them for further analysis. In addition, with the help of modern online platforms that provide their users with organized access to numerous services for data analysis and processing, you can even support some stages of empirical research.

The noosphere of humankind is always evolving, constantly enriched with new and useful knowledge, invaluable experience gained in practice. This is a natural evolutionary process. At the present stage of development of society, thanks to the use of powerful information technology, we have the opportunity to witness (and even be involved) in the most dynamic growth of the scientific potential of our civilization in the history of its existence. In the future, the pace and volume of this growth will increase.

DOI 10.36074/24.07.2020.v2.07

RELEVANCE OF THE SUBJECTIVE COMPONENT IN CYBERSECURITY RISK ASSESSMENT

Sergii Honchar
PhD, Leading Researcher
Pukhov Institute for Modelling in Energy Engineering

Alla Onyskova
Junior Researcher
Pukhov Institute for Modelling in Energy Engineering

UKRAINE

The risk management system should provide: risk identification, classification, selection of risk measures, risk measurement, selection of risk processing algorithm, implementation of the selected algorithm, analysis of the results obtained - for today, in the processing of cybersecurity risks.

The cybersecurity risk assessment process includes three main stages - risk identification, risk analysis and risk assessment.

The process of identifying cybersecurity risk includes the identification of the causes and sources of dangerous events, situations, risk circumstances that may significantly affect the achievement of the organization's goals, and the nature of these impacts.

Regardless of the methods actually used in risk identification, it is important to consider human and organizational factors. Deviations caused by human and organizational factors, as well as dangerous events related to information technology, must be taken into account in the process of risk identification.

Risk assessment is part of the risk management process and is a structured process that identifies the means to achieve goals, analyzes the consequences and likelihood of dangerous events to decide on the need for risk processing.

B. Schneier notes [1, 2] that decision-making in the field of risk management largely depends on the sense of risk, i.e. the perception of risk. Money is used as a universal characteristic of the possible results of any loss, because they are a measure of the value of goods and services, play the role of the general equivalent, express the value of all other goods and exchange for any of them. But it turns out
that the approach in which the "price of risk" is calculated in money is far from perfect. This is noted in his new theory of measuring risk D. Bernoulli [3]. His main thesis is that the risk perceived by everyone in their own way and can not be assessed equally. In this case, the assessment of the usefulness of benefits depends on the person who is at risk. Thus, knowledge of cost / loss and probability is not always sufficient to determine the value of the result, as the usefulness in each case may depend on the individual making the assessment. Each individual has its own value system and responds to risk in accordance with this system. The philosophical and methodological significance of D. Bernoulli's theory is that he was the first to show that risk assessment depends on the individual.

When building models of rational choice in conditions of risk, they try to make them universal, independent of the individual of decision-making - objective. Each individual has its own system of goals, values and assessments, and his behavior in terms of risk is determined by this system, rather than the same logical and methodological standards for all. As a result, the individual chooses the alternative that best meets his goals, assessments and value system. Here we can talk about the subjective risk. At the same time, general methodological approaches to decision-making in conditions of risk are needed, because a person in such a situation wants to have a rational basis for making sensible decisions [3]. Later, Bernoulli's ideas were further developed in the theory of utility by fon J. Neiman and O. Morgenstern [4].

Thus, decision-making in the field of risk management largely depends on the sense of risk, and the most typical factor on which the feeling of security may differ from the real security is the perception of risk, its awareness. Therefore, the correct quantitative assessment of total risk should combine not only the component of objective risk, but also the component of subjective risk, which is one of the main elements of information security [5, 6].

Thus, decision-making in the field of risk management largely depends on the sense of risk, and the most typical factor on which the feeling of security may differ from the real security is the perception of risk, its awareness. The correct quantitative assessment of total risk should combine not only the component of objective risk, but also the component of subjective risk.

References: