Abstact

Relevance of the work

Information systems of National Value (ISNV) have been widely applied in public sector management and accounting of the population. They can be used to control the entry and exit of citizens, for internal identification, and autentification as well as systems for the delivery of public services (a passport, visas, etc.).

Such ISNM use biometrics, specifically fingerprints, photograph and signature.

Identification of these systems can take place on several criteria, but the most important of these are biometrics, because they most closely identify any individual person.

Biometric data are key parameters to identify the system or to authenticate identity. And because the receipt or falsifying them are tasks that need to bypass malitious user identification and authentication.

Urgent task is protection against leakage of information on biometrics in the ISNM. Another reason to consider this urgent task lies in the fact that the standards in the regulations do not specify how exactly should be protected by the biometric data. And accordingly there are no clear requirements for the protection of such systems.

The purpose of

The aim is to:

1. Study of the peculiarities of constructing an information system on a national scale (INSM).

2. The study of channels of information leakage from INSM

3. Investigation of protection mechanisms of biometric passport.

4. Razrabotra recommendations for the construction and protection of ISNM-based studies.

Problem to be solved in

1. The study of standards for the recommendations for the protection of biometric data.
2. Investigation of threats of data leakage from the ISNV.
3. Investigation of the reliability of biometric passports.
4. Investigation of existing methods of protection ISNV.
5. Development of recommendations for improving protection of ISNV.

Results Achieved

Solving the problems that put in the work, the author defends:

- The results of the research standards for the protection of biometric data;
- Results of the study threats to data loss from ISNV;
- Results of the study the reliability of biometric passports;
- recommendations to improve protection of ISNV;

Scientific novelty

Scientific novelty robot lies in fact:

- Research identified and analyzed by standard biometrics are responsible for the protection of biometric data.
- Research identified the possible channels of leaks of biometric data from ISNV;
- The ways blocking channels of data leakage and gives recomedations on their elimination, as well as developed new guidelines for improving the level of protection ISNV;

The practical value of

The practical value of the work lies in the fact that:

- The study can be used to select remedies ISNM.
- Obtained in consequence of the analysis of threats of information leakage from

INSM, recommendations can be used to build systems for the protection of biometric data in the IP.

Conclusions

After analyzing the existing standards of biometric technologies that are relevant to the protection of personal data, it was found that standards of protection that are described there, are inadequate and weak and can protect against insiders and unauthorized access.

As you work, we analyzed the possible channels of information leakage from the ISNM. Solutions have been proposed to eliminate the information leakage channels using specialized software certified to eliminate the shortcomings of system security. Were also offered solutions for the development of ISNV, which would significantly increase the level of protection systems without resorting to special software, by constructing a system developed by taking into account the recommendations.

Work contains 84 p., 15 fig., 3 Tables., 8 sources.

Keywords: BIOMETRIC PASSPORT, METHODS OF PROTECTION OF INFORMATION SYSTEMS, BIOMETRIC DATA, OPTIMIZATION OF PROTECTION ISNM, ISNM.