Marketing and Management of Innovations
Issue 4, 2020

ISSN 2227-6718 (on-line)
ISSN 2218-4511 (print)

https://doi.org/10.21272/mmi.2020.4-23

JEL Classification: O34; L2; D2

Olena Skrynnyk,
Germany
ORCID ID, 0000-0001-8300-6616
email: skrynnykolena@googlemail.com

SOME ASPECTS OF INFORMATION SECURITY IN DIGITAL ORGANIZATIONAL MANAGEMENT SYSTEMS

Abstract. *Organizational development is one of the most important fields of organizational management. With increasing connectivity and digitalization of processes, systems, and data, intrusions via interfaces and subsystems can be affected by the entire system's security. The manipulation or loss of data in artificial intelligence-based systems takes on a serious role, as the technology learns and acts based on data. Since personal and person-related data and confidential company data, are of particular importance, this issue's relevance is significant. This study aimed to determine the data access limit for digital systems for organizational development and to investigate user attitudes towards the procession of personal data through artificial intelligence. The main purpose is to provide the research results to target selected security and data protection aspects in the design of organizational development systems based on artificial intelligence. Investigation of this topic is carried out in three logical phases. The first phase provides the analysis of scientific publications. It explores how and under which aspects and conditions digital systems for organizational development depend on information security and data protection. The literature review included keyword network analysis in Scopus with further visualization in VOSviewer. The second part provides a targeted data classification according to security classes, which can be directly applied to design organizational development or management software. In the third phase, there is a survey of respondents from Ukraine and Germany to determine the attitudes towards collecting and analyzing personal data through artificial intelligence. The investigation results show the close connection of the subject's security and data protection with the change management system, privacy, development of technological models in enterprises, applications for and of process analysis, the legislative basis for information security, etc. According to the survey, the respondents from Ukraine show more neutrality in accepting the collection of personal or personal data through artificial intelligence. Across age and nationality, it can be stated that the majority of respondents are not opposed to collecting and analyzing data about the execution of the activity or behaviour, personal details, family status, education. Scientists and practitioners can directly use the findings for further applications in developing digital systems for organizational development.*

Keywords: information security of organizational development system, artificial intelligence for organizational development, protection of organizational data, protection of personal data.

Introduction The alignment of industry and economy rapidly evolving technology is necessary to ensure the viability of an organization also on global markets (Balas and Kaya, 2019; Bilan et al., 2019 a; Bilan et al., 2019b; Bondar et al., 2015; Grena-Akovai et al., 2020; Hrytsenko and Isayeva, 2011; Khan, 2018; Lyulyov and Shvindina, 2017; Olefirenko et al., 2014; Pomianek, 2018; Pakhnenko et al., 2018; Vasilyeva et al., 2019). That applies not only to the financial and production-related aspects (Grytsenko et al., 2010; Kuzmenko and Kyrkach, 2014; Lyeonov and Liuta, 2016; Plastun et al., 2018; Rubanov, 2017; Ryabenkov and Vasyliyeva, 2013; Shvindina, 2019; Subeh and Yarovenko, 2017). It flows into the company's total management system (Karpishchenko et al., 2014; Peresadko et al., 2014; Shvindina, 2017a). It worth to mention that the researchers continuously consider the issues of innovations in the area of information security in their papers (Peresadko et al., 2014; Shvindina, 2017b; Zakharkina, 2009; Zakharkin and Zakharkina, 2014). The majority of large companies also have their internal information security systems (Bublyk et al., 2017; Grena-Akovai et al., 2020; Leonov et al., 2019). They function according to their own standards, which mainly comply with national (Bundesdatenschutzgesetz, EU-Regulation GDPR, Law of Ukraine on protecting personal data) and international guidelines (GDPR, ISO

Cite as: Skrynnyk, O. (2020). Some Aspects of Information Security in Digital Organizational Management System. *Marketing and Management of Innovations*, 4, 279-289. http://doi.org/10.21272/mmi.2020.4-23

27001, ISO 15408) considering the specifics of the company. To protect their data from exploitative attacks, companies implement data governance, an integrative approach to the availability, usability, integrity, and security of information requiring protection. In general, the enterprise has a variety of data that requires different levels of protection. According to its purpose, many companies effectively deploy proactive (prevention of data loss) and reactive (detection of security breaches) data protection measures. Data security is relevant because of at least three reasons, such as individual personal protection, complying with internal company standards and national and international regulations. This paper separates these interrelated reasons since they could have different weightings in different contexts. Therefore, to avoid inconsistency of the company's internal data and protect companies' stakeholders' privacy, the companies aim to comply with the legal data protection laws, such as the European Union's GDPR and the California Consumer Privacy Act (CCPA).

