statistical characteristics, include unique physical characteristics that a person acquires from birth and are present throughout their life. These include:

– DNA identification;
– Identification using a facial thermogram;
– Identification by the iris;
– Face recognition;
– Identification using manual geometry;
– Fingerprint identification;
– Identification by the type of vein;
– Identification by acoustic characteristics of the ear [6].

Behavioral characteristics, which are otherwise dynamic, on the contrary, acquire over time and constantly change due to aging or external influences. These features include:

– Identification by keyboard handwriting;
– Voice identification;
– Manual identification.

The most frequently used identification method in excavations is fingerprint identification. This was the answer of 57% of respondents in a survey conducted by Spiceworks [37]. The first place in this method is provided by the spread of technology to smartphones, the data are presented in Figure 2.

ISSN 3030-3907

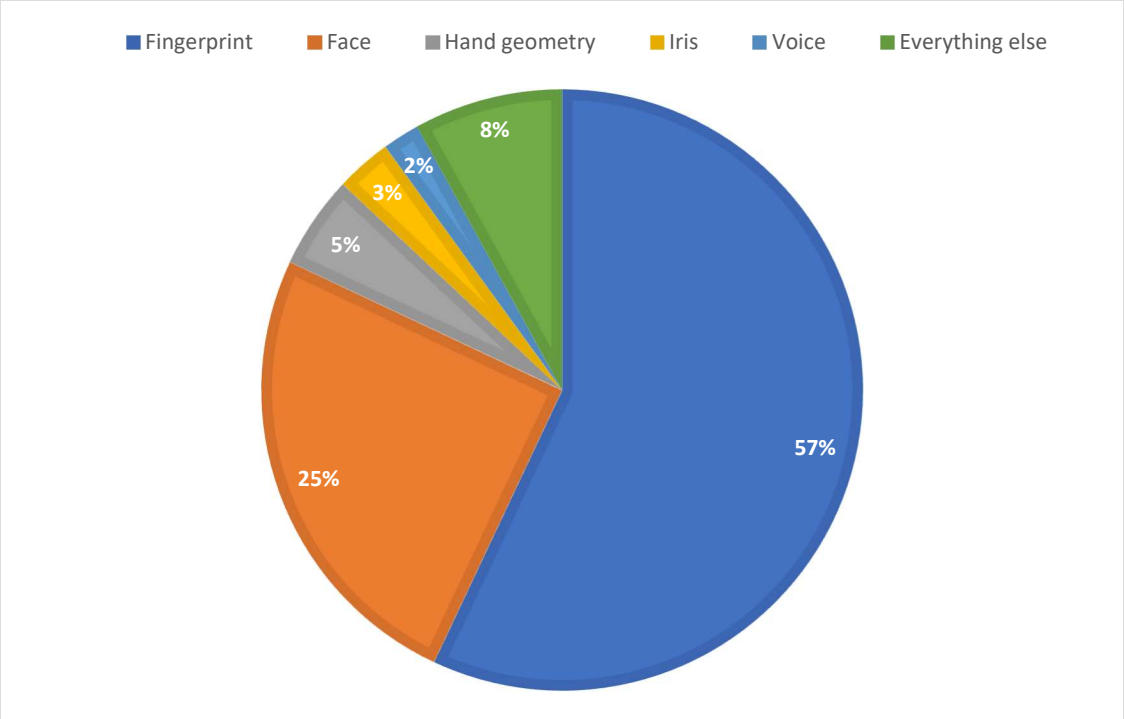


Figure 2 - Popularity of biometric identification methods (source: Spiceworks, 2020)

In a typical biometric authentication system, the identification process is divided into 4 stages according to Figure 3.

