Saule NYSANBAYEVA[1] , Waldemar WÓJCIK[2], Olga USSATOVA[3]

Institute of Information and Computational Technologies (1), Lublin Technical University (2), Al-Farabi Kazakh National University (3)

doi:10.15199/48.2019.05.25

Algorithm for generating temporary password based on the two- factor authentication model

Abstract*. the article describes methods for applying authentication based on the second factor for the use in an automated system. For automated control system, the model's two-factor authentication and consistent algorithm were developed to generate a temporary password by using mathematical functions. Implemented was the software implementation in the JavaScript programming language in console mode. The analysis of the software implementation of the proposed algorithm was performed.*

Streszczenie. *W artykule przedsawiono opracowane dwuskładnikowe uwierzytelnianie i spójny algorytm do użytku w zautomatyzowanym systemie w celu wygenerowania tymczasowego hasła za pomocą funkcji matematycznych. Wdrożono implementację oprogramowania w języku programowania JavaScript w trybie konsoli oraz przeprowadzono analizę implementacji. (****Algorytm generowania hasła tymczasowego w oparciu o dwuskładnikowy model uwierzytelniania****).*

Keywords: two-factor authentication, data security, temporary password generation, confidentiality
Słowa kluczowe: uwierzytelnianie dwuskładnikowe, ochrona danych, tymczasowa generowacja hasła, poufność

Introduction

Currently while ensuring information security in an automated priority management system is ensuring the availability, integrity of configuration management information and information about personal data. Increased attention has been paid to the prevention of unauthorized access to the system to maintain its stable functioning [1]. However, due to the constantly increasing number of different services and various attacks on user accounts, there is a need to use two-factor authentication methods to ensure information security. In the past decade, these methods have been widely used in various areas of information and communication technologies. They are related to issues of identification and access of a subject to confidential information [2, 3]. They are trusted by a large number of companies, including high-tech organizations, financial and insurance sectors of the market, large banking institutions and public sector enterprises, independent expert organizations, as well as research firms [1].

Two-factor authentication – a security processing algorithm, in which the user provides two different factor authentication, which will improve the protection of user's data and access to user credentials, and the user's resources. Traditional systems use a username and password for authentication. This method provides a minimum level of security, since the names and passwords can be easily intercepted and even guessed. Two-factor authentication provides a higher degree of protection than single-factor authentication, in which the user offers only one factor, usually a password.

Authentication methods with two factors depend on the password and the second factor. Two-factor authentication is used to control access to sensitive systems and data. Development and use of two-factor authentication algorithm for the automated control systems.

Goals and objectives of the study

The purpose of the article is to develop a two-factor authentication model to protect information in automated system.

To achieve this goal, the following task were set and solved:

- analysis of some used two-factor authentication methods;
- development of a two – factor authentication model based on the application — the authenticator a using a mobile application;
- algorithm development generating a temporary password for two-factor authentication and its software implementation.

Research results

According to the law Republic of Kazakhstan "On personal data and their protection" [4], the three main properties ensure actions for the storage of personal data - its confidentiality, accessibility and integrity. Password authentication is one of the first barriers that appeared in info communication systems simultaneously with operating systems that implement multiple access to information resources. The main advantage of this method of protection – its simplicity, allowing sufficient use of password authentication in many organizations and Shade safe use information. According to the company TAdviser risk of information is password theft: 76% of network attacks are possible due to unreliable or stolen passwords, 61% of users use the same password to log into an account, 44% of users change their password once a year [5].

According to the company PositiveTechnologies in the II quarter of 2018 most criminals attracted Information about the personal DATA (30%) or the accounts and Password information for access to various services and systems (22%), including an online – Personal Banking, in 15% of cases payment card data was stolen and in 5% - and from customer databases [6]. According to the company PositiveTechnologies we can highlight common vulnerabilities: the use of outdated software versions and the lack of up-to-date security updates for operating systems; multiple configuration errors (including excessive user and software privileges, as well as setting local administrator passwords through group policies); the use of dictionary passwords by privileged users; lack of two-factor authentication for access to critical systems. The collection of practical security studies for 2018 shows that the use of two-factor authentication in online - banks and web - Applications built on ready-made solutions, was 29%, and in 2017 in 2016 - 75% [7]. These DATA confirm the need for reliable user authentication based on two-factor authentication for increased security.

