

relevant for the Ukrainian system of territorial development, which is connected with the internal factors and development problems.

References:

1. Bogashko O. L. Study of the regional innovation policy of foreign countries based on the cluster approach. *Scientific Bulletin of the International Humanitarian University. Series: Economics and management*. 2016. No. 15. P. 8–11.

2. Lishchynsky I. O. Paradigm of spatial organization of local economic development. *Bulletin of Odessa National University*. 2018. Volume 23. Issue 6 (7). P.13-17

3. M. Dyomin, K. Vyatkin, O. Syngaivska (2022). Projection of the development trends of the Kharkiv regional population settlement system in the conditions of post-war reconstruction. *Urban planning and territorial planning*, (81), P.3–12. Access mode: <https://doi.org/10.32347/2076-815x.2022.81.3-12>

DEVELOPMENT OF THE INSTITUTE OF INFORMATION SECURITY IN UKRAINE

VLADYSLAV KOSHELNYK, graduate student

OLEKSANDR A. FISUN, Professor, Doctor of Political Sciences, Scientific Adviser

NATALYA M. SAVCHENKO, Associate Professor, PhD in Philology, Language Advisor

V. N. Karazin Kharkiv National University

In our time, information security is one of the main elements of society's security. With the rapid development of technologies and the worldwide Internet, threats to the regional and national security of states have grown rapidly. The rapid development of civilization creates a number of new challenges for humanity, in particular, the creation of a safe information space. The formation of the information society, the introduction of new technologies, in turn, create a number of new threats.

We note that the study of information as a strategic resource for the development of humanity has shown that it can be reliable and relevant, new and outdated, but it cannot be transmitted, accepted or preserved in its pure form. Any information has its own carrier and is transmitted through communication channels. In the most general form, "information" means that any information and/or data must be stored on physical media or displayed in electronic form [1].

The current legislation of Ukraine does not contain a definition of the term "information security", however, as stated in the Law of Ukraine "On National Security", state policy in the spheres of national security and defense is aimed at ensuring military, foreign policy, state, economic, informational, environmental security, cyber security of Ukraine [2].

To combat information attacks and to create a truly secure and favorable information environment, the first step is to create an effective regulatory framework. Today, the issue of information security is regulated in such normative legal acts as:

- in 1997, the National Security Concept of Ukraine was approved, however, the Information Security Concept of Ukraine was not created on the basis of this document, and the document itself has only a doctrinal character and serves as a basis for the further regulatory framework;

- in 2003, the Verkhovna Rada of Ukraine adopts a fundamental legal act in the field of national security - the Law of Ukraine "On the Basics of National Security of Ukraine", however, information security is not given due attention. In 2009, the first state act in the field of information security appeared, which was signed by the President of Ukraine, and later the Doctrine of Information Security of Ukraine was adopted.

However, truly effective mechanisms for countering propaganda and information attacks appeared only in the National Security Strategy of Ukraine dated September 14, 2020. The Doctrine of Information Security, which was put into effect by the Decree of the President of Ukraine dated February 25, 2017 No. 47/2017, deserves special attention. One of the directions of the adopted Doctrine is the use by the Russian Federation of hybrid war technologies against Ukraine, which turned the information sphere into a key arena of confrontation [3].

We note that information security of Ukraine is regulated by the following laws: Law of Ukraine "On Information" of 1992, Law of Ukraine "On Protection of Information in Information and Telecommunication Systems" of 1994, Law of Ukraine "On State Secrets" of 1994, Law of Ukraine "On the protection of personal data" 2010 [4]. The main subject in the field of information security of Ukraine is the Interdepartmental Commission on Information Policy and Information Security, which operates under the National Security and Defense Council (NSDC). Among its main tasks, in particular, is the analysis of the state and possible threats to the national security of Ukraine in the information sphere and the generalization of international experience in the formation and implementation of information policy [5].

We should also note that the country should have strong and independent mass media as the main mechanism for conveying information to the population. A quality Ukrainian information product should appear in the world, both on television and on the Internet. A unified regulatory framework should be created in Ukraine, which will provide for methods and ways of ensuring a favorable information space, and the information sector should be prioritized at the same level as the economy and politics. The creation of a secure information environment requires complex and decisive work by the state leadership: the introduction of effective state institutions, the adoption of relevant normative legal acts that would regulate information security issues, perhaps even a codified law in the field of information security.

Therefore, information security is a priority area, like the economy or the social sphere. Success in the field of information security can only be achieved through a comprehensive approach that combines proper management (administrative level), the company's efforts to convince employees of the need to improve information security (procedural level), the creation of legislation and state control over the level of information security (legislative level), use of domestic software and information technologies (software and technical level).

References:

1. Law of Ukraine «On Information». Information of the Verkhovna Rada of Ukraine. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (Last accessed on: 12.03.23).
2. On the national security of Ukraine: Law of Ukraine dated June 21, 2018 № 2469-VIII. URL: <http://zakon.rada.gov.ua/laws/show/2469-19#n355> (Last accessed on: 12.03.23).
3. The doctrine of information security of Ukraine, approved by the Decree of the President of Ukraine dated February 25, 2017. № 47/2017. URL: <http://president.gov.ua> (Last accessed on: 15.03.23).
4. Dmytrenko M.A. Problematic issues of information security of Ukraine. *International relations*. Political science series. 2017. № 17. 236–243.5.B.V. Ostroukhai, B.M. Petryk, M.M. Prysiazhniuk. etc. ed., Information security (social and legal aspects): textbook. Kyiv. 2010.

ACTUAL PROBLEMS OF DESIGNING AUXILIARY DIRECT CURRENT POWER SUPPLY SYSTEMS FOR ENERGY FACILITIES IN UKRAINE

GENNADII LOKTIONOV, PhD student, Head of EPC projects department of ELCOR CORPORATION

VLADISLAV PLIUHIN, Associate Professor, Doctor of Science in Engineering, Scientific Adviser

OLENA ILIENKO, Professor, Doctor of Science in Education, Language Adviser
O. M. Beketov National University of Urban Economy in Kharkiv
ELCOR CORPORATION

Auxiliary direct current power supply system (ADCPSS) is an important subsystem of any energy facility - power plants and high-voltage distribution substations. ADCPSS is designed for uninterrupted and high-quality power supply of such critical systems as a relay protection system, a process automation system, emergency technological equipment and emergency lighting, which are essential for the overall operation of the energy facility.

Therefore, standardized, enhanced requirements should be applied to the design of the DC EPS to ensure the following parameters:

- high reliability and durability of the system;
- required quality of electrical power in the DC power supply network;
- quick fault localization in individual sections of the system (sensitivity and selectivity of short-circuit protection);