Literature Review. The unique aspect of the investigated topic consists in the fact, that, depending on the depth of involvement, the organizational management or development system could be primarily concerned with personal or personal-related data, which require special protection (Ipatov and Grebeniuk, 2018), (Kolomiiets and Petrushenko, 2017). The possibilities to disrupt the protection and prevent it are social engineering principles concerning organizational development software. Although conventional organizational development means only long-lasting, planned and ongoing processes, the system characteristics of artificial intelligence technologies (data tracking, adaptation, flexibility, determination of intermediate results, accuracy and continuity of results, etc.) require examining the data beyond the organizational and group levels. The rapid development of artificial intelligence leads to the introduction of technologies. On the one hand, these technologies support employees (e.g., through decision-making or correction of manual actions), while on the other hand, they monitor personal behaviour, communication, execution of activities, etc. (Bilan et al., 2019c; Kwilinski, 2018; Njegovanovic, 2018).

Information security, social engineering and data protection form a triangle of the key areas of this analysis. Despite these areas being different issues, they are usually considered together due to the implemented software development measures, especially focused on confidential, personal or personal-related information (Carcary et al., 2019). In this context, informational security focuses on ensuring confidentiality, availability and integrity through information processing and storage systems. It worth mentioning that confidentiality is a degree to which a specific person (group) or role is permitted to access specific information. In turn, availability means the permanent accessibility of data for selected person (group) or role. Integrity is defined as the permanent condition of data throughout its life cycle. Data protection generally focuses on legal protection against improper data processing, especially personal data, informational self-determination, and privacy protection. The term «social engineering» is generally defined as all conceivable forms of human influence that make it possible to obtain a person's information, property or services illegally. Regardless of legal regulations, individuals contribute to the protection of their private data. Notably, new technologies are new challenges. This article provides a description of the relevance of the topic and the development trend. There are results of personal and person-related data analysis and surveyed study participants' attitude toward data protection, particularly, to artificial intelligence.

Methodology and research methods. To obtain a comprehensive overview of the investigated topic and ensure the preparation of security assessments of organizational development systems based on artificial intelligence and determine the future trend in data protection, this study performed by several steps as follows. First, the literature overview about information security and data protection of the digital organizational management or development systems was conducted. The literature analysis was provided based on the data of the Scopus database. It allowed understandштп better the trends in the development of information security and data protection for organizational management or development systems and suggest the relevance of related subject areas. For selecting the relevant scientific publications, the

following search terms were used: «security», «data protection», «artificial intelligence», «machine learning», «neural network», «organization*», «organizational management», «organizational development». Besides, on this intermediate step, the study provides filtration of the total amount of publications according to a predefined set of criteria. Therefore, the study sample consists of the remained publications. The software tool VOSviewer was used to analyze the network of the keywords. The obtained results present the mapping of the term clusters and their interrelation. Because of considering the topic of data protection and information security in artificial intelligence and organizational issues, this study provides research on the current literature in the mentioned field.

Analysis of data processed by organizational development systems. The data governance framework is a highly structured set of various policies, processes, rules, and involved members, documents, and tools. Herewith, the security concept plays a significant role. The purpose of this is the planned continuous collection, analysis, implementation and execution of measures to secure data protection. One of the central parts of the security concept of a company is security assessment. Data protection and security activities in software product development and service generally follow the same pattern. That is based on the standards described above and have the following general structure:

1. Definition of security classes according to security goals of Confidentiality, Integrity, Availability and Privacy.

In this step, the so-called primary assets (the contextual data types, which are processed, transmitted, stored or retrieved, are defined and assigned to the corresponding risk class). In detail, the intermediate steps proceed as follows:

- Identification and evaluation of primary assets – data processed by the software system, e.g., reads, modifies, transfers, stores (standards of conduct, corporate culture principles).
- Definition and evaluation of corresponding supporting assets – components of the software system that use primary assets (client, database, service etc.). Assessment is performed according to the security goals.
- Derivation of security.

2. Definition of security measures.

In this step, the software's data protection measures and the associated components are defined according to the security requirements.

- Identification of requirements according to the security levels.
- Selection of security measures according to the security requirements of the relevant catalogs.

3. Implementation of security measures.

Since artificial intelligence could be implemented in one of the software components (e.g. as a service), the security measurements would be selected from the catalogues of corresponding component types. If the service is based on artificial intelligence, the security measures have to be applied to other components from related catalogues (client database).