Two-factor authentication (2FA) is a method for identifying a user in a service using a request for authentication data of two different types, which provides a more effective two-layer account protection from unauthorized access, in which the user needs to present more than one to gain access to information factor.

Authentication methods with two factors depend on the password and the second factor. Two-factor authentication adds an extra level of security to the authentication process and this makes it difficult for intruders to access accounts. The basis of two-factor authentication is the use of not only the traditional login-password combination, but also an additional level of protection, the so-called second factor, the possession of which needs to be confirmed in order to gain access to an account or other data.

Two-factor authentication is used to access databases of automated control systems, social network accounts, mail, and other services. The classification of two-factor authentication methods is presented in Figure 1.

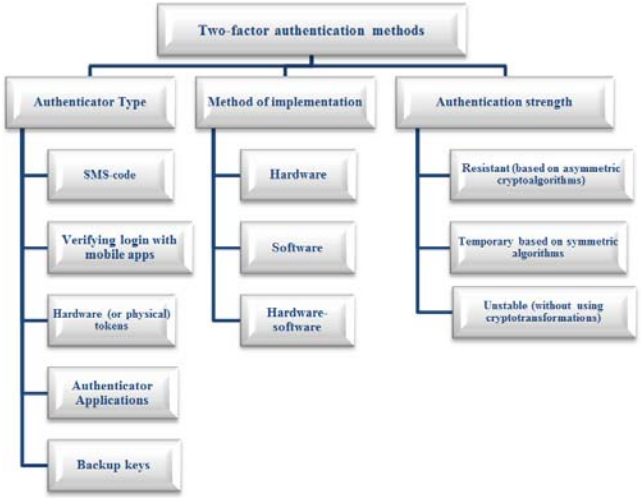

Fig.1. Two-factor authentication methods

Consider some types of two-factor authentication [8-10].

1. SMS code. You enter your username and password, and then you receive SMS with a verification code on your phone that you need to enter to log in to your account. At the next login, another SMS code is sent. The advantages of this type are the generation of a new password at each entrance and binding to the user's phone number. The disadvantages are the lack of a cellular network signal, wherein the input impossibility. There's vulnerability: the substitution of numbers by a service operator or employees of the salons of connection. If authorization E occurs via a mobile device (e.g., Smartphone) and receiving the code takes place through the same apparatus, it ceases to be a two-factor protection.

2. Verify login using mobile apps. In this case, instead of requesting codes or one-time passwords, the input is confirmed from a mobile device with the service application installed. A private key is stored on the device, which is verified at every entrance.

Advantages: there is no need to additionally enter the confirming password at the entrance; no cellular communication or SMS service is required, and in some cases the Internet; multi account support. Disadvantages: when intercepting a private key, a fake identifier is possible; using one of the first and the same device and from which the input, lost two-factor protection.

3. Hardware (or physical) tokens. They are the most reliable way of two-factor authentication and can be represented as USB sticks with their own processor that generates cryptographic keys, which are automatically entered when connected to computer the choice of key depends on the specific service. Benefits about: completely independent device without the need to use a mobile phone. Disadvantages: device purchased separately; not all services have support for this method; multiple accounts require multiple tokens; the loss of the token entails the hacking of the system by the attacker.

4. Applications - authenticators. Generated on the device using a special application. During configuration, the user receives a primary key, on the basis of which one-time passwords are generated using cryptographic algorithms with a validity period of 30 to 60 seconds.

