Yu. V. Baryshev, Cand. Sc. (Eng.); M. M. Chaikin; O. V. Kokhan

METHOD AND MEANS OF THE TEXT PASSWORDS SECURITY IMPROVEMENT, UNDERSTANDABLE FOR THE USERS

Paper contains the results of the analysis of users authentication process characteristic features, which enabled to substantiate the expediency of using the passwords as the authentication factors. The problem of generation of the strong password by the users who may not possess the sufficient competence in the sphere of cyber security has been considered. Known approaches to passwords generation, which can be applied for the solution of this problem, focusing the attention on the methods, allowing to generate the passwords, understandable for the users and hence are simpler for memorizing have been analyzed. The usage of learning samples or dictionaries, chosen, depending on the users that negatively influences the scalability of the methods application was considered as the common drawback. Method of improving the password strength, based on using words, wordforms or word combinations introduced by the users and their further modification was suggested. The proposed modifications are based on of the table of the symbols replacement, the table is suggested to form prior to method application. In particular, in the given research the formation of this table was performed on the base of users enquiry. The method, where the results of the enquiry were taken into account during the symbols replacement was described. For the improvement of the flexibility of the method application the control parameter was provided — probability of the modification of a certain symbol from the row, suggested by the user as a password. Algorithm, enabling to realize the proposed method, is presented. In order to substantiate the possibility of the realization, the developed platform-independent programming tool that realizes the suggested method, was described. The results of the tool testing were presented. On the base of the analysis of the presented results the characteristic features of the method and the impact of the replacements table on the output set of potential passwords, obtained as a result of the application operation were demonstrated. The conclusions were made from the research carried out, further development trends were outlined.

Key words: *password, strength, authentication, user-friendly, table of replacements.*

Introduction

In information systems there appears the need in high level of security to provide confidence, integrity and access to the information which is stored, transferred or processed in these systems. For this purpose the authentication is used. It is a procedure of establishing the fact of conforming the belonging to the user the presented identifier [1]. Objects, on the base of which this fact is conformed, are called factors of authentication [1, 2]. In general case, any accessible only to the user information can be used as the authentication factor, which must characterize him in a unique manner.

In spite, at first glance, of the diversity of users authentication means, the application of the greater part of the authentication factors for separate practical problem is limited by the requirements, regarding the users convenience or practical possibility of their integration into the information systems, already developed and, at the same time, did not take into account the requirements of cyber security at the stage of their design [2 – 4]. That is why, from practical considerations [1, 5] the passwords are most often used as authentication factors. However, the common drawback for the authentication on the base of the passwords is the need to solve the problem of searching the compromise between the strength of the password and complexity of its memorizing [1, 5, 6]. Passwords, generated on the base of random or pseudorandom series [7], allow to provide high level of the strength, but complexity of their memorization causes problems, connected with the necessity to create back-up copies of the passwords and inappropriate conditions of their further storage [8], because the authentication the user has to pass several times during the work day [4, 9]. Correspondingly, such generation method causes a number of problems, connected with the human factor, which can be solved only applying organization measures, which will introduce more impact of the human factor. That is why, the passwords must be understandable for users, and, consequently, convenient for memorizing.

If the usage of the passwords, conveying the semantic charge for the users are considered, then, proceeding from the principle of minimizing the number of persons, familiarized with the confidential information [6], the solution of this problem is laid on the users, who, in greater part of cases, do not have sufficient competence or desire for the solution of the problem [4, 9], but not on the officer or on the corresponding service of the cyber security of the enterprise, for instance – Information security service in the banks [10], who are the specialists in this sphere. Thus, contradiction emerges, on one hand, passwords must have high level of strength, on the other hand – this strength must provide persons, who do not have sufficient level of the competence in the sphere of cybersecurity [3, 4]. For this very reason, the development of the tool, that without the disclosure of the password itself allows the users to increase its strength, keeping the password understandable and, hence – easier for memorizing is a relevant problem.

