INFORMATION SECURITY SYSTEMS ARCHITECTURE IN TRANSPORT LOGISTICS

Degtyareva L.[1], **Miroshnykova M.**[2]

[1] *Poltava National Technical Yuri Kondratyuk University, Poltava, Ukraine*
[2]*Volodymyr Dahl East Ukrainian National University*

In information systems of automated control systems for any purpose: in the areas of government, military, banking, vehicle management, etc., the volume and value of strategic and confidential information, which is used and transmitted through information and communication facilities, is constantly growing, therefore Of great importance are the speed and information reliability of data transmission, which determine the effectiveness of information systems.

Since the information security system is a structural unit of information systems, therefore, it is a structural, functional and organizational substructure that reproduces the architecture of the system that requires protection.

One of the options for a possible architecture is presented in Fig. 1.

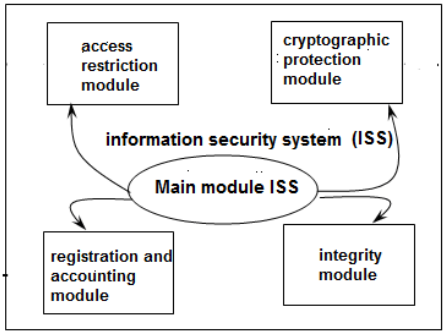

Fig.1. Architectural construction of information security system

Information systems of transport logistics accumulate a large amount of information about the location of objects and possible options for optimal routes. These data allow you to optimize the routes of movement and transportation, to fix the illegal use of the vehicle without supporting documents (route sheets), violation of the time frame for transportation, but also to reduce operating costs, as well as to fix offenses or theft of vehicles. Information systems that are used on the workstations of operators serving transpor-

tation services, record changes in the schedule of movement of motor vehicles and trucks, trains or buses in real time. They should take into account all possible adjustments in routes and travel time.

The main module may include organizational (a group of employees specifically designated to ensure the protection of information in accordance with the developed rules and regulatory framework governing the performance of these functions by the information protection service) and technical components (a set of ISS technical equipment, reflection of their condition, access control, and control of their inclusion etc.).

The access restriction module is designed to perform the functions of identification, authentication and control of user access and processes to the system, server, networks and communication channels: peripheral devices, programs, disks and files-carriers of confidential information.

The access restriction model, in response to attempts at unauthorized actions, must perform one of the procedures, depending on the means and methods of intervention: interruption of data processing, protected destruction of information that may become available as a result of identified unauthorized impacts; urgent message about the dangerous situation the existing service, which is responsible for the state of information security; taking steps to detect the intruder and / or eliminate the danger.

The module, which is designed for cryptographic protection, ensures the integrity and confidentiality of stored information on various types of media and information that can be transmitted via communication channels; Providing data source authentication and hiding the content of confidential messages.

Among the possible modules that make up the information protection system, the integrity module is mandatory and one of the most important. Its functions may include tools and methods to ensure the administration of information security; restoration of the information security system in case of possible failures: periodic testing of personal data protection system functions. Threats to integrity violations exist at all levels of the information system: threats to the integrity (reliability) of information or information carrier (destruction of the carrier and information stored on it); threats to the integrity of the software environment and the hardware configuration of the information system; threats to the integrity of the premises are subject to the building, the surrounding area, etc.

The registration and accounting module using the means of recording and recording events / resources with an indication of the time and event participant, is responsible for collecting data on events occurring in the information system, recording the date and time of printing a document and the number of its printed copies; control and fixing of information on data

transmission in the form of packets or messages on lines and communication channels. Registration can be carried out by means of manual or automatic logging and the formation of summary reports of the work of users and equipment on selected parameters, which must be pre-registered. This module is necessary to identify the recording and analysis of events related to the security of information, despite the fact that this module is not used directly to prevent security breaches.

The security management system monitors the work of the hardware and software, controls the processing of data and signals the possible penetration of the system into the security personnel, who act in accordance with established rules and regulations.

Transport logistics systems are developing rapidly and are of great importance for Ukraine in modern conditions, therefore the security of information for these systems is of paramount importance.

References:

1. Stepanov O.O., Kornyeyev I.K. Informatsiyna bezpeka ta zakhyst informatsiyi. – M.: YNFRA-M, 2001. – 304 s.
2. Khoroshko V.A., Chekatkov A.A. Metody i zasoby zakhystu informatsiyi – K.: Yunior, 2003. – 504 s.
3. Degtyareva L., Miroshnykova M. The problems of the security of information transport and logistics systems // Theses of international scientific and practical conference "Globalization of scientific and educational space. Innovations of transport. Problems, experience, prospects", May 2018, Italy. – S. 32-34.
4. Kormych B.A. Informatsiyna bezpeka: orhanizatsiyno-pravovi osnovy: Navch. posibnik. – K.: Kondor, 2004.-384 s.