Nicholay Kuleba
I.V. Oleshko, research supervisor
K. T. Umyarov, language adviser
Kharkov National University of Radioelectronics, Kharkov

Biometric Authentication Systems

Today, such terms as identification and authentication are not unusual. Systems, that implement these concepts, find widespread use in everyday life, such as in subway travels or in using bankcards. These systems are aimed at ensuring secure human activity in different areas and tracking the legality of people's actions.

The use of identification and authentication systems based on three factors, each of them contains a group of methods for their practical implementation - property, knowledge and ownership. The use of one or another factor in the construction of systems determine the requirements of the object security, in which a system is installed, and the requirements for reliability.

The aim of this report is to review the principles of biometric authentication systems and analysis of their species, as well as to give an example of the components of these systems and evaluation of their effectiveness and to discuss the problems of use.

Biometric authentication is a kind of "property" factor. The diversity of the human body and availability of each person's unique distinguishing features allows to apply different approaches in building systems based on biometric recognition. One of the main advantages of using these systems is the fact that people in normal life conditions cannot lose "property", which is necessary for the successful completion of the authentication, since it is inherent to him from birth and practically does not change during lifetime.

Almost all biometric systems basically use a probabilistic approach to the determination of the individual. Consequently, during the object recognition, using one or another feature, error probability should be reduced to a minimum. Therefore, any system, in addition to recognition modules, contains an error reduction module, the essence of which lies in neutralizing or reducing unwanted extraneous factors, which affect the system performance, as well as in improving the accuracy of recognition.

With the increased security requirements and to improve the reliability of the final recognition result there is a practice of creating multi-biometric systems, which are based on consistent recognition of multiple biometrics.

Biometric systems have a great potential of development. By using biometric technologies, access procedures should be made simpler, faster and more secure. But the construction of these systems introduces additional safety requirements for personal biometric data used to commit the appropriate checks, biometric identification of people with certain physical disabilities, training professional personnel, etc.