Aim of the given research is to improve the strength of the passwords, obtained on the base of the words and word combinations from the natural human language.

The following problems are to be solved for achieving this aim:

– analyze the known methods of the users authentication;

– develop the method for improvement the strength of the passwords;

– realize the method in the form of the tool.

Analysis of the approaches to users' authentication

In program applications, operation systems, data bases there appears a necessity in security facilities to provide the confidentiality of the information. For this purpose, access rights differentiation of the users to information resources is performed. Key element for the realization of this differentiation is users authentication [1]. As a result of the execution of the authentication procedure the confirmation of the belonging to the user the presented identifier occurs. For the confirmation any other secret information, accessible only to the user or characterize him in a unique manner can be used. Accordingly, the following types of the users authentication factors are allocated [1, 3, 6]:

– knowledge of something;

– possession of something;

– on the base of the biometric characteristics;

– on the base of the location.

The most popular approach to authentication is the usage of the text passwords as the authentication factors [1, 2, 5, 6], which belongs to the category of the users authentication factors on the base of knowledge of something. Spreading of the passwords usage is stipulated by a number of the pragmatic considerations [1, 9]:

– usage of the passwords does not require financial resources for the additional hardware of the information systems, which is necessary when other groups of factors of users authentication are used, this improves scalability of the information system, where the authentication occurs;

– low complexity of the additional software, that stipulates low cost of the of the development of the corresponding programming modules as compared with the corresponding modules for other types of authentication;

– availability of the best practices for the development of the password authentication modules as this is the most popular and most investigated method of the authentication.

Under such approach, when the $user_i$ with the associated $password_i$ is registered in the system, the password is hashed and stored the obtained hash-meaning on the side which performs the authentication [5, 11] that protects against the improper activity of the administrator. Thus, the information, that is the mapping of the identifiers of the registered users and hashed passwords which correspond to them, must be stored in the information system in the users database (*UserDB)*:

$$UserDB = Map\big(User, hash(Password)\big)$$

As *UserDB* is accessible for the administrators of the information system, there exists the danger of the hashed passwords leakage. Hashing prevents the rapid password cracking, however, if the corresponding resources are available, the intruders can construct the pre-image of the user`s password. Accordingly, for the risks management, there appears the need of periodical changes. As the studies show [9], even those of the users who are aware of the basic notions of the cyber hygiene often neglect the security for their own convenience. Due to the above-mentioned principle of minimization of the number of persons familiar with the confidential information [6], it is rather problematic to perform the control of the new password adequacy.

The approach to the generation of the passwords on the base of partial information about it in order to restore the access of the users to the accounts is known [12]. This approach is based on the AI methods. In spite of the fact, that initially it was not oriented on the generation of new passwords, it can also be used for the achieving the aim of the given research, although with certain drawbacks, connected with the initial designation. Direction, using the approaches of AI seems promising, when learning samples, taking into account the peculiarities and personal experience of the user or certain group of users are used. At the same time, preparation of the learning sample in such a way that the generated passwords were understandable and easy for memorizing will decrease the number of the passwords, which can evoke certain associations in each user.

In the paper [13] the approaches, based on the replacements, exchanges and vocabularies with words, which can evoke certain associations are suggested. Depending on the scheme, passwords, obtained by the users can be both simple for memorizing (for instance, the word “AMAZON” is transformed in the password “amzon”), and complex (for instance, the word “AMAZON” is transformed into the password “NHTFHT”). The suggested schemes [13] may become useful for the specialists of SUIB. However, within the frame of the given research, which is aimed at the users who do not have special training in the field of cybersecurity, such approaches can not be useful. Besides, usage of the stable vocabularies is a weak point of such an approach.

Thus, in spite of the expediency of the passwords usage as the factors of the users authentication their usage is complicated by the lack of the methods of the reliable passwords generation, oriented at the users without special training.

