O P E R A T I O N S R E S E A R C H A N D D E C I S I O N S
No. 1 2016
DOI: 10.5277/ord160103

Tadeusz GALANC[1]
Wiktor KOŁWZAN[2]
Jerzy PIERONEK[3]

INFORMATICS SYSTEMS OF DECISION SUPPORT AND ANALYSIS OF THEIR SECURITY

A new approach to security issues associated with the use of teleinformatics systems in the decision-making process has been presented. There is a discussion of the relationship between the security of informatics systems and the security of the decision-making process in which they are used, in particular regarding the threats resulting from the use of informatics systems and modern teleinformatics technologies. In addition, an overview of the dangers that could have a significant impact on appropriate decision-making has been performed. The paper points out the possible ways to ensure security depending on the type of threats encountered. In particular, threats particularly linked with the security of informatics systems supporting decision-making have been identified.

Keywords: *informatics system, threat, security, management, decision-making*

1. Introduction

Over recent years, the increasing level of support of decision-making processes through the use of appropriate informatics systems and teleinformatics infrastructures has been observable. Currently, the boundaries of decision support are no longer discussed but rather the impossibility of undertaking it without adequate informatics support. This support concerns both gathering and accessing data up to the time a decision is made or suggesting a set of potential solutions after defining a decision problem and

[1]College of Management „Edukacja”, ul. Krakowska 56–62, 50-425 Wrocław, Poland, e-mail: tadeuszgalanc@gmail.com

[2]Department of Management, Gen. Tadeusz Kościuszko Military School of Higher Education, ul Czajkowskiego 109, 51-150 Wrocław, Poland, e-mail: wiktor.kolwzan@pwr.edu.pl

[3]Department of Computer Science and Management, Wrocław University of Science and Technology, ul. Łukasiewicza 5, 50-371 Wrocław, Poland, e-mail: jerzy.pieronek@pwr.edu.pl

determining possible criteria for its resolution. Therefore, the range of use of informatics tools more often concerns complex decision-making support.

Advances in teleinformatics have hugely influenced the emergence and development of the information society. The current environment (conditions) requires that appropriate technical means are provided to senior executives, giving them a chance to improve management. Appropriately designed informatics tools can provide support to decision-making process which as a consequence not only ensures appropriate decision making but can also contribute to improving the quality of the management process. This necessity results from various reasons. These include, among other things, the rapidly changing environment, which in turn requires faster decision-making, because any decision or action may become outdated in a short time.

The widespread use of information technologies has enabled, among other things, the implementation of systems and processes on a worldwide scale, thus playing a role in the globalization of economies. It could be stated that the globalization of information needs in a natural way to overtake the postulate, now proclaimed, of the globalization of economic processes. In a globalizing society experiencing growing competition, speed in taking decisions becomes increasingly important. Under certain conditions, it is better to abstain from making a decision than to take it too early or too late, because a decision taken at the wrong moment can bring irreversible damages.

In this paper, issues related to the security of informatics systems which have an impact on the security of computer-aided decision-making will be presented. The significance of this problem is even greater today because from year to year, the spectrum of uses for informatics systems and teleinformatics technologies is widening into more and more areas of the functioning of organizations and citizens' lives. At present, even our dependence on these systems and technologies is becoming a huge topic for discussion, since without these technologies it is becoming difficult to carry out even the most elementary tasks, which is, in turn, connected, among other things, with the time factor and surrounding competition.

2. Decision-making and environmental conditions

A decision-maker, who analyzes a particular situation in order to make the right decision, should take into account not just the character of the decision but also the environmental conditions in which it is taken [4]. Because of the rapid rate of changes occurring and their unpredictability, three categories of states in which the decision-maker acts are widely described in the literature (cf. [7]):

- A state of certainty in which the decision maker has precise knowledge of the potential impact (benefits and risks) resulting from the selection of a particular decision. Very few decisions are taken in such a state.