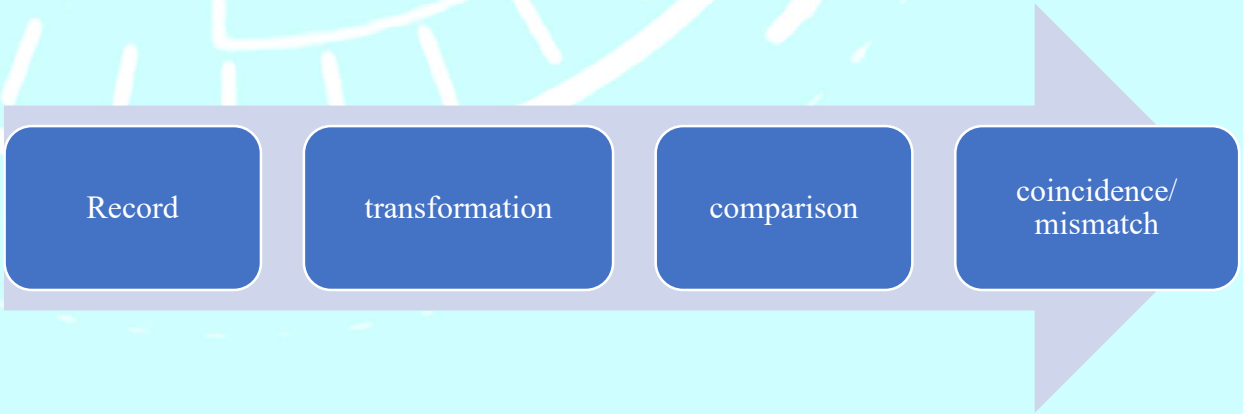


Figure 3 - Identification process diagram

Identification process steps:

1. Record - Behavior or physical parameters are recorded and stored by the system. The more the recording is repeated, the higher the similarity of the expression to the user's reading characteristics.

2. Transformation - data is analyzed using mathematical operations, unique information is assigned, and biometric templates are created in the form of information codes;

3. Comparison - biometric templates stored in a secure database are compared with recently sent biometric samples. A digital binary code with a recording length of up to 1000 bits is stored in the memory of a biometric system associated with 1 user of this system.

ISSN 3030-3907

4. Match / Mismatch - the system transmits a message about the similarity of two biological samples and makes a decision about match or mismatch [23].

The reliability of biometric authentication methods is assessed as follows: 1. and 2. Type errors are usually taken as a measure of the main characteristics. Incorrect Failure Rate The first type of FRR error is the probability of incorrectly refusing access to a legitimate user. False reception factor - FAR, 2. The type of error is the probability of incorrect access if the system passes through an unfair user and behaves like someone else. The lower the FRR value for the same headlight value, the better and safer the system is [20].

Let's compare the main identification methods with statistical parameters. The average values of FAR and frr for the most common biometric methods are shown in Table 1.

Table 1

Average values of FAR and FRR.

Биометрическая СКУД использует:	FAR	FRR
Отпечаток пальца	0,001	0,6
Распознавание лица 2D	0,1	2,5
Распознавание лица 3D	0,0005	0,1
Радужная оболочка глаза	0,00001	0,016
Сетчатка глаза	0,0001	0,4
Рисунок вен	0,0008	0,01

To develop an effective access control and management system, it is insufficient to consider only FAR and FRR indicators. For comprehensive and in-depth analysis and comparison of biometric access control and management systems, it is necessary to rely on the following parameters:

Counterfeit resistance - assessment of the complexity of deceiving a biometric identifier;

constancy of biometric characteristics - stability of biometric data over time;

resistance to environmental influences - system's sensitivity to changes in external conditions;

processing speed - system efficiency;

cost of implementation and operation - economic efficiency of the system.

CONCLUSION

In conclusion, the conducted research demonstrates that user identification and authentication remain fundamental elements of modern information security systems. Traditional methods based on passwords and physical tokens, while still

ISSN 3030-3907

widely used, no longer meet the requirements of reliability and protection in the face of growing cyber threats.

The comparative analysis of various identification techniques showed that biometric methods — particularly fingerprint, facial, and iris recognition — ensure the highest level of accuracy and resistance to unauthorized access. However, these systems also require advanced protection of biometric data to prevent potential misuse.

The study confirms that a combined, multi-factor authentication approach provides the most effective balance between usability and security. Integrating knowledge-based, possession-based, and biometric mechanisms significantly reduces vulnerability to cyberattacks and human error.

Overall, this work contributes to the understanding of how modern identification technologies evolve and highlights the necessity of developing adaptive, intelligent authentication systems to ensure the sustainable security of digital infrastructures.

LIST OF USED SOURCES

1. Добрякова Г.Э. Проблемы идентификации в информационных системах // Правовая информатика. 2014. № 3. С. 28–32.
2. Фам З.Т. Современные системы идентификации личности для развития национальной информационной инфраструктуры социалистической республике Вьетнама // Международный научно-исследовательский журнал. 2015. № 6-1. С. 83–85.
3. Кубитович С. Н. ДНК как носитель информации неограниченного круга лиц // Вестник экономической безопасности. 2017. № 4. С. 184—188.
4. Голубев М. Н. “Использование информации о цвете в алгоритме выделения лиц на базе бустинга”, Сб. науч. труд. 13-й всерос. науч.-техн. конф. “Нейроинформатика – 2011”, М, 2011. Ч. 3. С. 55 – 62.
5. Официальный сайт Biometric Update. [Электронный доступ] - URL: http://www.biometricupdate.com/201412/globalbiometrics-market-projected-to-reach-24-6-billion-by-2020 (дата обращения: 25.12.2022)

ISSN 3030-3907