Method of improving the strength of the passwords

Analysis showed, that the method of the password authorization is convenient and widely used in the systems of the authorization of the network user. However, such method provides the availability of certain characteristics of the user’s memorable word, one of such main characteristics is the password strength and its convenience for the usage. Availability of special symbols, letters of different register, figures improves the strength of the passwords and at the same time it becomes more difficult to memorize such key words. On the other hand, usage of simple, predictable words and symbol combinations will have adverse effect on the strength of the password phrase. That is why, the method of passwords generation is suggested that enables to combine these two properties and will give the possibility to the users, on the base of the word, which they would like to use as the password, to obtain variants of more stable passwords.

The suggested method provides the following preliminary preparation, namely the formation of the table of the letters replacement by the symbols. Table 1 contains the fragment of such table, that was used during the practical realization within the frame of the given research.

Table 1

Example of the symbols replacement table

Letter	Symbols for replacement
A	@; 4; (L; /\
B	8; I3; |3;
C	<; (
H	#; /-/;]-[; }{
...	...

When the replacement table was formed, taking into account the peculiarities of the language, natural for the users, the authors suggested to conduct a survey of the users regarding the preferred version of the replacement. In particular, in the given study the questionnaire was formed for the on-line survey, fragment of the questionnaire is shown in Fig. 1.

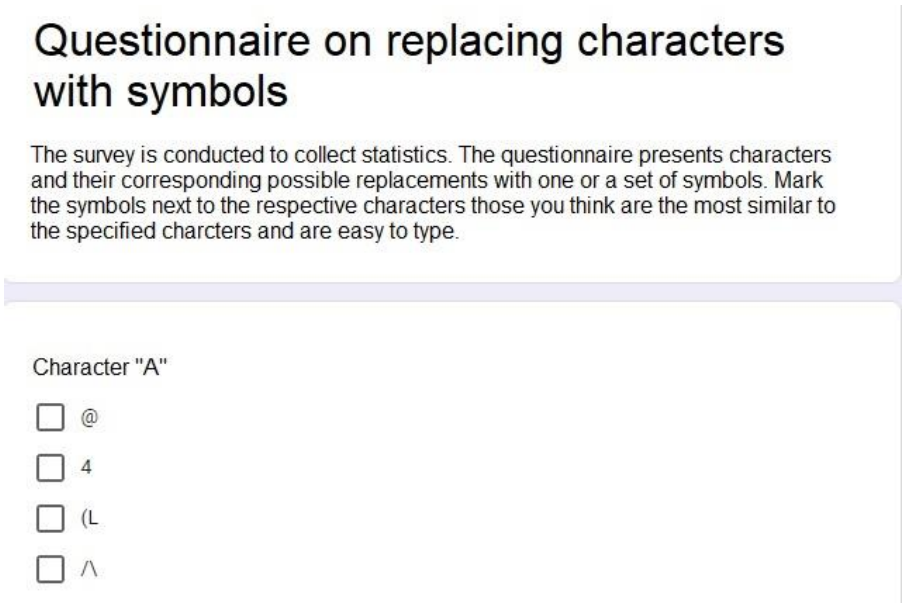

Fig. 1. Fragment of the survey questionnaire

After the survey, the results of the desired replacement for the users are obtained. In particular, Fig. 2 contains the results, obtained by this survey on answering the fragment of the questionnaire, shown in Fig. 1.

As a result of the aggregation of the results of the survey the probability of the replacement of each letter, available in the replacement table is determined, in case, if in the process of the realization of the method, there appears the need in such replacement. Besides, depending on the characteristic features of the information systems, where the authentication is expected, prior to the realization of the method it is necessary to determine the value of symbol *n* replacement probability. It is worth mentioning, that in case, when the value of this probability equals 0, then the suggested method will degenerate into classical approach, when the password is chosen by the user.

