INTERNET OF THINGS AS A DETERMINANT OF SECURITY AND CONTINUITY OF FUNCTIONING

Dariusz PAŁKA

Warsaw School of Computer Science

Piotr ZASKÓRSKI

Military Academy of Technology

Abstract. One of the fastest developing information technologies, the Internet of Things (IoT) facilitates integration of diverse devices and objects. The IoT technology is based on the strengths of the Internet, particularly on the ability to establish networks of cooperating devices used on a mass scale. More and more numerous devices are connected to the Internet which also serves to monitor their condition and work. This shows the future potential utilization of the Internet for various aspects of the management of economic processes and for complex systems of assuring the security and continuity of functioning of individual subjects and of the entire state. Farther development of this technology may, in the future, become the basis of the development of other technologies and of the implementation of diverse network models in economic and organizational processes in order to improve their effectiveness. This effectiveness can be directly related to the collection of very large amounts of data and to the multifaceted data exploration online (Big Data systems). Increasingly essential are therefore the issues of data explosion, of data processing security and of the security of the whole technology.
Keywords: Internet, Internet of Things, Big Data, Business Intelligence.

Introduction

Internet of Things (IoT, Internet of Things) is one of the fastest growing information technologies that positively influences integration of various devices. This technology is based on the advantages of the Internet network, with particular emphasis on the possibility of establishing a network of cooperating devices for general use. Connecting to the Internet of more and more devices and the use of the Internet to monitor their work give an image of the potential of future Internet use in various aspects of economic processes management, as well the management of complex security and business continuity systems in the context of both individual entities and the whole country. Further development of this technology may become the basis for the development of other technologies and the implementation of various network models in economic and organizational processes in order to improve their operational efficiency. The effectiveness of these activities can be directly related to the collection of a very large amount of data and their multi-aspect on-line exploration (the Big-Data systems). That is why the issue of data explosion

and of security of processing and sharing these data, as well as the security of the whole technology, has become crucial.

1. Identification of IoT functionality

The Internet of Things is a kind of extension of the functionality of the Internet platform. The Internet of Things (commonly referred to as the Internet of Everything, IoE) is becoming the basis for the development of most information and IT technologies and thus drives the development of many areas of human activity. The Internet itself is a global system of logically connected objects through the homogeneous Internet Protocol space and is able to provide communication and digital services without significant time and space constraints. The Internet operational limitations are purely technical. It is a platform of unlimited access. Thanks to the widespread use by various types of organizations (including business entities, administrative, those contributing to the common security, etc.). The Internet enables ongoing monitoring of activities and control of the use of various resources at particular stages of operations. Continuous access to resources and their ongoing control over the Internet network facilitates remote work. The Internet allows to organise the work from anywhere on the Earth. Virtual meetings, which are becoming more and more popular, make international projects and scattered research possible. Remote work can also significantly contribute to the increase of productivity and efficiency, and even the effectiveness of internal processes. A computer network built on the basis of the Internet network allows easy access to an unlimited amount of information with the possibility of exploring a very large amount of data.

All the above-mentioned advantages are only a part of the development of the Internet of Things. In its assumptions we can find another technological revolution in the field of mutual communication, not only between humans but, above all, communication between various devices and objects. Because of the sensors built into these devices and the access to the network, this technology highlights a new dimension of the creation of so called smart objects. The Internet of Things thus is becoming the environment for automatic communication of active elements of technical systems, which can be unmistakeably identifiable, and which can directly or indirectly collect, process or exchange data via the Internet. What's more, various devices and their sensors can communicate with people and other objects in order to develop proposals for specific actions and forecasts. Already today we can say that the possibilities of mutual cooperation and information exchange in such a network of connections seem to be very large. Additional mutual integration at any level may produce many advantages in the decision-making and organizational processes. However, taking full advantage of this technology is not so obvious and simple. It involves not only the ability to handle a variety of connected devices and control tools but also the ability to clearly interpret and understand the data they

generate, the results of their analysis and ensuring the security of their existence in global cyberspace.

