ECONOMIC ASPECTS OF ANALYSIS OF OCCURRENCE OF INCIDENTIAL EVENTS ON THE SCOPE OF SECURITY OF INFORMATION IN A PRODUCTION ENTERPRISE

doi:10.2478/mape-2018-0069
Date of submission of the article to the Editor: 03/2018
Date of acceptance of the article by the Editor: 07/2018

MAPE 2018, volume 1, issue 1, pp. 545-552

Eng. Żywiołek Justyna, PhD
Częstochowa University of Technology, **Poland**

Abstract: This article presents structure and analysis of possible events for information security of a production company. The aim of the analysis is to identify incident events, their time and frequency. The analysis includes occurrence of notifications, threatening events, employee errors and false alarms. Also, the conducted research takes into account the functions performed in the enterprise. For these events, a daily distribution of events and statistical analysis of their occurrence were developed. Thanks to the analysis of the phenomena in time, enterprises can introduce actions preventing the occurrence of incidents. The conducted research has shown that employees report incidents which, in their opinion, constitute an incident, which greatly facilitates the work of the information security administrator. These events are analyzed and classified accordingly. The analysis showed that most events take place between midnight and two in the morning. The conducted analysis is a pilot study carried out in one large enterprise in the metallurgical industry.

Keywords: analysis of phenomena in time, information security, incidents

1. INTRODUCTION

Situations threatening information security may occur at any time and in any place. This means that enterprise is a place of potential threats, activated due to the unfavourable changes in space. The purpose of this analysis is to show the periods of probability of potentially incidental events. The study was carried out on the basis of data provided by the metallurgical and multi-faculty enterprise.

Man's natural aspiration is to ensure the safety of himself and his surroundings. Every person, a work or social group that takes action to influence the environment in this way to eliminate all dangers ensures safety (Żywiołek, 2016, Ulewicz et al., 2013). Situations threatening the life and health of a human being can take place at any time and in any place have the nature of threats. Therefore, every person lives in an environment of potential and possible threats that may occur as a result of adverse changes. The level of security is a component of many elements that can occur in specific situations, individually or in certain combinations (Szymonik, 2010). One of the elements that affect the security of an enterprise is information management. Effective and efficient information management in crisis situations can be carried out by organizing them in a correct manner.

2. INFORMATION IN COMPANY

Management is a special way of managing the enterprise's resources. It boils down to organizing, creating an adaptation of rules of conduct for the needs of the enterprise in order to optimally function and develop as well as to control the application of developed and implemented rules (Wołowski and Zawiła-Niedźwiecki, 2015). On the other hand, information security management is a process used to achieve an adequate level of confidentiality, integrity, availability, authenticity, accountability and reliability that represent information

properties (Żywiołek, 2017). For information security management purposes, organizations prepare and create an information security management system. It is part of a comprehensive management system. This part of the system is based on the approach resulting from business risk, and refers to the establishment, implementation, operation, monitoring and improvement of information security (Zou et al., 2017). The system has an organizational structure, policies, planned activities and even the responsibilities of individual employees. Security management includes various projects, the most important of which are (Pawełoszek, 2014):

- defining goals, strategies and policies as well as information security needs in the enterprise,
- identifying and analyzing threats to enterprise resources,
- identifying and analyzing risk,
- specification, monitoring, implementation and operation of safeguards,
- raising awareness of information security needs,
- analysis of the occurrence of phenomena in time,
- detecting incidents and responding to them.

Elements of the information security management process: resources, threats, risks, vulnerabilities are elements that affect the process of managing information security in an enterprise (Skowron-Grabowska and Lenort, 2015, Anttila and Jussila 2018). Effective management of resources in the organization in the presence of various threats and incidents leads to the achievement of the required level of information security (Lemańska-Majdzik and Smoląg, 2016).