It worth notice that Carcary et al. (2019) describes a completely different approach, according to which the framework on the definition of the processed data and evaluation of the technology for organizational management is based on open innovation. Their study provides an approach to alternative or complementary prevention or protection options.

The current study's approach suggests that the correct analysis of primary assets is the key to the successful implementation of security risk assessment. In this step, data analysis corresponding to the privacy class and individual security classes was performed. Therefore, the researchers and practitioners can successfully use the provided results to develop software for organizational issues.

The second stage of this study provides a survey on the importance of personal data protection for the employed population in Germany and Ukraine. The investigation of respondents' attitudes to collecting and analyzing different data by work-related artificial intelligence systems were surveyed. This survey

aimed to find out the respondents' current behaviour regarding social engineering and identify the future trend by analyzing the data collected from younger respondents and observing the similarities or differences in respondents' survey responses from both countries.

The survey consisted of questions on three topics as follows: acceptance of data collection by artificial intelligence: data that may be collected: and data that may be analyzed. The last two types' questions were about views, opinions, convictions; execution of the activity or behaviour; personal details, family status, and education.

When creating the survey, the rules according to the type of survey (face-to-face interview and online survey) were followed. The online survey was conducted on erhebung.de website. Standard rules for this survey art define the selected respondent group as the employed population aged between 16 and 70 years (the minimal age for trainees and students and the maximal age for people with a work experience) (Courage and Baxter, 2005; Lavrakas, 2008). Respondents were selected randomly with predefined age and gender criteria (equal number of men and women). The respondent sample was calculated according to the formula (1):

$$k = (z^2 p (1 – p) / e^2) / (1 + (z^2 p (1 – p) / e^2 N)) \quad (1)$$

where k – number of required respondents; N – population size (we set this value at 45,000,000 for Germany and 16,000,000 for Ukraine as the employee number) (Employed population in Germany), (Employed population in Ukraine); e – error range as a decimal number (we define as 5%); z – confidence level (we took z = 1.65 for confidence level 90%); p – percentage as decimal number (we choose p = 0.5 for optimal sample size)

According to this formula, 272 responders were questioned in Germany and 272 respondents in Ukraine. The same number of respondents is correlated with the population's size (with every factor of 10, the number changes to decimal places and does not increase from 1,000,000). This study's methodologies allowed investigating the various aspects of security and privacy issues in AI-based systems for organizational management purposes. These aspects cover relevance and scientific interest; used, stored, transmitted or retrieved data in such systems and their protection class; and the working population's sensitivity to this issue.

Results. Figure 1 indicates a sharp increase in scientific interest from the year 2000, while its peak was in 2018. The rapid descent in 2020 could be explained by the publication period. It is suggested that research publications on this subject have not yet been published. Therefore, it is supposed a slight increase in the next five years. The 967 results of the search in Scopus database have been refined to analyze only the relevant sources. There were excluded the publications older than ten years and those belonging to the irrelevant subject area.

For illustrating the trends in the development of the topic, it was conducted a keyword network analysis. The VOSviewer allowed visualizing the data exported from Scopus. The obtained results show that out of 2186 keywords, 54 were mentioned at least 5 times. These form 7 thematic clusters (Figure 2). Herewith, the most mentioned keywords are «system», «management», «security», «development», «framework», «organization». It worth mentioning that these keywords are the cluster centres. Furthermore, it is remarkable that different thematic directions supported scientific interest in these focal points: China, change management system, security and privacy approach, development of technological models in enterprises, a framework for information security in an organization, applications for and of process analysis, the legislative basis for information security.

Results of analysis of personal and person-related data. Table 1 demonstrates the obtained results of scientific background analysis on the data content. These findings resulted in data classification related to

organizational development that refers to Confidentiality, Integrity, Availability goals according to the following common data classes.

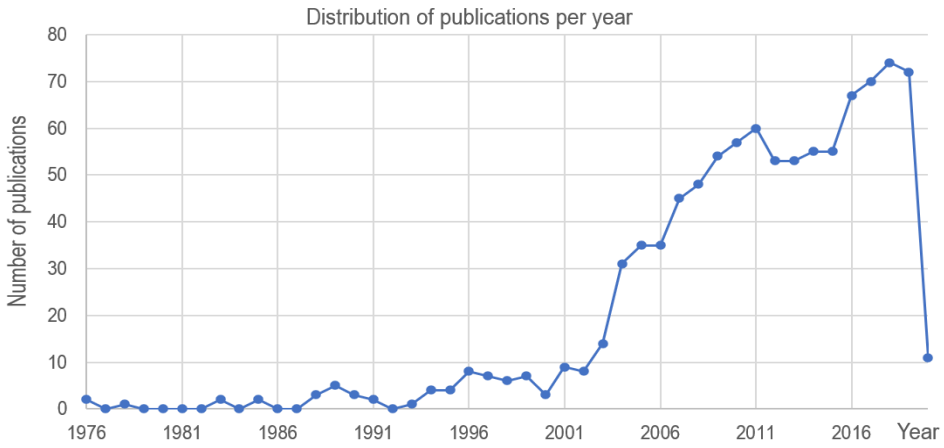

Figure 1. The tendency in the scientific interest on the research topic
Source: developed by the authors.

