Vol. 4, No. 1, 2023

Ganna Weigang, Kateryna Komar
Ivan Franko National University of Lviv
1, Universytetska St., Lviv, 79000, Ukraine

https://doi.org/10.23939/tt2023.01.062

ANALYSIS OF THE SECURITY OF ON-BOARD INFORMATION SYSTEMS IN VEHICLES

Summary. *The features of the functioning of the on-board information systems of a car are considered. Threats to their security are analyzed, and methods for ensuring information security and functional security of on-board information systems are proposed. The design of road networks in the organization of road traffic is one of the factors in ensuring the functional security of modern intelligent transport systems, that is, compliance with such information security attributes as data confidentiality, integrity, availability, authenticity and novelty of data. The security of on-board vehicle information systems is a critical issue in the modern world, as more and more vehicles are equipped with electronic systems that may be vulnerable to cyber attacks. One of the main challenges of protecting on-board information systems is the wide range of devices and technologies used in modern vehicles. Different systems may have different security requirements and vulnerabilities. They may interact with each other in a complex way. Another challenge is that many of these systems were not designed originally with security in mind. They may lack basic security features such as encryption and authentication and use outdated software and protocols that are vulnerable to known attacks. The main types of attacks and threats to the elements of the transportation system that interact with the VANET were identified to analyze the information security of vehicle in-vehicle systems. Based on the theory of fuzzy sets under conditions of uncertainty and using the Fuzzy Logic Toolbox in the integrated Matlab environment, the level of information security of the OBU-VANET system was modeled. The obtained results allowed us to formulate the degree of information security of vehicle operation elements against unauthorized access to data. The results of the study showed that technical communication systems have the highest security level (> 0.7), and vehicles become the most vulnerable in public places.*

Key words: *on-board information systems, information security, functional security, road network, model of information security of transport systems, risks.*

1. INTRODUCTION

The popularization of the use of a vehicle's on-board devices requires more and more high-tech elements of the vehicle's information control system (ICS) [1, 2]. Therefore, improving the quality, reliability, and performance of a car's ICS is an essential and urgent task. The way to solve this problem is to develop methods for the synthesis of ICS using a multifactorial and multilevel mathematical model of the control object, taking into account its nonlinear characteristics, parameters of intelligent control systems, the latest information technologies, as well as stochastic characteristics of external influences (attacks) acting on the car [3, 4].

Requirements for improving ICS began to be put forward at the stage of developing the methods for creating automatic control systems for complex machines and complexes. Information technology has become the backbone in the process of complete digitalization of all layers of industrial society. Therefore, the qualitative development of automation systems for controlling work processes, movement and

diagnostics of vehicles using microprocessors, and computer equipment with appropriate software is a necessary component of the entire transport system [5].

In intelligent transportation systems, each vehicle assumes the role of a sender, receiver, and router to transmit information to a transportation network or environment. Then it uses the received data to ensure the safe and free traffic flow. Vehicles must be equipped with an On Board Unit (OBU) or any other radio interface that allows for the transmission of information over wireless ad hoc networks to communicate between vehicles and Roadside Units (RSUs).

2. RESEARCH STATEMENT

The aim of the article is to study the information security of computer on-board vehicle systems and analyze the relationship with the level of accidents on megacities' highways. Providing drivers with up-to-date and reliable information about road conditions, traffic flows, and the state of the driven vehicle is one of the ways to regulate dangerous situations caused by overloading and congestion.

The following tasks need to be solved to achieve this goal:

- classification of automotive sensors;
- analysis of communication and navigation technologies used in intelligent transportation systems
- use of systematic analysis of urban environment parameters to assess traffic safety;
- identification of elements of the car information system;
- formation of interconnections between information security subsystems.

3. LITERATURE REVIEW

Fig. 1 shows a typical block diagram of a modern digital automotive information display system. Signal processing and logic functions are performed by an electronic control unit (ECU). The standard sensors are connected to the ECU, which controls the necessary information display devices and the display. The ECU allows the system configuration to be customized for a specific vehicle model and data processing environment. Modern vehicles are equipped with wireless communication facilities and access to global information systems and networks.

The interaction of the car's ECU with other ITS elements and traffic participants must meet the needs of drivers for fast and up-to-date information. Increased mobility has a negative impact on the safety of people (drivers and pedestrians). Traffic incident management is a functional part of a holistic approach to solving traffic problems and one of the primary tasks of ITS. Continuous improvement and development of communication and navigation technologies and their implementation at different stages of emergency management can significantly reduce the consequences of events occurring in an incident, such as congestion, delay, pollution and quite dangerous secondary accidents [6, 7].

