Nowoczesne Systemy Zarządzania
Zeszyt 19 (2024), nr 1 (styczeń-marzec)
ISSN 1896-9380, s. 75-88
DOI: 10.37055/nsz/192815

Instytut Organizacji i Zarządzania
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

Modern Management Systems
Volume 19 (2024), No. 1 (January-March)
ISSN 1896-9380, pp. 75-88
DOI: 10.37055/nsz/192815

Institute of Organization and Management
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

Qualitative aspects of Industry 4.0 as a determinant of the improvement of the information security management system

Jakościowe aspekty Przemysłu 4.0 jako determinanta doskonalenia systemu zarządzania bezpieczeństwem informacji

Katarzyna Zawierucha-Kozłowska
War Studies University, Warsaw, Poland
k.zawierucha@akademia.mil.pl; ORCID: 0000-0002-9439-5589

Abstract. Summary of issues and justification for taking up the topic The basic goal of the article is to emphasize the importance of Industry 4.0, which intersects with today's reality. The fourth industrial revolution combines the concepts of classical and digital technologies, using the industrial Internet of Things. Every activity carried out using technology requires an appropriate flow of all types of information to ensure data security. The article also shows the importance of the Information Security Management System, because the amount of data processed using information technology is huge. Nowadays, society systematically shares its data without thinking about the consequences. Increasingly, personal data is equated with currency, as in order to obtain a discount or future financial benefits, data is shared regardless of the consequences. The Information Security Management System requires continuous improvement of organizations processing data about identified or identifiable persons. However, independent verification and consent to data processing are also extremely important.
Keywords: Industry 4.0, Information Security Management System, quality, personal data, management

Abstrakt. Podstawowym celem opracowania jest podkreślenie istotności Przemysłu 4.0, który przenika się z dzisiejszą rzeczywistością. Czwarta rewolucja przemysłowa sprawia, że koncepty technologii klasycznych i cyfrowych łączą się, wykorzystując w swoim działaniu przemysłowy Internet Rzeczy. Każde działanie realizowane za pomocą technologii wymaga odpowiedniego przepływu wszelkiego rodzaju informacji w celu zapewnienia bezpieczeństwa danych. Artykuł ukazuje również znaczenie Systemu Zarządzania Bezpieczeństwem Informacji, ilości bowiem przetwarzanych danych z wykorzystaniem technologii informatycznych są ogromne. Obecnie społeczeństwo bardzo często ujawnia swoje dane, nie myśląc o konsekwencjach.

Coraz częściej dane osobowe utożsamia się z walutą, ponieważ w celu uzyskania rabatu lub przyszłych korzyści majątkowych udostępnia się dane bez względu na skutki. System Zarządzania Bezpieczeństwem Informacji nawołuje do ciągłego doskonalenia organizacji przetwarzających dane o osobach zidentyfikowanych lub możliwych do zidentyfikowania. Niezmiernie ważna jest jednak także samodzielna weryfikacja i zgoda na przetwarzanie danych.
Słowa kluczowe: Przemysł 4.0, System Zarządzania Bezpieczeństwem Informacji, jakość, dane osobowe, zarządzanie

Introduction

The article presents the qualitative aspects of Industry 4.0 in the context of improving the Information Security Management System. The main aim of the article is to draw attention to the growing position of information technologies operating on the basis of all types of information, as well as to indicate the directions of current technological trends taking into account good practices encouraging continuous improvement. It is assumed that information technologies affect the Information Security Management System. The analysis of available literature and empirical research allowed for the creation of recommendations and assessment of the current state of the Information Security Management System in public and private sector entities and the indication of directions of changes in order to increase the quality of processed information using what the fourth industrial revolution has to offer.

The article discusses issues related to the Information Security Management System in public and private sector entities, taking into account the aspects of Industry 4.0 and factors enabling the improvement and continuous increase in the quality of processed data. The justification for choosing the topic of the article and undertaking research in the scope indicated above is the limited number of documents, studies and literature on the described topic and insufficient awareness of people processing the data.