Benefits: only need the Internet to open the beginning of the session multi account support. Disadvantages: possible breaking of the primary key, then the attacker is able to generate all subsequent passwords; two-factor is lost when used on the same device from which the input is made.

Backup keys. This is not a separate method, but a backup option in case of loss or theft of a smartphone that receives one-time passwords or verification codes. When you configure two-factor authentication in each service is given several backup keys for use in emergency situations. With their help, you can log into your account, disable configured devices and add new ones. The analysis of modern systems show that the use of two-factor authentication allows to ensure the availability, integrity, configuration management information and information about the personal data in an automated system [11, 12].

Model of the two-factor authentication for automated systems

When developing an information security system, two-factor authentication model is proposed (Figure 2).

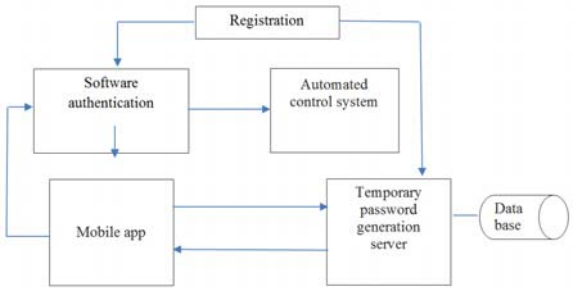

Fig.2. Mode of the proposed two-factor authentication

The developed model is based on two types of two-factor authentication: applications – authenticator and login verification using mobile applications.

Consider an example of a use. The proposed method of protecting information in an automated control system using a combination of two factors: a permanent and temporary password [13]. The user chooses a permanent password (the first factor) himself and uses it when registering an account (account).

Before automation, you must register in the application. There after you must run the application to enter user data (login and password) should correspond to registered data. Upon successful data entry, you must enter the application on your mobile device and enter the initial data to generate a temporary password. A temporary or one-time password (the second factor) is generated on the server using a specific algorithm and is valid for a specific length of time for one session authentication. The advantage of disposable the password is that the password cannot be reused. Thus, an attacker who intercepted data from a successful authentication session can not use the copied password to gain access to the protected system.

The generation of a temporary password is possible in two modes: online and offline. To obtain a temporary password using additional software. Online is the software sends a request to the authorization server to generate a temporary password.

A temporary password is generated on the server and displayed to the user in additional software. This temporary password may have a short duration, for example, up to 1 minute. In offline mode, a temporary password is also generated in the additional software. This temporary password will have a longer duration due to its autonomy, but not more than 15 minutes (optimal time - from 3 to 5 minutes).

A temporary password is generated based on the result of a selected specific mathematical function, which will have a number of variable parameters. Mathematical functions will be combined into a table, the dimension of which should be a multiple of degree two.

The choice of the mathematical function and its initial parameters is based on the result of the hash function of the SHA256 or SHA512 standards [14, 15]. SHA 2 - is a cryptographic hash function, which has been developed an agency national security [16,17]. Purpose hash function – converting e (hash or e) an arbitrary set of data elements in a fixed-length value. This value will characterize the set of source data, without the possibility of extracting these source data.

As the input string to the hash function, and uses a combination of user credentials, the current time and GMT additional secret string. The result of the hash function is divided into individual numbers, which will be the indices for selecting a mathematical function and initial data.

The secret string is a required field, which the user enters to select a mathematical function. The secret line will be changed at each entry, which will allow installing additional system protection.

The algorithm for generating a temporary password

According to the proposed model, a temporary password generation algorithm was developed for two – factor authentication (Figure 3). This algorithm is implemented in JavaScript in console mode using the Crypto JS. SHA256 library for I data encryption.