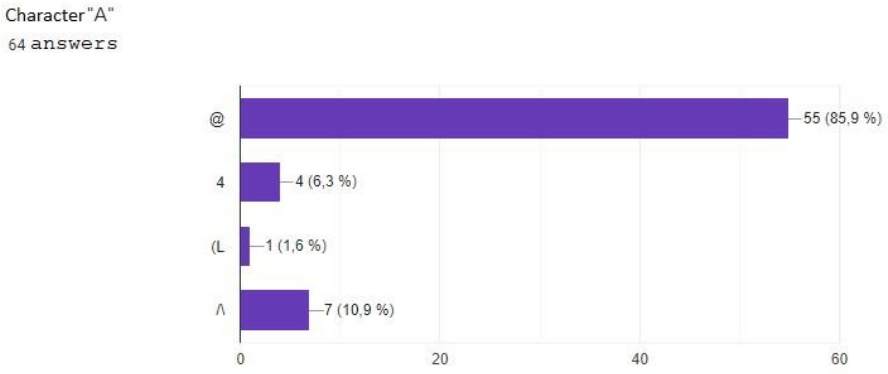

Fig. 2. Results of the conducted survey

After the termination of the preliminary preparation the realization of the method, which will contain the following steps is to be performed:

Step 1. User introduces a word or word-combination, which is desirable for him base of the password formation.

Step 2. Pseudorandom number *rand_n* is generated, it is scaled according to the probability values *n* and the comparison is performed. If *rand_n* is less than *n*, then the replacement of the symbol occurs – step 3, otherwise, step 4 is performed.

Step 3. One more pseudorandom number *rand_s*, is generated, it is scaled according to the probability values. Depending on the value of *rand_s*, the scenario of the replacement is determined according to the roulette principle ("width" of the sector" depends on the results of the aggregation of the users` answers).

Step 4. If steps 2 and 3 were performed for each symbol, introduced by the user, then the execution of the algorithm is terminated, otherwise the transition to the next symbol and transition to step 2 occurs.

In order to generate the random numbers, the usage of the specialized coprocessors are provided [14]. As the alternative to random numbers generator, in case when their usage is impossible or if the distrust is expressed [15], it is expedient to use cryptographically secure generators of pseudorandom numbers [15, 16].

For the formalization of the method, one of the algorithms, realizing it, is shown in Fig. 3.

As these studies were aimed at users, who may not have sufficient competence for the realization of the method, on the base of the developed algorithm (Fig. 3), which realizes the suggested method, the authors developed the tool, enabling to use the suggested method in practice.

Tool for the improvement of the passwords security

In order to realize the tool for improving the passwords security the programming language Java was chosen due to the possibility to use application on different devices, with different operation systems provided by Java, improve the scalability of the application usage. Data are sent to the input of the device, these data are entered by the user, namely, key word, wordform or word combination, on the base of which the password will be generated. In case of the very short word (less than 8 symbols), the user will get the warning about the insufficient length. Besides, for the adaptation for various tasks the field, intended for the introduction of the probability of symbols replacement in the password phase is provided in the interface (Fig. 4).