For the purposes of this article, theoretical and empirical methods were used. In terms of theoretical methods, mainly: analysis of available literature, synthesis, inference and analogy. Empirical methods allowed for the verification of the theoretical elements of the article and made it possible to learn the opinions and experiences of individual public and private sector entities regarding the qualitative aspects of Industry 4.0 as determinants of improving the Information Security Management System.

1. Industry 4.0 – the fourth industrial revolution

The term Industry 4.0 is associated with the fourth industrial revolution, also called the fourth generation industry. This means a transition from an industry based on computers and automation of logistics processes to an industry using the Internet and new technologies, which are increasingly integrated into human life.

Industry 4.0 is the next stage of socio-economic changes in the world, which follows breakthrough discoveries defining the framework of previous revolutions (see Table 1).

Table 1. Industrial revolutions

INDUSTRY 1.0 (1st Industrial Revolution)	late 18th and early 19th century	The invention of the steam engine and the development of the machine industry, which began to replace factories and craft production
INDUSTRY 2.0 (2nd Industrial Revolution)	second half of the 19th century	Electricity (electric engine) and combustion engine as two new energy sources; development of mass production
INDUSTRY 3.0 (3rd industrial revolution)	since the late 1960s	The development of electronics and information technology, which resulted in the automation of industry
INDUSTRY 4.0 (4th Industrial Revolution)	postulated since 2011	Systemic use of information technologies, further development of automation, cyber-physical systems, Internet of Things, Internet of Services, smart factories, new generations of robots, etc.

Source: own study based on: Logistics manager, 2019, p. 106

The development of information systems has undoubtedly been and is determined by computer technology, and technological evolution has influenced the modernization of techniques used in information processes, i.e. processing, transmitting and storing information. The creation of IT systems, which is a consequence of the information revolution, has resulted in more processes taking place in organizations or activities carried out every day being supported by IT systems integrating with social media due to the development of IT systems (Szczepaniuk, 2016, p. 59). It is worth noting that these media provide access to all information and become a non-state player influencing the ongoing decision-making processes (Ciekanowski, Nowicka, Załoga, 2018, p. 199).

The turn of the 20th and 21st centuries is an increase in the amount of information generated and processed and the permanent development of technology creating a network infrastructure based on access to data and their exchange, i.e. connecting the IT system with information (Ciekanowski, Nowicka, Załoga, 2018, p. 199).

The industrial revolution focusing its attention on the systemic use of information technologies, which seemed to be the future a few decades ago, is now the present. Smart technology has revolutionized both industry and everyday life. Decisions that were once made only by humans can now be, and often are, made by intelligent machines.

Industry 4.0 technologies can also include (Leidel, 2017, pp. 18-20):

- artificial intelligence;
- additive printing (3D printing);
- digital twin and digitization of production;
- cloud computing;
- Big Data;
- virtual and augmented reality;
- collaborative robots;
- mobile robots;
- RFID;
- mobile interfaces;
- blockchain;
- geolocation.

All subsequent generations of IT systems increase the scope of their operations, becoming more useful and functional. The fourth industrial revolution is leading the way for the society of the future. This means the integration of the above-mentioned IT systems, intelligent machines and systemic changes in production, which will contribute to the increase in the efficiency of production processes and the development of information technology, the aim of which is to reduce human work and perform many activities in a short time, and also to overcome insurmountable barriers and implementation of visualized plans for the future. The fourth industrial revolution also means responsibility for directing the course and development of information technologies.

Information technologies provide easy access to knowledge and culture, and enable more efficient time management by using services without leaving home. Technologies are also intelligent machines that improve things and they take action for people. However, information technologies also facilitate huge data flows within countries and abroad.

However, some industries do not take full advantage of what modern technological development has to offer. This is usually caused by the lack of appropriate qualifications of employees and the so-called industrial policy conditioned by the processing of huge amounts of data. Industry 4.0 is a concept that completely changes the current operating model of both service and industrial enterprises. The fundamental change is the amount of current (existing) data received on an ongoing basis and processed in real time. This change affects the supervision of the state of technological processes (control processes), and in the future it will allow for the estimation of behavior, flexibility of processes and changes in quality parameters. The basic factor proving the limited willingness to completely interfere with technology in the Polish economy is low labor costs, which favors the limited implementation of information technologies. Industry 4.0 is implemented when organizations are adapted to changes and when it is an economically profitable process (Bondyra, Zagierski, 2019, p. 10).