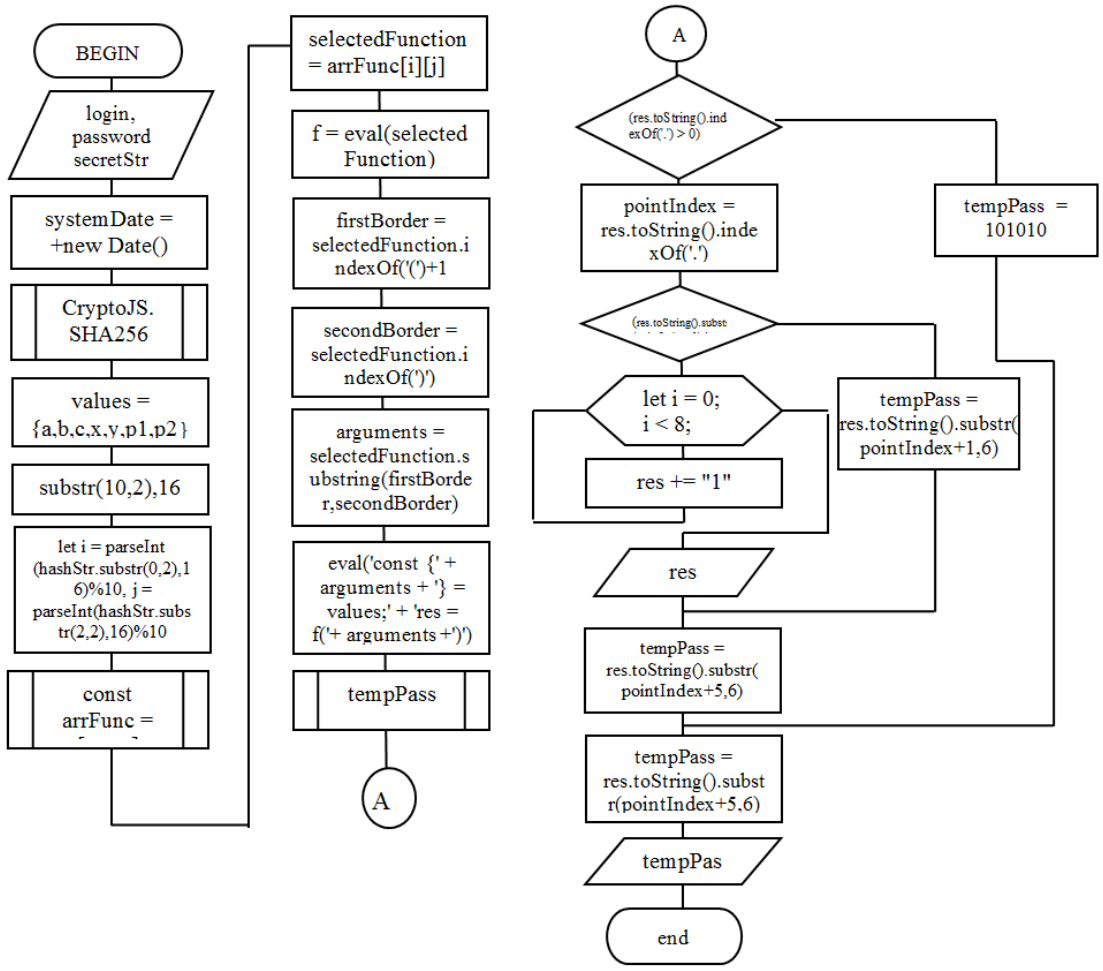

Fig.3. Temporary password generation algorithm

Step 1 - Data entry. The initial data for the input string will be the following values:

- login: olga;
- password: ussatovaolga;
- secret string: nikdar.

Step 2 - Reading the system date and time (1 December 9, 2018 12:21:18). The current time is read from the system automatically and depends on the setting of the operating system.

Step 3- Using the CryptoJS.SHA256 libraries for data encryption. Split input string into words. Calculate hash - values.

The input string will look like:

olgaussatovaolga20181219122118nikdar

The result is as follows:

8CD63646C6EE48DD3C542121A146144547E1B6D7DFA0423CE753B8C695CC7D58

Step 4 - Formation of variables based on hashStr. Assignment of variables for calculating mathematical functions.

