II Всероссийская (национальная) научная
конференция с международным участием
«Российская наука, инновации, образование»
(РОСНИО-II-2023)

8 (2023)

УДК 004.9

EDN AVQSEA

Обзор видов идентификации в системах контроля и управления доступом

Е.В. Зайцева[*], Н.О. Кулигина, Е.А. Тарлаковская

Нижегородский государственный технический университет им. Р.Е. Алексеева, г. Нижний Новгород

*E-mail: zaitseva.eee@yandex.ru

Аннотация. Оборудование территории учреждения, офисного комплекса или предприятия системами контроля и управления доступом (СКУД) существенно увеличивает безопасность учреждения или организации. СКУД является инновационным решением проблем учета, наблюдения и охраны любого рабочего или торгового комплекса. Осуществляется это путем объединения вышеперечисленных факторов в единую систему контроля. Идентификация является одним из наиболее важных аспектов в системе контроля и управления доступом. Для эффективной работы СКУД необходимо точно определить идентичность каждого пользователя, имеющего доступ к системе.

В статье рассматриваются все возможные способы организации идентификации. Каждый вид идентификации имеет свои особенности, которые могут быть плюсом для одного проекта, и минусом для другого. Поэтому следует изначально на начальном этапе проектирования системы рассмотреть все возможные виды идентификации, чтобы выбрать для своего проекта максимально подходящий вариант.

Ключевые слова: СКУД, идентификация, биометрия, отпечаток, сканирование, распознавание, пароль, PIN-код, штрихкод, смарт-карта.

Overview of identification types in access control and management systems

E.V. Zaitseva[*], N.O. Kuligina, E.A. Tarlakovskaya

Nizhny Novgorod State Technical University n.a. R.E. Alekseev, Nizhny Novgorod

*E-mail: zaitseva.eee@yandex.ru

Abstract. Equipping the territory of an institution, office complex or enterprise with access control and management systems (ACS) significantly increases the security of an institution or organization. ACS is an innovative solution to the problems of accounting, monitoring and protection of any working or shopping complex. This is done by combining the above factors into a single control system. Identification is one of the most important aspects in an access control and management system. For the effective operation of the ACS, it is necessary to accurately determine the identity of each user who has access to the system.

The article considers all possible ways of organizing identification. Each type of identification has its own characteristics, which can be a plus for one project, and a minus for another. Therefore, at the initial stage of system design, you should consider all possible types of identification in order to choose the most suitable option for your project.

Keywords: ACS, identification, biometrics, fingerprint, scanning, recognition, password, PIN code, barcode, smart-card.

1. Introduction

The access control and management system is a complex of integrated methods and technologies that allow you to control access to restricted areas or resources in physical premises or information systems. ACS includes hardware and software that allows you to identify users, verify their credentials and restrict access to unauthorized zones or resources. [1]

ACS is used in various fields, including offices, manufacturing enterprises, banks, government agencies, airports, shopping malls, warehouses, medical institutions, etc. [1]

The access control and management system can be organized as a physical barrier that does not allow access to the zone without using a special access card or scanning biometric data, such as fingerprints or facial recognition.

ACS can be used to protect information resources, such as database servers, which are accessed only by authorized users.

ACS allows you to significantly increase the level of security in access zones and prevent unauthorized access. It also provides easy access for authorized users, which helps to reduce the time for checking each person entering the access zone [1].

2. Materials and methods

Identification is one of the most important aspects in the access control and management system. For the effective operation of the ACS, it is necessary to accurately determine the identity of each user who has access to the system.

Identification errors can lead to unauthorized access, violation of the security and integrity of information. For example, people can gain access to secure premises or important data using compromised credentials of other users. Therefore, to ensure the safety and effectiveness of ACS, it is necessary to use reliable identification methods that can determine the identity of the user with high accuracy.

The choice of the identification method in the access control and management system depends on the goals and requirements that the system must meet, and may include the following factors:

- Accuracy. Some identification methods are more accurate than others. For example, biometric methods such as fingerprint scanning or personality trait recognition may be more accurate than using keys or magnetic stripe cards.

- Security. The identification method must be secure and capable of providing a sufficient level of protection against unauthorized access. For example, biometric methods with high accuracy can provide a higher level of security than passwords and PIN codes that can be stolen or picked up.
- Convenience. The system should provide user-friendliness for users. For example, identification methods such as access cards or keys may be more convenient to use than biometric methods, which may require additional time to verify identity.
- Costs. The cost of the access control system should also be taken into account when choosing the identification method, since different methods may have different costs. For example, biometric methods can be more expensive than using passwords or keys.
- Easy to control. The system should be easily manageable and configurable. For example, systems using access cards can be more easily managed and configurable than biometric methods.