Both micro, small and medium-sized enterprises operating on the Polish market are often not sufficiently developed to implement modern solutions, including the automation of processes implemented by the organization. Currently, employees of the organization who manage the organization and are responsible for its profits must acquire skills in programming processes, creating system documentation (procedures, instructions, etc.) and transmitting instructions to the machines and devices involved. Taking a supervisory position in the case of previously implemented processes may result in dissatisfaction, mainly in the case of employees with significant generational differences. It seems justified to involve employees willing to implement changes and further technological development of the organization, because "Industry 4.0 is, above all, evolution" (Błasiak, 2018).

An additional element influencing changes in modern organizations is the IT infrastructure, and thus the system that must handle integrated organizational processes involving machines, devices and robots. Another important aspect is logistics, i.e. supply chain management involving all processes from the moment the customer places an order to the delivery of the product or service and the settlement of this transaction (Bondyra, Zagierski, 2019, p. 10).

The idea of Industry 4.0 indicates that the efficient operation of an organization's business models depends on the mutual cooperation of technological solutions and those appropriate for traditional business development. The use of modern digital technologies will allow to connect and manage your enterprise in an optimal way. Additionally, the development factors of Industry 4.0 include (Bondyra, Zagierski, 2019, p.10):

- increase in investment processes enabling the transformation of business models into an integrated environment;
- increased awareness of the future benefits resulting from the implementation of the idea of Industry 4.0 at the level of various types of organizations;
- effective supply chain management and properly correlated with the production process;
- competent, properly educated and trained IT staff who constantly improve their skills;
- change in lifestyle, profile and mentality of consumers, which will affect enterprises;
- meeting customer expectations in terms of modern technological solutions;
- increase in economic profitability resulting from the solutions offered by Industry 4.0;
- changing the model of the country's industrial policy,
- focus on promoting solutions in the field of Industry 4.0;
- the influence of research institutions and universities on the creation of modern solutions for implementing ideas characteristic of Industry 4.0.

Industry 4.0, from a technological perspective, is part of a complex of new and constantly developing technologies creating current and future changes. Technological innovation enables the use of modern management and information processing methods, which are an inherent element of modern times. It is also worth noting that Industry 5.0 is being mentioned more and more often, which focuses on a more advanced use of human skills with intelligent systems and the technological potential of the created robots.

The ongoing changes characteristic of both industries undoubtedly pose a huge challenge to the integration of IT and technological systems. Because artificial intelligence, robotics, development of IT systems and the Internet of Things must work harmoniously. The philosophies of both industries involve collecting and processing huge amounts of information. Therefore, it is necessary to maintain data security and protect against cyberattacks.

2. Adapting the organization to the economic requirements of Industry 4.0

The ongoing industrial revolution is changing the foundations of how companies operate, their processes and organizational structures. Many employees are replaced by artificial intelligence or automated machines and devices, but in order to create contemporary and future competitive advantages, it is necessary to increase innovation. However, the possibilities of enterprises to adapt to the changing guidelines for competing in terms of innovation are different, as are the types of technologies used that are characteristic of Industry 4.0 (see Figure 1).

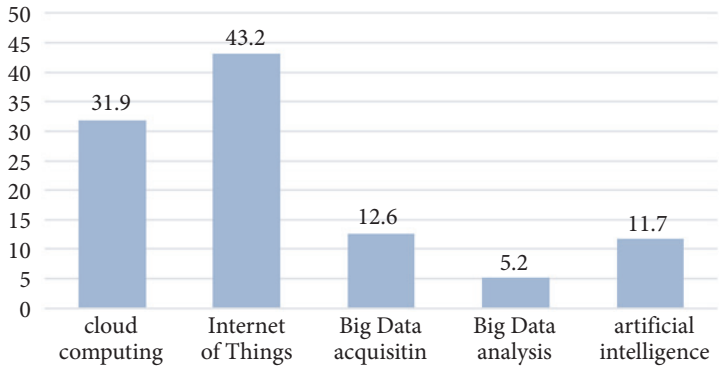

Fig. 1. Enterprises using technologies typical of Industry 4.0 (in % of surveyed enterprises)
Source: own study based on: GUS, 2023

