Information security of printing organizations

Dmytro Kucherov [1], Andriy Fesenko [2], Igor V. Ogirko [3], Olha I. Ogirko [4] and Andrei Berezkin[5]

[1,2] National Aviation University, 1 Liubomyra Huzara ave., Kyiv, 0358, Ukraine
[3] Ukrainian Academy of Printing, 19, str. Pidgolosko, Lviv, 79020, Ukraine
[4] Lviv State University of Internal Affairs, 26 Horodotska str., Lviv, 79007, Ukraine
[5] G.E. Pukhov Institute for Modelling in Energy Engineering, 15, General Naumov Str., Kyiv, 03164, Ukraine

Abstract

The paper discusses the main options for technical protection at the stages of pre-printing and post-printing preparation of products by a printing company using modern cloud technologies. In the study course, insufficient security of the SSL / TLS protocol for transferring data between websites was established, which is confirmed by numerous reports in the press about the theft of personal data and the constant improvement of this protocol. Additionally, it has been established that data security has a dependency on the user's responsibility for personal information protection. In essence, options for protecting documents of a printing company can be supplemented by the introduction of digital signatures or passwords. Based on the theory of planning and processing the results of experiments, the whole factor experiment was prepared and carried out to analyze the password "strength" based on two signs of password strength: length and different types of categories of characters used in passwords. An experiment execution plan has been built based on an orthogonal matrix. According to the matrix plan, the unknown coefficients of the response function were determined; and we determined their significance as well; we have also confirmed the adequacy of the obtained equation. In the paper, we also present a model experiment is, confirming the validity of the hypothesis of the relativity of the importance of the message length concerning the types of categories of symbols used.

Keywords

password complexity, experiment planning, processing of experiment results, experiment model

1. Introduction

Information security at the present stage of information technology development, when communication and interaction between employees are carried out via wired and wireless networks, has been the main factor in the activity of any organization and particular (specific, individual) person [1, 2]. This concept applies regardless of the form in which the data to be protected is stored and used. The general problem of information security is to ensure the confidentiality, integrity, and availability of data that makes the organization's activity uninterrupted.

Following [3], the average loss of a company from one information leak in Britain is approximately 1.7 million pounds. The situation with leaks and loss of information in Ukraine is no better. Risk groups of information leakage include unscrupulous employees, hardware, and software used in the enterprise.

Printing organizations constitute a significant group of enterprises that heavily use information networks and cloud technologies for production.

XXI International Scientific and Practical Conference "Information Technologies and Security" (ITS-2021), December 9, 2021, Kyiv, Ukraine
EMAIL: d_kucherov@ukr.net (D. Kucherov); aafesenko88@gmail.com (A. Fesenko); ogirko@gmail.com (I. Ogirko); ogirko@gmail.com (O. Ogirko); abis1999@ukr.net (A. Berezkin)
ORCID: 0000-0002-4334-4175 (D. Kucherov); 0000-0001-5154-5324 (A. Fesenko); 0000-0003-1651-3612 (I. Ogirko); 0000-0002-4645-7933 (O. Ogirko); 0000-0003-3087-1184 (A. Berezkin)

The main goal of this paper is to show additional possibilities for the protection of printed products based on the differentiation of access rights to information and the value of protecting information by passwords.

The rest of the paper is organized as follows: the next Section is devoted to a review of the relevant literature and the main achievements taking place in the chosen field; in Section 3, the research problem is formulated; in section 4, the approach for solving it is presented, based on the methods of the theory of planning and processing data from the results of experiments; Section 5 discusses the main results and draws conclusions based on them.

2. Related Work

Recently, there has been a sharp leap in the development of the printing industry due to the widespread introduction of digital content publications into the practice of publishing organizations, based on the consistent distribution of computer technology in the 90s of the last century [4].

The advance of computer publishing systems made it possible to transfer an electronic layout of a publication directly from a computer or to a photographic form, or a photographic plate, and later directly to a digital printing machine, which determined the prospect of obtaining a personalized publication of any required circulation. Digital processes (prepress, print, and post-press) at all manufacturing stages of printed products have created the basis for the transition to full automation of production of a printing company based on online solutions [5]. Innovations in computer technology offer to abandon traditional servers and switch to Cloud Computing technologies. The problems of automating the task of accounting for the budgetary process to discharge are presented in the works [6-18].