As an initial parameter selected two hexadecimal numbers end with the result of the hash function, and as the

values «X and Y» hexadecimal numbers with positions 10-11 are taken. Then they will take the following values:

1. a:"58"
2. b:"7D"
3. c:"CC"
4. p1:"95"
5. p2:"C6"
6. x:"6E"
7. y:"E4"

Step 5 – Variable translation in decimal number system:

1. a:88
2. b:125
3. c:204
4. p1:149
5. p2:198
6. x:110
7. y:228

Step 6 -The definition of the index function (mod 10, because the size of the array a (10x10)).

Step 7- fill 10x10 array, consisting of lowercase his mathematical functions.

Step 8 - Selecting a function from an array at a specific index. In this example, the table was taken by a 10 x 10 size in this connection will be the following function:

$$P1 * \cos(y)^2 - \sin(2C) - \cos(P2)^3. \quad (1)$$

Step 9 – Broadcast at f - string function in the form of program code.

Step 10,11 - Definition of boundaries change function arguments.

Step 12 – Receive ix function argument as string.

Step 13- Occurs transformation «values» of the object from the given, then the output of the function with the given variables are represented as arguments. As a result, you will receive about following function value:

$$149 * \cos(228)^2 - \sin(2 * 204) - \cos(198)^3 = \quad (2)$$
$$= 9.43306576524.$$

Step 14 - Declaring a temporary password.

Step 15 – Checking the integrity of the result and the desired number of digits after the decimal point.

Step 16 – Numbers determines the temporary password after the comma.

Step 17 –Checking the password length - after the comma at least 8 characters.

Step 18 - Cyclic brute force.

Step19 - If the password has less than 7 digits after the decimal point, then the password is added to the password in a sequence of numbers.

Step 20 - Displaying the result.

Step 21 - Starting from the 1st position - 6 digits length.

Step 22 - Starting from the 5th position – the length is 6 digits.

Step 23 - Check the result to be 6 digits.

Step 24 – The temporary password is determined by numbers after the comma, starting from the 5th position, the length is 6 digits. Then the temporary password takes the value 657652.

Step 25 - Display a temporary password.

Application of two-factor authentication allows avoiding unauthorized cracking of a system, reducing the risk of leakage of personal data and other important information in an automated system. The advantages of two-factor authentication can also be attributed the ability to protect information from internal and external intrusions [18].

The described algorithm is implemented in JavaScript in console mode. This application will allow you to visually display the generation of a temporary password using the algorithm described above. The implementation of the algorithm is shown in Figure 4.