One of the essential conditions for achieving the maximum level of safety of the system is high-quality communication between road users, i.e., information transparency and secure real-time data flow. The absence of such an approach, which combines cooperation, communication and training, is one of the main reasons for the ineffective incident management process. Information about a vehicle in traffic involves the activation of various means of disseminating information related to incidents, affected motorists, etc.

The media used to disseminate information about a vehicle include:

- commercial radio broadcasts;
- highway advisory radio (HAR);
- variable message signs (VMS);
- telephone information systems;
- route guidance information or systems;
- Internet/online services;
- various information dissemination mechanisms provided by information service providers.

Thus, in a modern car, an efficiently and reliably operating ICS, as a rule, should contain three types of interfaces for combined exchange in the communication process [1]:

1. A high-speed interface used in highly loaded and critical nodes of the vehicle safety and control systems;
2. An interface for implementing a single two-wire vehicle information system and connecting various nodes and control systems to it with medium data exchange rates;
3. A relatively inexpensive and reliable interface with a low exchange rate that can be used to connect various final actuators or sensors with control systems.

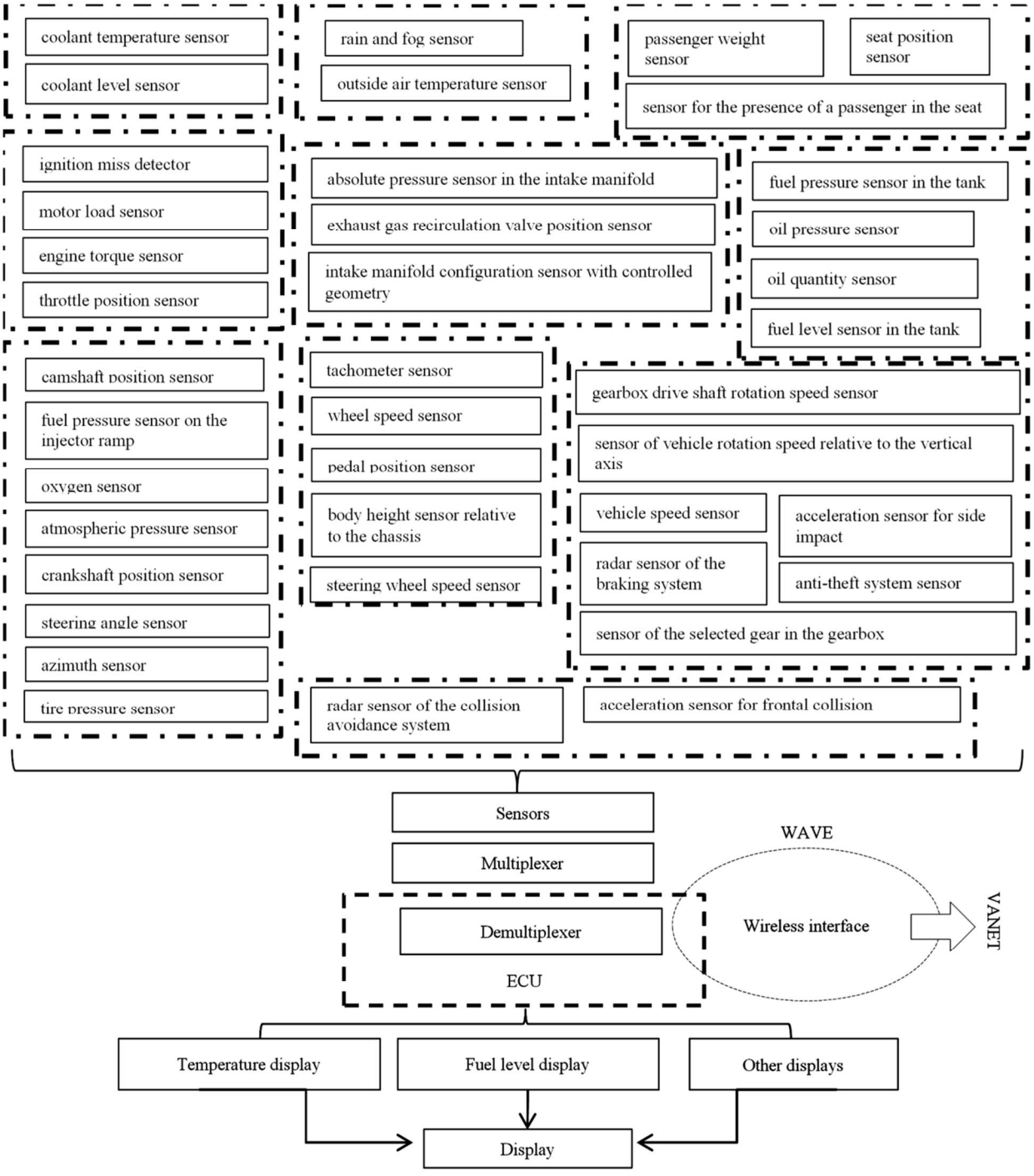

Fig. 1. A typical block diagram of a digital information display system.