The paper [19] explores the security technology of transpromo printing based on the corresponding Internet protocol.

To evaluate the security of printing depending on its cost, the authors of [20] proposed a method, based on linear programming.

The emergence of cloud solutions along with several advantages, namely: an unlimited amount of data storage, independence from the operating system when working with documents, the possibility of constant and shared access to this one, the rational use of resources, reduction in software costs, the ability to regularly update it; there was a strict need to protect deleted data.

So, it is possible to intercept confidential and private data when one's working with the "cloud"; and the internet provider can view the client's data if they are not protected by a password; this data can also become the property of hackers who have managed to break into the provider's security systems.

The reliability, timeliness, and availability of data in the "cloud" strongly depend on the intermediate parameters, which include data transmission channels on the way from the client to the "cloud"; the reliability of the last mile, the quality of the client's Internet provider, the availability of the "cloud" itself in the given moment. When the online storage company is liquidated, a computer customer can lose all their papers.

Some papers [21-27] presented at recent conferences are dedicated to password strength studies. Thus, the authors of the article [21] studied the methods used to assess the strength of passwords, which made it possible to establish the advantage of neural networks over traditional methods.

The paper [22] studied password strength and the dependence on the sensitivity of users' information. The study established the function of assessing the confidentiality of personal data and proposed an assessment method for password strength based on sensitive personal information.

The authors of the paper [23] establish the need to improve the methods for assessing the strength of passwords based on measuring the strength of passwords.

The paper [24] proposes group methods for estimating password strength using the attention mechanism (AM) in a neural network model. The long-short-term memory model (LSTM) is used for password processing, and a more accurate estimate of password strength is obtained.

The authors [25] propose a password-generation algorithm. It is based on information provided by users. The authors tested the reliability of the generated passwords when exposed to the dictionary and brute force password cracking attacks.

Based on prototyping methods, the architecture and main functions of the user interface [26] are proposed for developing a strong password.

Authors [27] propose protection against targeted attacks using personalized password strength meters.

The purpose of this study is to establish an effective system for protecting printed products at all stages of their preparation.

3. Problem statement

The preparation process of a digital layout of products by some printing companies using some publishing system is considered. A feature of the preparation process is its multistage nature (character), the essential component of which is prepress preparation. An electronic version of the final document is prepared in the prepress process. The electronic layout development of a printed document involves participation in the cloud storage of various staff members that provides collective access.

3.1. A problem in cloud storing

As you know, the problem of storing data in the "cloud" is the data protection in the case of interception during transmission over a communication channel; there is also a problem associated with devices of the "last mile"; in addition, there is a problem with data integrity during remote storage.

The most common technical solutions for data protection are data encryption, closing documents with a password, and using a digital signature.

Usually, data transmission performs by the SSL/TLS protocol. It is worth noting that despite the similarities between SSL and TLS, a series of technical documents (for example, RFC 8446) have recently been promoting TLS 1.3 for browser use. Google, Facebook, and Cloudflare have provided the TLS 1.3 protocol support for the web space since July 2019, in addition, to the main branches of the Chrome and Firefox browsers. The protocol supports three services: authentication, encryption, and message integrity checking. The safety experts consider the suggested protective measures sufficient. Nevertheless, the message interception problem is relevant, as evidenced by the numerous confirmations of theft of personal data. Thus, the user himself should be primarily concerned about his data protection.

From the point of view of protecting printed information, one of the most effective measures is to set a password for a printed document. The problem here is the establishment of obvious passwords, which may be available to an attacker, or the creator of the documents does not consider it necessary to use a password here. To secure your information and not use external audit services, it is recommended that you independently acquire a strong password.

3.2. Several requirements for passwords

We must abide by some rules to avoid the negative consequences of data theft due to the introduction of "weak" passwords. To create a strong password, [19] is recommended:

- avoid primitive passwords (repetitive words, English terminology, widespread digital combinations, etc.);
- avoid the same passwords for all services and resources;
- store the password in an open, visible place (on a table, on a monitor, in a browser, etc.);
- change the discredited password;
- do not use short passwords;
- a complex password must have a uniform distribution of alphanumeric and other symbols.