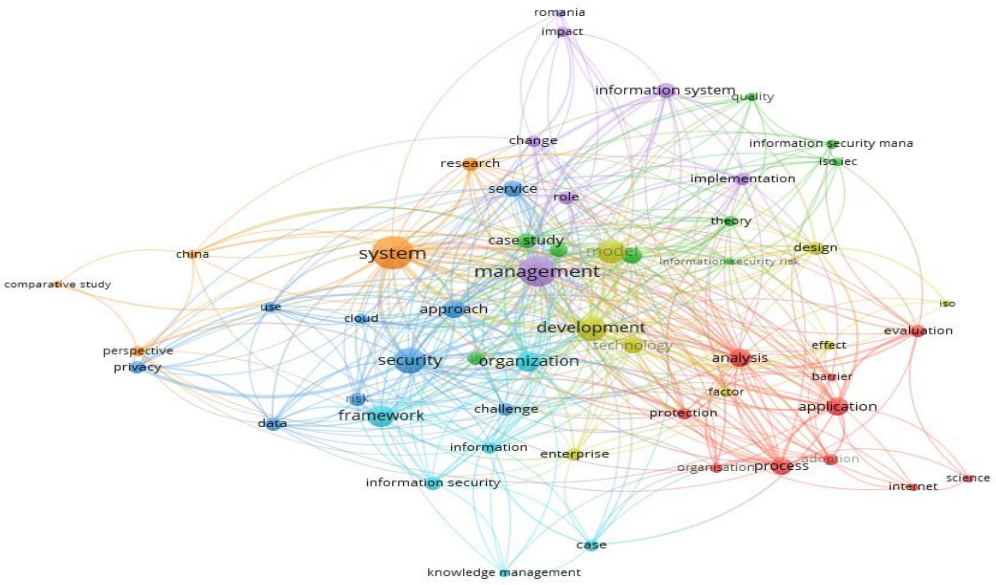

Figure 2. Thematic clusters based on the keyword network analysis
Source: developed by the authors.

The class «0» was deliberately eliminated because all datasets do not have such a general class.

Table 1. Common data classes for the organizational data system

Data class		Data type
High	3	Union membership, racial or ethnic origin, political views, religious or ideological beliefs, health data. Standards and instructions (management manuals, guidelines), audit documentation (assessment reports, home page information).
Medium	2	General data on employment (job tasks, skill data, social data, working time), business activity of the person (behaviour of the person concerned in the business environment, internal user accounts), protocols (Automatically or occasion-related copies of call content, (web) tracking, GPS data, log files/activity log).
Low	1	Personal data (gender, name, photo), family, social situation and lifestyle, information on education, internal correspondence.

Source: developed by the authors.

Table 2 shows the data processed by the system of organizational development belong to identified and therefore have at least the privacy class 2 (in the classification from 0 to 3).

Table 2. Privacy classes for the organizational data system

Privacy class		Data type
Sensitive data	3	Union membership, racial or ethnic origin, political views, religious or ideological beliefs, health data
Identified data	2	Personal data (gender, name, photo, video), family, social situation and lifestyle, information on education, internal correspondence. Business activity of the person (behaviour of the person concerned in the business environment, internal user accounts), protocols (Automatically or occasion-related copies of call content, (web) tracking, GPS data, log files/activity log). General data on employment (job tasks, skill data, social data, working time). Internal correspondence.

Source: developed by the authors.

The evaluation of the data according to performed safety classes considers only the treatment of confidentiality, integrity and availability. Nevertheless, it is recommended to consider privacy and all of the security classes in software development. Tables 3-5 suggest the assignment of the data to the appropriate security class.

Table 3. Confidentiality security classes for organizational data system

Security class confidentiality		Data type
Strictly confidential data	3	Union membership, racial or ethnic origin, political views, religious or ideological beliefs, health data. Personal data (gender, name, photo, video), family, social situation and lifestyle, information on education, internal correspondence.
Confidential data	2	Business activity of the person (behaviour of the person concerned in the business environment, internal user accounts), protocols (Automatically or occasion-related copies of call content, (web) tracking, GPS data, log files/activity log). External correspondence.

