PROTECTING THE CORPORATE INFRASTRUCTURE FROM CYBER THREATS: AN INNOVATIVE RESEARCH APPROACH

OLEH SNIEOSIKOV, PhD student
OLEKSII P. NARIEZHNII, Associate Professor, PhD in Engineering, Scientific Adviser
IULIIA I. SHAMAIEVA, Associate Professor, PhD in Philology, Language Adviser
V. N. Karazin Kharkiv National University, Kharkiv, Ukraine

In recent years, particularly in the twenty-first century, the development of information technologies, cybernetics, and the Internet has determined and is continuing to cause significant changes in the cyberspace and society as a whole. In this connection, it is critically important to ensure the functioning of enterprises and corporate businesses and to be resilient to these changes [2; 4]. For their stable operation, the continuity of the company's business processes is crucial, which makes uninterrupted operation of networks and server infrastructures, preservation of important data, as well as high and reliable protection against cyber threats highly necessary. Thus, there is an obvious need for professional skills in utilizing security methods to ensure the high-quality functioning of information systems by enterprise cybersecurity specialists [1]. The above-mentioned justifies the relevance of developing innovative research solutions to the scientific and at the same time applied problem of creating a generalized methodology for protecting the corporate segment from cyber threats that can be implemented both in Ukraine and abroad.

For that matter, the main objective of this work is to enhance the effectiveness of developing and implementing methods for cybersecurity strategies and protection of IT infrastructures in enterprises in Ukraine.

The theoretical foundations of the research are based on the principles and methods of cybersecurity implementation used by global governments, higher mathematics, probability theory, applied cryptography and steganography, statistical decision theory, and other theories and methodologies. The research also includes mechanisms for implementing various cybersecurity strategies from Internet resources and cybersecurity decision strategies of major companies in Ukraine [3].

As for the outcomes of the present study, the practical significance of the research results lies in the fact that the proposed models, methods, and strategies can be used to organize protection against cyber threats for both the corporate segment of Ukraine and every citizen of Ukraine, and to reach a qualitatively new level in this field.

Our findings have enabled IT infrastructure protection mechanisms to become more flexible, secure, technological, and of a higher quality. Additionally, the methods of providing cybersecurity will become highly professional and sophisticated, providing the active prevention, detection, and mitigation of cyber incidents.

The recommendations advanced will be refined in such a way that they can be universally applicable to any enterprise in the country, thereby ensuring a more

reliable cybersecurity system and information protection at both national and international levels.

References:

1. Council of Europe Convention on Cybercrime of 7.09.2005 No. 2824-IV. URL: http://zakon.rada.gov.ua/laws/show/994_575.
2. On the Basic Principles of Ensuring Cybersecurity of Ukraine: Law of Ukraine of 05.10.2017. URL: http://zakon.rada.gov.ua/laws/show/2163-19
3. On Approval of the Regulation on the Organization of Measures to Ensure Information Security in the Banking System of Ukraine: NBU Resolution No. 95 of 28.09.2017: https://zakon.rada.gov.ua/laws/show/v0095500-17.
4. On measures for a high common level of security of network and information systems in the Union: Directive of the European Parliament and of the Council (EU) of 06.07.2016. № 2016/1148. URL: http://zakon.rada.gov.ua/rada/show/984_013-16.

OPPORTUNITIES AND CHALLENGES OF PLANT-MICROBIAL FUEL CELL USING

ANNA SVERGUNENKO, PhD student
DMYTRO DIADIN, Associate Professor, PhD in Engineering, Scientific Adviser
OLENA DROZD, Associate Professor, PhD in Engineering, Scientific Adviser
O. M. Beketov National University of Urban Economy in Kharkiv

Biotechnology using a microbial fuel cell (MFC) is one of the newest technologies for electricity production. Currently, generation of bioenergy via MFCs draws considerable attention [3] due to its green nature and the ability to simultaneously resolve the problem of waste management. In Ukraine, this issue is not studied enough, so it is a current and promising direction of technologies development for waste treatment and environment protection in general.

It should be noted that one of the varieties of MFC technology is PMFC. The PMFC utilizes root exudates and rhizodeposits secreted by plants in the rhizosphere region as a result of photosynthetic activity into bioelectricity using metabolic activities of microbial community residing in the rhizosphere region [4]. Moreover, PMFC could be suggested for solving technical challenges in the classical MFC like complete utilization of substrate by bacterial species.

However, more efforts remain to be done to apply PFPM to power generation, as well as to wastewater treatment or phytoremediation, due to some limitations, such as the high cost of running the system and low electricity density. This work is a sincere attempt to gather and interpret recent research results related to CFMP research in order to set a course for future aspects of technological progress.

The factors that can influence the PMFC performance on longer duration and enhance magnitude of voltage generated are plant species used in PMFC, operation parameters, electrodes materials, characteristics and properties of available wastewater, type of available microbial inoculum.