In the Internet of Things, every object or device (including an access module) can automatically connect to each other via the Internet and exchange various information, mainly presenting either its status or the status of its environment. Grouped data from multiple devices can be simultaneously transferred to specialized devices – servers in order to develop a further decision or forecast of activities. Thanks to this, we can create additional mechanisms of machine learning networks, thereby enriching the advantages of the whole technology. This, in turn, may give rise to support for the design of completely new and difficult technological and educational solutions. The area of supervisory-control systems for critical infrastructure of various entities (states), including crisis management systems, may be a particular area of use of IoT functionalities.

2. Areas of IoT applications

The Internet of Things is a technology oriented towards the integration of all kinds of things (objects) taking into account their mutual relations. Things are all devices and objects, drivers and sensors of these devices that represent (monitor) the status of a given object/ device in the Internet network in order to send or exchange generated data. In addition, this technology is associated with the dynamic development of smart devices (for example, smart watches that enable automatic monitoring of heart rate, especially during exercise), equipped with sensors and having access to high-speed Internet, so that there is a possibility of remote data transfer and monitoring by other entities and objects (element of the health safety system). Generally, in technical terms, the use of devices on the Internet of Things should be seen twofold as:

- devices for mutual communication of the devices themselves in order to optimize their functioning;
- devices equipped with various sensors generating data in the Internet network for other purposes, including dedicated purposes.

The specified perspectives indicate the possibility of using devices on the Internet for monitoring, optimization, control and mutual interaction. The monitoring process should take into account the possibility of observation and direct control of the device's operating status, the ability to collect information about the environment and the ability to collect data about the operation of each object. The optimization process seeks to increase the efficiency of operations with the possibility of dynamic diagnostics, servicing and self-repair. Smart object can also "teach" their users, thus enabling the control of various systems, including control and signalling of deviations from standards of various human life functions. What's more, such devices are often programmed with elements of artificial intelligence, making

them a "thinking machine". Because of that, they can independently increase their efficiency and work efficiently (including the ability to connect with other devices). This constitutes a new dimension for the implementation of routine tasks, requiring constant observation of many different sources of risk in systems ensuring personal security and systemic security.

Nowadays the dominant areas of application of IoT technologies are the following:

- control of home "smart" appliance, such as refrigerators (automatically ordering products based on eg. consumption forecasts) or smart furniture etc.;
- control of medical devices to maintain satisfactory state of work of various ill human or animal organs and at the same time continuously or periodically sending messages to "supervisors" including leading physicians;
- monitoring and steering of wheeled vehicles including automatic detection of sudden non-standard vehicle behaviours, including automatic notification of accidents – eCall[1] system;
- control of house sensors and planning of their operation depending on changes in atmospheric conditions supported by the nearest weather forecast available in trusted online weather services;
- device remote control by the operator/ administrator or automatically on the basis of data flowing from other devices or sensors/ sensors;
- monitoring the operation status of specialized devices (eg. critical infrastructure components of a given entity), work modes and the operating environment of these devices/ facilities.

The Internet of Things thus creates a special ecosystem of devices communicating with each other and exchanging data through a human factor or in accordance with programmed mechanisms and procedures in order to optimize various life, administrative or business processes. The purpose of this model is to increase the efficiency of their operation. The Internet of Things can contribute to increasing the effectiveness of activities for applications that are strongly time-related and displaying the mobility of resources. An example may be systems of monitoring hazards resulting from the impact of natural forces and human activities. Hence the special role for IoT (IoE) is seen in the systems of ensuring the security of the state (citizens) and in the so-called mobile crisis response systems, both military and non-military.

[1] E-Call – automatic emergency call system, which has become mandatory equipment for all new cars with M1 and N1 homologation that have been placed on the EU market since April 1, 2018. The M1 homologation applies to vehicles equipped with no more than 8 seats in addition to the driver's seat. N1 homologation applies to delivery vehicles with a dmc of up to 3.5 tones. Source: http://www.auto-swiat.pl/.