Continued Table 3

Internal data	1	General data on employment (job tasks, skill data, social data, working time). Standards and instructions (management manuals, guidelines), audit documentation (assessment reports, home page information). Corporate principles, strategy and goals. Structure and organization. Standards and instructions. Internal correspondence.
Public data	0	Published information (corporate principles, strategy and goals, home page information).

Source: developed by the authors.

Table 4. Integrity security classes for the organizational data system

Security class integrity		Data type
High	3	Union membership, racial or ethnic origin, political views, religious or ideological beliefs, health data. Standards and instructions. Audit documents. Personal data (gender, name, photo, video), family, social situation and lifestyle, information on education, internal correspondence.
Moderate	2	Business activity of the person (behaviour of the person concerned in the business environment, internal user accounts), protocols (Automatically or occasion-related copies of call content, (web) tracking, GPS data, log files/activity log). External correspondence. Published information.
Low	1	General data on employment (job tasks, skill data, social data, working time, evidence of employee training). Corporate principles, strategy and goals. Structure and organization. Internal correspondence.

Source: developed by the authors.

Table 5. Availability security classes for organizational data system

Security class availability		Data type
Highly available	3	Business activity of the person (behaviour of the person concerned in the business environment, internal user accounts), protocols (Automatically or occasion-related copies of call content, (web) tracking, GPS data, log files/activity log). Health data. External correspondence.
Hours to one day	2	Personal data (gender, name, photo, video), family, social situation and lifestyle, information on education, internal correspondence. Standards and instructions, audit documents. Internal correspondence.
Days to one week	1	General data on employment (job tasks, skill data, social data, working time). Corporate principles, strategy and goals. Structure and organization. Published information.
Weeks to months	0	Union membership, racial or ethnic origin, political views, religious or ideological beliefs.

Source: developed by the authors

The results of our analysis provide a framework for security-relevant information for digital systems with organizational issues. Besides, companies could supplement them, if required. Results of surviving on the importance of personal data protection for employed population in Germany and Ukraine. Figure 3 shows that the number of respondents aged between 18 and 46 is comparatively high in Ukraine and Germany. The proportion of employed respondents is 87.6%. The remainders are pensioners (0.9%) and those who are currently unemployed (11.5%). Figure 2 demonstrates that compared to Germany's respondents, the ones from Ukraine have more acceptance of personal data collected through artificial intelligence. This tendency is partly due to the understanding of technology. It is worth mentioning that most responders in Ukraine do not know the benefits and risks of using artificial intelligence. These conclusions were obtained from face-to-face interviews.

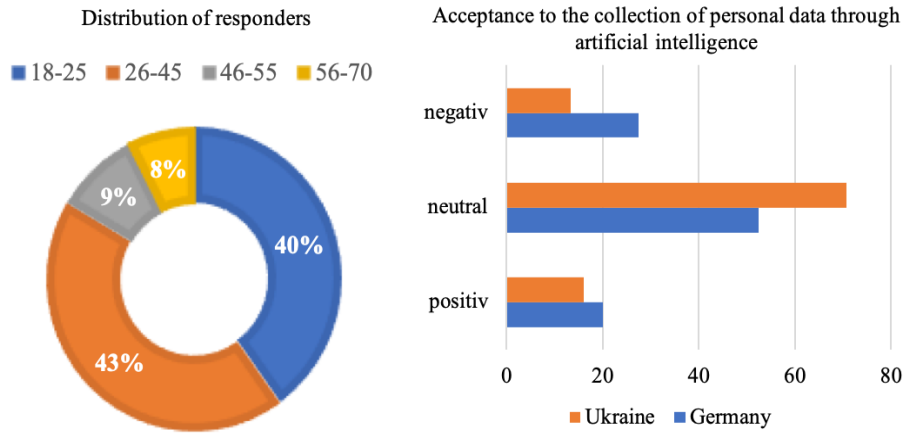

Figure 3. Presentation of survey results (Part I)

Source: developed by the authors

Figure 4 shows the distribution of attitudes toward individual data assets.