Analyzing Figure 1, it should be noted that the most frequently used technology typical of Industry 4.0 among enterprises is the Internet of Things, which is used in many processes (43.2%). Research conducted by the Central Statistical Office showed that cloud computing is used by 31.9% of the surveyed organizations. 12.6% of respondents obtain Big Data data, but only 5.2% of them analyze it, which indicates that the acquired data is only stored by organizations and does not serve a higher purpose. In turn, artificial intelligence, i.e. intelligence demonstrated by artificial devices, was used by 11.7% of enterprises.

Research conducted among Local Government Units (LGUs) regarding the use of modern technologies is presented in Figure 2. These studies took into account the responses of respondents from various units located in Poland. The diagnostic survey method was carried out using a survey questionnaire. The results obtained from the conducted research allowed us to determine the extent to which local government units use the indicated digital technologies:

- employee working time monitoring systems;
- cloud computing;
- video monitoring;
- biometric gateways (face recognition system);
- monitoring systems for entrances to specific rooms;
- settlement and recording systems;
- fingerprint readers;
- systems for reporting irregularities;
- devices, applications and platforms using the Internet of Things;
- technologies that provide Internet services;
- profiling systems;
- monitoring of e-mail IT systems;
- monitoring of IT systems and software used;
- website monitoring;
- access cards;
- identity verification for access control.

Local government units most often use technologies that provide Internet services. 75% of respondents answered yes. 64% of local government units use video monitoring, and 54%, i.e. more than half of local government units, use monitoring of IT systems and software used in their activities. Many organizations also use website monitoring (43%) and e-mail IT system monitoring (40%). It should be noted that all technologies highlighted in the survey question are used by local government units. However, entities use biometric gateways (1%), profiling systems (3%) and devices, applications and platforms using the Internet of Things the least frequently.