3. Big-Data systems and the Internet of Things

The Internet of Things technology as a network of connected and cooperating various devices, sensors and controllers will generate very large amounts of data. This data will be collected on the Internet. The incoming data should be collected and properly analysed in order to increase the efficiency of the devices that generate these data until specific decision proposals are generated. It should be noted that a single sensor collecting and transmitting, for example, information about the current air temperature once every 10 seconds, sends to the database over 3 million records (6 x 60 min x 24 h x 365 days) all year round. Hence, the number of data circulating in the network can be very large. However, for the network and the data collected from it to have value, they must be subjected to appropriate search and processing algorithms so that they are the basis for further analysis and decision making. Just storing such a volume of data in computer systems is quite difficult. Therefore, big data solutions based on the cloud technology are beginning to play an increasingly important role. Working with such amounts of data requires building specific models according to which the collected data resources will be analysed, taking into account the models of classification, correlation, trend discovery, exclusion/ rejection, similarities, statistical schemes, critical points, etc. It is often a very complex problem, all the more if we want to analyse data in real time. Nevertheless, it is important to create a data storage and selection structure so that the analysis focuses only on data relevant in the context of specific applications or activities.

Data collected from the Internet of Things can be of great value if they are constantly subjected to appropriate searches in order to discover connections and correlations that lead to knowledge discovery. Application of data mining techniques (eg. Data Mining) with advanced processes of exploration of large data resources in search of regular patterns and systematic interdependencies between variables leading to performance evaluation by applying detected patterns to new subsets of data – can be added value and in the final prediction process give direct economic, social or administrative benefits (including, for example, correlations of threats and consequences in security systems).

Gathering all data in various forms is becoming a challenge today. Maximising knowledge is an important attribute for Big-Data systems with extensive functions of analysing numerical data, text files and images (movies). Classical BI systems (OLAP) today are only a subset of analytical capabilities regarding the analysis of structured data. Big-Data systems, in their essence, overcome the barrier of data structuring, gathering large-volume multiform information.

4. Model of organization and creation of IoT resources

The general model of the IoT technology implementation process may be based on the general principles of building information and IT systems, including agile methodologies. Designing devices for the Internet of Things and creating a comprehensive model of their implementation can be a rolling process and a kind of innovation for each participant in this process. The implementation and development of proven solutions can give rise to further IoT devices and technical and technological projects.

The creation of the Internet infrastructure of Things is described by many different models. Microsoft, for example, prefers a model based on cloud technologies provided by Microsoft Azure (Figure 1).

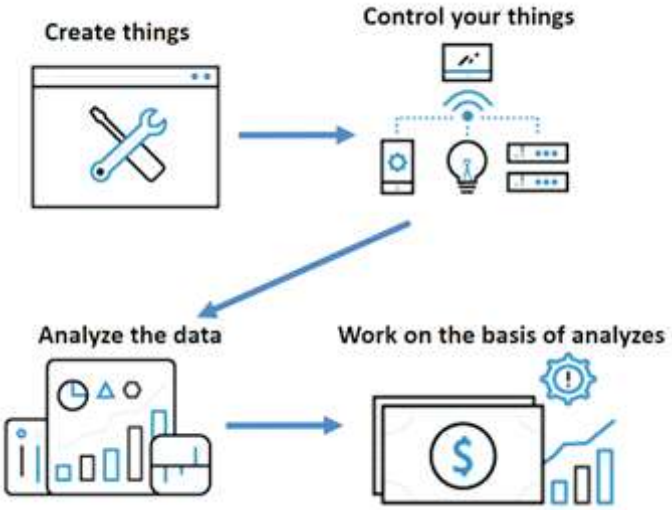

Fig. 1. The model of IoT platform by Microsoft
Source: own elaboration based on: https://www.microsoft.com/pl-pl/internet-of-things/