To analyze the phenomena in time it is useful to estimate the number of information and categories of information we are dealing with. The company under investigation belongs to a group of production enterprises, classified as large. The amount of information processed by them is shown in Figure 1.

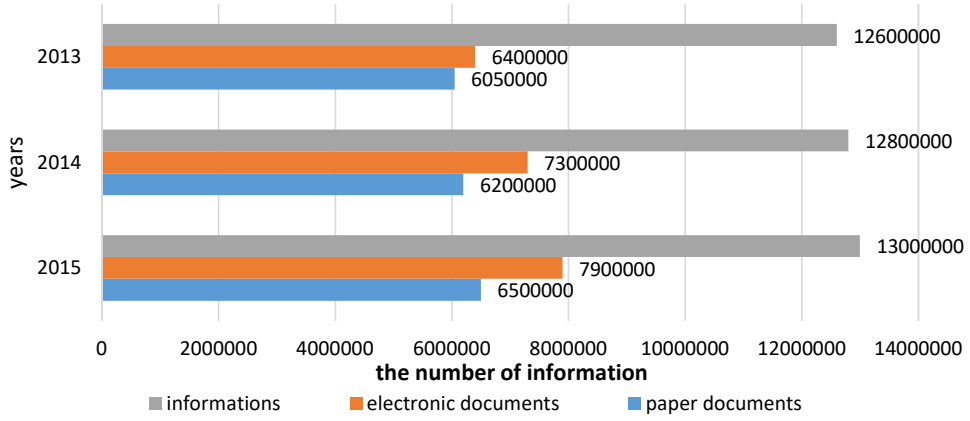

Fig. 1. Number of information processed in the surveyed enterprise

It can be noticed that in the examined enterprise in the subsequent years the amount of information processed increases. The number of electronic documents also increased considerably during the period under consideration. Understanding the necessity of using the information value stream mapping also requires getting acquainted with the type of information processed (Figure 2).

