ABSTRACT

Actuality. Modern vehicles offer a vast number of digital features. They are varying from safety systems, digital assistant to comfort and cars are becoming more and more part of human and business life. By 2020, approximately 220 million vehicles expected to be equipped with network systems.

However, along with new opportunities, there are associated risks. Enhanced networking capabilities (Bluetooth, Wi-Fi, 4G, and GPS) significantly increase the ability to manipulate parts of the system.

Vehicles attract the attention of hackers, for which the car is not fundamentally different from a stationary computer, ATM or smartphone. Now it is not enough to ensure the normal operation of all components of the car and to protect the driver along with passengers from an accident. All these threats necessitate the implementation of a system for detecting attacks for embedded network systems of the car.

Relationship of work with scientific programs, plans, themes. The work was carried out at the Department of Automated Systems for Information Processing and Management of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" within the objective of the work "Creation of simulation methods for discrete-event systems" (State registration number 0117U000923).

Purpose of the study is to analyze the safety of the car and create a system for detecting threats.

The following tasks must be fulfilled to achieve the goal of the study:

- analysis of the architecture of electronic components of the car;
- carry out an overview of existing intrusion detection systems;
- the choice of the neural network architecture and the method of training;
- review carrying out attacks on vehicle ECUs and consequences;
- construction of a threat model;
- create attack surface for ECUs and provide quantitative assessment for it;
- providing features of ECUs for modeling them;
- ECUs modeling and data for normal behavior and performing attacks;
- statements of general attack algorithms and features for their detection;
- development of the intrusion detection system architecture;
- creation of software that implements selected architecture;
- provide analysis of achieved results.

The object of research is the analysis of information security of the vehicle electronic control units and counteraction to threats.

The subject of research is the analysis of existing threats and methods of detecting their use.

The research methods used in this paper are based on machine learning methods, hazard categorization models, and expert judgment.

The scientific novelty of the results obtained is to create a threat model based on previously detected attacks against vehicle electronic control units, assessing the surface of

threats, taking into account the effects of interference with the operation of the car, and not just the loss of data. The parameters of modeling of electronic control units, signs of detection of abnormal behavior in the car network for the training of the neural network were proposed.

Publications. The materials of the research were issued with two research articles «Analysis of threats for vehicle electronic control units in CAN network», «Assessment of attack surface for vehicle electronic control units in CAN network», in the collection of articles of the International scientific-practical conference «Informatics and Computing Technology-IOT-2018».

VEHICLE, ELECTRONIC CONTROL UNITS, INTRUSION DETECTION SYSTEM, THREAT MODELING, ATTACK SURFACE, MACHINE LEARNING.