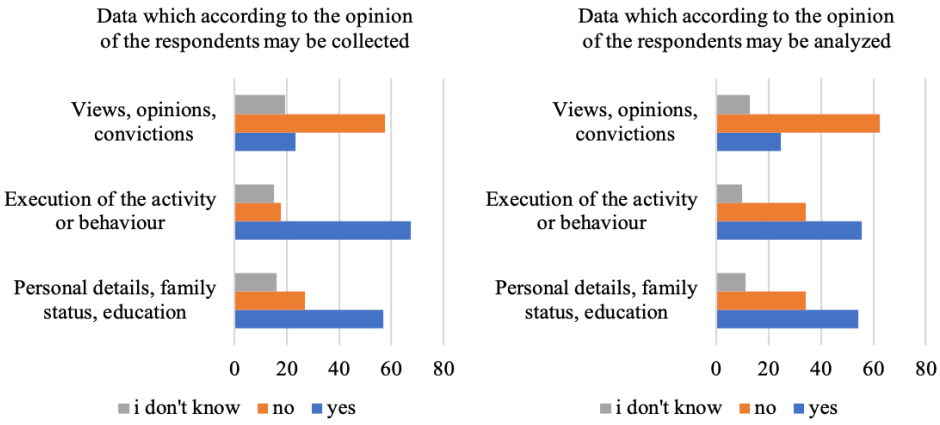

Figure 4. Presentation of survey results (Part II)

Source: developed by the authors.

The personal data were chosen from three categories according to the security classes. The respondents from both countries refuse the collection and analysis of visions, opinions and convictions. The highest proportion of respondents is in the 46-55 and 56-70 age group. It may seem that the younger respondents are more open to the collection and analysis of data through artificial intelligence. However, this statement is not correct, as the number of older respondents was much lower.

Discussion. Based on the findings, some limitations could be identified from the quantity of data analyzed and the approach to security assessment to the relevance for other fields of knowledge. This study is restricted to the survey. It has the following limitations:

1. The scope of the investigation determines the first delimitation. Since the investigation's main objective was to determine the attitudes of probands as against the collection and analysis of personal data, the survey was specifically adapted to this question. Other aspects were not explicitly examined. Therefore, the results of this survey could only be used in general.
2. The second limit is the respondents. The examined group of persons was sporadically surveyed, i.e., the respondents' delimitation was based on country, age and employment and not on their professions or organizations. That is inherent in the type and dissemination method of the survey (online). Respondents share the link to the survey within the group of known persons, whereby the respondent diversity is demarcated.
3. The third limitation is the validity of the results. The results of this survey can be used in the first line for general statements. If the concrete view, not explored questions would be required, they have to be researched additionally.

Conclusions. The information systems for organizational development operate with the personal, group and organizational data, which belong to different security classes, depending on the intervening technology's depth. With the data acquired through holistic analysis offered in this article, the security levels could be easily derived and enable the quick selection of appropriate security measures. The performed survey was intended as a small part of the investigation of obstacles in implementing artificial intelligence technologies in organizational development. However, the results are also useful for further applications. Although the range of the research themes is not large, it gives a comprehensive impression of the personal preferences for applying this technology. The investigation reveals how the respondents' preferences concerning artificial intelligence applications are distributed and their attitudes towards the use of personal data. The researchers could use this study's findings as a starting point for further preference analysis, while the practitioners - as a possible basis for developing future applications.

References

Balas, A., & Kaya, H. (2019). The Global Economic Crisis And Retailers' Security Concerns: The Trends. *SocioEconomic Challenges*, 3(2), 5-14. [Google Scholar] [CrossRef]

Bilan, Y., Brychko, M., Buriak, A., & Vasilyeva, T. (2019a). Financial, business and trust cycles: The issues of synchronization. *Zbornik Radova Ekonomskog Fakultet au Rijeci*, *37*(1), 113-138. [Google Scholar] [CrossRef]

Bilan, Y., Đšuzmenko, Đ., & Boiko, A. (2019b). Research on the impact of industry 4.0 on entrepreneurship in various countries worldwide. In *Proceedings of the 33rd International Business Information Management Association Conference, IBIMA 2019: Education Excellence and Innovation Management through Vision 2020* (pp. 2373-2384). [Google Scholar]

Bilan, Y., Rubanov, P., Vasylieva, T., & Lyeonov, S. (2019c). The influence of Industry 4.0 on financial services: determinants of alternative finance development. *Polish Journal of Management Studies*, *19*. [Google Scholar] [CrossRef]

Bondar, T., Matvieieva, Y., & Myroshnychenko, I. (2015). Assessment of the social, ecologic and economic development of machine building enterprises. *Economic Annals-XXI*, 7-8(1), 40-44. [Google Scholar]

Bublyk, M., Koval, V., & Redkva, O. (2017). Analysis impact of the structural competition preconditions for ensuring economic security of the machine building complex. *Marketing and management of innovations*, 4, 229-240. [Google Scholar] [CrossRef]

Bundesdatenschutzgesetz.(2018).Retrieved from [Link]