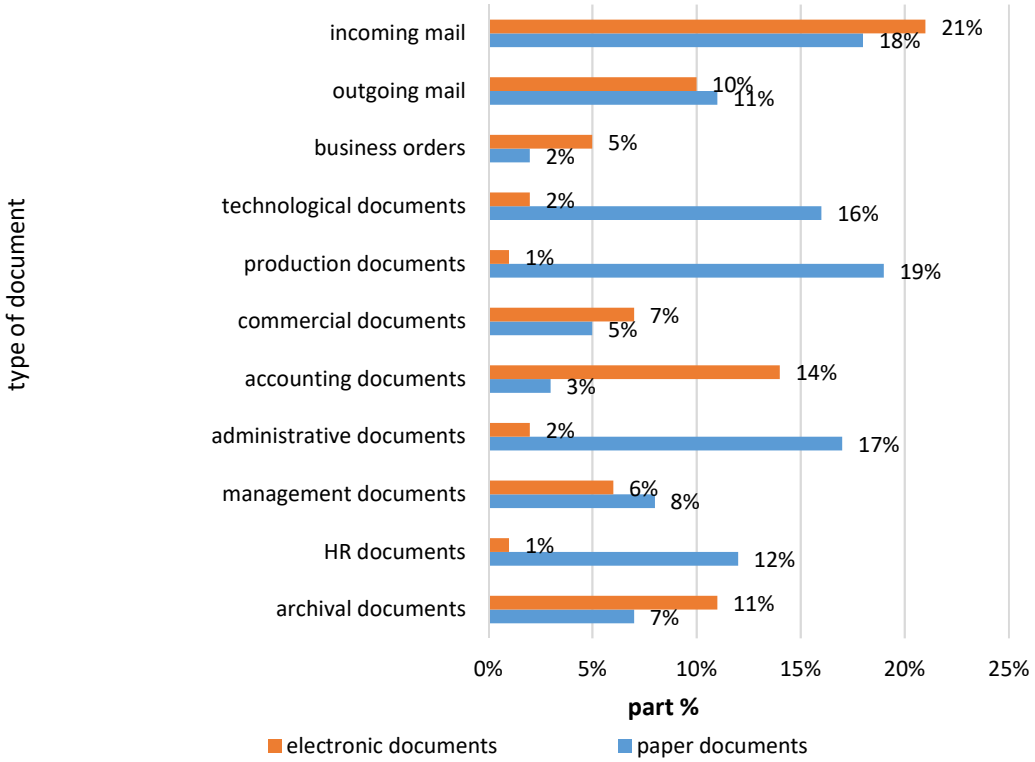

Fig. 2. The type of information processed in 2015 together with the division of the form of the record

An increasing number of documents are processed in the surveyed enterprise. It is particularly difficult to create proper document flows with two possibilities of information processing. The process of creating correct workflows of documents is labor-intensive, however, it allows easier access to a given document only to the employees to whom this document applies. The creation of correct document and information flows can be facilitated by the method of value stream mapping.

3. OCCURRENCE OF POSSIBLE EVENTS

For information security, there has been created a hierarchy of events which may appear in the company's both global and internal environment (Nowicka-Skowron and Ulewicz, 2015, Pacana and Ulewicz 2017). They may also threaten human, his surroundings, or even the whole company. The structure of the occurrence of particular types of events divided into months is presented in Figures 3, 4 and 5. Figure 3 describes the occurrence of events threatening information security, while Figures 4 and 5 illustrate in detail the physical and IT threats.