As part of this technology elements (things) are developed based on the latest IT technologies (databases, Big Data, Machine Learning, neural networks, etc.). The first stage of building a model according to Microsoft's idea is the original process of creating things. Then, after switching the device on to the network, data are collected and analysed, flowing from the device to the database. The analyses are used to make decisions and then to expand the field of activity, including the control of other devices. In this model, four basic stages are foreseen for the Internet of Things. The first stage is to create things or devices with a set of sensors and

drivers to establish the status of smart devices. Then, after the implementation of things, they are monitored and controlled as well as supervision of the correctness of the work of things by monitoring and managing them, enabling the collection of data in real time and the collection in databases.

The collected data is analysed using advanced analytical tools. The analyses of aggregated and selected data that has been converted by advanced applications, constitute new sources of improvement, e.g. business opportunities (including others depending on the subject of the activity). On the basis of this model, one can attempt to build a universal model that takes into account primarily the development element of the solution (Figure 2).

Openness and development of IoT is another key attribute of this technology. Designing new generations of "smart" devices and solutions is the element that enables the development of not only the Internet of Things technology but also the entire branch of knowledge.

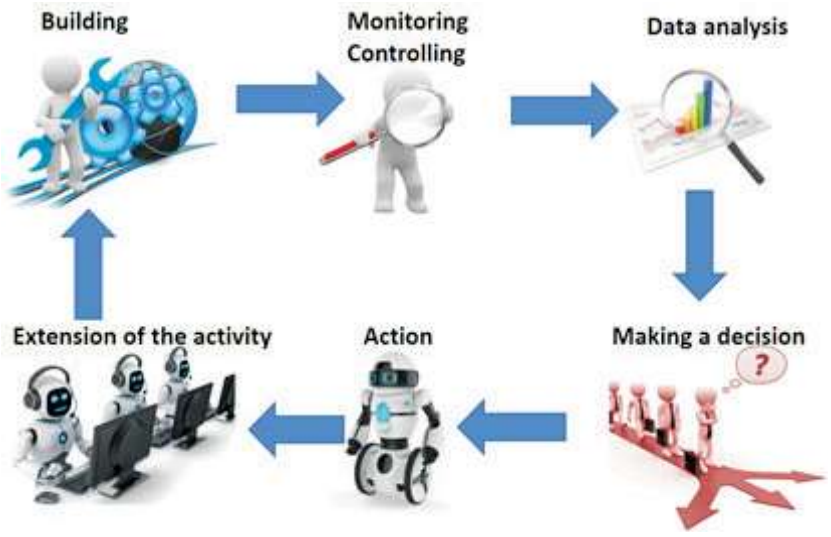

Fig. 2. A universal model of the Internet of Things functioning
Source: own elaboration

IoT becomes an important determinant of the process of development of civilization and the possibility of protecting its broadly understood resources thanks to a significant improvement of communication, also of the threats and their prevention with the use of optimization mechanisms of allocating the necessary and available resources.

5. Limitations and assumptions for the implementation of IoT technology, taking into account the safety and information continuity criterion

Heterogeneity of available solutions of the Internship of Things, their models and concepts makes their level of security difficult to evaluate. Usually, trusted solution providers decide about it. Of course, the key element is the access to the Internet network itself, guaranteeing the continuity of operation, taking into account various difficulties and threats. It is worth noting here that especially mobile access to the Internet network may be burdened with the risk of temporary or prolonged interruptions in the functioning of IoT solutions. On the other side of the Internet of Things issues there are IT solutions supporting the functioning of the technology itself, where the use of advanced tools for building and supporting technologies provided by proven suppliers is justified. Among the leaders of such solutions, above all stand out: AMAZON, MICROSOFT, IBM, GOOGLE. It should also be noted that the so-called proven suppliers use advanced solutions and procedures in the area of security using the scale phenomenon. In fact, only external, professional solutions are able to guarantee an adequate level of data security, including protection against loss, theft, damage or deletion. In addition, care for the security of data generated by IoT – in particular stored in the cloud – should be an essential requirement for security policy, supervision rules for privileged administrators of server equipment as well as methods of controlling access to the resources processed in them. Particular care is required for data protection procedures as well as mechanisms guaranteeing information continuity of operations combined with data integrity, including the use of mechanisms and effective data replication models.