• Decisions made under the existence of risk in which the decision-maker can assign specific probabilities to the benefits and costs arising from a specific decision.

• A state of uncertainty which often accompanies decision making is characterized by a lack of full knowledge of the set of potential decisions and the consequences related to these decisions.

The distinction between decision-making under uncertainty and risk was first introduced by Knight [3].

Stages of the overall decision-making process

Decision-making is a complex process and most frequently split into the following important stages:

• identification of a scenario requiring a decision (diagnosis),
• identification and description of possible decisions (elaboration),
• evaluation of the possible decisions and selection of a rational one (choice),
• creating conditions for the implementation of the chosen decision,
• assessment of the effects of the chosen decision.

Very often, when making decisions, we have to return to a previously realized step (Fig. 1), which complicates this process even more. At each of these steps, specific needs for information have to be satisfied and such a continuous flow of relevant information is only possible with a well-functioning informatics system.

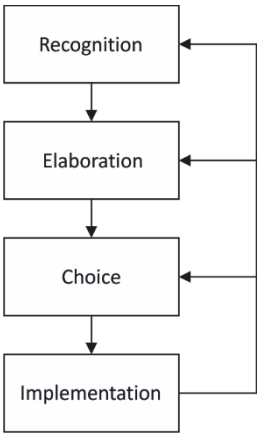

Fig. 1. Realization (steps) of a decision-making process.
Source: author's elaboration based on [5]

Going into even more detail into this process, it can be seen that its specifics do not only encourage the use of teleinformatics technologies in supporting its realization but

such technology even becomes a necessity. This depends, among other things, on the complexity of the data required to make a decision, or on (other factors related to taking a decision– in a broader approach) the need to make a quick decision. Depending on the complexity of a decision problem, a more detailed diagram may adopt a more complicated shape and sometimes becomes difficult to interpret, not only because of the number of elements occurring in it but also because of the scientific terminology used (Fig. 2).