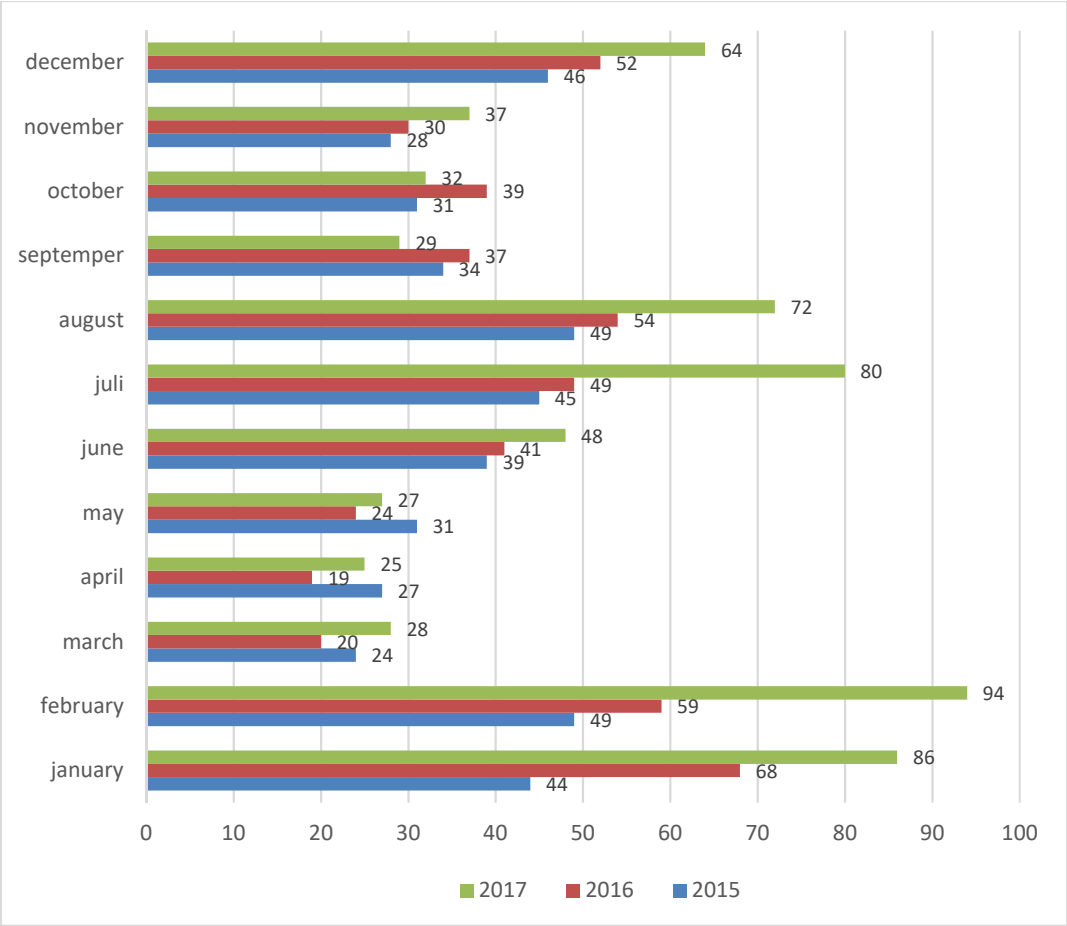

Fig. 3 Reporting events that threaten information security

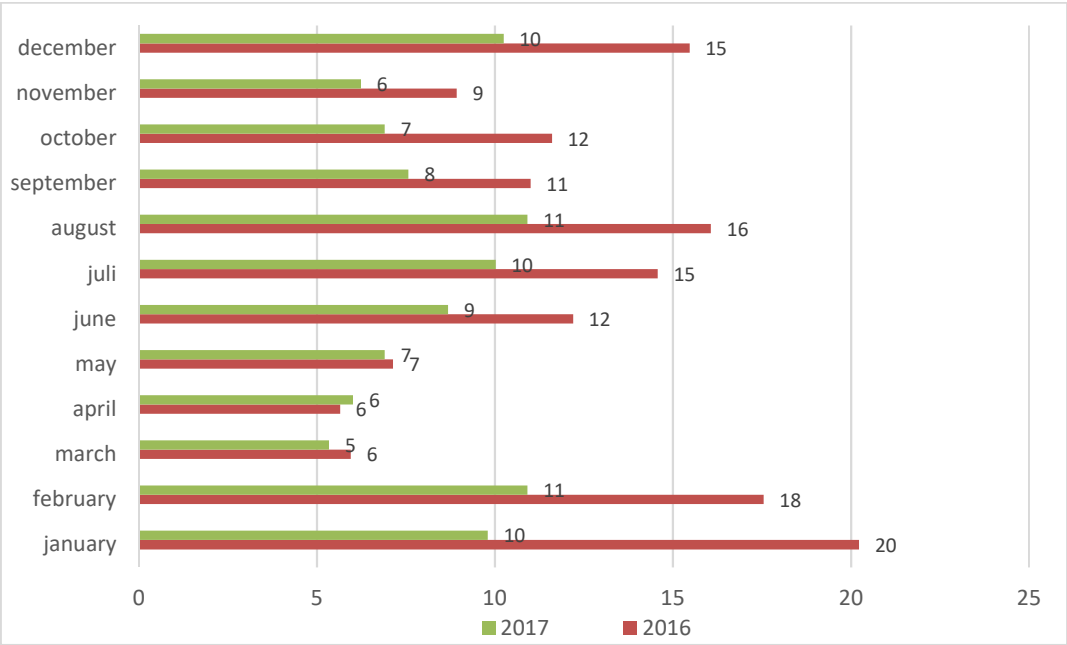

Fig. 4 Real physical threat by months

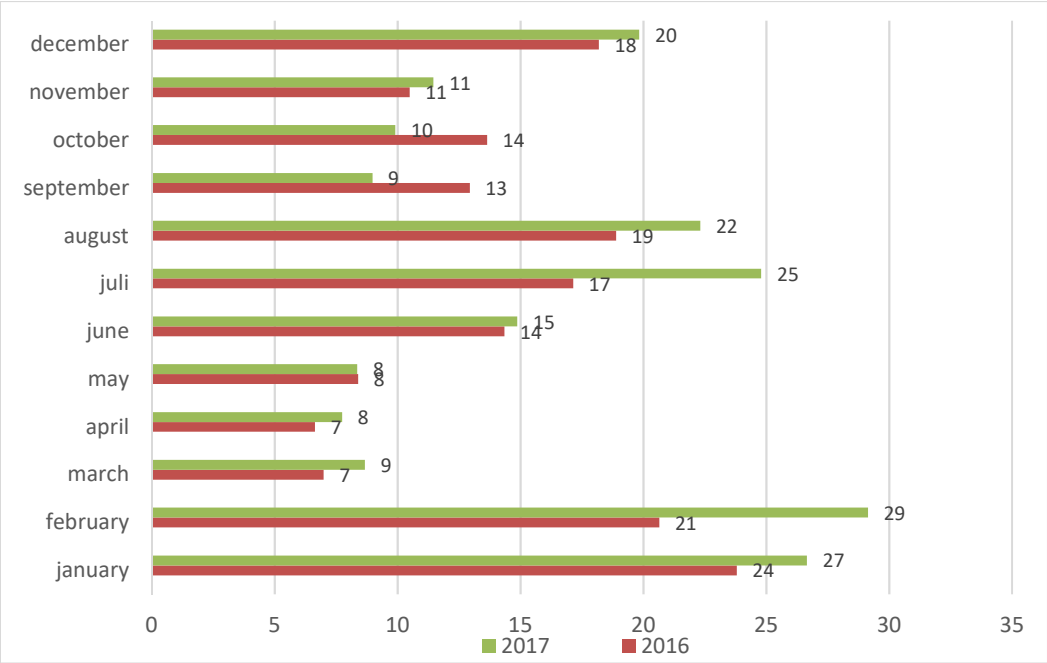

Fig. 5 Real IT threat divided into months

Analysis of Figure 5 proves that during the holiday season and in the months of January, February and December, the occurrence of the largest number of situations threatening the security of information can be noticed. It is related to the holiday period, winter breaks and festive seasons, during which employees often replace each other without paying much attention to the information security. In the months with the lowest intensity of information security threats their number decreases at least several times. In July and August, it ranges from 20% to 25% in the studied period. When it comes to physical threat, there is a large variation in the number of events in particular months in the considered period. July, August, December, January and February are the periods of the most frequent occurrences of physical and IT threats. It is in these months that more than half (64.2%) of the total number of threats is created. The difference between the largest and the smallest number of incidental situations in the month is very large: in February it reaches 18.6%, while in March only 2.7%. Analyzing the data of the total number of events in particular months, it can be concluded that the majority of events falls on February, July and August. The most peaceful months are March, April, May. The period of low activity of the occurrence of events could be used for:

- familiarization with possible threats;
- conducting exercises to protect from threats;
- staff training;
- IT system tests.

The diversity of the occurrence of the largest and smallest numbers of local hazards in different periods could be used to analyze events including division into days of the week and the function fulfilled in the enterprise (Figure 6).