Mobile (wireless) communications and related technologies and services have become increasingly important recently. Cars are becoming more robotic and equipped with a large number of mobile applications (Fig. 2). The development of wireless communication systems and their application in the daily lives of users have made it possible to use mobile communication technology in urban processes and opened up the possibility of totally new solutions that have not been implemented so far.

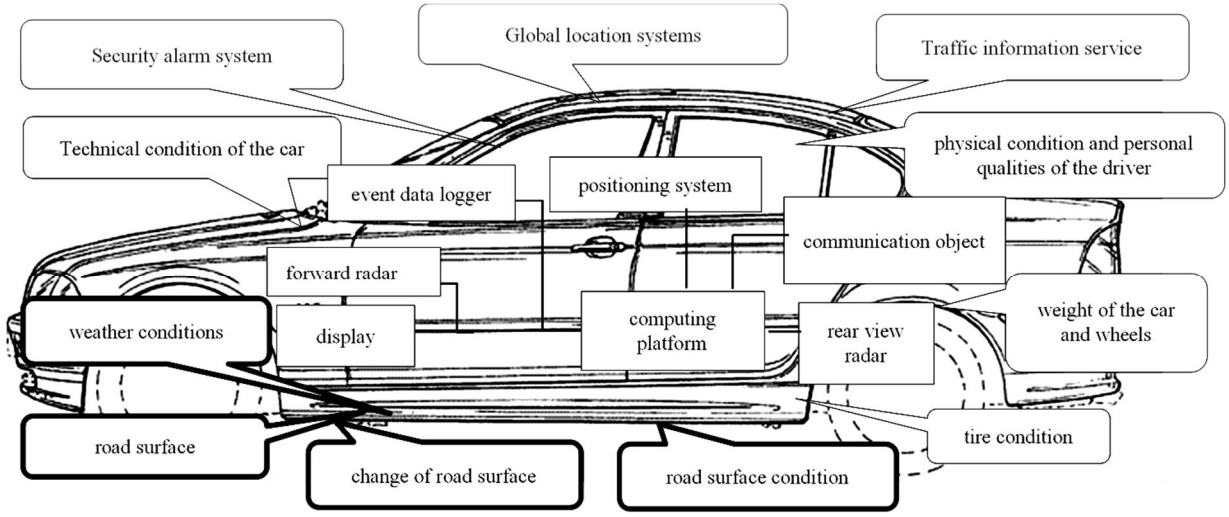

Fig. 2. Diagram of the human-machine-environment system

Technologically advanced solutions based on mobile communication systems have made it possible to create urban and transport policies aimed at meeting the growing necessities of the population to ensure their mobility, accessibility, efficiency, energy efficiency and environmental protection.

Equipping a car with modern communicators improves the driver's interaction with other traffic participants and systems in general and significantly increases the quantitative indicators of penetration into the ECU and ICS.

4. MAIN PART

The analysis of the security of the car's onboard systems made it possible to identify the main types of attacks used for OBU and external influences of the systems, VANETs, for example.

The vehicle security system includes a remote control system for the anti-theft device, protection of the ICS and communication channels with GPS, GIS, etc.

The composition of security systems and options of their configuration depend on the vehicle model and its configuration. These indicators are crucial for choosing an attack method. The availability of wireless communication devices and the use of remote security systems made it possible to group attacks based on the location of the distribution.

For automotive security systems, this is [8]:

– playback of previously recorded code,
– reproduction of previously recorded code using scanners or grabbers,
– cryptanalysis,
– hacking during maintenance.

For on-board computers, this is [9]:

– failure to immobilize the engine,
– failure of vehicle systems,
– cryptanalysis.

However, the most prevalent attacks are directed through communications and navigation systems, as well as vehicle-automated networks (VANETs).

The list of attacks is given below [10]:
- broadcasting false information,
- malicious software,
- spam,
- black hole attack,
- masquerading,
- spoofing,
- privacy threats.

The above attack options indicate the vulnerability of vehicle security systems, including information security, combined methods of protection, a complication of user authentication process, technical capabilities and algorithms.

Studying and determining the causes and consequences of information attacks on a vehicle requires the use of several methods to obtain relevant and reliable information about the security or vulnerability of on-board computers from various types of threats and their configurations. Therefore, in addition to the analytical method, the fuzzy modeling method was chosen [11–13].

This mathematical apparatus allows the determination of quantitative characteristics by a subjective method using a given rule base and a clearly defined value of the output element [14, 15]. The input and output data are the types of threats and the level of information security, respectively. The grouping was done according to the location of the attack (Table 1). The number of rules will depend on the number of input criteria and form the knowledge base of each group, 27 for 3 input elements and 81 for 4, respectively (Table 2).