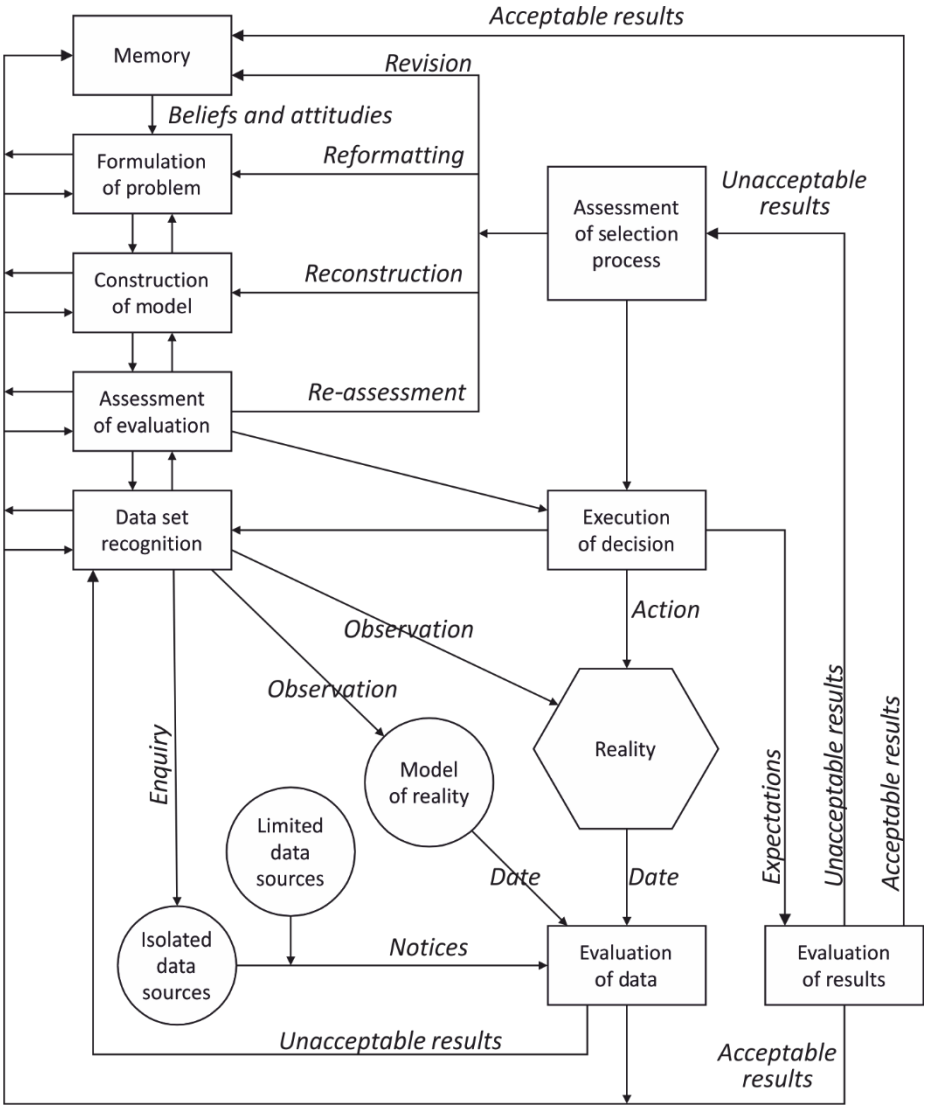

Fig. 2. A model of a decision-making process. Source: [9]

Any interpretation of Figure 2 presented below indicates very clearly that in the process of decision-making it is difficult to determine the number of elements required for appropriate analysis of the problem under consideration. This is the well-known academic issue of complexity. Ashby considered this problem many years ago, and he related the problem of defining the complexity of a given system to its (natural) scope of diversity [1].

In summary, it can be said that the adoption of too many concepts to represent a given problem can cause ambiguity in its interpretation. This is evident in a significant way in relation to the diagram discussed here[4].

The decisions taken may be correct or incorrect. This may result from many factors. The following section will consider selected factors influencing the correctness of a decision arising directly from the use of informatics systems in such a process.

3. Systems and informatics technologies supporting decision-making

Selection of the appropriate informatics tools to support decision-making is a difficult task. Some technologies will be used in the case of tactical decision-making, and others for decisions of a strategic character. Moreover, the scope of the tasks involved may be limited to certain stages of decision-making, as well as ensuring comprehensive support for this process.

Systems may be categorized as follows: partial, uni-disciplinary, multidisciplinary or universal applications, according to the freedom given to set the parameters and criteria necessary to determine the situations in which decision-making can be supported. Of course, such systems should take into account the type of situation a decision is taken in, because different kinds (scales) of data are required according to whether operational, tactical, or strategic decisions are made[5].

Therefore it is important to carefully design the appropriate use of informatics tools, starting from the level of data acquisition and storage. Use of the simplest tools, for example, universal usable packages (office suites), should be considered here, as their basic functionality provides the possibility of data entry to the user with without having to specify a method for inspecting the correctness of the data inputted. However, in the case when electronic documents (spreadsheets, databases) are used in the longer term, or when systems may involve collecting data of great importance (sensitive data), then the available control mechanisms for entering data (e.g., data masking, data validation rules, lists of suggestions, limiting the range of allowable values or the size of data sets) and preserving the consistency of data offered by these informatics systems are not only acceptable, but even desirable.

---

[4]For example, in Figure 2 the term *observation* occurs several times. Nevertheless, are the activities related to this term the same regardless of context?

[5]The terms: operational, tactical and strategic are universal and not only military.

Universal systems, as well as systems dedicated to supporting a given process, beneficially affect the elimination of errors that can arise, starting at the stage of data collection up to the time at which they are processed for the purpose of decision making. If such a process is carried out without the use of informatics systems, then achieving the same effect is much more difficult, and costs increase significantly with the amount of data collected.

