

The theme of the final qualifying work: the Rationale for the choice and development of a system of layered information security for the management of integrated security of the UKB FGBOU VO "PSU»

Author WRC: Tolstoguzov Daniel Vladimirovich

Scientific supervisor: Cand. Techn. Sciences, Assoc. Department of "Information and communication technologies, mathematics and information security" V. A. Kozlov

Information about the customer organization: PYATIGORSK state University»

The relevance of the development of a system of layered information security is due to the fact that unauthorized access to confidential and confidential information circulating in the enterprise or illegal acquisition of this information by direct competitors can result in large material losses for the enterprise, and possibly complete bankruptcy.

Purpose: the study of technologies that can be used to increase the level of security of the enterprise.

Tasks:

- study of the structure of the organization and the subject area of its activities;
- analysis of methods and means to ensure control of information security incidents, classification of identified incidents by the nature of the violation;
- study and analysis of issues related to the protection of information of the institution;
- development of proposals to improve engineering and technical support of information security at different levels of defense.

Theoretical significance of the study:

- identified the shortcomings of the existing enterprise system of integrated information security;
- analyzed legal and legislative documents in the field of information security;
- studied the existing enterprise systems of software and hardware information security;
- the structural two-level scheme of the system of the echeloned defense of external and internal subnets of the enterprise is offered.

Practical significance of the results: the possible variants of the two-level scheme of the enterprise security circuit are analyzed and investigated. The first circuit is the internal network (Internal network), and the second circuit – and the perimeter network (perimetr network) which are separated by a firewall (internal gate). Next, after the perimeter network is the network of the Internet provider. A perimeter network is called a demilitarized zone (DMZ) – a buffer zone in which servers with public resources are located, namely a WEB server and an FTP server to provide access to public resources from the Internet and a local network.

Results: the analysis of the structure and subject area of the object of study; a description of the material and hardware and software of the object of study; formulated the problem and developed a block diagram of a multi-level layered system of security and information protection.

Recommendations: a block diagram of a multilevel layered system of security and information protection has been developed. The global layered system allows, proceeding from insignificant redundancy to create technology of protection when each separate level of protection is protected by more than one subsystem of protection. At the same time, the mathematical basis of each such subsystem is different mathematical models and methods. Therefore, by hacking one of the security subsystems of a particular level, the attacker will not be able to use the result of their efforts, as will not pass the protection of the second subsystem of this level.