Table 1

Distribution of input elements

Group	Type of attack		Intermediate indicator		Output indicator
1	Breakage during maintenance	s_{CS1}	Car system security	S_{CS}	Information security S_I
	Failure to immobilize the engine	s_{CS2}			
	Failure of car systems	s_{CS3}			
	Broadcasting inaccurate information	s_{CS4}			
2	Play previously recorded code	s_{OBU1}	OBU security	S_{OBU}	
	Malware	s_{OBU2}			
	Black hole attack	s_{OBU3}			
3	Spam	s_{V1}	VANET security	S_V	
	Masquerade	s_{V2}			
	Spoofing	s_{V3}			
	Threats to confidentiality	s_{V4}			

Table 2

Knowledge base with rules of output dependence on the state of inputs

No. of the rule	Condition	The value of the linguistic term at the input			Condition	Level
1	2	3			4	5
1	IF	L	L	L	THEN	Low probability
2		L	L	A		
3		L	L	H		
4		L	A	L		

Table continuation 2

1	2	3			4	5
5	IF	L	A	A	THEN	
...		…	…	…		
...		…	…	…		Average probability
13		L	H	H		
...		…	…	…		
...		…	…	…		
21		H	A	L		
22		H	A	A		
23		H	H	L		
24		A	H	H		High probability
25		H	A	H		
26		H	H	A		
27		H	H	H		

According to the data of Table 1, the hierarchical structure (Fig. 3) of the dependence of vehicle security and its information security was graphically depicted.

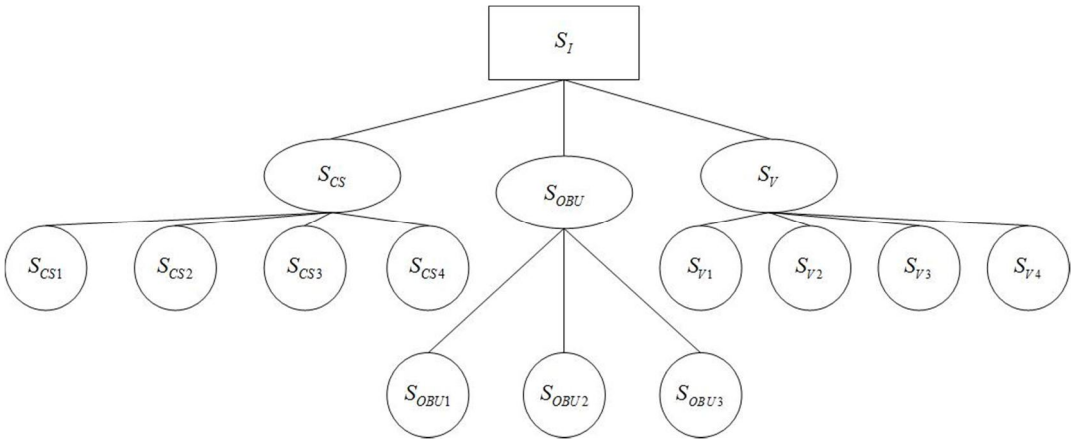

Fig. 3. Hierarchical tree of logical output of the determinant level

Fig. 4 shows the input and output indicators. The evaluation range and the definition of levels and comparison conditions are necessary for the next stage of creating a rule base. It is possible to use graphs of one or more types for convenience and simplicity of determining the evaluation limits for the proposed scale in advance.

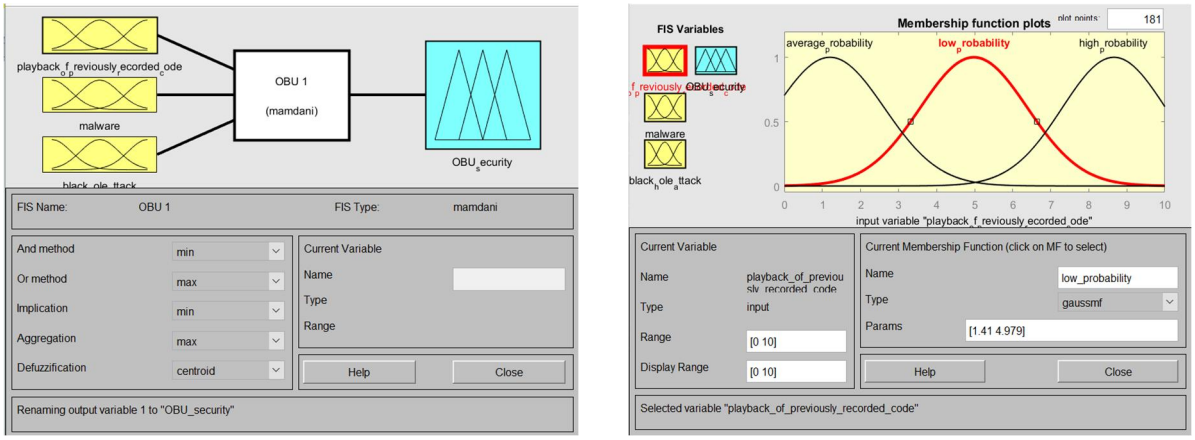

Fig. 4. Visualization of the stages of input elements and comparison conditions

The rules described above are entered into the Rule Editor Matlab environment, which is used to build the response surface (Fig. 5).