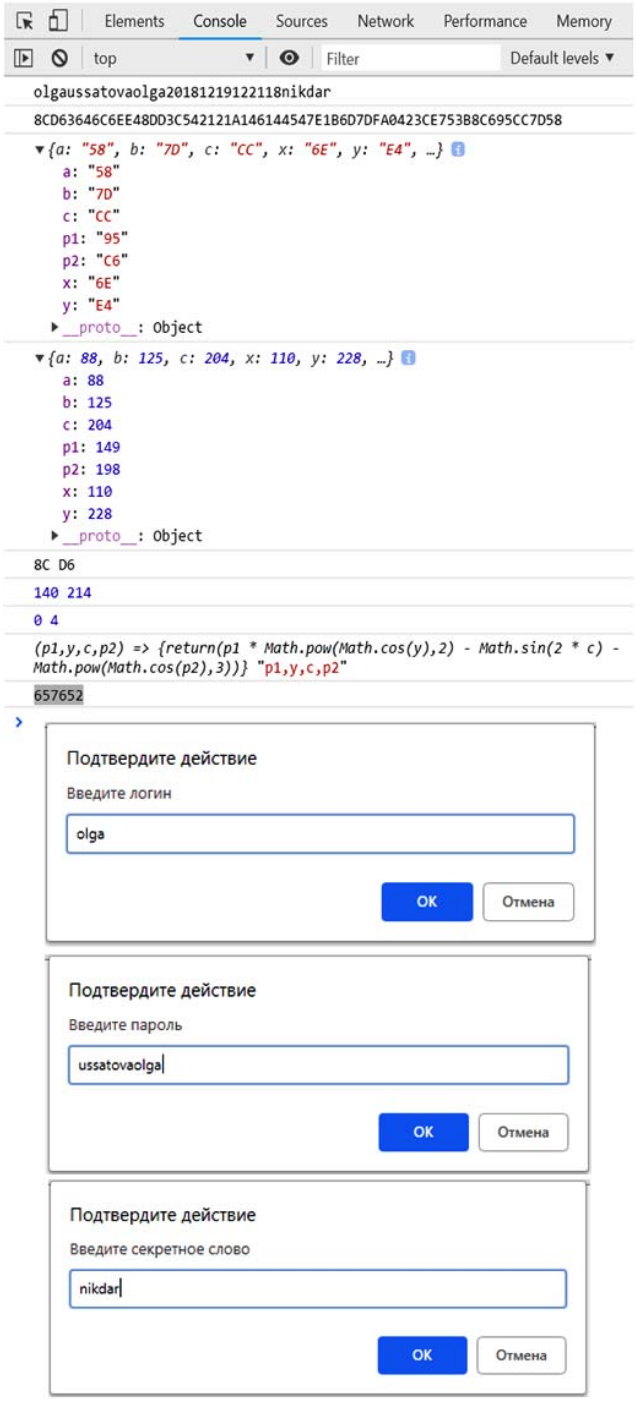

Fig.4. The implementation of the described algorithm in the JavaScript language

Consider the effect of generating a temporary password on the software implementation of information security tools based on two-factor authentication. For assessment of the sgenirovanny temporary password, different input data that show efficiency of realization of an algorithm were taken. Table1 shows the results of the study of the generation of a temporary password according to the algorithm described above.

Table 1. The results of the study of the generation of a temporary password according to the algorithm

No.	Input data	Mathematical function	Hash - value	Password generated
1	olga ussatovaolga 20181219135432 nikdar	(p1 * Math.pow (Math.cos(y),2) - Math.sin(2 * c) - Math.pow(Math.cos(p2),3))	63BB50493F3379876B5D7F3A B1A965DA197EB1B5AAB95561 422E230773427D5F	747284
2	user1 password1 20181219135913 secret	((Math.cos(y) * (x * Math.sin(c))) /Math.tan(Math.sqrt(b)))	FD9DD2954C1C325CD0AA684 D1D2C6B2CA644873535AB207 A2B385DAF3A914255	233776
3	user2 pa345ssword 201812191410 topsecret	((y * Math.pow (Math. cos(x),2) - Math.sin(2 * c) - Math.pow(Math.sin(p1),2))/y*p1)	E85B7AFF855021099FDFB0C2 24D297D290A9F7484CBB8B9D A77CE74DA40E4524	041825
4	new passnew 2018121914315 confidentially	((c * Math.pow (Math.sin(x),3) + 3 * Math.pow (Math.cos(x),2))/p2)	F2DC97A5FB776DBC807F18D 84151763C9C25B67DFC56818 95D12C289276D1414	766192
5	newpassnew2018 121914825confide ntially	(Math.sqrt(Math.pow((Math.pow(Math.si n(b),2)),3))/Math.sin(a))	EF44F3AB2D854E18DDB26905 25E75316CD72092533EA766D 86CB36570CF63FA8	005739

The results of the analysis and show that the generated temporary password will not be repeated and changed even when entering repetitive data. This is due to the fact that in about input considering not only a username and password, but the system date and the secret string. The proposed method allows the use two-factor authentication to ensure information security in an automated system.

Conclusion

Two-factor authentication methods are considered as mechanisms for enhancing the strength of authenticators. The proposed approach allows to eliminate the existing disadvantage of the authentication based on the mobile application and the generated temporary password. Studies show, that the use of two-factor authentication allows for enhanced protection in the information. The software implementation of the temporary password generation shows that this password is generated correctly and corresponds to the algorithm described above.

