Original scientific paper

Method of Two-Factor Authentication of Electronic Documents Using Enhanced Encrypted Non-Certified Digital Signature with the Use of Security Token with Biometric Data

Tanzilya A. Burganova, Dilyara R. Fakhreeva, and Nail N. Fakhreev

***Abstract* — The purpose of this study is to develop a method for two-factor authentication of electronic documents using an enhanced encrypted non-certified digital signature with the use of a security token with biometric data (fingerprint image). In order to achieve the goal, the method of comparative analysis was used. Existing algorithms for the electronic signature operation were studied. The method of multi-factor authentication of an electronic signature using biometric data has been studied in detail. Biometric data included: a handwritten password, an autograph, typing biometrics when typing a pass phrase, a facial image, typing biometrics when typing a free text. An external storage medium with a biometric authentication method based on a fingerprint image was also studied. Information on this media was accessed by scanning a fingerprint image. After conducting a comparative analysis and studying in detail these methods, a method for two-factor authentication of an electronic signature using a security token with biometric data was developed.**

***Keywords* — two-factor authentication, digital signature, security token, fingerprint image, algorithm.**

I. Introduction

According to the Resolution of the Government of the Russian Federation of 28 July 2017 No. 1632-p "Digital Economy of the Russian Federation", the state is transitioning to a digital economy. As a result, hard-copy document workflow in various fields (government services, banking services, etc.) is transferred into electronic document management. In this regard, there is a need to protect electronic documents from unwarranted access. Protection of electronic documents today is carried out using an electronic signature. Using an electronic signature is an effective way to protect documents from falsification. However, passwords that are used to authenticate users of an electronic signature may be stored improperly, may be lost, stolen, and the owners of the electronic signature may transfer it to third parties (for the purpose of signing documents). Such misuse of an electronic signature can lead to unwarranted access to information and falsification of documents. Thus, there is a problem of using the electronic signature by third parties. One of the solutions to this problem can be the use of electronic signatures with biometric activation. The authors suggest using fingerprint image as biometric data to activate the electronic signature. This type of biometric data was chosen because it corresponds to the largest number of biometric modalities. Biometric modality is a characteristic of biometric data. The more biometric modalities correspond to biometric data, the more effective they are in authenticating access subjects. Fingerprint images correspond to the following biometric modalities:

– universality – every person has a fingerprint image (with the exception of those who have damaged or missing fingers);

– uniqueness – fingerprint images are unique, there are no two identical people with the same fingerprint images. For example, twins will have the same DNA profile but different fingerprints [1];

– constancy – fingerprint images remain stable and unchanged throughout a person's life;

– measurability – fingerprint images using dactyloscopic formula and whorl patterns can be easily collected and digitized within the system;

– efficient operation – the false acceptance rate (FAR) for fingerprint images is 0.001%, and the false rejection rate (FRR) is 0.6% [2], which allows achieving a low percentage of access error.

An example of biometric data is a handwritten password. So, in the work of B.N. Epifantsev et al [3], the scientific interest of researchers was focused on the recognition of subjects by the features of the reproduction of handwritten passwords – autographs. The error probabilities in this case reach 0.01% if there are 150 templates in the database. However, the handwritten password is dynamic (human-changeable) biometric data. The functional state of a person can affect the change in such biometric data. These include physical condition (state of health, physical activity, etc.); psychological state (psychological health, alcohol and drug intoxication, etc.). Therefore, the use of static biometric data (not changing during life) in the authentication of access subjects, such as fingerprints, is more efficient.

Paper received February 02, 2023; revised September 25, 2023; accepted December 22, 2023. Date of publication December 29, 2023. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Milo Tomašević.

Tanzilya A. Burganova, Kazan State Power Engineering University (tburganova@yandex.ru).

Corresponding author Dilyara R. Fakhreeva, Kazan (Volga region) Federal University (E-mail: fakhreeva.kfu@bk.ru).

Nail N. Fakhreev, Kazan State Power Engineering University (fakhreev.kspeu@ro.ru).

I.V. Kalutskiy and co-authors [4] carried out research in the field of dynamic biometric data. Facial geometry was studied as dynamic biometric data. The false acceptance rate for facial geometry was 0.0017%, and the false rejection rate was 0.3%. The disadvantage of using face geometry for access subjects authentication can be the following obstacles to recognition: room lighting, change in makeup, beard change, use of accessories (glasses, jewelry), etc.

