UDC [65.012.7+65.012.8]:656.6
DOI: 10.15587/1729-4061.2024.298144

DEVELOPMENT OF A MECHANISM FOR INFORMATION SECURITY RISK MANAGEMENT OF TRANSPORT SERVICE PROVISION SYSTEMS

Olexandr Melnychenko
PhD
Department of Manufacturing, Repair and Materials Engineering*

Oleksandr Ignatenko
Doctor of Technical Sciences, Professor
Department of Transport Technologies*

Vitalii Tsybulskyi
Corresponding author
PhD, Associate Professor
Department of Strength of Materials and Engineering Science*
E-mail: mega.sopromat@ukr.net

Anastasia Degtiarova
PhD
Department of Information Analysis and Information Security*

Mykola Kashuba
PhD
Cycle Committee of General Technical
Disciplines and Electromechanics
Separate Structural Unit «Nadvirnianskyi Vocational College
of the National Transport University»
Soborna str., 177, Nadvirna, Ukraine, 78405

Igor Derehuz
Manager
LLC Euroshpon-Trade
Oksamytova str., 22, Petropavlivska Borshchagivka vil.,
Kyiv reg., Ukraine, 08130

*National Transport University
Omelianovycha-Pavlenka str., 1, Kyiv, Ukraine, 01010

The object of the study is the process of analysis, assessment, and management of information security risks in transport service provision systems.

The problem of applying the information security risk management approach in the activities of transport business entities was investigated. As a result of the application of effective forms, methods, and means of information security risk management based on international standards, a risk management mechanism was developed. The risk assessment process of transport systems has been systematized. This allows business entities in the transport sector to determine ways to prevent and counter information threats and challenges in their activities, both when designing and operating systems for providing transport services.

Verification of the devised methodical approach to information security risk management was carried out on an example of the taxi company «Taxifay N». Threats and challenges of the company's information system were evaluated by an expert method. Based on the results of the analysis of expert risk assessment, it was found that the concordance coefficient (0.86) confirms the high level of agreement of experts' opinions. As a result, the company's information security risk management program was developed. The effectiveness of the program was assessed by the efficiency ratio, which was 0.64. This testifies to the effectiveness of the implemented program of measures to manage information security risks.

The scope of application may be the activity of business entities that provide transport services to the population, aimed at data storage and processing.

The prospect of this study is to expand the list of threats and categories of vulnerabilities depending on the characteristics of the economic activity of various enterprises

Keywords: information security, countering threats, transport services, risk management, vulnerabilities and threats

Received date 17.11.2023
Accepted date 02.02.2024
Published date 28.02.2024

How to Cite: *Melnychenko, O., Ignatenko, O., Tsybulskyi, V., Degtiarova, A., Kashuba, M., Derehuz, I. (2024). Development of a mechanism for information security risk management of transport service provision systems. Eastern-European Journal of Enterprise Technologies, 1 (3 (127)), 27–36. doi: https://doi.org/10.15587/1729-4061.2024.298144*

1. Introduction

With the rapid development of information technologies, the goals of storing information in transportation industry, its protection, increasing the influence of road safety, the occurrence of accidents and catastrophes have gained considerable relevance. Virtually all important information is currently not stored in paper form and is not processed using analog (non-digital) systems. Therefore, the methods of their protection should be digital [1].

Measures for information security in transportation industry have been implemented for more than a dozen years. However, the all-pervasive development of information technologies has led to the need for a significant expansion of the spectrum and purposes of their use. Information systems in transportation industry are increasingly becoming the object of possible sabotage aimed at disabling them or stealing valuable data. Ignorance of safety issues can harm the functioning of transport systems. Ignoring existing threats is naive, so assessing and managing risks and taking protective measures is becoming an increasingly logical response.

Transport systems belong to the critical information infrastructure (CII). In particular, these are information systems, information and telecommunication networks, automated management systems of CII subjects, as well as telecommunication networks used to organize their interaction. In turn, CII subjects are both transport systems and companies working in strategically important domains of transport provision of the state and society [2].

Modern knowledge of risk management in transportation industry allows skillful forecasting and response to threats and challenges. After all, transport, especially automobile, is one of the sources of increased level of physical, social, economic, and ecological danger. Thus, deepening the research into the information security in the systems of providing transport services is an urgent issue under today's conditions.

2. Literature review and problem statement

To a large extent, the attention of researchers is focused on the security analysis of business approaches, from the point of view of achieving the operational goal of the company [3]. In particular, in the aspect of dynamic modeling and optimization of the design of transport systems [4], risk management in the field of international forwarding and logistics operations [5], transportation of dangerous goods [6]. At the same time, aspects of the seriousness of the consequences of traffic accidents, routing efficiency, and the need for social risk assessment are taken into account. However, studies [3, 4] are of a review nature and do not offer clear tools for risk management. In studies [5, 6], transportation risks are analyzed, but little mention is made of the problems of ensuring the security of the information environment of the enterprise.