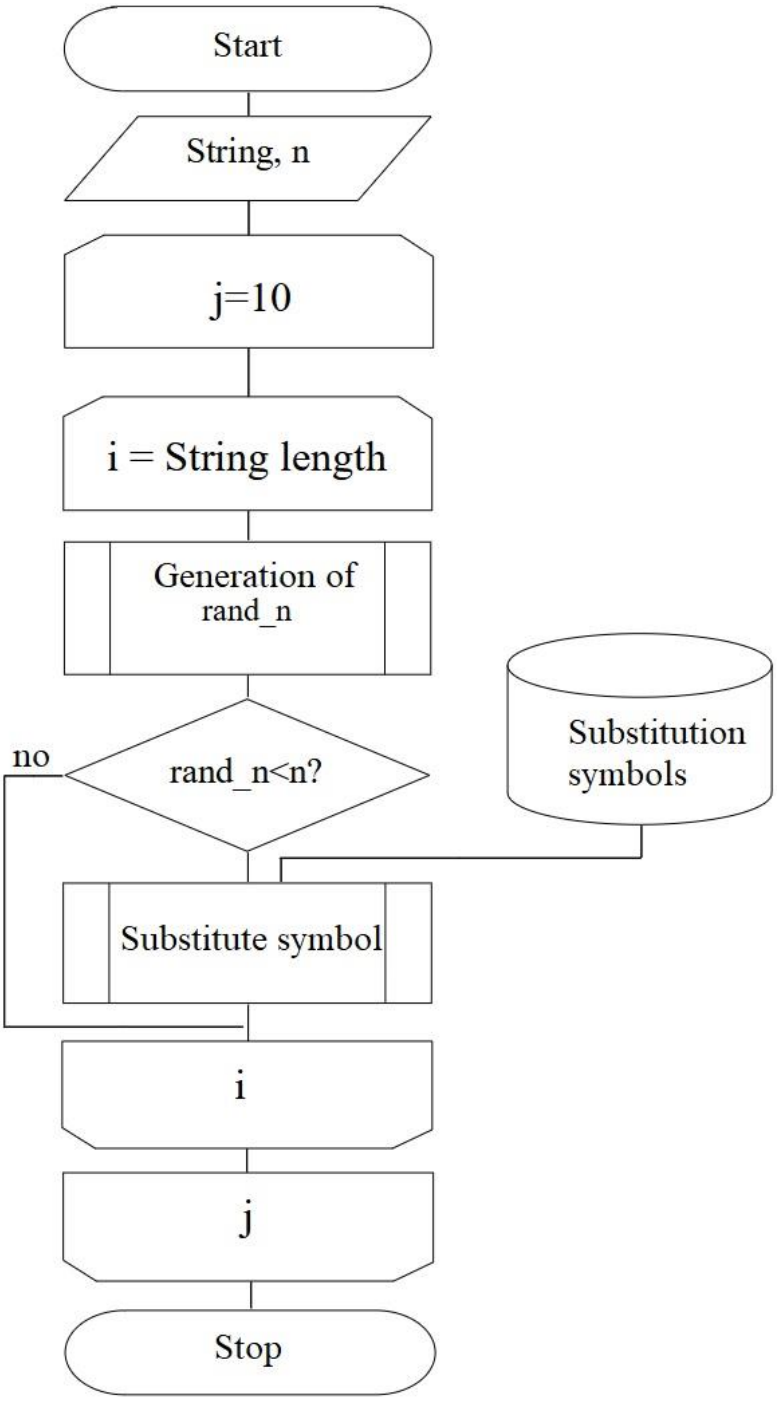

Fig. 3. Algorithm of passwords security improvement

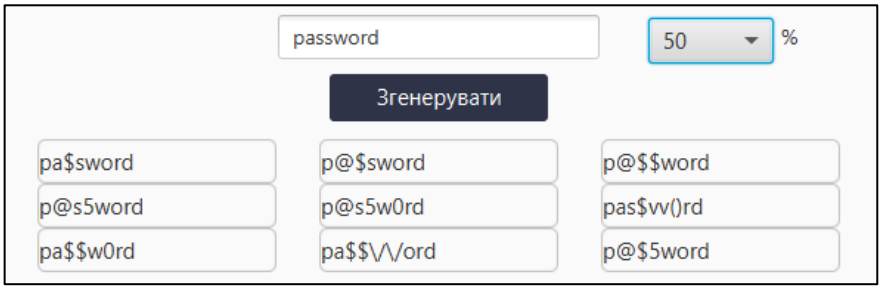

Fig. 4. Results of passwords generation by means of the tool

Replacement of each symbol will occur in the cycle, number of iterations of which depends on

the length of the entered word, where it will be determined if the replacement of the letter for the symbol from the table of replacements will occur.