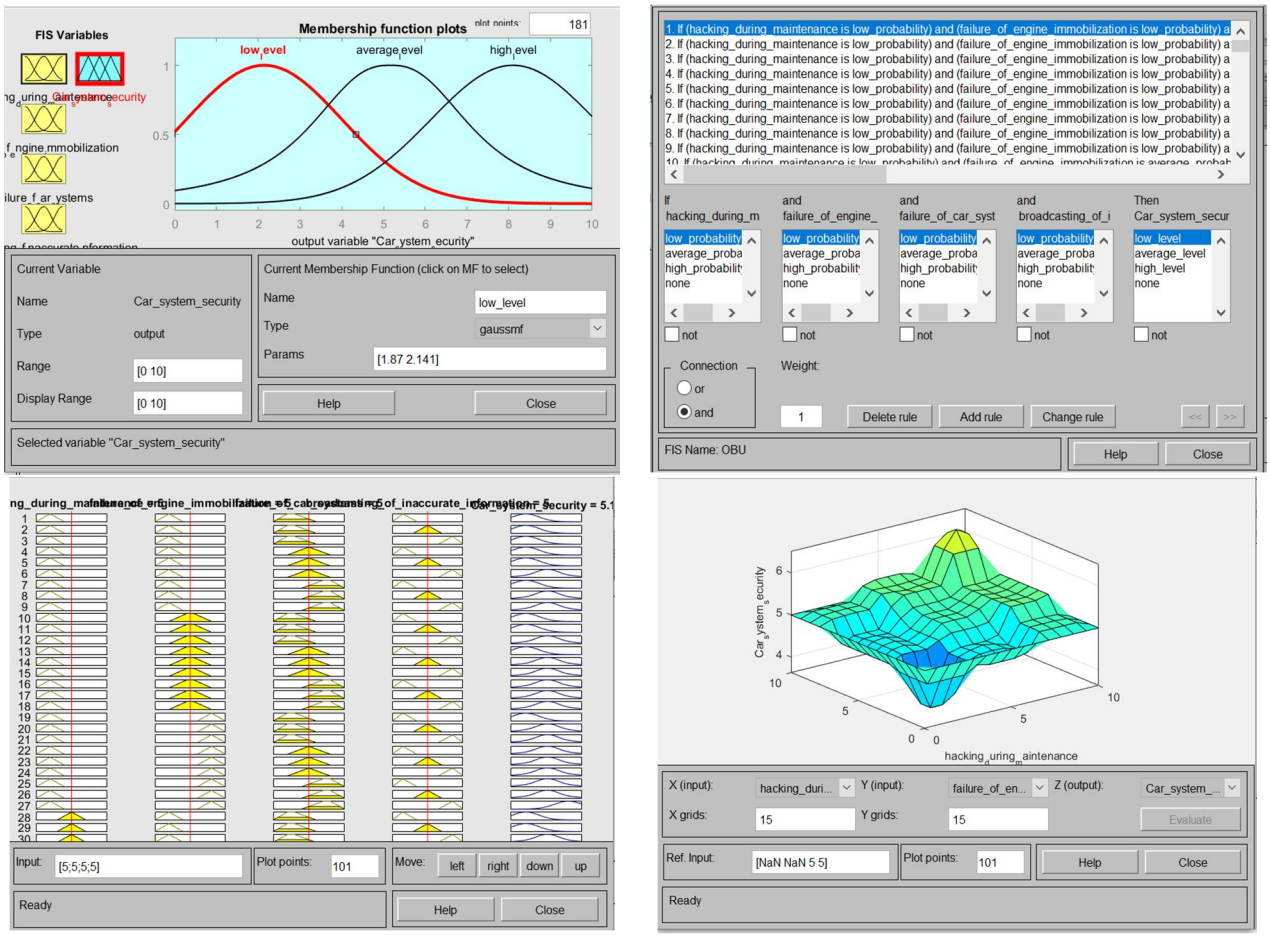

Fig 5. Final stages of visualization of building a feedback floor

To analyze vehicle security and select the effective functioning of OBU security, taking into account the attacks and the information component of the ITS. Groups of attacks were combined depending on the place of their distribution and functional limitations as a result of their operation.