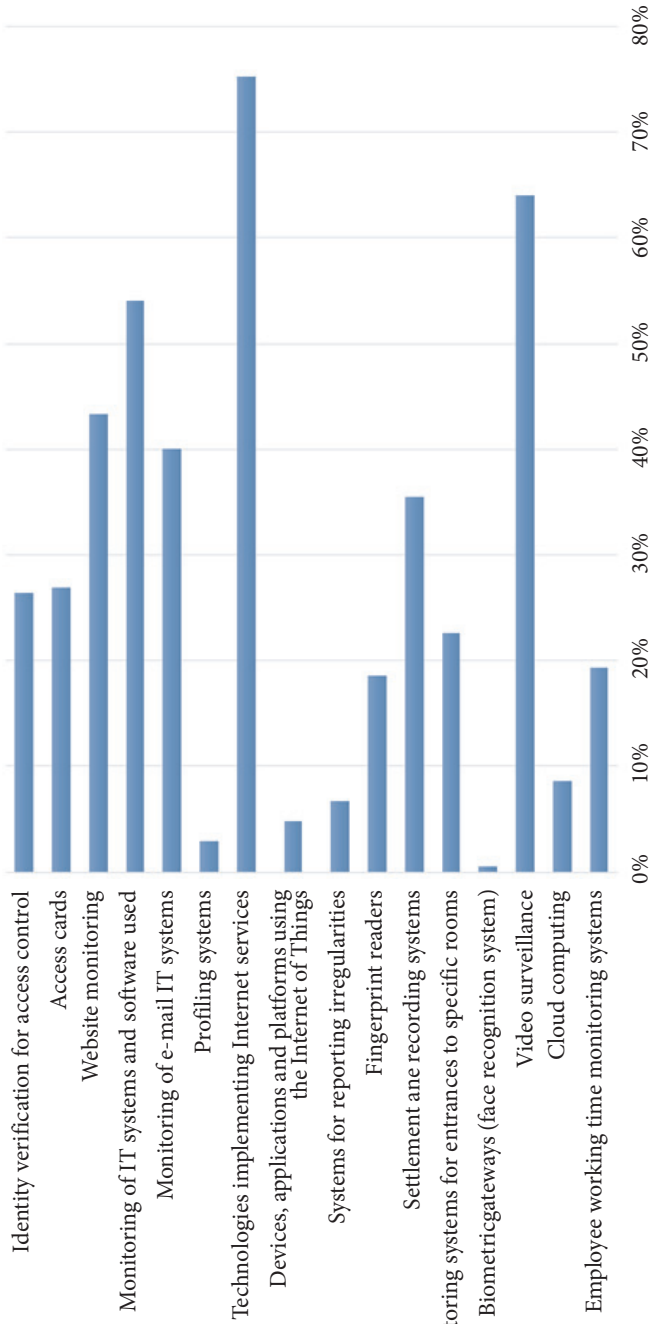

Fig. 2. Types of information technologies used by local government units

Source: own study based on: Zawierucha, 2022

It is worth noting that Internet of Things, which is the most frequently used technology typical of Industry 4.0 for the surveyed enterprises, is the least frequently used technology for local government units. The discrepancies may result from differences taking into account the diversity of processes implemented or the level of technological advancement in the indicated organizations. Therefore, we can see greater interest in technology or greater possibilities of using technology in enterprises compared to public entities. An additional advantage of enterprises may be better trained and qualified staff representing technological branch and expenditure on technology development (see Figure 3).

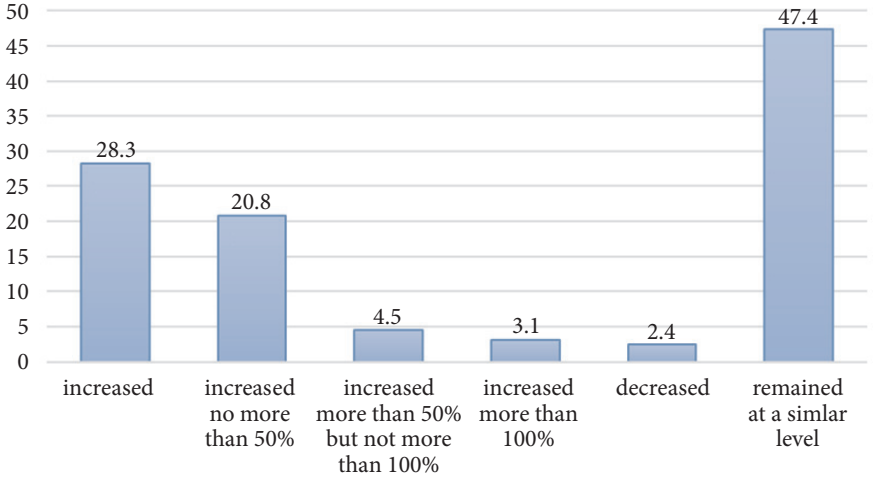

Fig. 3. Level of expenditure on Industry 4.0 technologies (in % of surveyed enterprises)
Source: own study based on: GUS, 2023

Research indicates that changes in the level of expenditure on modern technologies have increased in terms of the implementation, maintenance and expansion of Industry 4.0 (28.3%). The largest share falling within the scope of the described group of enterprises falls on units in which the level of expenditures in the examined period increased by no more than 50%, and the smallest among units in which the level of expenditures increased by more than 100% (20.8% and 3.1%, respectively). 47.4%, i.e. almost half of the surveyed enterprises, kept their investment expenses at a similar level.