In the case of systems providing their functionality via the Internet, it is important, in addition to the recommendations listed above, to ensure appropriate access to the data collected and transmitted. Authorization for access to resources and verification of the correctness of the data provided by teleinformatics networks are key here.

4. Types of threats to informatics systems

The safety of computer-aided decision-making is closely linked with the occurrence of threats associated with the security of informatics systems. It can be concluded that there is no system that is not exposed to threats [6]. Therefore, the use of informatics systems when making decisions entails the possibility such threats endangering the appropriate execution of this process, and thus the regularity and effects of decisions. Determining the set of potential threats should be carried out carefully, thus ensuring the appropriate level of security. This is hugely important, because *the effects of decision making are undoubtedly the driving force behind developing their mechanisms. The effects of a decision are evaluated in relation to the degree to which needs are satisfied.* (...) *Analysis of a decision is not possible without consideration of the relationship between a decision and its consequences* [8].

Threats deriving from the use of teleinformatics technologies in decision-making depend not only on the type of decision to be made but also on the range of its effects in space and time. They may be less serious if they are limited to a narrow environment. In the case of decisions taken within a state (e.g., the local elections conducted in Poland in October 2014.), the possible consequences of threats have a different meaning to those applying to decisions in response to the behavior of another country (e.g., decisions regarding a military response to the actions of an opponent). Hence, decision–making may be associated simply with implementing the plans of an organization and thus may have a limited range. It may also concern the role of the state in a given sector (e.g., the economy, health care, the education system, sport or culture), either aimed at increasing the prosperity of society as a whole, or within a few specific areas of a nation's life.

Depending on the criteria adopted, various classifications of these threats can be specified [6]. Classification according to the following criteria should be mentioned:

- the source of a threat,
- the consequences of emerging threats,
- the location and riskiness (randomness) of threats.

Using the first type of classification, a wide range of factors should be considered, which have varying impact on the functioning of teleinformatics systems. These include:

- natural phenomena,
- targeted actions,
- human activities,
- failures and technical faults,
- organizational failures and deficiencies.

Considering the consequences of emerging threats, the following should be taken into account, among other things:

- unauthorized access to a system, data and data processing mechanisms,
- interception of data during transmission,
- breaking into a security system,
- loss of data confidentiality,
- damage to or distortion of the data collected,
- loss of integrity of the information,
- ineffective use of the system's functionality (services).

Especially dangerous are those threats that are unnoticeable or difficult to detect. Damaged data can be quickly identified and repaired (e.g., using backups). However, data capture or monitoring the work of users over a longer period of time can lead to third parties coming into possession of confidential or secret information, which might affect the safety not only of a system, but the entire organization, together with its external network connections. The operating personnel should also be aware of the danger created by defective software, damage to technical infrastructure and disorder within transmission channels.

The last type of classification mentioned above involves dividing threats according to

- localization:

– internal threats (e.g., the theft of data by a user of a system),

– external threats (e.g., someone breaking into premises, lack of power supply),

- randomness:

– intentional threats (e.g., computer theft, deliberate erasure of data),

– accidental threats (e.g., accidental deletion of files, turning off a computer system or power failure during operation).

5. Ensuring the security of informatics systems

An informatics system is secure if its user can rely on it and its software operates according to its specification [2]. When designing an informatics system, the user should be aware of the following safety aspects (CIA, Fig. 3):

- confidentiality of information,

- integrity of information,
- availability of information.

Various threats and mechanisms counteracting these potential dangers, depending on the properties of information security, can be highlighted. Selected ones are discussed below.

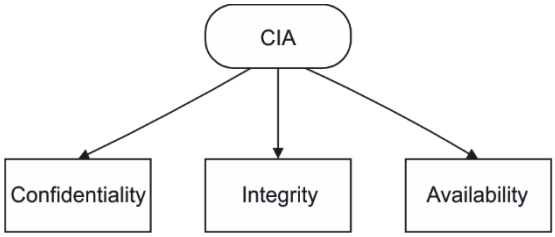

Fig. 3. General safety aspects

To prevent unauthorized access to data at the place of their storage and at the place of processing, as well as to avoid the interception of data transmitted in telecommunication networks, the identity of users should be confirmed before authorizing access to the system's resources. Appropriate methods for protecting against the interception and reading of information should be used in the process of data transmission. Also, technical infrastructure should be checked both periodically and randomly.