Presently (and, likely, in the near future), the user's password looks like a simple and accessible remedy for user authentication. Therefore, attempts to organize strong authentication based on a password are continuous nowadays. The application of special software and equipment for password generation leads to the creation of hard-to-guess passwords that cannot be remembered by users.

Therefore, passwords are stored in a convenient place for the user that is inconsistent with the notion of protecting the integrity of information.

A possible way out in these circumstances is the use of password strength meters, which allow you to assess the degree of password trust to the user. Users accept or complicate used passwords in a user feedback system. Building systems for evaluating password strength is currently a hot topic, as evidenced by recent publications [21-28] on this topic.

3.3. Study goal

According to the analysis of foreign publications [21-27], the most commonly used passwords at present are passwords associated with personal data, which include birthdays, passport numbers, phone numbers, e-mail addresses, etc. Using the proposed approach, we will establish how the dependence of personal information on the number of categories used in the password.

The study poses and solves the problem of determining an effective password based on the theory of planning and processing the results of experiments.

This analysis of the results obtained allows us to conclude that password efficiency is primarily affected by password duration. The effect of mutual influence, based on the initial conditions of the experiment, practically does not have a significant effect on the listed condition of reliability, which made it possible to exclude this regressor from the equation.

4. Problem solution

Based on the independence of the factors that affect the quality of the password, we will consider them independent, the combination of the same characters is not allowed, and all of the characters have the same distribution. Given the considerations, we assume that the password security function satisfies the regression equation in the form

$$y = b_0 + \sum_{i=1}^{k} b_i x_i + \sum_{i,j}^{k} b_{ij} x_i x_j + b_{123} x_1 x_2 x_3 \ldots \quad (1)$$

According to the results of testing user passwords, it has been found that the strengths of passwords, which are quantitatively expressed in relative units y, are most significantly influenced by two factors: the length of the password x_1, measured by the number of characters in a password, and the number of categories of characters x_2, measured by various types of characters.

4.1. Planning experiments

We will assume that at the user's disposal, lowercase and uppercase letters of the Latin alphabet can be used as symbols total of numbers are 26 characters, numbers are the total numbers 10 characters, and special characters are the total number of 33 characters. Thus, we have a total of numbers 4 categories of characters.

Based on the experiment planning theory [29], we also introduce the levels of variation by factors, the values of which are presented in Table. 1.

Table 1

Levels of factors

Levels of factors	x_1, symbols	x_2, categories
Main (zero)	14	3
Low	2	2
High	26	4
Interval of variation	12	1

The planning matrix looks as shown in Table 2. In this table j is the number of experiments, x_1 is the first sign, which means the number of symbols in the password; x_2 is the number of categories used in the password; y_i is the result of an experiment. In this test, we proposed that for each condition of experiment j we can obtain three results, therefore $\bar{y}_j$ is the average of these results; $\bar{S}_y^2$ is the variance characterizing the set of y_{jv} values under constant experimental conditions (i.e., at one point of the design) is found by the following formula

$$\bar{S}_j^2 = \frac{1}{m-1}\sum_{v=1}^{m}(y_{jv} - \bar{y}_j)^2 \quad (2)$$

Table 2
Planning matrix

j	x_0	x_1	x_2	x_1x_2	y_i	$\bar{y}_j$	$\bar{S}_j^2$	$\hat{y}_j$
1	+	+	+	+	27, 31, 35	31	16	29.5
2	+	–	+	–	15, 20, 25	20	25	20.5
3	+	+	–	–	51, 53, 55	53	4	53.5
4	+	–	–	+	30, 33, 36	33	9	93.5