Implementation of IoT solutions with particular emphasis on the safety criterion and ensuring business continuity requires security exposures in terms of:

- network access to IoT devices and solutions;
- security of operating systems and security of hardware resources;
- security of network devices;
- services provided, including services supported by security certificates;
- mechanisms of access to cloud computing services;
- data security mechanisms, including methods of data transportation by extensive computer networks and the Internet network;
- securing access to collected and aggregated data;
- safety mechanisms and procedures, including physical security;
- technology users and their responsibility.

An important component is the so-called physical security, which refers to comprehensive protection of solutions, including places where individual IoT devices are located. Such places must be protected with the highest levels of security, in particular resistant to their destruction and service providers should have

appropriate security certificates. The key element is the efficiency and security of the computer network, including the Internet. If there is a risk of interruption of any of the key elements, including access to the Internet network, substitute procedures should be run. What's more, IoT devices may work incorrectly due to incorrect configuration. In addition, IoT technologies do not have unmistakable standards, which equipment manufacturers can use to lower the level of security by reducing the cost of their production.

The constant development of IoT and the generation of very large amounts of data and the observed incidents related to their improper use indicate the need to highlight the issue of security of processed data. This data may be subject to loss, unintended actions of changing their quality as well as disclosure of sensitive information. Data confidentiality and the issue of its protection with limited possibilities of controlling data flow in Internet networks can reduce the trust of end users. Therefore, their awareness of the risk of loss of confidentiality of data generated by this technology and the possibilities of counteracting this phenomenon is important.

The above-mentioned threats and various aspects of the security of services on the IoT platform do undermine this technology but indicate the need to improve it. The offered tools and services do not have to pose a threat to various entities, but may be determinants of sustainable development. The security guarantee should be appropriate security management procedures and effective management of the risk of the loss of information continuity, including the use of data protection methods such as:

- data encryption (implementation of encryption protocols SSL[2] data exchange);
- creating virtual local networks VPN[3], which are transmitted and exchanged between IoT data devices;
- implementation of proven, safe and efficient devices and network systems (firewalls, data packet filters).

It should be noted here that data security in IoT technology is not only security procedures implemented by the service provider. An important element is also the need to implement appropriate security procedures for the use of technology by its recipients. This applies to the need to organize and conduct continuous training in the field of security policy and to grant users appropriate security certificates.

---

[2] SSL (Secure Socket Layer – Safe Data Packets layer), protocol operating below the HTTP protocol layer, and ensuring encrypted (confidential) data transmission, both one-way and two-way, enriched with the possibility of using ISO X.509 certificates, also ensuring the receivables and non-repudiation of transmitted data.

[3] VPN (Virtual Private Network) – a technical solution through which private network traffic flows between end customers through a public network (such as the internet) in such a way that the nodes of this network are transparent to the data packets sent in this way. Optionally, you can compress or encrypt the transmitted data to provide better quality or greater security.

Selection of appropriate methods of user access to data using user authentication procedures, implementation of appropriate mechanisms for their certification and logging into the system with the use of special user credentials and the use of cryptographic certificates – is an important element of preserving the security of data shared and processed within IoT.