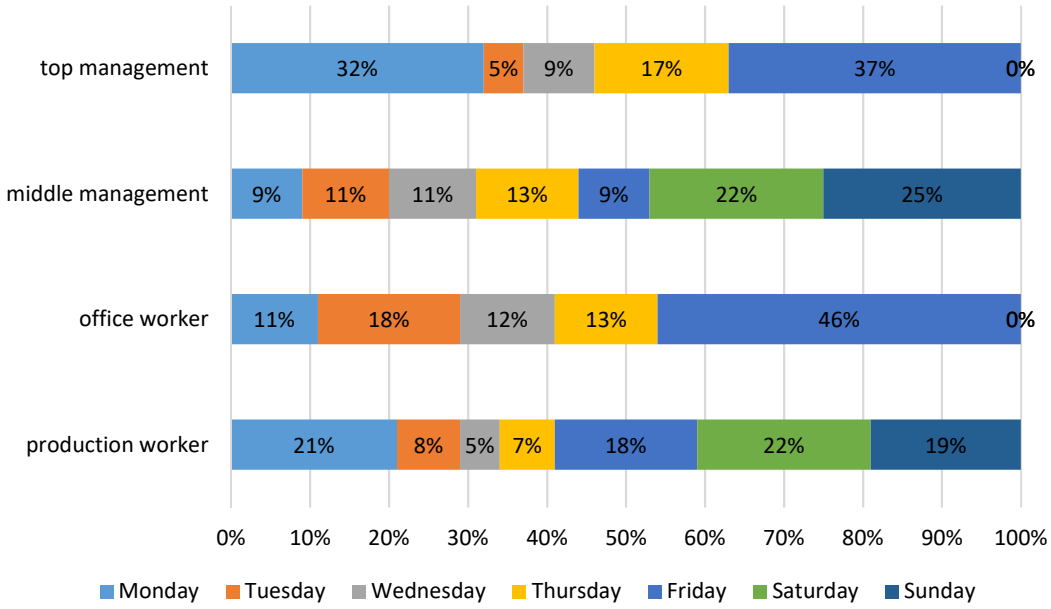

Fig. 6 Occurrence of threats on individual days including the function performed in the enterprise

The analysis shows that middle-level executives make the most mistakes on Fridays, as do office workers, which is caused by the five-day mode of working and fatigue at the end of it. Top executives usually make mistakes on Mondays and Fridays. The increase in the number of errors on Monday is associated with the board meetings, commonly carried on this day of the week. Additionally, the management rarely uses IT profiles requiring changing the password every 30 days, which brings problems to the management. Therefore, situations threatening the IT system are then demonstrated (Szczesniak et. al., 2018).
The daily schedule of reports presented Figure 7 may help in planning the activities of the examined enterprise and in preventive activities.

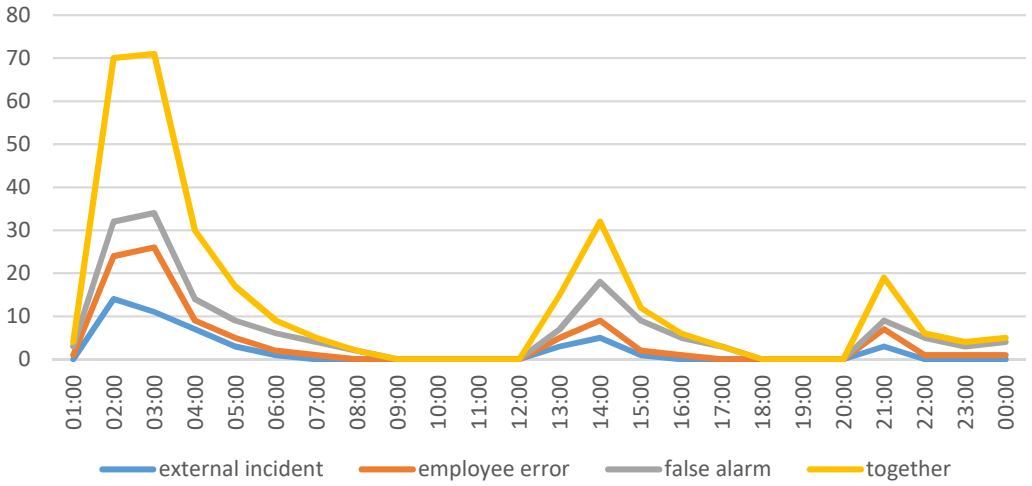

Fig 7. Daily distribution of events for the period 2015 – 2017

For individual types of events, the most commonly used measures in the statistical analysis were calculated (Pietraszek et al., 2014): arithmetic mean, standard deviation, coefficient of variation, quartiles and Pearson's correlation coefficient (Liderman, 2012).
The calculations for the remaining possible events are described in Table 2.