Replacement procedure is built on the generator of pseudorandom numbers, generating limits of which are further scaled within the range from 0 to 100 by applying the method of pseudorandom number generation, described in the work [16]. In case, when the user introduces the part of the symbols replacement (in the given example in Fig. 4 this value is set on the level of 50 %) and the generated number will be in the range from 0 to 50, the corresponding letter in a word will be replaced by a special symbol.

As it is seen from the Fig. 4, the tool suggests the user a number of the alternative passwords, which by means of the application of special symbols and figures in addition to letters, increase the set of the passwords, which the intruder must sort out, attacking the password. Due to this property the improvement of the obtained passwords security occurs as compared with the introduced word "password". Besides, it is seen from the Fig. 4 how the replacement table operates. In particular, letter "a" as a result of the absolute advantage of the replacement variant "@" was replaced during the realization of the algorithm only in such a manner (although it had a chance for other variants of the replacement), whereas the letter "o" in the proposed results in certain cases was replaced by "0", and in one case it was replaced by "()". Letters "p", "r", "w" and "d" were not changed as they were not present in the replacement table, formed within the frame of the given research.

Thus, for the determination of the level of the password security improvement it is expedient to analyze the obtained result. The word "password", that consists of 8 letters of English alphabet, written in the low register, in case, when the intruder knows the length of the password, the realization of the brute force attack requires the sorting out of $(26)^8 \approx 2 \cdot 10^{11}$ letter combinations. We will consider one of the worst for the suggested method, case, when the intruder possesses the information regarding the possible replacement of the symbols, used in the suggested method and knows the number of the letters of the original word. After the formation of the letter combination the intruder must apply all the possible variants of the replacement table. In the specific tool realization the replacement table for 12 letters, each of which has on average 2.83 variants of replacement (in case, when the decision, regarding replacement was taken), was used. Thus, the power of the combination set, which must be sorted out by the intruder is $\left(14 + 12 \cdot (1 + 2{,}83)\right)^8 \approx 1{,}68 \cdot 10^{14}$ of possible variants of the passwords. Then, for the considered type of the attack, the number of combinations to be sorted out by the intruder, increased 840 times as a result of the application of the suggested method.

Conclusions

As a result of the analysis, carried out, the problem of generation of the secure passwords, which must be solved the users, who may not have sufficient competence in the field of cyber security is shown. For the solution of the given problem, the tool, based on the suggested method of improvement the passwords security has been developed. Due to the developed tool, the users will have the possibility to improve the security of the passwords they select.

Further, the authors plan to improve the suggested method and tool, providing the user with the possibility to influence the length of the password, obtained after the processing and to determine analytical formulas for the computation of the level of the passwords security level, depending on the parameters of the upgrading, set by the user.

REFERENCES

1. Authentication. Theory and practice of the provision of the secure access to information resources. Manual for graduate students / [Afanasiev A. A., Vedeniev L. T., Vorontsov A. A. et al.] ; under the editorship of A. A. Shelupanov, S. L. Grudiev. – Moscow, Hot line-Telecom, 2012. – 550 p. (Rus).

2. Baryshev Yu. V. Method of authentication of the remote users for network services / Yu. V. Baryshev, V. A. Kaplun // Information technologies and computer engineering. – 2014. – № 2. – P. 13 – 17. (Ukr).

3. Dasgupta, Dipankar. Advances in User Authentication [Electronic resource] / Dasgupta, Dipankar, Roy, Arunava, Nag Abhijit // Springer. – 2017. – 360 p. – Access mode : https://www.researchgate.net/publication/334559194_Advances_in_User_Authentication.

4. Evaluation of user authentication methods in the gadget-free world [Electronic resource] / Halunen Kimmo, Häikiö Juha, Vallivaara Visa // Pervasive and Mobile Computing. – 2017. – DOI : 10.1016/j.pmcj.2017.06.017. – Access mode : https://www.researchgate.net/publication/318241904_Evaluation_of_user_authentication_methods_in_the_gadget-free_world.