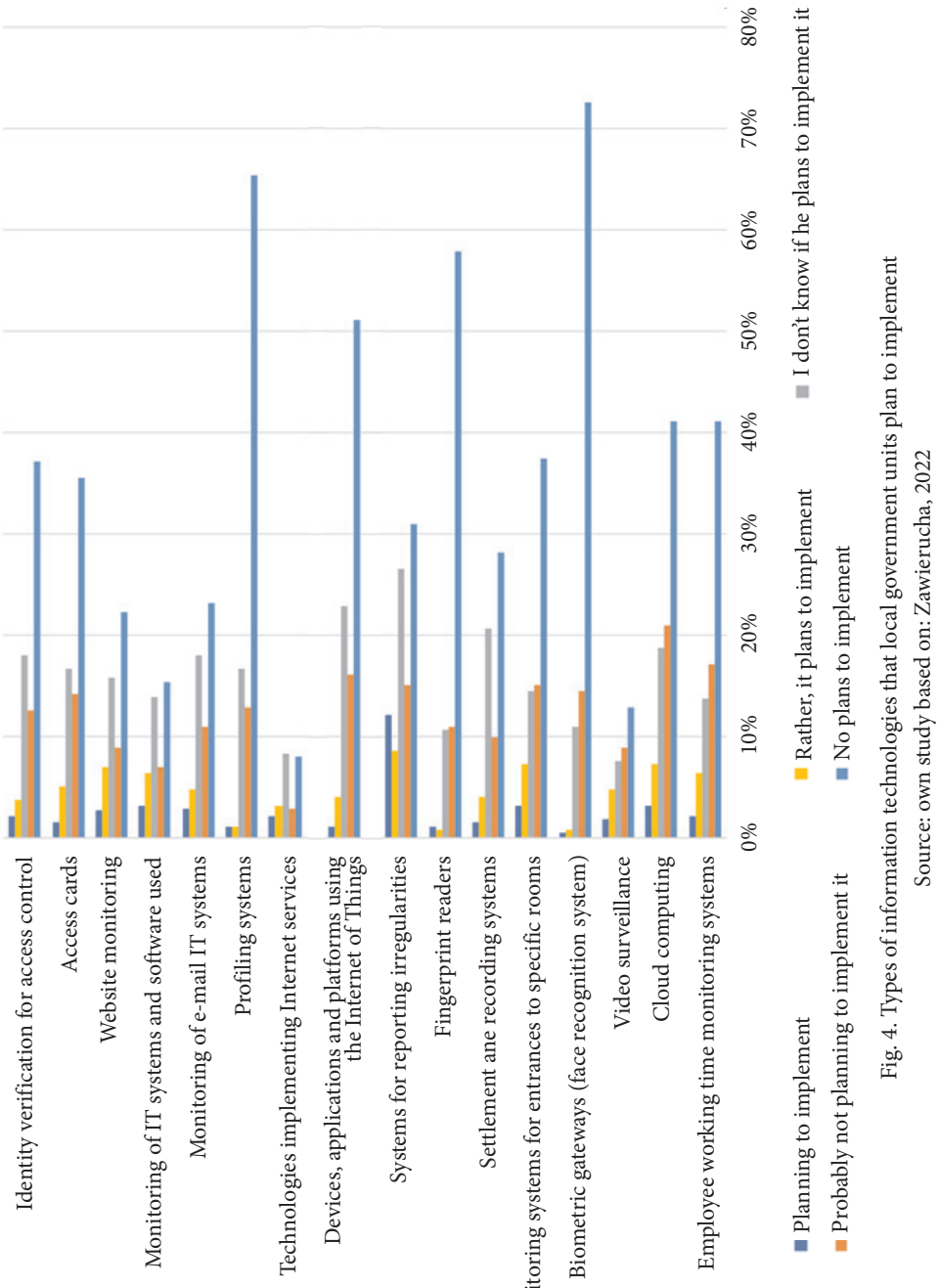

Fig. 4. Types of information technologies that local government units plan to implement
Source: own study based on: Zawierucha, 2022

Local government units indicated that the most likely implementation plans are related to systems for reporting irregularities (related to e.g. corruption or lobbying companies). 20% of respondents plan or rather plan to implement the mentioned technology. In turn, 10% of respondents are willing to implement the following technologies: cloud computing, systems for monitoring entrances to specific rooms and website monitoring. The vast majority do not plan or rather do not plan to implement biometric gateways (88%), profiling systems (78%), fingerprint readers (69%), devices, applications and platforms using the Internet of Things (67%), cloud computing (62%) , systems monitoring entrances to specific rooms (52%) and identity verification for access control (50%).

