НАН України – ефективний засіб формування академічної культури дослідника». *Педагогічні науки: теорія, історія, інноваційні технології*. 2020, № 10(104). С. 245–258.

8. Anna Dąbrowska, Urszula Dobesz, M. Pasieka, „Co warto wiedzieć. Poradnik metodyczny dla nauczycieli języka polskiego jako obcego na Wschodzie", Ośrodek Rozwoju Edukacji, Warszawa 2010, ss. 236.

DOI https://doi.org/10.30525/978-9934-26-277-7-214

MANAGING CYBERSECURITY FOR OIL AND GAS COMPANIES IN A CRISIS

Skakalina O. V.
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department
of Computer and Information Technologies and Systems
National University "Yuri Kondratyuk Poltava Politechnics"
Poltava, Ukraine

Kapiton A. M.
Doctor of Pedagogical Sciences,
Professor at the Department of Computer
and Information Technologies and Systems
National University "Yuri Kondratyuk Poltava Politechnics"
Poltava, Ukraine

Despite the widespread upward trend in the use of renewable energy sources, oil and gas occupy key positions in the world's energy sector. National oil and gas production companies (NPOs) have a significant impact on the development of the national economy due to the formation of the main source of tax revenues for the budgets of all levels, they ensure national energy security. However, management of energy systems, which belong to the class of complex territorially distributed dynamic systems, is a complex process in itself. Among the main difficulties are: the limitation of methods of adequate modeling, the contradiction between the detailing of the model structure and the possibility of dynamic processing of the information contained in it, the loss of adequacy of the model when the conditions of the subject area change and the internal conditions of the model change. Therefore, any national energy system must be resistant to risks that may be caused by physical and cyber threats [1, p. 5]. The energy sector covers the spheres of gas, electricity (including production and generation), oil and oil products, as well as related spheres that provide the function of energy supply for human life, society, the economy and the state. The energy supply ecosystem involves the construction of an ecosystem of separate component functions, such as electricity supply, heat supply, gas supply, continuity of management, continuity of management, etc. and is a synthesis of separate component functions on a system basis. Therefore, ensuring the cyber security of an oil and gas production company in crisis conditions is an urgent task.

Only 15% of companies in the oil and gas industry have a formalized cyber incident response program, according to a study conducted by experts from the British audit and consulting company Ernst & Young. As the survey of 40 respondents showed, while cybersecurity is a priority for businesses, they are more concerned than ever with the growing scale and complexity of the cyberthreat landscape. According to the survey results, 60% of companies have experienced a major cyber incident, while only 17% of businesses believe they will be able to detect a sophisticated cyber attack in the future. 78% of respondents named careless employees among the most likely sources of attacks, 63% noted that they did not intend to increase the cybersecurity budget after incidents that did not cause any harm. The reason for 43% of significant leaks was the negligence of end users who became victims of phishing, follows from the report. At the same time, 97% of companies do not assess the financial consequences of serious leaks. According to 87% of respondents, the current plans and strategies of their companies do not fully take into account the consequences of security incidents, as 95% of respondents noted that the implemented cybersecurity measures do not meet the needs of their organizations. According to the estimates of the British analytical agency Juniper Research, over the next five years, the total damage to companies and organizations around the world from data leaks will reach $8 trillion, including due to inadequate protection measures implemented by enterprises [2, p. 11].

Cybersecurity interests include:

– *security of critical infrastructure,* which includes facilities of oil and gas corporations with developed electrical networks, transport networks, automated control systems in the form of ERP systems, information and communication systems;

– *network security,* which includes the protection of the underlying network infrastructure from unauthorized access and misuse, as well as from information theft. The technology includes the creation of a secure infrastructure for devices, applications and users that are part of the OGPC ecosystem;

– *application security,* which implies security measures,

applied at the application level and aimed at preventing theft, hacking of corporate data and corporate applications;

– *cloud security,* which is an interconnected set policies, controls and tools to protect cloud computing systems from cyber threats. Cloud security measures are aimed at ensuring the security of data, online infrastructure, as well as applications and platforms. Cloud security has a number of common concepts with traditional cybersecurity, but this area also has its own advanced methods and unique technologies, which include technologies for using the concept of blockchains in the formation of electronic signatures in electronic corporate document management, the use of quantum coding principles when using data on actual and prospective locations of oil and gas fields, product pipelines, oil and condensate transportation routes.

The main goal of cybersecurity is to prevent the theft or compromise of information. An important role in achieving this goal is played by the triad of a secure IT infrastructure – *confidentiality, integrity and availability*. Confidentiality in this context refers to a set of rules that restrict access to information. Integrity ensures that information is accurate and reliable. Availability, in turn, is responsible for the reliability of access to information by authorized persons. Considering the principles of the triad together helps companies develop security policies that provide strong protection.

References:

1. Hybrid Warfare Against Critical Energy Infrastructure: The Case of Ukraine. NATO ENSEC COE, 2020, 87 p. URL: https:// enseccoe.org/data/ public/uploads/2020/11/hybrid-warfare-against-critical-energy-infrastructure-the-case-of-ukraine.pdf

2. Cybersecurity in the information society: Informational and analytical digest / resp. ed. O. Dovgan; according to O. Dovgan, L. Litvynova, S. Dorogykh; Research Institute of Informatics and Law of the National Academy of Sciences of Ukraine; National Library of Ukraine named after V.I. Vernadskyi. K., 2017. No. 12 (December). 82 p.