Based on Table 2 data and using the feature of the orthogonally-planning matrix for the full factorial experiment, we can significantly simplify the calculation of the coefficients of the response equation. For the number of factors k, sample estimates b_i are calculated by the formulas

$$b_j = \frac{1}{n}\sum_{j=1}^{n} x_{ij}\bar{y}_j \quad (3)$$

$$\bar{y}_j = \frac{1}{m}\sum_{j=1}^{m} y_{jv} \quad (4)$$

Using formulas (3) and (4), we obtain

$$b_0 = \frac{1}{4}\sum_{j=1}^{4} x_{0j}\bar{y}_j = 34.25$$

$$b_1 = \frac{1}{4}\sum_{j=1}^{4} x_{1j}\bar{y}_j = \frac{31 - 20 + 53 - 33}{4} = 7.75$$

$$b_2 = \frac{1}{4}\sum_{j=1}^{4} x_{2j}\bar{y}_j = \frac{31 - 20 - 53 - 33}{4} = -8.75$$

$$b_{12} = \frac{1}{4}\sum_{j=1}^{4} x_{1j}x_{2j}\bar{y}_j = \frac{31 - 20 - 53 + 33}{4} = -2.25$$

Next, we calculate $\bar{S}_y^2$ by using values $\bar{S}_j^2$ (these values are shown in Table 2)

$$\bar{S}_y^2 = \frac{1}{4}\sum_{j=1}^{4} \bar{S}_j^2 = \frac{16 + 25 + 4 + 9}{4} = 13.5 \quad (5)$$

Find the variance of the regression coefficients:

$$\bar{S}_{b_i}^2 = \frac{1}{n(m-1)}\bar{S}_j^2 = \frac{13.5}{4 \cdot (3-1)} = 1.6875 \quad (6)$$

$$\bar{S}_{b_i} = 1.299$$

We choose the level of reliability of calculations α = 0.95 and find from the table value $t_{\frac{1+\alpha}{2}} = t_{0.975}$ at $f = 4 \cdot (3 - 1) = 8$ degrees of freedom: $t_{0.975}(8) = 2.31$. Calculate Student Statistics for model coefficients, as follow:

$$t_i = \frac{|b_i|}{S_{b_i}} \quad (7)$$

Therefore

$$t_0 = \frac{|b_0|}{S_{b_i}} = \frac{34.25}{1.299} = 26.37$$
$$t_1 = \frac{|b_1|}{S_{b_i}} = \frac{7.75}{1.299} = 5.966$$
$$t_2 = \frac{|b_2|}{S_{b_i}} = \frac{8.75}{1.299} = 6.74$$
$$t_{12} = \frac{|b_{12}|}{S_{b_i}} = \frac{2.25}{1.299} = 1.732$$

We see that $t_{12} = 1.54 < t_{0.975}(8) = 2.31$. Therefore, the coefficient b_{12} does not differ significantly from zero. Then the regression equation takes the following form

$$y = 34.25 + 7.75x_1 - 8.75x_2 \quad (6)$$

Let us calculate now

$$\sum_{j=1}^{4} \left(\bar{y}_j - \hat{y}_j\right)^2 = 20.25$$

Following the task, the number of significant coefficients of the model is $d = 3$; and

$$S^2 = \frac{3}{4-3} \sum_{j=1}^{n} \left(\bar{y}_j - \hat{y}_j\right)^2 = \frac{3 \cdot 20.25}{4-3} = 60.75$$

Now we find

$$F = \frac{S^2}{S_y^2} = \frac{60.75}{13.5} = 4.5 \quad (7)$$

that, less than the critical value $F < F_{0.05;\ m1 = 1,\ m2 = 8} = 5.32$, and the final formula for the response function is:

$$y = 51.46 + 0.62x_1 - 8.75x_2 \quad (8)$$

Formula (8) allows you to evaluate the effectiveness of the entered password within the framework of the experiment. The analysis of equation (8), where the parameter x_1 varies from 4 to 6 symbols, and the parameter x_2 varies from 1 to 3 types of symbol categories, is presented in Table 3.

Table 3

Response function values for different types of passwords

Password	x_1, symbols	x_2, the number of categories	Y
a1cd	4	2	36,44
a1Cd	4	3	27,69
a1bcd	5	2	37,06
a1Bcd	5	3	28,31
a1Bcd!	6	1	46,43

The results presented in Table 3 have been derived from the algorithm shown in Figure 1. In this algorithm, the response function has been calculated according to (1); the variance of measurements has been calculated by the formula (4); the variance of the coefficients b_i has been calculated by the formula (6); the coefficients t_i have been calculated according to (7) to assess the significance; the adequacy of the response function has been determined by the Fisher criterion.