A no less important aspect is to preserve the integrity of data. Faulty data may cause an incorrect decision, even if appropriate methods are used to analyze them. The simplest methods that enable preserving the integrity of data are: the control of access to data, the use of anti-virus mechanisms and data control through, e.g., the use of checksums or digital signatures. In the case of interference in the system's resources, registration of the operations performed on data can also be very helpful in restoring their correctness.

In order to ensure access to data and thereby counter the negative effects resulting from hardware failure and software errors that may have different sources (e.g., random events, or intentional action), the following defense mechanisms can be used: ensuring continuity in power supplies to equipment and technical infrastructure (e.g., UPS type devices), data archiving, the use of anti-virus packages and ensuring their databases are updated. Neuralgic parts of a system can be doubled (in parallel), which in the case of an undesirable event will allow work to continue, as well as enabling an efficient and rapid return to the normal functioning of the system.

The influence of threats to the security of informatics systems used for supporting decision-making processes depends considerably on the extent to which these systems support such processes. Such threats will be of greater importance when informatics systems play a range of roles in decision support, and of lower importance when their role is limited only to individual tasks. Therefore, when planning the use of modern teleinformatics technologies to support decision-making processes, the range of their

use and the potential threats associated with this range should be taken into account with great care. This is connected with the necessity of incurring additional costs to ensure the safety of informatics systems. In contrast, this security may prove to be crucial in decision-making processes, for example, in relation to decisions of a strategic character. However, in consequence, the financial expenditure related to maintenance of security will be insignificant compared to the benefits that would be achieved.

6. Conclusions

Decision-making processes involve a wide range of decisions, among which there might be both correct and incorrect ones with beneficial and negative consequences, respectively. The appropriateness of a decision may result from many factors. The effect of a decision does not always depend on the security of the informatics systems used in this process. For example, a particular decision might simply be inappropriate. However, it may also prove that a decision is incorrect as a result of the improper use of an informatics system, or even the effects of a decision may be negative, due to a lack of security in an informatics system.

In the paper, selected factors affecting the efficacy of decisions have been presented arising directly from the use of informatics systems. The type and the number of threats resulting from the use of informatics systems depends on the degree of the dependence of these process on how such systems are used. In addition, the greater the role of computer systems and the greater the possible effects of an inappropriate decision, the more serious and numerous are the potential threats. Summing up, understanding the types of threats resulting from the use of informatics systems and the ability to identify them in specific cases can significantly improve the security of the decisions taken.

References

[1] ASHBY W.R., *An Introduction to Cybernetics*, Chapman and Hall, London 1956.
[2] GARFINKEL S., SPAFFORD G., *Practical Unix and Internet Security*, 3rd Ed., O'Reilly Media, 2003.
[3] KNIGHT F., *Risk, Uncertainty and Profit*, Houghton Mifflin Co., Boston 1921.
[4] KOŁWZAN W., PIERONEK J., *Elements of Decision Theory*, WSOWL, Wrocław 2012 (in Polish).
[5] LAUDON K.C., LAUDON J.P., *Management Information Systems*, Prentice Hall, New Jersey 2000.
[6] MADEJ J., *Classification of the threats to an informatics system*, Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie, No. 814, 2010, 76 (in Polish).
[7] SADOWSKI W., *Decisions and Forecasts*, PWE, Warsaw 1977 (in Polish).
[8] SZAPIRO T., *What decides a decision*, Wydawnictwo Naukowe PWN, Warsaw 1993 (in Polish).
[9] WAWRZYNIAK B., *Managerial decisions in management theory and practice*, PWE, Warsaw 1980.

Received 30 September 2015
Accepted 25 November 2015