P.S. Lozhnikov carried out more in-depth studies of biometric modalities for effective authentication of access subjects. In his works multi-factor authentication and electronic signature generation was developed using the following biometric data: handwritten password, autograph, image of a keyboard rhythm when typing a pass phrase, facial image, image of a keyboard rhythm when typing free text. However, their combined use has certain disadvantages, which are that:

1. There are increasing requirements for the equipment which is used for authentication and generation of an electronic signature.
2. The time of authentication and generation of an electronic signature increases.
3. A large amount of storage is required to store a database with biometric data on the servers of organizations.

However, none of these authors investigated the two-factor protection of electronic documents using an electronic signature and a fingerprint image. In this regard, the authors of this article are developing an algorithm for two-factor authentication of electronic documents using an enhanced encrypted non-certified digital signature with the use of a security token with biometric data (fingerprint image).

A token was proposed for two-factor authentication of an electronic signature user. A token is a device that is equipped with a secure memory card that stores data pertaining to an electronic signature. Tokens are issued in the form of USB tokens, individual modules, smart cards, and SIM cards. In this work, a token in the form of a USB drive was considered. The uniqueness of this token is that it facilitates the technology of biometric identification of a person by means of fingerprints when accessing an electronic signature. Primary authentication is carried out by scanning a fingerprint image using a sensor embedded within the electronic signature token. Next, the system identifies the user and provides access to the electronic signature. Secondary authentication is performed using a password. Upon entering a password, an electronic signature will be created, and electronic documents will be signed with it. It is impracticable to contrast an electronic signature that has been created by utilizing an encryption certificate and a privacy key, which is secured by a PIN code, with the two-factor authentication of an electronic signature proposed by the authors, which involves a token and biometric data because two-factor authentication of an electronic signature using a token with biometric data is an improvement on the electronic signature using an encryption certificate. Before an electronic signature is signed, the user is biometrically identified using a fingerprint and then authenticated using a password. To perform a falsification, an attacker will need to falsify a fingerprint and to have available a password. Using two-factor authentication of an electronic signature a user reduces the risk of document falsification. This is the scientific novelty of this work.

II. Materials and Methods

The purpose of this study is to develop an algorithm for two-factor authentication of electronic documents using an enhanced encrypted non-certified digital signature with the use of a security token with biometric data (fingerprint image). In order to achieve the goal, it is necessary to solve the following tasks:

1. Study of existing algorithms for the operation of an electronic signature.
2. Study of existing external storage media with user authentication based on biometric data.

For solving problems and achieving the goal, the method of comparative analysis was used. Within this method, an analysis of existing algorithms for the operation of an electronic signature and an analysis of existing external storage media with user authentication based on biometric data was carried out. The search for existing algorithms for the operation of electronic signature and authentication based on biometric data was carried out in the databases of the Federal Institute of Industrial Property of the Russian Federation and in the Eurasian Union Patents Database.

III. Results

The authors of this article carried out a comparative analysis and proposed a new scheme for using an electronic signature with the use of a token and user authentication using biometric data.

The prerequisites for creating a new authentication scheme for the user of an electronic signature were the works of D.M. Brechka [5] and D.A. Gulyaev [6], which, if necessary, require a cryptokey device (token).

Specifications of using an electronic signature with a cryptokey device are presented in the form of a flow chart in Fig. 1.

According to the algorithm in Fig. 1, a private key is used for creating an electronic signature, and a public key and a certificate are used to verify it. Private and public keys are generated at the same time, upon receipt of a signature in a specialized certification authority. Only the owner knows the private key; it is stored on a special token. The security of this method lies in restricting access to the token by unauthorized persons, since this particular method is used for encrypting the signature of the electronic document [6]. All this assumes that it is necessary to protect the electronic signature from unauthorized entry with user authentication.