Table 2.
Values of calculated statistical measures used to determine the structure of the occurrence of events over time

	max	min	The arithmetic mean	The standard deviation	The coefficient of variation
Reporting events	18	0	3.91	3.72	0.95
Real events	2	0	0.25	0.21	0.84
Employee error	6	0	0.58	0.46	0.79
False alarm	6	0	1.125	1.052	0.94

Source: Preparation based on (Jóźwiak and Podgórski, 2006).

The values of standard deviation and variability coefficient show that the daily distribution of the number of false positives is the most diversified. Their average number over five years is 1.125 applications in one hour, with the maximum of 12 reports falling from 1:00 to 02:00 a.m., while the minimum equal to 0 is from 10:00 to 02:00 p.m.. False alarm type reports have the highest correlation coefficient between their number and the total number of reports, and reach 0.94. The hours at which the most false alarms should be expected are 00:00 to 04:00. Similarly, the hours when applications will be relatively less are between 02:00 and 04:00 p.m., and 06:00 and 09:00 p.m.

By analyzing in a similar way the data on employee errors, it is possible to obtain information that the dispersion for these applications is high (coefficient of variation equal to 0.79). During the period from which the data were collected, an average of 0.58 applications per hour occurred. The most, i.e. 6 reports were recorded between 01:00 and 02:00, while for the smallest number of events reporting employee errors, these data are dispersed within 24 hours.

In turn, real events constituting threats to information security, of which 0.25 per hour on average in the analyzed period, are poorly correlated with the total number of applications. This allows to state that the more applications are made, the smaller percentage of them will be real threatening events. Analyzing the daily distribution of applications, one could conclude that the maximum number of recorded events is 2. The largest percentage was recorded between 6:00 and 8:00 p.m.. During the night hours between 00:00 and 02:00 there can also be noticed a small amount of this type of events. In other hours, events threatening information security are not noticed.

4. CONCLUSION

The analysis indicates that the majority of events threatening the information security of the examined enterprise occurs in January, February and during the holiday period. The information about physical IT events, with the highest frequency of such events, occurs in a similar period as general occurrences. For employee errors and false alarms, a daily distribution of events was also performed. This distribution in dicated that the occurrence of these events intensifies especially during the night shift. Statistical analysis was also carried out for individual types of events. Maximum occurrence of real events, employee errors and false alarms appears between 00:00 and 02:00, whereas the minimum depends on the type of the event. The distribution of events, which include division into days of the week and the function performed in the enterprise, indicates that office employees, middle and senior managers make mistakes in a similar period of time. On the other hand, production workers commit a similar number of errors throughout the week.

From an economic point of view, the lack of analysis of events in time often leads to repeated information incidents. This analysis allows to determine periods of work in which employees make mistakes or intentionally provide information to unauthorized persons.

The reason for the research was the previous numerical analysis regarding the occurrence of information security threats. Their repeatability led to the analysis of events in time.

Establishing, for example, that office workers repeatedly make mistakes on Friday afternoons in connection with sending data on the amount of scrap delivered, are confused with the size of delivery. It orders the creation of a file facilitating work and setting another day for sending data. Thanks to the improved information security, other customers will not know the amount of scrap delivered by competitors, the work of accounting will be simplified and the company's image will improve.

REFERENCES

Anttila, J. and Jussila, K. (2018). Organizational learning in developing the integrated quality management. Production Engineering Archives, 18, pp.3–13. [online] Available at: http://dx.doi.org/10.30657/pea.2018.18.01. [Accessed 30 Jun. 2018].

Brendziel-Skowera, K. and Turek, T. (2015). The Prospects of E-commerce in Poland. Procedia Computer Science, Vol. 65, pp. 1114 – 1123.