An important element of security in the end-user perspective is the continuous and stable operation of the entire system, which is a consequence of proper configuration of the entire equipment and telecommunications infrastructure, both on the service provider's side and on the recipient's side – starting from routers, servers, through traffic control devices, until to the last telecommunication element. All these elements should be fully redundant in a continuous activity model with the possibility of concurrent takeover of tasks by the doubling device without the risk of configuration differences. In addition, the risk of data loss in the event of any breakdown or unwanted intrusion may be limited by the redundancy of technical and technological resources. However, the risk of losing data for unexpected reasons must always be taken into account, which is why an important element is the constant analysis of the data status and the possibility of their reproduction / replication (strong replication and mirroring mechanisms). Special protection of confidentiality of selected data may be ensured by the use of encryption applications that guarantee selectivity of access to data in accordance with the access rights.

IoT technology, due to its mobility and data protection capabilities as well as providing business continuity information, may be particularly useful in security systems (Figure 3), including crisis management systems with a strong emphasis on the crisis response phase, and so in the phase of counteracting the effects different types of threats.

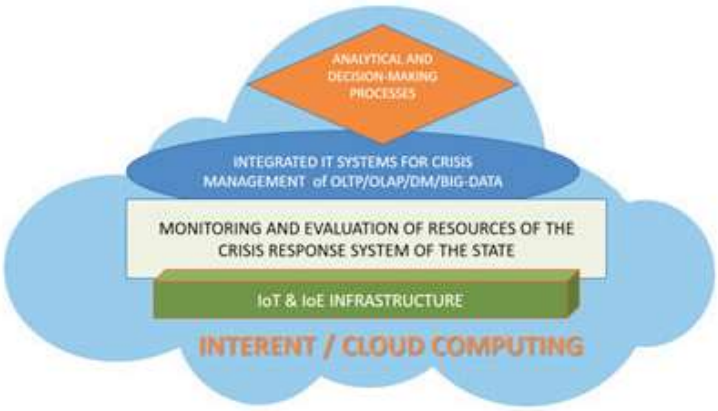

Fig. 3. The idea of the implementation of IoT in security systems

Source: own elaboration based on: M. Ogórek, P. Zaskórski, *Internet Rzeczy w integracji procesów zarządzania kryzysowego*, Międzynarodowa Konferencja Naukowa „Rozwój organizacji w turbulentnym otoczeniu", P. Zaskórski, W. Zaskórski, *Systemy „Big-Data" w doskonaleniu współczesnych organizacji*, WAT

This requires, above all, streamlining the flow of current information between different types of entities, which will affect the assurance of business continuity at every level (in a given area of operation) of various objects present in a particular configuration. In order to fulfil the criterion of providing information on business continuity, appropriate resources must be secured according to legislative regulations and appropriate infrastructure created or modified. Relevant entities in the crisis response system should be authorized to use selected infrastructure elements. This can be one of the conditions for uninterrupted exchange of information between different nodes of the system and creating the basis for continuous operation in various geospatial dimensions. The possibility of constant monitoring of various facilities – not only critical infrastructure, but also executive elements (including devices and other resources) – can be conducive to the verification and actualization of current action plans/ crisis response. Access to current information coming directly from monitored objects, often endangered (signals from various types of sensors, eg. temperature, smoke, contamination, water level and others) becomes an important determinant of the effectiveness of crisis management processes and actions in the crisis response system. Data shared from "cloud" data centers can support planning processes and, in a sense, automatically initiate crisis response processes. In addition, planning the rational use of all resources is conditioned by access to current information about them, with particular emphasis on their availability/ availability.

The use of IoT class services may become in a sense a guarantee of access to current data on current needs in the area of crises and the available state of power and resources. The concept of integration of information sources, including the IoT platform, gives great opportunities in the case of tasks in a situation of strong time pressure. Improved information flow and data exchange and the use of automation of the online data collection and exchange process should improve the efficiency and speed of preparatory decision-making activities and the effectiveness of the implementation of security and enforcement processes. Hence, the IoT platform can become the basis for the construction of a modular, integrated IT system supporting the crisis management process at all its levels and in unlimited space. Such IT solutions in the area of national security in both the civil and military subsystems give the opportunity to increase the level of security of the state and each constituent entity.