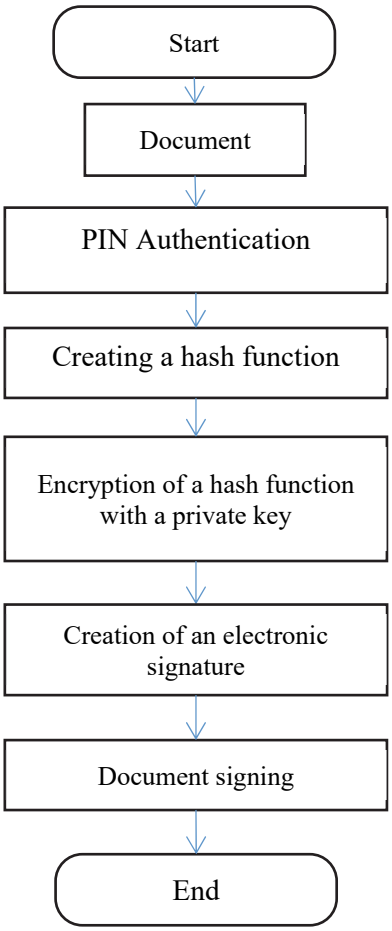

Fig. 1. Usage of an electronic signature with a cryptokey device.

In order to solve this problem, user authentication schemes using biometric data, the so-called biometric authentication, are used [7].

P.S. Lozhnikov in his work uses the proven Viola-Jones method for detection of faces and features of the face [8]. According to this analog, biometric authentication uses from one to several biometric images, each of them is converted into a vector of attribute values, after which the vectors are combined into a single attribute vector (by the concatenation principle). The vector is fed into the neural network, where it is converted into a unique cryptographic key code. A bit sequence is being generated. This sequence can be a password or a private key of an electronic signature. This mechanism of authentication of the user of the electronic key is presented in the flow chart in Fig. 2.

This method of generating an electronic signature key describes a method and algorithm for multi-factor authentication and generation of an electronic signature key based on biometric data of handwritten images, keyboard rhythm and a face.

Implementing this method of protecting an electronic signature [7] allows to achieve the following results: FRR = 3% with FAR < 1%. But there is a drawback that the periodic training of the recognition system ranges from two weeks to several months.

