UDC004.056.479

Dmytro Yevstihnieiev, student
Supervisor – Pererva K., senior lecturer
Dnipropetrovsk National University of Railway Transport
named after academician V. Lazaryan

TECHNICAL PROTECTION OF INFORMATION

The object of protection may be information which is a state secret or other provided by law. Confidential information is information which belongs to state or given to the state for possession and using or information with restricted access (IWRA). Secret information is information with restricted access which contains data constituting a state or other secret provided by law [1]. Object of protection, goal and tasks are determined and established by persons who own, use and manage IWRA.

Information carriers with restricted access can be physical fields, signals, chemical substances, which are created in the process of information activities, production and exploitation of products for different purposes. Communication lines, alarm and control lines, power networks, engineering communications, enclosing engineering structures, heating constructions and light-permeable elements of buildings (apertures) can be environment of distribution of IWRA carriers. Leakage or integrity violation of IWRA (distortion, modification, destruction) may happen due to the impact of information security threats.

The goal of technical protection of information (TPI) is prevention of information leakage or integrity violation. This purpose can be achieved by creating information security system, which is organized set of methods and tools for ensuring TPI [2]. TPI must be implemented by stages – first stage is identification and analysis of threats, second stage is development information security system, third one is information security plan implementation and last fourth is operation control and information security system’s management.

Information leakage is uncontrolled data distribution which leads to unauthorized access to it. Integrity violation is info distortion or destruction. Blocking of information is excluding the possibility of authorized access to that data. Threat for data is leakage, possibility of blocking or integrity breaching. It can be implemented by using technical tools and information security technologies [2].

Access to information is a possibility to get and process data. Unauthorized access is access to info which violates the procedure for its implementation and established legal norms [1]. Inset device is hidden installed technical tool threatening information. Drop dead device is a secretly implemented program threatening information which is stored in the computer.

These are the basic concepts related to the technical protection of information. Despite the fact that recently the emphasis shifts to software protection, we should not forget about the hardware (hardware) protection of information because it is much more complex and important.

Literature:

1. Shaffer, M. Protection from noise and vibrations in HVAC systems [Text]: management / M. Shaffer .- M.: Avok-Press, 2009. 231 p.

2. Engineering and technical protection of information: A manual for universities / AA Torokin .- M.: Helios ARV, 2006. 958 p.