The vehicle security model is a function of individual indicators that determine the level of protection and information security of the vehicle.

According to Formula 1, it can be represented as follows:

$$S_I = f(S_{CS}, S_{OBU}, S_V) \Rightarrow S_{CS} \cup S_{OBU} \cup S_V \quad (1)$$

Since each of the subsets of Formula (1) is an element of a hierarchical structure and contains a number of possible threats that may affect its effective operation, the indicators were processed using the theory of fuzzy sets according to the Mamdani algorithm.

The calculation method allowed us to obtain the results of fuzzy inference for individual indicators. The results are shown in Table 3.

Table 3

Results of calculating the values of indicators

No.	Location where an attack is possible	Values of indicators on a scale [0;1].		
		S_{CS}	S_{OBU}	S_V
1	2	3	4	5
1	Service station	0,47	0,3	0,47

Table continuation 3

1	2	3	4	5
2	Parking lot	0,50	0,48	0,38
3	When stopping at an intersection	0,59	0,61	0,58
4	While driving	0,61	0,73	0,62
5	During Bluetooth headset operation	0,89	0,81	0,13
6	Android applications	0,66	0,91	0,27
7	Mobile communication	0,32	0,53	0,48
8	Files in the stereo system	0,11	0,44	0,33
9	Synchronization with GPS systems	0,26	0,23	0,46
10	WAVE communication standards	0,33	0,35	0,86

As a result of data processing, we obtained the values of three separate indicators in the range from 0 to 1.

We determined the level of information security of the vehicle (S_I) (Table 4) in accordance with the hierarchical structure proposed by us (Fig. 3) based on the calculated data and using fuzzy inference methods.

The locations were proposed taking into account the peculiarities of the building and parameters of the road network and the relevant technologies for communication.

Table 4

Degree of information security

No.	Location where an attack is possible	Degree of information security on a scale [0;1].
1	Service station	0,24
2	Parking lot	0,33
3	When stopping at an intersection	0,49
4	While driving	0,65
5	During Bluetooth headset operation	0,21
6	Android applications	0,62
7	Mobile communication	0,71
8	Files in the stereo system	0,21
9	Synchronization with GPS systems	0,82
10	WAVE communication standards	0,75

According to the calculated data, we have determined the following:

- the locations with the highest probability of attack are technologies for communication between the car and external communication and navigation systems;
- attacks are possible in places with a sufficiently effective level of communication, so we can conclude not only about the degree of protection of communication systems but also about their feasibility in ITS for quick notification of road users, for example;
- an integrated approach to improving security is not possible without the use of information technology and communication networks.

A graphical representation of the dependence of our proposed attack groups under the hierarchy tree (Fig. 3) is shown in Fig. 6, and the response surface is in Fig. 7.

The analysis of threats to on-board information systems made it possible to identify vulnerabilities in the process of protecting the vehicle and the places of their spread. The application of fuzzy set theory in the course of the study made it possible to assess in detail the threats and their impact on changes in the level of information security from the implementation of various attacks and their combinations.

For example, the assessment was carried out for the VANET network, given its relevance and novelty in its application in intelligent transport systems and urban mobility systems.