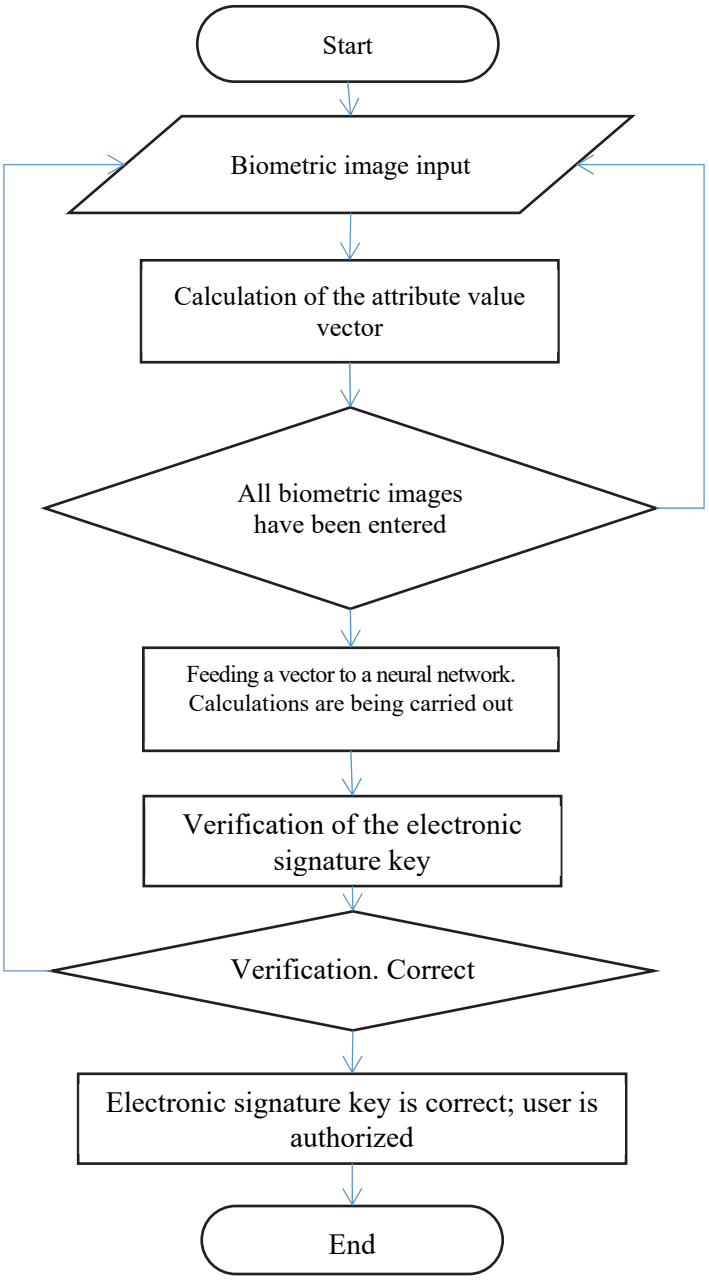

Fig. 2. Scheme of the algorithm for generating the private key of the electronic signature.

In order to solve the problem of trusting an electronic signature (determination of the ownership of a public key by a specific user) is biometric authentication. Thus, the author has carried out a literary and patent review of existing methods for biometric user authentication and presents the following solution to this problem.

Poo Teng Ping and Lim Lai Chuan developed a portable storage device with biometric authentication capabilities. The flowgraph of user authentication according to the authors' device (Poo Teng Ping & Lim Lai Chuan, 2004) given in Fig. 3 works as follows. At the stage of reading, the sensor built into the device reads the image of the user's fingerprint placed on it. Next, the device generates codegrams. The user is notified when a reread is required. The preferred number of retries is user-configurable. According to this preferred implementation, a step also includes generating a codegram based on the read

fingerprint image and storing the resulting codegram in a volatile memory. In the next step, the stored codegrams are read from the flash-memory to be used as a basis for user identity authentication whose fingerprint was read in the previous step. According to this preferred implementation, the microprocessor orders the flash controller to extract the registered codegrams from the flash-memory.

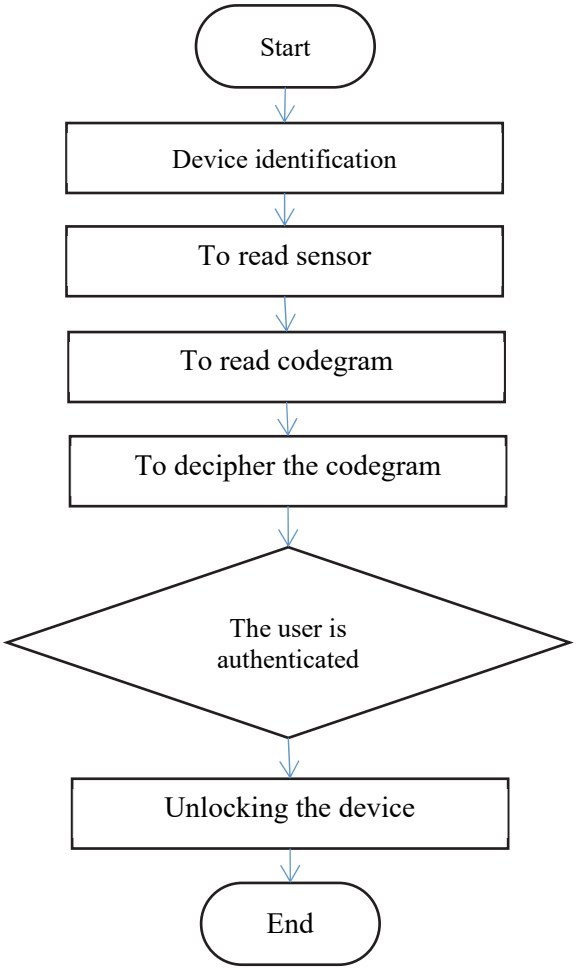

Fig. 3. The logical flowchart of the user authentication process carried out on a portable [9].

Having studied these methods of user authentication, the authors come to the conclusion that the false acceptance rate (FAR) for fingerprint images is 0.001%, and the false rejection rate (FRR) is 0.6% [9], which leads to the idea of combining these methods of signing and authenticating electronic signature users using a token.

Having investigated the known methods of user authentication, the authors suggest the following scheme for signing a document with two-step user authentication, presented in the form of a flowchart in Fig. 4.

