ОСВІТА, НАУКА ТА ВИРОБНИЦТВО: РОЗВИТОК ТА ПЕРСПЕКТИВИ

МАТЕРІАЛИ
III Всеукраїнської науково-методичної конференції

(Шостка, 19 квітня 2018 року)

BIOMETRIC AUTHENTICATION SYSTEMS

O.M. Putienkov, A.V. Bulashenko

National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute"
alex_putienko@ukr.net, an_bulashenko@i.ua

Authentication - authentication of the user-submitted identifier. Authentication is required when accessing such Internet services as e-mail, web-forum, social networks, Internet banking, payment systems, corporate websites, online stores.

Authentication tools can be divided into three groups, according to the authentication information used (some unique information that only this user and no one else should have):

- the "what you know" principle, which is the basis of password authentication methods;
- the principle of "what you have", when authentication is carried out using magnetic cards, tokens and other devices;
- the principle of "who you are", which uses the personal properties of the user (fingerprint, the structure of the retina, etc.).

Biometric authentication systems are authentication systems that use their biometric data to authenticate people. Biometric data can be: fingerprint, iris, retina, hand geometry, facial features, shape and method of signature, etc.

Currently, a large number of methods of biometric authentication are widely used, which fall into two classes: static and dynamic methods of biometric authentication.

Static methods of biometric authentication are based on the physiological characteristics of a person present from birth to death, which are there during his entire life, and which can not be lost, stolen and copied. Static methods of biometric authentication include fingerprint authentication, palm form, vein location on the front side of the palm, retina, iris, face shape (2D and 3D), face thermogram, DNA, ear shape, body odor, etc. .

Dynamic methods of biometric authentication are based on behavioral characteristics of people (subconscious movements in the process of reproduction or repetition of some ordinary action). Dynamic methods of biometric authentication include authentication of handwriting, keyboard handwriting, voice, lip movement during the reproduction of the codeword, the dynamics of turning the key in the door lock, etc.

The main advantages of biometric authentication systems include:

1) high degree of reliability due to the uniqueness of biometric features;
2) the inseparability of biometric characters from a capable person;
3) the difficulty of falsifying biometric features.

A common disadvantage of biometric authentication is the need for equipment for reading biometric characteristics, which can be quite expensive.

In general, biometric authentication is the most reliable authentication system, although it is subject to numerous attacks by intruders. In this case, biometric authentication can be combined with the requirement for the user to enter a password (PIN code) for the electronic key. The sharing of biometric data and passwords provides reliable three-factor authentication.

References

1. Authentication methods [Electronic resource] - Access mode. - URL: http: // www.panasenko.ru / Articles / 69 / 69.html.
2. Alekseev D.M., Kutnyak N.A. // Protection of software against unauthorized use // Synthesis of science and society in solving global problems of our time: Sat. Art. on materials of the International scientific and practical conference "Synthesis of science and society in solving global problems of our time", part 3, Penza, February 18, 2016.