Carcary, M., Doherty, E., & Conway, G. (2019). Personal Data Protection (PDP): A Conceptual Framework for Organisational Management of Personal Data in the Digital Context. In *ECCWS 2019 18th European Conference on Cyber Warfare and Security* (p. 87). Academic Conferences and publishing limited. [Google Scholar]

Courage, C., & Baxter, K. (2005). *Understanding your users: A practical guide to user requirements methods, tools, and techniques*. Gulf Professional Publishing. [Google Scholar]

Dstatis. (2020). Employed population in Germany. Retrieved ferom [Link]

Minfin. (2020). Employed population in Ukraine. Retrieved from [Link]

General Data Protection Regulation.(2016). Retrieved from [Link]

Grena-Akovai, A., Bilan, Y., Samusevych, Y., & Vysochyna, A. (2020). Drivers and inhibitors of entrepreneurship development in central and eastern European countries. In *Proceedings of the 33rd International Business Information Management Association Conference, IBIMA 2019: Education Excellence and Innovation Management through Vision 2020* (pp. 2536-2547). [Google Scholar]

Grytsenko, L., Boyarko, I., & Roenko, V. (2010). Controlling of enterprises cash flows. *Actual Problems of Economics,* 3, 148-154. [Google Scholar]

Hrytsenko, L., & Isayeva, O. (2011). Approaches to classification of forms and types of enterprise restructuring. *Actual Problems of Economics*, 118(4), 111-116.

Ipatov M., & Grebeniuk N. (2018). Assessing the level of adaptation of employees to the transformation processes in the company. *Business Ethics and Leadership*, 2 (1), 106-115. [Google Scholar] [CrossRef]

ISO. (2009). ISO 15408. Retrieved from [Link]

ISO. (2018)ISO 27001. Retrieved from [Link]

Karpishchenko, O. I., Peresadko, G. O., & Olefirenko, O. M. (2014). Enterprise management systems: the case of Primary Radiology Group. *Актуальні проблеми економіки*, (4), 218-227. [Google Scholar]

Khan, Y. (2018) The Effectiveness of Entrepreneurial Activities for Economic Development: A Route to Innovation and Job Generation. *SocioEconomic Challenges*, 2(2), 32-40. [Google Scholar] [CrossRef]

Kolomiiets, U., & Petrushenko, Y. (2017). The human capital theory. Encouragement and criticism. *SocioEconomic Challenges*, 1, (1), 77-80. [Google Scholar] [CrossRef]

Kuzmenko, O., & Kyrkach, S. (2014). The use of regression analysis in the financial planning of banks, mathematical formalization of the stages of financial planning in banks. *Banks and Bank Systems*, 9(1), 120-126. [Google Scholar] [CrossRef]

Kwilinski, A. (2018). Mechanism of modernization of industrial sphere of industrial enterprise in accordance with requirements of the information economy. *Marketing and management of innovations*, 4, 116-128. [Google Scholar] [CrossRef]

Lavrakas, P. J. (2008). *Encyclopedia of Survey Research Methods*. SAGE Publications. [Google Scholar] [CrossRef]

Law of Ukraine about protection of personal data. Retrieved from [Link]

Leonov, S., Yarovenko, H., Boiko, A., & Dotsenko, T. (2019). Prototyping of information system for monitoring banking transactions related to money laundering. In *SHS Web of Conferences* (Vol. 65, p. 04013). EDP Sciences. [Google Scholar] [CrossRef]

Lyeonov, S., & Liuta, O. (2016). Actual problems of finance teaching in Ukraine in the post-crisis period. *The Financial Crisis: Implications for Research and Teaching*, 145-152. [Google Scholar] [CrossRef]

Lyulyov, O., & Shvindina, H. (2017). Stabilization Pentagon Model: application in the management at macro-and micro-levels. *Problems and Perspectives in Management*, 15(3), 42-52. [Google Scholar] [CrossRef]

Njegovanovic, A. (2018). Artificial Intelligence: Financial Trading and Neurology of Decision. *Financial Markets, Institutions and Risks*, 2(2), 58-68. [Google Scholar] [CrossRef]

Olefirenko, O., Nagornyi, Y., & Shevliuga, O. (2014). Methodical approach to estimation of industrial enterprises' technical and technological development level. *Actual Problems of Economics*, 158(8), 464-470. [Google Scholar]

Pomianek, I. (2018). Historical and Contemporary Approaches to Entrepreneurship. Review of Polish Literature. *Business Ethics and Leadership*, 2(2), 74-83. [Google Scholar] [CrossRef]

Peresadko, G., Kovalenko, E., & Kulyk, L. (2014). Mechanisms of investing into innovative projects of enterprises. *Actual Problems of Economics*, 160(1), 184-187. [Google Scholar]