Authors: *PhD Saule Nysanbayeva, Institute Information and Computational Technologies CS MES RK, Almaty, Kazakhstan, e-mail: info@ipic.kz; Prof. Waldemar Wójcik, Lublin University of Technology, Institute of Electronics and Information Technology, Nadbystrzycka 38A, 20-618 Lublin, Poland, e-mail: waldemar.wojcik@pollub.pl; M.Sc. Olga Ussatova, Al-Farabi Kazakh National University, Almaty, Kazakhstan, e-mail: uoa_olga@mail.ru.*

REFERENCES

[1] Davydov A.E., Protection and security of departmental integrated information and communication systems, *OJSC Voentelecom*., (2015), 519

[2] Stobert E., Biddle R., Authentication in the Home, *Workshop on Home Usable Privacy and Security (HUPS)*, (2013)

[3] Wang, D., Wang, P., Ma, C.G., Chen, Z., iPass: Robust smart card based password authentication scheme against smart card loss problem, *Cryptology ePrint Archive*, 439 (2012)

[4] Law of the Republic of Kazakhstan dated May 21, 2013, On Personal Data and Their Protection, (with amendments and additions as of December 28, 2017), https://online.zakon.kz/Document/? Doc_id = 31396226, (last accessed November 05, 2018), No. 94-V

[5] Multifactorial (two-factor) authentication http://www.tadviser.ru/index.php/ (last accessed July 12, 2018)

[6] Current cyber threats, II quarter of 2018, https://www.ptsecurity. com/ upload/ corporate/ru-ru/analytics/Cybersecurity-threatscape-2018-Q2 - rus.pdf. - 2018. - p 23. (last accessed July 13, 2018).

[7] Collection of researches on practical safety PositiveResearch, https:// www.ptsecurity. com/upload/ corporate/ru-ru/analytics/Positive-Research-2018-rus.pdf - p 206

[8] Yuriev D.R., Rogova O.S., Comparative analysis of two-factor authentication, Technical Sciences, 66 (2017), No. 6, 46-51

[9] Kumari S., Khan M.K., Cryptanalysis and improvement of a robust smartcard-based remote user password authentication scheme, *International Journal of Communication Systems,* (2013)

[10] Huang X., Chen X., Li J., Xiang Y., Xu L., Further observations on smart-cardbased password-authenticated key agreement in distributed systems, *IEEE Trans. Parallel Distrib. Syst*., 25 (2014), No. 7, 1767–1775

[11] Wang D., He D., Wang P., Chu C.H., Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment, *IEEE Trans. Depend. Secur. Comput.*, (2014)

[12] Wang D., Wang P., On the Usability of Two-Factor Authentication, *Proceedings of 10th International Conference on Security and Privacy in Communication Networks (SecureComm 2014)*, (2015), 141–150

[13] Nysanbayeva S., Ussatova O., Two-factor authentication in the automated control system, III International scientific conference Information Science and Applied Mathematics 448 (2018), No. 2, 239-242

[14] National Institute of Standards and Technology (NIST), https://www.nist.gov/ (last accessed September 02, 2018)

[15] FIPS 140-2 standard and self-encryption technology, //https://www.seagate.com/files/ www-content / solutions-content / security-and-encryption / id / docs / faq-fips-sed-lr-mb-605-2-1302-ru.pdf / (last accessed November 12, 2018)

[16] Barr T.H., Invitation to Cryptology,*Upper Saddle River*., (2002), 396

[17] Leńczuk E., Java application as a tool to control intelligent building installations realized in KNX system, *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska – IAPGOŚ*, 2 (2012), No. 1, 21-23

[18] Convenient and secure access to applications //https://identityblitz.ru / products / blitz- identity-provider /? Ref = main (last accessed July 10, 2018)