So, when choosing the method of identification in the access control and management system, the above factors should be taken into account and choose the method that best meets the requirements of the system, meets the needs of users and at the same time ensures security and efficiency.

3. Results and discussion

Access control systems (ACS) represent various methods of user identification. Each method has its advantages and disadvantages.

All possible identification methods in the ACS are listed below:

1. Identification by password or personal identification number (PIN)

A password or PIN is one of the oldest identification methods in the ACS. This consists in using a predefined password or PIN code to gain access to specific resources. The system compares the entered password/PIN with the stored value and gives access if they match. Password identification is easy to implement and deploy, but it is vulnerable to attacks such as brute force and dictionary attacks. In addition, it is vulnerable to the use of shared passwords or compromised password databases.

Usually, PIN codes are generated automatically by the access control system when registering a new user or when changing access for an existing user. The PIN code consists of numbers or letters and numbers and can be generated by the system randomly or based on a certain formula.

In some cases, the PIN code can be assigned manually by the user, provided that the selected code is sufficiently complex and secure. In such cases, you can use the minimum code length requirement, the use of numbers and symbols, and other rules to create a secure and reliable PIN code.

2. Identification by smart card

Smart card-based identification involves the use of a plastic card with a built-in chip that stores data used to identify and authenticate the user. The card may also contain a magnetic stripe or radio frequency identification (RFID) technology to facilitate access. The system compares the data on the map with the user identification information to give access. Smart cards are more secure and provide additional features such as one-time password generation and data encryption. However, they are subject to major risks, such as card cloning, physical theft or damage, and require additional hardware to read information.

Smart cards come in the following formats:

- A smart card with a magnetic stripe. This technology is based on the principle of magnetic recording of information on a thin magnetic strip, which is placed on the surface of the card. The magnetic stripe on the card contains data about the user, such as his name, position, access number and other information necessary for identification. To read information from the magnetic stripe, you need to use a special device - a card reader. As soon as the card with the magnetic stripe is brought into contact with the card reader, the magnetic information is read automatically. After that, the system can verify the authenticity of the card and grant or restrict user access. One of the main advantages of magnetic stripe smart cards is their relatively low cost in comparison with other identification technologies, such as biometric scanners or RFID tags. Thanks to this, magnetic stripe smart cards are widely used in various sectors of industry and access control, including offices, warehouses, airports, hotels, shopping malls and other organizations where access control is needed.
- RFID (Radio Frequency Identification) is a wireless identification technology that uses a radio frequency electromagnetic field to read and write information on special tags or tags. In the case of RFID smart cards, such tags are embedded in the card [2].

3. Biometric identification

Biometric identification is a method that applies unique physical or behavioral features to authenticate a user. The most common biometric identification methods include fingerprint recognition, facial recognition, iris and retina recognition, and voice recognition. Biometric identification is more secure and accurate compared to other identification methods. However, it can be implemented only if the necessary hardware and software are available. [5]

- Fingerprint is a technology based on capturing and processing the image of a unique pattern of the finger surface. This method is one of the most reliable and secure ways to identify an individual, since the fingers are unique and cannot be faked. The system scans the finger and creates a unique pattern of folding patterns on the fingers, which is processed by special equipment. [6]
- Palm vein print is a technology that uses a special infrared camera to scan blood vessels and create a unique pattern of veins on the palm. This method of identification is more reliable than a fingerprint, since the veins on the palm are almost not subject to change over time and cannot be forged.
- Face recognition is a technology that allows you to identify the identity of a user by his photo or a live image of a face by analyzing unique features, such as the shape and size of eyes, nose, mouth, figure and other characteristics. To determine the identity of the user, a camera with software is required that compares the information received with the model stored in the database. [7]
- Iris scanning is a technology that allows you to determine the identity of a user by creating a unique iris pattern. To do this, a special camera is used that scans the eye and analyzes unique features, such as the size, shape and position of the iris.
- Voice recognition is a technology that uses a special software voice analyzer that allows you to identify a user by voice. This requires a headset or microphone that collects information about the properties of the voice, such as tone, frequency and intonation. The analytical software compares the received data with the model in the database.
- Manuscript scanning is a technology that allows you to identify a user by his handwriting. This requires special equipment that scans the handwriting and compares it with the model in the database.