Research shows visible differences between enterprises and public organizations in terms of interest in modern technologies. It should be noted, however, that the continuous development and increasing importance of technologies representing Industry 4.0 means that both private enterprises and public institutions are obliged to implement activities based on information technology. It is reasonable for organizations to implement their processes using what modern technological progress offers, in order not to be digitally excluded and to build a competitive advantage. Very often, changes taking place in the processes implemented by organizations are conditioned by the obligation, for example, to submit documents electronically. Therefore, a large amount of data processed using technology must be properly secured, which is handled, among other, by: Information Security Management System (ISMS).

3. Relevance of ISO 27001

Information is one of the most valuable assets of an organization, therefore ensuring its security should be a priority for enterprises, regardless of the type of business activity. The implementation of the ISO 27001 standard (Information Security Management System) guarantees the most comprehensive method that ensures the quality of processed data.

Most organizations have their own control mechanisms, which should be effective in order to be able to implement all the provisions of the General Data Protection Regulation (GDPR). Thanks to appropriate safeguards, the organization's stakeholders can be sure that their data is properly processed. However, proper information security management must demonstrate conscious controls that are effective and provide real protection of IT resources.

The implementation of the ISO/IEC 27001 standard ensures high-quality aspects of threat identification and the introduction of appropriate safeguards to protect against information security breaches. These safeguards can be developed based on the organization's experience, effectively conducted risk analysis and practices used

by other enterprises. The ISO 27001 standard (ISO/IEC 27001) is an international standard that standardizes (normalizes) Information Security Management Systems. This standard presents requirements for the establishment, implementation, maintenance and continuous improvement of an Information Security Management System. The ISMS also contains guidelines for estimating and dealing with information security risks (Resilia, 2022).

The areas of the ISO 27001 standard affecting information security include the following:

- organizational security area;
- people security area;
- physical security area;
- technological security area.

The comprehensive nature of the standard means that there are many benefits from its implementation. The most important of them include (Resilia, 2022):

- maintaining data privacy and integrity;
- ensuring that information is adequately protected;
- strengthening the organization in the event of various types of incidents;
- increased awareness of the organization's employees about threats and the obligation to use important safeguards;
- meeting the expectations of stakeholders and meeting these expectations;
- meeting legal requirements;
- increase in competitive position;
- supervision of data processing processes;
- increase in the quality of services;
- avoiding financial losses resulting from data breaches;
- increased credibility and trust of the organization's stakeholders.

Information security management and personal data protection aims to minimize the risk of theft, negative use of data or loss of data. Increasing the security of information and personal data is a series of activities aimed at determining procedures for securing data and information. Qualitative standards that constitute determinants of ISMS improvement include:

- procedures;
- organization policy;
- operating instructions;
- audits;
- services of a personal data protection inspector;
- social engineering tests;
- training;
- security measures used;
- risk analysis.

These possibilities are additionally complemented by knowledge obtained from international standards, relevant acts and GDPR. Information Security Management System – ISMS, operating on the basis of international standardizing standards, indicates the model of the continuous improvement cycle (PDCA) in accordance with the concept of W.E. Deming (Wołowski, Zawiła-Niedźwiecki, 2012, p. 35):

- Plan – plan, establish an ISMS;
- Do – act, implement and establish an ISMS;
- Check – check, monitor and review the ISMS;
- Act – perform, maintain and improve the ISMS.

In its principles, the continuous improvement cycle strictly refers to quality management and involves using the right approach to implementing specific activities. It can therefore be used to improve the Information Security Management System.

Information, including personal data, penetrates IT systems regardless of geographical, cultural or political boundaries. Christopher Kuner very aptly compares the contemporary flow of information in an IT system to "liquid in a pipeline system", leading to positive and negative consequences on many levels, e.g. in the individual sphere (meeting individual needs), in the social sphere (e.g. issues related to freedom statements), corporate, medical or official spheres (Kuner, 2013, p. 102).

A system based on ICT means that the data obtained and transmitted, as well as information management, enable the achievement of specific goals important for the organization. Achieving goals is effective if companies use appropriate safeguards to limit the negative impact of modern technologies. The use of appropriate standards in the use of technology will enable the organization to operate efficiently and contribute to its development.