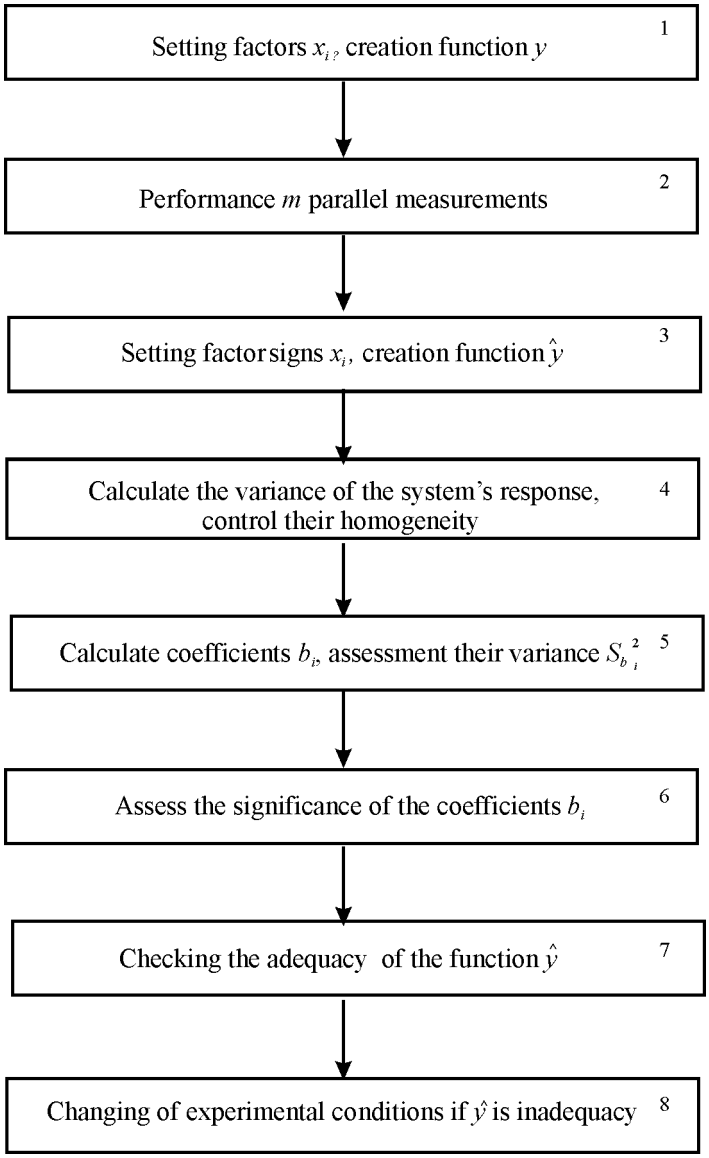

Figure 1: Response function calculation algorithm

4.2. Results

The model experiment consisted in changing the number of symbols of categories 1 and 2, under the initial data, and establishing the result by the response function (5). The results of the calculation are shown in Figures 2 and 3.