Each type of biometric identification has its advantages and disadvantages, as well as its unique features in the field of security, efficiency and reliability. Therefore, the choice of biometric identification technology should depend on the specific needs and limitations of the access control and management system.

4. Tokenized Identification

Tokenized identification involves the use of a unique device, such as a keychain or USB stick, to identify and authenticate users. The device generates a random code or password that expires after a certain time, and the system uses it to authenticate the user. Tokens are more secure than passwords/pins, as they are less susceptible to attacks such as brute force and dictionary attacks. However, tokens can be lost, and they need to be replaced and maintained frequently.

5. Two-factor authentication

Two—factor authentication is a combined identification method that involves the use of two different identification mechanisms for authentication. For example, a user may be required to provide a password and a one-time code sent to his phone or email. Two-factor authentication provides an additional level of security compared to other identification methods and is a suitable solution for applications requiring high security. However, it can be expensive, especially for small businesses.

When passing two-factor authentication, the user usually first presents his access card to gain physical access to the premises, servers or information systems, and then enters his unique password or PIN code to obtain access permission.

Thus, an unauthorized user who has gained access to the access card will not be able to pass identity verification without a password or PIN code. Similarly, if an unauthorized user has found out the password or PIN code, but does not have access to the access card, they will also not be able to pass the identity verification.

Other methods of two-factor authentication can be the use of biometric methods (for example, fingerprint scanning or facial recognition) as a second factor or the creation of temporary passwords that are valid only for a certain period of time.

6. Behavior-based identification

Behavior-based identification involves identifying users based on their patterns of behavior, rather than unique physical features. The system identifies users based on their print patterns, mouse movements, or other behavioral factors. Behavior-based identification can detect fraudulent behavior and helps protect against identity theft. However, it requires the collection of data on user behavior patterns, which can cause privacy issues.

One of the ways to use behavior—based identification in ACS is to monitor user actions for unauthorized access attempts. For example, the system can remember the unique digital profile of each user, including the style of mouse movement, keyboard typing speed and other parameters that can help determine whether the user is real or fake.

Another way to use behavior—based identification is to manage access in buildings based on user behavior. In this case, the system can use user behavior data and compare it with pre-set parameters to determine whether the user has the right to access a specific zone or whether it is necessary to reject the request.

It should be noted that behavior-based identification should be used together with other technologies and security measures, such as smart cards, RFID tags, biometric scanners, etc. This approach allows you to ensure the maximum level of security of the access control system and prevent the possibility of fraud and identity forgery.

7. Identification by QR code or barcode

Identification by QR code or barcode is a method in which a special code in the format of a QR code or barcode is used to determine the identity of the user. Such a code can store information such as user credentials, access card number, workplace data, etc.

This identification method can be used in access control and management systems, for example, for issuing access cards, identifying and verifying the identity of users at the entrance to the access zone. The code can be represented by.

4. Conclusions

In conclusion, the choice of the identification method in the ACS depends on the specific security requirements and budgetary constraints of the organization. The methods listed above have various advantages and disadvantages, and organizations should weigh these factors to make sure they implement the appropriate ACS.

References

1. СКУД от «А» до «Я» // Интемс. – URL: https://securityrussia.com/blog/vibrat_skud.html (дата обращения: 04.04.2023).
2. What Is RFID Access Control And How Does It Work? // nortechcontrol. – URL: https://blog.nortechcontrol.com/rfid-access-control (дата обращения: 01.04.2023).
3. Em-Marine - обзор стандарта // SecurityRussia. – URL: https://securityrussia.com/blog/em_marine.html (дата обращения: 01.04.2023).

4. SECURE IDENTIFICATION BASED ON MIFARE CARDS // Sigur. – URL: https://sigur.com/en/features/ident_mifare/ (дата обращения: 01.04.2023).
5. Biometrics for access control? // screencheckme. – URL: https://www.screencheckme.com/different-types-biometrics-access-control/ (дата обращения: 01.04.2023).
6. O'Gorman L. 2 Fingerprint Verification, Pers. Identif / L. O'Gorman, N.J. Chatham // Networked Soc. – 1999. – Vol. 3. – no. 1. – P. 43.
7. Abate A. F. 2D and 3D face recognition: a survey / A. F. Abate, M. Nappi, D. Riccio, G. Sabatino // Pattern Recognition Lett. – 2007. – Vol. 28. – P. 1885-1906.