Conclusions

The Information Security Management System is a comprehensive approach to data security, which is why organizations should strive to implement the ISO 27001 certificate. Digital progress, including modern business practices and Industry 4.0, are becoming more and more popular. The implementation of all the requirements of the standard makes it possible to accept and influence the next industrial revolution. The dependence of process implementation on digital technologies makes it necessary to carry out more detailed controls and introduce protections against highly advanced information security threats. Organizations should strive to build their own competitive position, which depends on the security measures used. Business continuity is also a value provided by the ISMS.

More and more organizations decide to implement the ISO 27001 certificate, which certifies the high-quality implementation of all activities related to the identification of threats and the introduction of appropriate safeguards to protect against

information security breaches. Unfortunately, this mainly applies to manufacturing or service companies. The number of implemented certificates for compliance with the ISO 27001 standard in the public administration sector is small compared to other sectors.

It is important to understand the following changes and their impact on the organization. Only knowing the positive aspects and fighting the negative aspects of digital technologies can lead to the appropriate level of information security. The use of good practices and the implementation of standards from the 27000 family will ensure the continuity of the organization's operation and its improvement.

REFERENCES

[1] Błasiak, M., 2018. Ekspert PwC w dziedzinie automatyki i cyfryzacji przemysłowej, *Magazynowanie i Dystrybucja*, No. 4.

[2] Bondyra, K., Zagierski, B., 2019. *Przemysł 4.0. Na jakim etapie przemysłowej rewolucji znajduje się województwo wielkopolskie*, Poznań: Wielkopolskie Regionalne Obserwatorium Terytorialne, http://wrot.umww.pl/wp-content/uploads/2019/10/Przemys%C5%82-4.0.pdf (access: 20.01.2024).

[3] Ciekanowski, Z., Nowicka, J., Załoga, W., 2018. Komunikacja strategiczna w naukach o zarządzaniu i jakości oraz w naukach o bezpieczeństwie, *Zeszyty Naukowe Wyższej Szkoły Zarządzania Ochroną Pracy w Katowicach*, nr 1(14).

[4] GUS, 2023. Wypracowanie metodologii oraz badanie stopnia dostosowania wybranych przedsiębiorstw do wymogów gospodarczych, jakie stawia czwarta fala rewolucji przemysłowej (Przemysł 4.0), Warszawa: Główny Urząd Statystyczny, https://stat.gov.pl/files/gfx/portalinformacyjny/pl/defaultaktualnosci/6337/13/1/1/streszczenie_przemysl_4.0.pdf (access: 20.01.2024).

[5] Kuner, Ch., 2013. *Transborder Data Flows and Data Protection Privacy Law*, Oxford: Oxford University Press.

[6] Leidel, S., 2017. *Kluczowe technologie*, [in:] Mychlewicz, C., Piątek Z. (Eds.), *Od Industry 4.0 do Smart Factory. Poradnik menedżera i inżyniera*, Warszawa: Siemens, https://publikacje.siemens-info.com/webreader/00085-001733-od-industry-4-0-do-smart-factory-poradnik-menedzera-i-inzyniera/index.html#p=1 (access: 20.01.2024).

[7] Resilia.pl, 2022. *Co to jest norma ISO 27001 i dlaczego jest tak ważna dla organizacji?*, https://resilia.pl/blog/iso-27001-czym-jest-jakie-daje-korzysci/ (access: 20.01.2024).

[8] Szczepaniuk, E., 2016. *Systemy informatyczne zarządzania w społeczeństwie informacyjnym*, [in:] Szczepaniuk, E., Gawlik-Kobylińska, M., Werner, J. (Eds.), *Bezpieczny rozwój społeczeństwa informacyjnego*, Warszawa: Akademia Sztuki Wojennej.

[9] Wołowski, F., Zawiła-Niedźwiecki, J., 2012. *Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi*, Kraków–Warszawa: edu-Libri.

[10] Zaskórski, P., 2008. Zarządzanie zasobami informacyjnymi w firmie, *Biuletyn WAT*, vol. LVII, nr 4.

[11] Zawierucha, K., 2022. *The use of information technologies in the protection of personal data* [doctoral dissertation], Warszawa: Akademia Sztuki Wojennej.