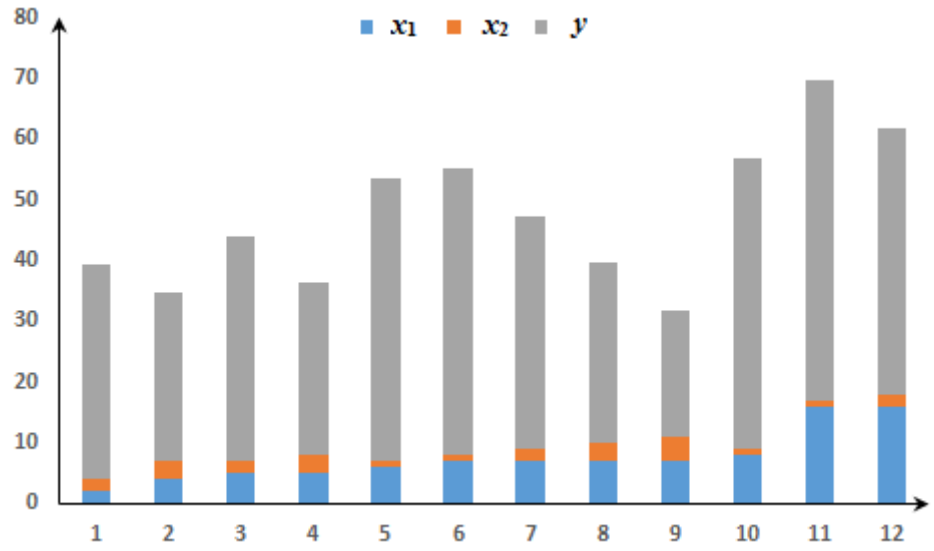

Figure 2: Diagram of the influence of factors x_1 and x_2 on the response function y

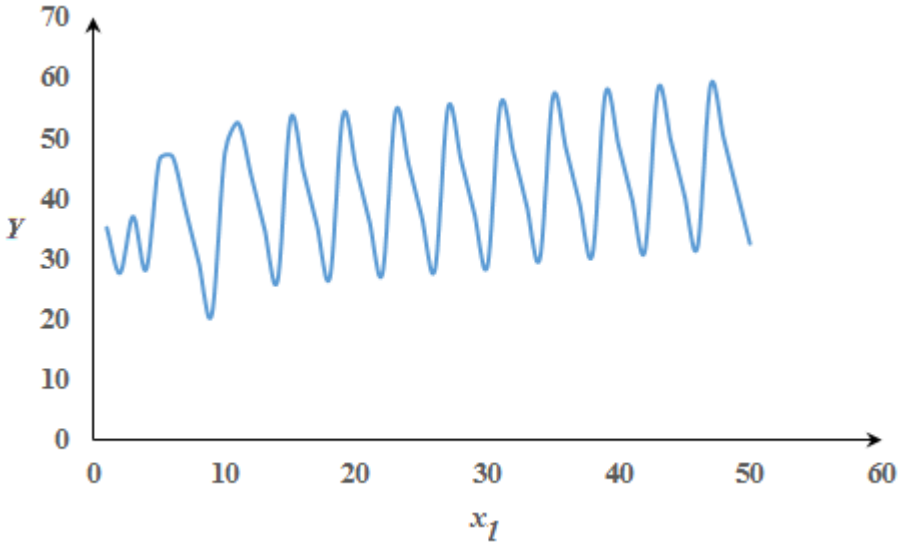

Figure 3: Graph of the dependence of the influence of the factor x_1 on the response function y

4.3. Discussion

The article discusses the problem of increasing password strength with personal information use. To solve this problem, we propose a system that uses personal information when the weak strength password has initially been set, the strength of which step-by-step increases based on the results of measurements. Unlike other approaches, the article analyzes the results of our measurements based on the input response function, which is usually used in the theory of planning and processing the results of experiments.

In creating the system model, we build the response function that in the study takes into account not only various sign of factors but also their mutual influence. As variable factors of the response function, the length of the password symbols and the number of symbol categories involved in the formation of the password has been chosen. The algorithm proposed in the article is based on the statistical characteristics of the set used. Apart from, based on these findings, the dispersion of the response function coefficients is calculated, and their homogeneity and significance are checked.

In the course of the study, it has been found that the mutual influence of various categories of symbols on the result of the response function is not significant, which makes it possible to bring the response function to a linear form and use it in further research.

However, the primary analysis regarding the lack of significance of their mutual influence made it possible to discard the need for such an analysis. During the study, we also concluded the satisfactory results of the research; and it was considered feasible to recommend the use proposed approach to the construction of practical password strength meters.

5. Conclusions

The article proposes the centralization of technical computing resources, IT specialists, and software in the general budget cloud. Access to the cloud via the Internet, individualized access to data, and a set of software functions provided by the bandwidth of network communication channels will be transferred to the sites.

To increase the security of printed products at the stages of pre-print and post-print preparation, it is recommended to use passwords consisting of a large number of characters, including lowercase and uppercase letters of the Latin alphabet, numbers, and auxiliary symbols. Based on a whole-factor experiment, a type of response function has been established that allows you to compare passwords and set the strength of a password.