IV. Discussion

The developed algorithm was created based on a comparative analysis of alternative technologies. The comparison criteria were taken to be the false acceptance rate and the false rejection rate, and the memory space required to be allocated on the servers of the organization/enterprise for storing biometric data was also taken as an important criterion for comparative analysis.

The results of the comparative analysis are presented in Table 1.

As we see, the false rejection rate is much less than fingerprint authentication. In the column “The memory space used in biometric databases”, the advantage is behind the handwritten password, but at the same time, false rejection rate clearly demonstrates high figures.

This algorithm should be experimentally tested using a two-factor token with biometric data in the electronic document management of organizations and enterprises because at this stage, it is impossible to assess the reliability of the developed algorithm and find out its shortcomings. The alleged drawbacks of this algorithm include the expense of a token equipped with a fingerprint identification sensor. The expense associated with an electronic signature utilizing a token equipped with a fingerprint sensor will be greater than that of an electronic signature generated using an encryption certificate and a privacy key. Furthermore, there are risks of fingerprint falsification.

V. Conclusion

As a result of research, an algorithm for two-factor authentication of electronic documents was developed using an enhanced encrypted non-certified digital signature with the use of a token with biometric data. A fingerprint image was used as biometric data. This algorithm was developed based on a comparative analysis of existing algorithms for the operation of an electronic signature, an algorithm for multi-factor authentication of an electronic signature using biometric data, and an algorithm for operating external storage medium with user authentication based on biometric data.

Based on the developed algorithm for two-factor authentication of electronic documents, a token with biometric data can be created. A token with biometric data for two-factor authentication of electronic documents can be used in the internal workflow of organizations. Using this token, electronic documents will be protected from falsification and unwarranted access.