6. Summary

The Internet of Things is the present but also the future. This is one of the main trends in the modern development of information and electronic technologies, which can significantly contribute to the development of global economy and human life in the aspects of savings resulting from reduced costs and time constraints, increased efficiency and performance. Thanks to the network of connected devices,

human resources and collected data, administrative and economic organizations (including business ones) will be able to better understand the requirements of the environment and change their activities much faster. The Internet of Things can also improve the quality and comfort of life as well as increase the sense of security of people through constant monitoring of the surrounding environment or health, but also by supporting decision-making processes and optimizing the use of resources, especially in crisis situations. All these elements are only an outline of the potential of this technology and at the same time access to necessary data.

The analysis of data generated by devices operating in the Internet of Things technology is currently undergoing a very intense evolution. This evolution includes not only the collection of descriptive data, but primarily leads to the generation of more sophisticated prediction models releasing advanced decision-making processes that increase the efficiency and the alternative of action. In addition, this technology is increasingly used in the development of devices and business processes. Access to the collected data and their multi-aspect use will be a determinant of the effective operation of various social systems.

BIBLIOGRAPHY

[1] Dominique D., Vlad M., *Internet Rzeczy. Budowa sieci z wykorzystaniem technologii webowych*, Helion, Gliwice 2017.

[2] Miller M., *Internet Rzeczy. Jak inteligentne telewizory, samochody, domy i miasta zmieniają świat*, PWN, Warszawa 2016.

[3] Nitesh D., *Abusing the Internet of Things. Blackouts, Freakouts, and Stakeouts*, O'Reilly Media, USA 2015.

[4] Ogórek M., Zaskórski P., *Internet Rzeczy w integracji procesów zarządzania kryzysowego*, Międzynarodowa Konferencja Naukowa „Rozwój organizacji w turbulentnym otoczeniu", Wrocław, 19-21 kwietnia 2018.

[5] Russell B., van Duren D., *Practical Internet of Things Security*, Packt Publishing Ltd. Birmingham, UK 2016.

[6] Sułkowski Ł., Kaczorowska-Spychalska M., *Internet of Things. Nowy paradygmat rynku*, Difin, Warszawa 2018.

[7] Zaskórski P. (red.), *Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania*, ISBN 978-83-62954-04-9, Wyd. WAT, Warszawa 2011.

[8] Zaskórski P., Zaskórski W., *Systemy „Big-Data" w doskonaleniu współczesnych organizacji*, WAT, NSZ, Warszawa 2016.

INTERNET OF THINGS JAKO WYZNACZNIK BEZPIECZEŃSTWA I CIĄGŁOŚCI DZIAŁANIA

Streszczenie. Jedna z najszybciej rozwijających się technologii informacyjnych, Internet of Things (IoT), ułatwia integrację różnych urządzeń i obiektów. Technologia IoT bazuje na mocnych stronach Internetu, w szczególności na możliwości tworzenia sieci współpracujących urządzeń używanych na masową skalę. Coraz więcej urządzeń jest podłączonych do Internetu, co służy również do monitorowania ich stanu i pracy. Wskazuje to na przyszłe potencjalne wykorzystanie Internetu do różnych aspektów zarządzania procesami gospodarczymi oraz złożonych systemów zapewnienia bezpieczeństwa i ciągłości funkcjonowania poszczególnych podmiotów i całego państwa. Dalszy rozwój tej technologii może w przyszłości stać się podstawą rozwoju innych technologii i wdrażania zróżnicowanych modeli sieciowych w procesach gospodarczych i organizacyjnych w celu poprawy ich efektywności. Efektywność ta może bezpośrednio odnosić się do gromadzenia bardzo dużych ilości danych oraz do wielowymiarowych eksploracji danych w Internecie (systemy Big Data). Coraz ważniejsze są zatem kwestie eksplozji danych, bezpieczeństwa ich przetwarzania i bezpieczeństwa całej technologii.

Słowa kluczowe: Internet, Internet of Things, Big Data, Business Intelligence.