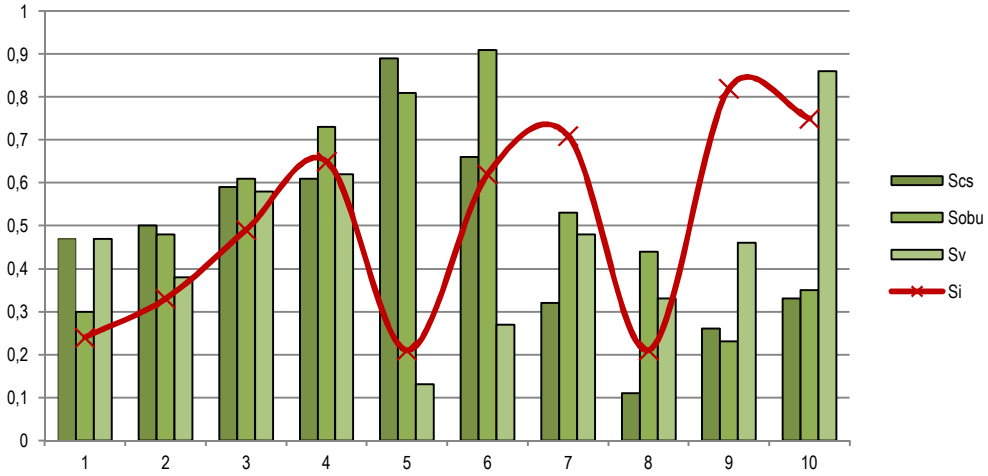

Fig 6 Degree of information security

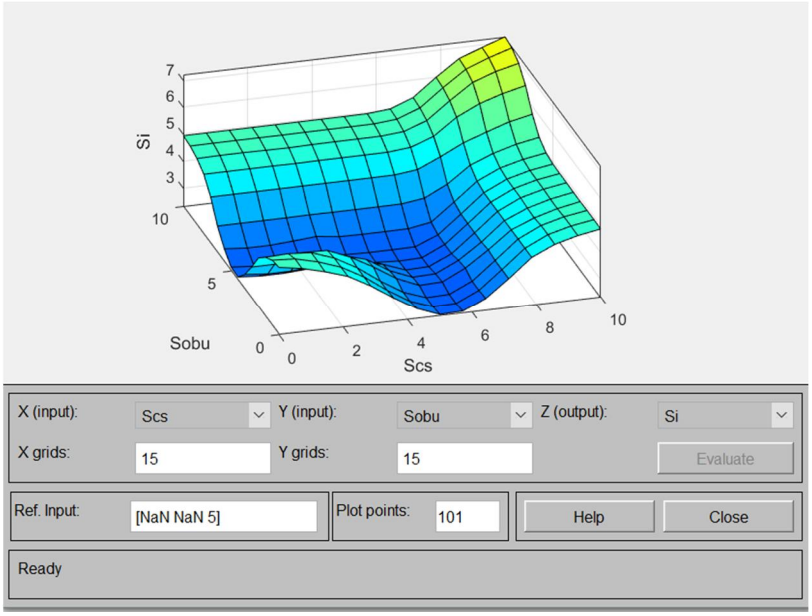

Fig 7 Response surface of the degree of information security

5. CONCLUSIONS

Thus, ECUs and ICSs are increasingly using innovative technologies, which, on the one hand, contribute to the efficient use of transportation systems, but on the other hand, are becoming more vulnerable to external threats. The study of VANET security and the most vulnerable locations showed that the level of vulnerability depends on many factors. However, the development of VANETs contributes to effective incident management and requires an integrated approach to the selection of this network, taking into account the parameters of the road network and traffic conditions. Therefore, continuous monitoring of the network reduces the risk of unauthorized interference with the operation of both individual ITS elements and the entire transport system and is advisable to improve traffic safety in the central areas of the city.

References

1. Chatti, W. (2020). Information and communication technologies, road freight transport, and environmental sustainability. *Environmental Economics*, *11*(1), 124–132. doi: 10.21511/ee.11(1).2020.11 (in English).

2. Karoń, G., Janecki, R., & Mikulski, J. (2022). Selected issues of systems engineering methodology in the design of transport systems. *Transport technologies*, *3*(2), 85–101. doi: 10.23939/tt2022.02.085 (in English).

3. Ziakopoulos, A., Petraki, V., Kontaxi, A., & Yannis, G. (2022). The transformation of the insurance industry and road safety by driver safety behaviour telematics. *Case studies on transport policy*, *10*(4), 2271–2279. doi: 10.1016/j.cstp.2022.10.011 (in English).

4. Miler, R. K., Kisielewski, M. J., Brzozowska, A., & Kalinichenko, A. (2020). Efficiency of telematics systems in management of operational activities in road transport enterprises. *Energies*, *13*(18), 4906. doi: 10.3390/en13184906 (in English).

5. Khudyakov, I. V., Hrytsuk, I. V., Chernenko, V. V., Hrytsuk, Y. V., Makarova, T. V., & Manzheley, V. S. (2021). Osoblyvosti modeliuvannia ta pobudovy informatsiinoi systemy dystantsiinoho monitorynhu tekhnichnoho stanu transportnykh zasobiv [Features of modeling and construction of the information system of remote monitoring of the technical condition of vehicles]. *Visnyku mashynobuduvannia ta transportu [Journal of Mechanical Engineering and Transport], 2*(14), 140–148. doi: 10.31649/2413-4503-2021-14-2-140-148 (in Ukrainian).

6. Alekseev, O. P., Alekseev, V. O., & Neronov, S. M. (2021). Telematychna synerhiia mekhatronnykh system u transportnykh zastosuvanniakh [Telematic synergy of mechatronic systems in transport applications]. *Visnyk Kharkivskoho natsionalnoho avtomobilno-dorozhnoho universytetu [Bulletin of Kharkiv national automobile & highway university], 1*(92), 17–26. doi: 10.30977/BUL.2219-5548.2021.92.1.17-26 (in Ukrainian).

7. Dobromirov, V., Verkhorubov, V., & Chernyaev, I. (2018). Systematizing the factors that determine ways of developing the vehicle maintenance system and providing vehicle safety. *Transportation research procedia*, *36*, 114-121. doi: 10.1016/j.trpro.2018.12.052. (in English).