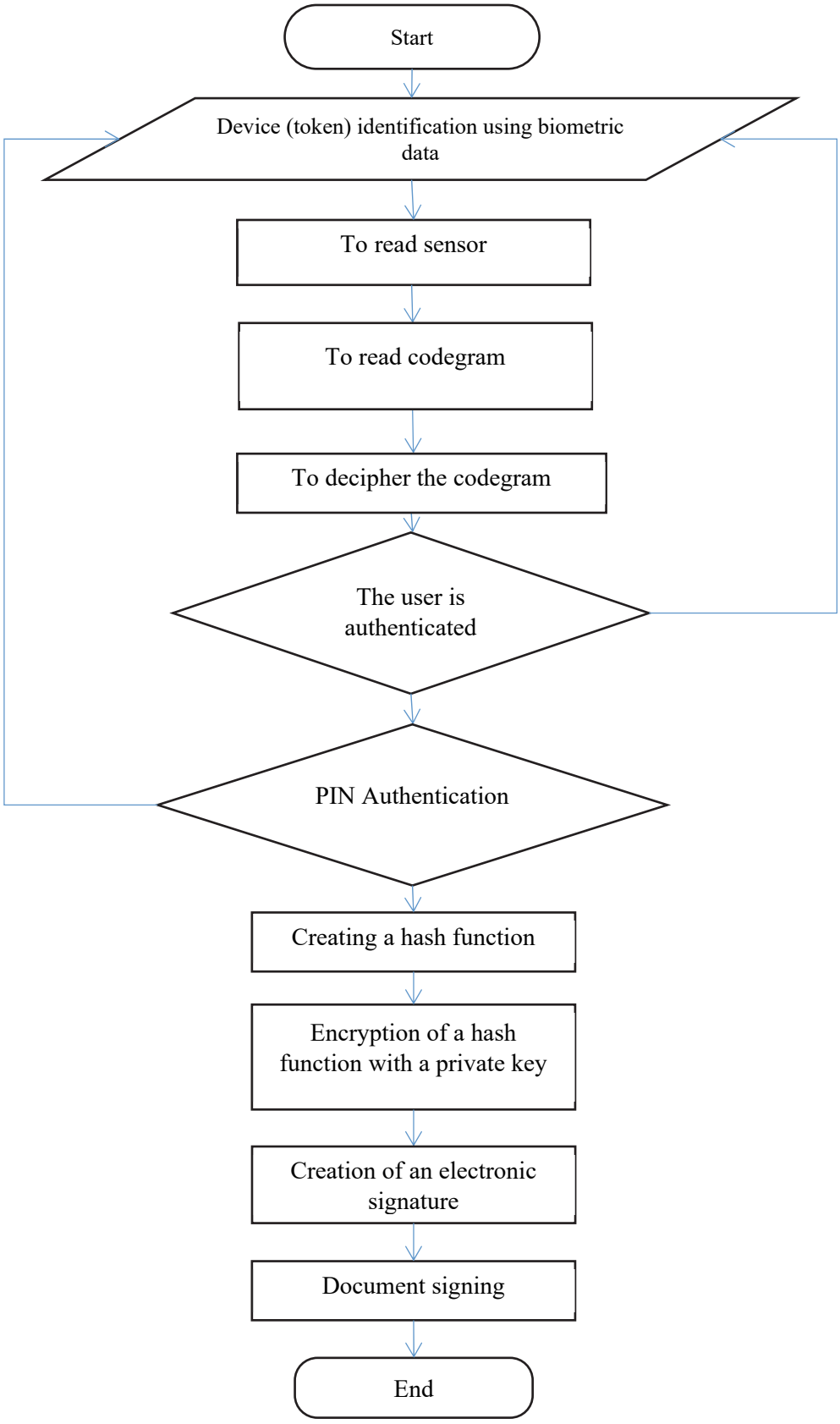

Fig. 4. The flowchart of two-factor authentication of electronic documents using an enhanced encrypted non-certified digital signature with the use of a token with biometric data.

TABLE 1. COMPARATIVE ANALYSIS OF BIOMETRIC AUTHENTICATION TECHNOLOGIES.

Authentication technologies	**FAR,%**	**FRR,%**	**Memory space, Kbyte**
Handwritten password	0,001	3	1.02 [10]
Facial image	0.1	2.5	300
Fingerprint image	0.001	0.6	70 [11]

REFERENCES

[1] A Summary of the United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism. Available: https://www.unodc.org/pdf/terrorism/Compendium-Biometrics/_.pdf

[2] A.A. Mahkamov, Kh.U. Inadullayev, Comparative analysis of biometric systems in providing information security. *Universum*, 2021, 12(93).

[3] B.N. Epifantsev, P.S. Lozhnikov, A.E. Sulavko, S.S. Zhumazhanova. Identification potential of handwritten passwords in the process of their reproduction. *Autometry*, 2016, 52(3), pp. 28-36.

[4] I.V. Kalutskiy, Yu.S. Matiushin, S.V. Spevakova, Analysis of Modern Static Methods of Biometric Identification. *Proceedings of the Southwest State University*, 2019, 23(1), pp. 84-94. https://doi.org/10.21869/2223-1560-2019-23-1-84-94

[5] D.M. Brechka, Introducing electronic signatures in higher education institutions. *Modern Science: Current Problems of Theory and Practice. Series: Natural and Technical Sciences*, 2020, 8, pp. 47-54.

[6] D.A. Gulyaev, (Ed.). The principle of operation of an electronic digital signature and its application in practice: Modern information technologies and information security. Kursk, Russian Federation: Southwestern State University, 2022.

[7] P.S. Lozhnikov, A.E. Sulavko, E.V. Buraya, V.Yu. Pisarenko. Authentication of computer users in real-time by generating bit sequences based on keyboard handwriting and face features. *Cybersecurity Issues*, 2017, 3(21), pp. 24-34.

[8] P. Viola, & M. Jones, (Eds.). Rapid Object Detection using a Boosted Cascade of Simple Features. *IEEE Conf Comput Vis Pattern Recognit*. 2001, 1. I-511. 10.1109/CVPR.2001.990517.

[9] Poo Teng Ping & Lim Lai Chuan (February 26, 2004) *Device and Method for Authentication based on Biometric Data.* SG Patent No. 4262.

[10] A.E. Sulavko, Highly reliable authentication based on handwritten passwords using hybrid neural networks with protection of biometric templates from being compromised. *Information and Control Systems*, 2020, 4, pp. 61-77. https://doi.org/10.31799/1684-8853-2020-4-61-77.

[11] M.M. Kokkoz, E.N. Toishybek. Integration of a fingerprint into smart cards. *Young Scientist*, 2016, 4(108), pp. 155-158.