Grodzki ,G. and Piech, H. (2017). Audit Expert System of Communication Security Assessment. Procedia Computer Science, [online] Available at: https://www.sciencedirect.com/science/article/pii/S1877050917315454, [Accessed 30 Jun. 2018].

Ingaldi, M. and Dziuba, Sz.. (2016). Market of the Organic Products in Poland According to Potential Customers. 16th International Multidisciplinary Scientific GeoConference, Sodia, p 67.

Jędrzyjczyk, W. and Kucęba, R. (2016). Teaching Managerial Competences at Universities. Trends of Management in the Contemporary Society, Brno, pp. 126-138.

Jóźwiak, J. and Podgórski, J. (2006). Statystyka od podstaw. Warszawa: PWE, pp. 114.

Lemańska-Majdzik, A. and Smoląg, K. (2016). Role and Importance of Fanpage in Promotion of Products and Services. In: The Economies of Balkan and Eastern Europe Countries in the Changed World (EBEEC 2016), Split, Chorwacja.

Liderman, K. (2012). Bezpieczeństwo informacyjne. Warszawa: PWN, pp. 163.

Nowicka-Skowron, M. and Ulewicz, R. (2015). Quality management in logistics processes in metal branch. TANGER Ltd, pp. 1707-1712.

Pacana, A. and Ulewicz, R. (2017). Research of Determinants Motiving to Implement the Environmental Management System. Polish Journal of Management Studies (16)1, pp. 165-174.

Pawełoszek, I. (2014). Semantic Organization of Information Resources for Supporting the Work of Academic Staff. Annals of Computer Science and Information Systems. [online] Available at: https://annals-csis.org/Volume_2/pliks/320.pdf, [Accessed 8 Apr. 2018].

Pietraszek, J., Gądek-Moszczak, A. and Torunski, T. (2014). Statystyka, aplikacja przemysłowa, system zapewnienia jakości, zliczanie błędów. Adv. Mat. Res.-Switz, pp. 139.

Skowron-Grabowska, B. and Lenort R. (2015). Production of Steel and Environmental Requirements. TANGER Ltd., Ostrava, pp.31.

Szczesniak, B., Midor, K. and Zasadzien, M. (2018). A Concept of an IT Tool for Supporting Knowledge Transfer Among Facility Maintenance Employees as Part of Intelligent Organization. Intelligent Systems In Production Engineering And Maintenance (ISPEM 2017), Advances in Intelligent Systems and Computing, 637, pp. 3-12.

Szymonik, A. (2010). Logistyka w bezpieczeństwie, Warszawa: Difin, pp. 24-26.

Ulewicz, R., Selejdak J., Borkowski, S., et al. (2013). Process management in the cast iron foundry. Metal 2013: 22nd International Conference on Metallurgy and Materials, pp. 1926-1931.

Wołowski, F. and Zawiła-Niedźwiecki, J. (2015). Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi. Warszawa: eduLibri, pp. 45.

Zou, P., Lun, P., Cipolla, D. and Mohamed S. (2017). Cloud-based safety information and communication system in infrastructure construction. Safety Science, Volume 98, [online] Available at: https://www.sciencedirect.com/science/article/pii/S0926580517309561 [Accessed 1 Apr. 2018].

Żywiołek, J. (2016). Międzyorganizacyjna wymiana informacji jako element zagrożenia bezpieczeństwa informacji. In: Systemy bezpieczeństwa w podmiotach gospodarczych, Częstochowa: Oficyna Wydawnicza Stowarzyszenia Menedżerów Jakości i Produkcji, pp. 78.

Żywiołek, J. (2017). Zarządzanie wiedzą o systemie bezpieczeństwa i higieny pracy w przedsiębiorstwie, In: Światowy Dzień Bezpieczeństwa i Ochrony Zdrowia w Pracy 2017, Częstochowa: Oficyna Wydawnicza Stowarzyszenia Menedżerów Jakości i Produkcji, p. 114.