This analysis of the results obtained allows us to conclude that password efficiency is primarily affected by password duration. The effect of mutual influence, based on the initial conditions of the experiment, practically does not have a significant effect on the put-forward condition of reliability, which made it possible to exclude this regressor from the equation.

Acknowledgements

The work has been carried out on an initiative basis. The authors thank the anonymous reviewers, whose comments significantly improved the content of the paper.

The authors also thank both the authorities of the Ukrainian Academy of Printing, Lvov State University of Internal Affairs, and National Aviation University the especially leadership of the Faculty of Cybersecurity, Computer and Software Engineering for their support during the preparation of this paper.

References

[1] M. E. Whitman, H. J. Mattord, Principles of Information Security, Cengage Learning, Boston, USA, 2021. URL: https://inlnk.ru/XO3VB0

[2] M. Stamp, Information security, principle and practice, Wiley Interscience, Hoboken, USA, 2021. URL: http://surl.li/cubpv

[3] E. Varaksa, Underestimating risks can lead to loss of business, Independent Ukrainian magazine F+S: Technologies of business and fire protection, (2011). URL: http://security-info.com.ua/articles/?ELEMENT_ID=526. [in Russian].

[4] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M. Zaharia, A View of Cloud Computing, Communications of the ACM, 53 (2010): 50-58. doi: 10.1145/1721654.1721672.

[5] P.I. Machuga, Virtualization and cloud technologies in accounting: distant future or real present? Efficient economy, 5 (2013). URL: http://www.economy.nayka.com.ua/?op=1&z=2008. [in Ukranian]

[6] E.S. Bondar, M.M. Glubovetc, S.S. Gorohovskii, Cloud computing, and its applications. Bulletin of KNU named after T. Shevchenko, 1 (2011): 74-82. [in Ukranian]

[7] L.A. Voloshchuk, O.I. Roznovets, D.D. Voloshchuk, Support for the decision making on implementation of applications in the hybrid cloud infrastructure, Informatics and Mathematical