Pakhnenko, O., Liuta, O., & Pihul, N. (2018). Methodological approaches to assessment of the efficiency of business entities activity. *Business and Economic Horizons*, 14(1), 143-151. [Google Scholar]

Plastun, A., Makarenko, I., Yelnikova, Y., & Sheliuk, A. (2018). Crisis and financial data properties: A persistence view. *Journal of International Studies*, *11*(3), 284-294. [Google Scholar]

Rubanov, P. M., & Marcantonio, A. (2017). Alternative finance business-models: Online platforms. *Financial Markets, Institutions and Risks*, 1 (3), 92-98. [Google Scholar] [CrossRef]

Ryabenkov, O., & Vasyliyeva, T. (2013). Comprehensive approach to application of financial controlling methods in the context of efficient application of profitability potential. *Actual Problems of Economics*, 148(10), 160-165. [Google Scholar]

Shvindina, H. (2019). Coopetition as an emerging trend in research: Perspectives for safety & security. *Safety*, 5(3), 61. [Google Scholar] [CrossRef]

Shvindina, H. (2017a). Leadership as a driver for organizational change. *Business Ethics and Leadership*, 1(1), 74-82. [Google Scholar] [CrossRef]

Shvindina, H. (2017b). Innovations of strategic management development: from competition to coopetition. *Marketing and management of innovations*, 1, 180-192. [CrossRef]

Subeh, M. A., & Yarovenko, H. (2017). Data Mining of Operations with Card Accounts of Bank Clients. *Financial markets, institutions and risks*, 1(4), 87-95 [Google Scholar] [CrossRef]

Vasilyeva, T., Kuzmenko, O., Bozhenko, V., & Kolotilina, O. (2019). Assessment of the dynamics of bifurcation transformations in the economy. *CEUR Workshop Proceedings* 2422, 134-146. [Google Scholar] [CrossRef]

Zakharkina, L. (2009). Balancing of innovative development of machine building enterprises in strategic planning process. *Actual Problems of Economics* (3), 88-95. Retrieved from [Link]

Zakharkin, O., & Zakharkina, L. (2014). Enterprise's innovation development strategy substantiation and its AIMS. *Economic Annals-XXI* 7-8, 76-79. [Google Scholar]

Олена Скринник, *Німеччина*

Забезпечення інформаційної безпеки в цифрових організаційних системах управління

У статті розглянуто процес цифровізації бізнес-процесів як одного з найважливіших сфер управління розвитком організації. Автором відмічено, що зі зростанням рівня цифровізації процесів, безпека даних всієї системи компанії знаходиться під загрозою. Зокрема, маніпулювання даними або їх втрата може спричинити порушення в роботі штучного інтелекту. Метою статті є оцінювання рівня безпеки та захисту даних при проєктуванні систем організаційного розвитку на основі штучного інтелекту. У рамках дослідження оцінено ставлення споживачів до обробки персональних даних за допомогою штучного інтелекту. Для досягнення поставленої мети, аналіз здійснено у наступній логічній послідовності. На першому етапі проаналізовано науковий доробок з досліджуваної тематики, що представлений у базі даних Scopus. За результатами першого етапу визначено як та на яких умовах цифрові системи організації залежать від інформаційної безпеки та захисту даних. На другому етапі дослідження здійснено класифікацію даних за рівнем їх безпеки, які можуть бути застосовані для проєктування програмного забезпечення організаційного розвитку або управління коанією. Для аналізу ключових слів та їх візуалізації, застосовано програмне забезпечення VosViewer. Таким чином, встановлено тісний зв'язок безпеки та захисту даних суб'єкта з системою управління змінами в організації, конфіденційністю, розробкою технологічних моделей на підприємствах, додатками та аналізом процесів, законодавчою базою для захисту інформації тощо. На третьому етапі проведено опитування респондентів з України та Німеччини з метою визначення їх ставлення до збору та обробки персональних даних за допомогою штучного інтелекту. За результатами опитування встановлено, що респонденти з України менш стурбовані про збір та обробку персональних даних за допомогою штучного інтелекту. Автором зазначено, що вік та національність не впливають на згоду респондентів надати інформацію для обробки персональних даних щодо їх сімейного стану, рівня освіти, сфери діяльності. Отримані результати мають теоретичне та практичне значення, можуть бути використані вченими та практиками для подальшого розроблення цифрових систем з організаційного розвитку.

Ключові слова: інформаційна безпека систем розвитку організації, штучний інтелект в розвитку організації, захист даних організації, захист персональних даних.

Manuscript received: 03.02.2020