5. Multilayer Access for Database Protection [Electronic resource] / Olesia Voitovych, Leonid Kupershtein, Vitalii Lukichov, Ivan Mikityuk // International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T). – 2018. – P. 474 – 478. – Access mode : https://ieeexplore.ieee.org/abstract/document/8632152.

6. Luzhetskyi V. A. Fundamentals of information security : manual / V. A. Luzhetskyi, A. D. Kozhukhivskyi, O. P. Voitovych. – Vinnytsia : VNTU, 2013. – 221 p. (Ukr).

7. Roebuck Kevin. Random Password Generators: High-impact Strategies - What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity / Kevin Roebuck. – Vendors : Lightning Source Incorporated, 2011. – 426 p.

8. A very weak and widespread password is written on a sticker / st. [Electronic resource] / Katherine Parker // Secure Networkers. Blog Space. – June 29, 2020. – Access mode : https://securenetworkers.com/a-very-weak-and-widespread-password-is-written-on-a-sticker-st/.

9. Password Security : What Users Know and What They Actually Do [Electronic resource] / Shannon Riley // Usability News. – 2006. – Vol. 8, Issue 1. – Access mode : https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.597.5846&rep=rep1&type=pdf.

10. State standard of Ukraine ISO/IEC 27000:2019 Information technologies. Methods of protection. Control systems of information security. Review and glossary (ISO/IEC 27000:2018, IDT). [Valid from 01.11.2019]. [Electronic resource] – Access mode : http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85795. (Ukr).

11. Discretion model and method of access rights differentiation to distributive information resources [Electronic resource] / Yu. V. Baryshev, V. A. Kaplun, K. V. Neujmina // Scientific works of VNTU. – 2017. – № 2. – Access mode to journal : https://praci.vntu.edu.ua/index.php/praci/article/view/506/501. (Ukr).

12. Advances in Password Recovery Using Generative Deep Learning Techniques. Artificial Neural Networks and Machine Learning / D. Biesner, K. Cvejoski, B. Georgiev [et al.] // ICANN 2021: 30th International Conference on Artificial Neural Networks, Bratislava, Slovakia. – September 14–17, 2021. – Proceedings, Part III. – P. 15 – 27.

13. Publishable Humanly Usable Secure Password Creation Schemas. Proceedings [Electronic resource] / Manuel Blum, Santosh Vempala // The Third AAAI Conference on Human Computation and Crowdsourcing (HCOMP-15). – 2015. – Access mode : https://www.aaai.org/ocs/index.php/HCOMP/HCOMP15/paper/viewFile/11587/11430.

14. Intel Digital Random Number Generator (DRNG) : Software Implementation Guide [Electronic resource] / Revision 1.1. – 2012. – Access mode : https://www.intel.com/content/dam/develop/external/us/en/documents/441-intel-r-drng-software-implementation-guide-final-aug7.pdf.

15. Randomness generation [Electronic resource] / Daniel J. Bernstein, Tanja Lange. – 16 May 2014. – Access mode : https://cr.yp.to/talks/2014.05.16/slides-dan+tanja-20140516-4x3.pdf.

16. Baryshev Yu. V. Methods of the formation of pseudorandom numbers for pseudonondeterministic hash-functions / Yu. V. Baryshev, T. A. Kravchuk // Abstracts of the reports at the Third international scientific-practical conference "Information technologies and interactions", Kyiv, 8-10 November 2016. – Kyiv, Publishing-polygraphic center "Kyiv University", 2016. – P. 207 – 208. (Ukr).

Editorial office received the paper 18.06.2022.
The paper was reviewed 22.06.2022.

Baryshev Yuriyi – Cand. Sc. (Eng.), Assistant-Professor with the Department of Information Security.
Vinnytsia National Technical University.

Chaikin Mykhailo **–** Post Graduate.
G. E. Pykhov Institute of problems modeling in power engineering, National Academy of Sciences of Ukraine.

Kokhan Olexander – student of group 1БС-20м, Department of Information technologies and computer engineering.
Vinnytsia National Technical University.