8. Chen, C., Chen, L., Liu, L., He, S., Yuan, X., Lan, D., & Chen, Z. (2020). Delay-optimized V2V-based computation offloading in urban vehicular edge computing and networks. *IEEE Access*, *8*, 18863–18873. doi: 10.1109/ACCESS.2020.2968465 (in English).

9. Serikov, G. S., Serikova, I. O., Smirnov, O. P., & Borisenko, A. O. (2020). Analiz funktsionalnykh mozhlyvostei sensornykh dyspleiv v informatsiinykh systemakh transportnykh zasobiv [Analysis of functional features of touch displays in vehicle information systems]. *Avtomobil i elektronika. Suchasni tekhnolohii [Vehicle and electronics. Innovative technologies], 17*(2020), 42–47. doi: 10.30977/VEIT.2020.17.0.42 (in Ukrainian).

10. Trigub, O. A. (2021). *Tekhnolohichne obladnannia dlia obsluhovuvannia ta remontu avtomobiliv [Technological equipment for car maintenance and repair]*. Cherkasy: CHSTU. (in Ukrainian).

11. Mchergui, A., Moulahi, T., & Zeadally, S. (2022). Survey on artificial intelligence (AI) techniques for vehicular ad-hoc networks (VANETs). *Vehicular Communications*, *34*, 100403. doi: 10.1016/j.vehcom.2021.100403 (in English).

12. Debnath, A., Basumatary, H., Dhar, M., Debbarma, M. K., & Bhattacharyya, B. K. (2021). Fuzzy logic-based VANET routing method to increase the QoS by considering the dynamic nature of vehicles. *Computing*, *103*(7), 1391–1415. (in English).

13. Barui, T. K., Goswami, S., & Mondal, D. (2020). Design of digitally controlled DC-DC boost converter for the operation in DC microgrid. Retrieved from: https://essuir.sumdu.edu.ua/handle/123456789/82704 (in English).

14. Karande, A. M., & Kalbande, D. R. (2020). SCM Enterprise Solution Using Soft Computing Techniques. In *Soft Computing: Theories and Applications: Proceedings of SoCTA 2018* (pp. 137–146) (in English).

15. Bayir, B., Yalinkilic, I. B., Bora, S., & Can, O. (2020, October). Company Security Assesment with Agent Based Simulation. In *2020 Innovations in Intelligent Systems and Applications Conference (ASYU)* (pp. 1–6). (in English).

Received 24.03.2023; Accepted in revised form 04.05.2023.

АНАЛІЗ ЗАХИЩЕНОСТІ БОРТОВИХ ІНФОРМАЦІЙНИХ СИСТЕМ АВТОМОБІЛІВ

Анотація. *Розглянуто особливості функціонування бортових інформаційних систем автомобіля. Проаналізовано загрози їх безпеці та запропоновано методи забезпечення інформаційної безпеки та функціональної безпеки бортових інформаційних систем. Проєктування дорожніх мереж під час організації дорожнього руху є одним із факторів забезпечення функціональної безпеки сучасних інтелектуальних транспортних систем, тобто дотримання*

таких атрибутів інформаційної безпеки, як конфіденційність даних, цілісність, доступність, автентичність і новизна даних. Безпека бортових інформаційних систем транспортних засобів є критично важливою проблемою в сучасному світі, оскільки все більше транспортних засобів оснащуються електронними системами, які можуть бути вразливими до кібератак. Однією з головних проблем захисту бортових інформаційних систем є широкий спектр пристроїв і технологій, що використовуються в сучасних транспортних засобах. Різні системи можуть мати різні вимоги до безпеки та вразливості, а також складну взаємодію між собою. Інша проблема полягає у тому, що багато з цих систем не були спочатку розроблені з урахуванням безпеки. Вони можуть не мати базових функцій безпеки, таких як шифрування та автентифікація, а також використовувати застаріле програмне забезпечення та протоколи, які є вразливими до відомих атак. Для аналізу інформаційної безпеки бортових систем транспортних засобів було визначено основні типи атак та загроз для елементів транспортної системи, які взаємодіють з VANET. На основі теорії нечітких множин в умовах невизначеності та з використанням інструментарію Fuzzy Logic Toolbox в інтегрованому середовищі Matlab було змодельовано рівень інформаційної безпеки системи OBU-VANET. Отримані результати дали змогу сформулювати ступінь інформаційної захищеності елементів експлуатації транспортного засобу від несанкціонованого доступу до даних. Результати дослідження показали, що найвищий рівень захищеності (> 0,7) мають технічні системи зв'язку, а найбільш вразливими стають транспортні засоби в громадських місцях.

Ключові слова: *бортові інформаційні системи, інформаційна безпека, функціональна безпека, вулично-дорожня мережа, модель інформаційної безпеки транспортних систем, ризики.*