Methods in Simulation, 1 (2018): 86–97. URL: http://immm.op.edu.ua/files/archive/n1_v8_2018/2018_1(9).pdf.
[8] S. Ramgovind, M. M. Eloff, E. Smith, The Management of Security in Cloud computing, in: Proceeding of 2010 Information Security for South Africa (ISSA), Johannesburg, South Africa, 2010, pp. 1–7. doi: 10.1109/ISSA.2010.5588290.
[9] Yu. S. Ganzhurov, Strategic directions of development of enterprises in the printing industry, printing activities and book trade, NTUU «KPI», Kyiv, 2015. URL: https://ela.kpi.ua/handle/123456789/15408 [in Ukranian]
[10] Ya. Yu. Zmihov, I.V. Shablyi, I.V. Ogirko, Data formats of the automated control system of the printing house, Qualology of the book, Proceeding of Ukrainian Academy of Printing, 2 (2018): 51–56. URL: https://inlnk.ru/QwQ1j6 [in Ukranian]
[11] D. C. Wyld, Moving to the Cloud: An Introduction to Cloud Computing in Government, IBM Center for the Business of Government, USA, 2009. URL: https://www.businessofgovernment.org/sites/default/files/CloudComputingReport.pdf.
[12] O.O. Gudzovata, Cloud services: possibilities, security, perspectives, in: O.A. Parshina, Theoretical and applied aspects of entrepreneurial competitiveness, Gerda, Dnipropetrovsk, Ukraine, 2013. URL: https://www.ipu.ru/taxonomy/term/21062. [in Ukranian]
[13] L. M. Kaufman, Can Public-Cloud Security Meet Its Unique Challenges? IEEE Security & Privacy, 4 (2010): 55–57. doi: 10.1109/MSP.2010.120.
[14] G. Anthes, Security in the Cloud, Communications of the ACM, 53 (2010): 16–18. doi: 10.1145/1839676.1839683.
[15] M. Christodorescu, R. Sailer, D. L. Schales, D. Sgandurra, D. Zamboni, Cloud security is not (just) virtualization security: a short paper, in: Proceedings of the 2009 ACM workshop on Cloud Computing Security, Chicago, Illinois, USA, 2009, pp. 97–102. doi:10.1145/1655008.1655022.
[16] C. Shaver, J. M. Acken, Effects of Equipment Variation on Speaker Recognition Error Rates, in: Proceeding IEEE International Conference on Acoustics Speech and Signal Processing, Dallas, Texas, 2010, pp. 1814 – 1818. doi: 10.1109/ICASSP.2010.5495401.
[17] T. Ristenpart, E. Tromer, H. Shacham, S. Savage, Hey, you, get off of my cloud: Exploring Information Leakage in Third-party Compute Clouds, in: Proceedings of the 16th ACM conference on Computer and Communications Security, Chicago, Illinois, USA, 2009, pp. 199–212. doi: 10.1145/1653662.1653687.
[18] D.P. Kucherov Control of computer network overload, in: Proceeding of the XVII International Scientific and Practical Conference on Information Technologies and Security (ITS 2017), Kyiv, Ukraine, November 30, 2017, pp. 69 -75, 2017, CEUR-WS.org, online. URL: http://ceur-ws.org/Vol-2067/paper10.pdf.
[19] A. Seto, J. Lisi, M. K. Ahmed, Ensuring document security and privacy in transpromo printing, in: Proceeding of 2009 IEEE Toronto International Conference Science and Technology for Humanity (TIC-STH), Toronto, ON, Canada, 2009. pp. 290-295. doi: 10.1109/TIC-STH.2009.5444488.
[20] P. Zhernova, A. Bizuk, V. Diachenko, Optimizing the parameters of the security printing complex, in: Proceeding 2015 Xth International Scientific and Technical Conference "Computer Sciences and Information Technologies" (CSIT), Lviv, Ukraine, 2015, pp. 94-96. doi: 10.1109/STC-CSIT.2015.7325441.
[21] Z. Tao, C. Zelei, Q. Yi, L. Qiang, S. Lin, Deep Learning for Password Guessing and Password Strength Evaluation: A Survey, in: Proceeding of 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 2020, pp. 1162-1166. doi: 10.1109/TrustCom50675.2020.00155.
[22] C. Xinchun, L. Comxueqing, Q. Yiming, D. Yong, A Password Strength Evaluation Algorithm Based on Sensitive Personal Information, in: Proceeding of 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 2020, pp. 1542-1545. doi: 10.1109/TrustCom50675.2020.00211.
[23] D. Pereira, J. F. Ferreira, A. Mendes, Evaluating the Accuracy of Password Strength Meters using Off-The-Shelf Guessing Attacks, in: Proceeding of 2020 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), Coimbra, Portugal, 2020, pp. 237-242. doi: 10.1109/ISSREW51248.2020.00079.

[24] D. He, B. Zhou, X. Yang, S. Chan, Y. Cheng and N. Guiana, Group Password Strength Meter Based on Attention Mechanism, IEEE Network 4, (2020): 196-202. doi: 10.1109/MNET.001.1900482.
[25] F. Z. Glory, A. U. Aftab, O. Tremblay-Savard, N. Mohammed, Strong Password Generation Based On User Inputs, in: Proceeding of 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2019, pp. 416-423. doi: 10.1109/IEMCON.2019.8936178.
[26] E. Stavrou, A situation-aware user interface to assess users' ability to construct strong passwords: A conceptual architecture, in: Proceeding of 2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), London, UK, 2019, pp. 1-6. doi: 10.1109/CyberSA.2017.8073385.
[27] B. Pal, T. Daniel, R. Chatterjee, T. Ristenpart, Beyond Credential Stuffing: Password Similarity Models Using Neural Networks, in: Proceeding of 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2019, pp. 417-434. doi: 10.1109/SP.2019.00056.
[28] Passwords – the good ones, the bad ones, and the ugly ones, 2021. URL: https://itglobal.com/ru-ru/company/blog/paroli-horoshie-plohie-i-uzhasnye [in Russian]
[29] A.I. Kobzar, Applied mathematical statistics. For engineers and scientists, Fizmatlit, Moscow, Russia, 2012. URL: https://inlnk.ru/LABao5 [in Russian]