Theme of final qualifying work: Development of a remote authentication algorithm for entering the database over an unprotected communication channel (using the example of the FSUE IC Stavropolkraivodokanal "Pyatigorsk Vodokanal", Pyatigorsk)

WRC author: Vladislav Denisovich Minskov

Supervisor WRC: Cand. tech. Sci., Associate Professor, Department of Information and Communication Technologies, Mathematics and Information Security V. A. Kozlov

Information about the customer organization: FGBOU VO "Pyatigorsk State University"

Relevance of the research topic: The procedure for entering the database is always relevant from the point of view of unauthorized access to the database.

therefore, the authentication algorithm developed by us based on cryptographic transformations is an urgent scientific task.

Objective: is to apply the acquired theoretical knowledge in practice in the processing of the collected material in order to design a graduation project, having developed professional skills and abilities in the field of engineering and technical protection of information in the enterprise.

Tasks:

• become familiar with the purpose and activities of various departments of the Pyatigorsk Vodokanal enterprise;

• evaluate the material and technical support of the enterprise;

• to study the systems of engineering and technical protection of information operating in the enterprise;

• perform the problem statement and check the cryptographic strength of the remote authentication algorithms at the enterprise;

• develop proposals for improving the engineering protection of enterprise information.

Theoretical and practical significance of the research:

Theoretical significance:

- revealed the shortcomings of the remote authentication acting on the object under study;

- analyzed legal and legislative documents relating to the protection of information and information security of the enterprise;

- the systems of program and technical means of information protection functioning on the object of study were studied;

- a mathematical model and algorithm for its implementation of a remote authentication module based on a hybrid probabilistic model of cryptographic transformations have been developed.

The practical significance of the results:

- analyzed the options and types of remote authentication systems;

- a mathematical model and algorithm for solving the problem of transmitting information via unprotected wireless communication channels were proposed.

The results of the study: authentication based on a hybrid probabilistic model of cryptographic transformations.

will significantly improve the reliability of authentication of the person who receives access to the database

Recommendations:

• Authentication based on a hybrid probabilistic model of cryptographic transformations.

• Kerberos network authentication protocols. One of the main advantages of the Kerberos protocol, which guarantees a high level of network security, is based on the fact that in all client-server network interactions, neither passwords nor password hashes are transmitted in the clear.