Information risks relate to the rationality of logistics chains [7], the vulnerability of the logistics service provider [8], and the effectiveness of information processing [9]. But paper [7] offers only tools to protect information systems from cyberattacks and does not take into account other risks of enterprise activity. Study [8] is based only on its own static data. In work [9], risks associated only with information processing are taken into account. The problems of taking into account uncertainties in logistics chains, their optimization [10] and substantiation of management strategies [11] were studied. However, studies [10, 11] are more focused on the influence of external factors and the risks they create.

A number of methodological approaches to risk assessment and management belong to [12], in particular, they relate to the use of a certain scale of probability or confidence, the need to connect security with knowledge of the principles and methods of information transmission. Study [12] adapted Nassim Taleb's concept of anti-fragility, which focuses on the condition that risks are considered according to their importance. The author focuses attention on the need to comply with the conditions of compliance with scientific quality requirements, taking into account social aspects, interdisciplinary approaches. However, study [12] emphasized the bias of risk measurements.

In favor of the importance of the conducted analysis, the provisions of the ISO and NIST standards, which establish requirements, specifications, guidelines and characteristics, processes for achieving the goals of risk management, testify. In particular, in the field of information security, they are guarantors of high quality, reliability and safety of services of motor transport enterprises. According to [13], these standards are powerful and effective tools for solving information security issues at the enterprise or in the management system in the conditions of the modern market. However, study [13] reports only the analysis of information security standards and does not provide a comprehensive view of risk management.

The above research results based on the review of [3–13] are largely indirectly related to the chosen topic but are important for the formation of approaches to the management of information security risks in transportation industry. However, they emphasize the importance of forming and complying with information security requirements in terms of complexity and the need for optimization, the priority of ensuring reliability, taking into account dynamism and social orientation, as well as complexities in design and operation.

Thus, the scientific problem is defined by the need to improve the risk management methodology of information security of the system of providing transport services by developing an appropriate mechanism for its implementation in practice. These questions are related to the study of vulnerabilities and threats, the choice of methods and criteria for probabilistic assessment of information security components. In addition, the problem is related to the justification of forms, methods, and means of information risk management in the presence of contradictions in existing approaches.

3. The aim and objectives of the study

The purpose of our study is to develop a mechanism for managing information security risks of transport service provision systems, which could become a new integrated prospect of preventing and countering risks in the information domain. This will provide an opportunity to improve the methodology of risk management, prevention and countermeasures against threats and challenges to information security in transportation industry. In practice, this will facilitate the process of assessing and managing contingencies based on a toolkit of vulnerability analysis, assessment and risk management strategies.

To achieve the goal, the following tasks were set and completed:

– to carry out a categorization of cause-and-effect relationships between vulnerabilities and threats to the information security of transport service provision systems;

– to systematize the process of risk assessment and devise a methodical risk management approach for information security of transport service provision systems;

– to validate the devised methodical approach to information security risk management.

4. The study materials and methods

The object of this study is the process of analysis, assessment, and management of information security risks in the systems of providing transport services to the population to prevent and counter threats and challenges.

The main hypothesis of the study assumes that determining the cause-and-effect relationships between vulnerabilities and threats to the information security of transport service delivery systems could lead to an objective assessment of risks.

The basis of the development is the information security management system, which is considered part of the management of technologies for providing transport services to the population. The research methodology is based on the results of the analysis of the literature and provisions of international standards. In particular, ISO 27001 approaches were used to protect and manage confidential information, build a system for responding to information security incidents, determine the conditions for the operation and development of the information security system. Methodological approaches were used during the risk assessment: identification of risk-prone assets; determination of importance status by magnitude, sensitivity and criticality; detection of potential threats. The study combines safety management tools (ISO 27001) with the organizational structure of the management system of transport services (ISO 27002).

Risk management processes are evaluated in accordance with the ISO 31000 methodology, which includes the following stages: specifying the scope, context, and criteria; risk assessment; risk management; data collection and reporting; monitoring and review; communication and consultation.

The NIST SP 800–30 standards, the NIST FIPS 200 Cybersecurity Framework of the US National Institute of Standards and Technology (NIST) are also included in the methodological support of the research. This approach is based on five functions: identification; protection; detection; reaction; recovery [14]. Also taken into account are the cyber security rules in force in the European Union – NIS2 [15], which are aimed at improving the management of information risks, including in the field of transport.

Systematization methods with appropriate models were used to determine the location of threats in the information security system, which indicates its properties.

The study of the mechanism of risk management was carried out on the example of a system of providing transport services to the population of a large city. For security reasons, the name of the city is hidden, and the organization, which takes care of providing transport services to the population, and the object of specification is given the conditional name «Taxifay N». The developed IS SNTP risk management mechanism was assessed by an expert method based on the results of its implementation during 2022 in the Taxifay N transport system. Taxifay N uses information technologies to automate and optimize the business processes of providing taxi transport services that use managed data with the help of appropriate software and related services.

5. Results of development a risk management mechanism for information security of transport service provision systems

5. 1. Construction of a categorical model of causal relationships between vulnerabilities and threats

The structure of cause-and-effect relationships and the threat modeling methodology are considered at the functional and operational levels and are the basis of risk assessment [16]. Systematic methods have been established for the analysis of information security problems in transportation industry service provision systems, which are not identical and must be used taking into account specific conditions. They are listed below:

1. In the process of solving information support tasks at the pre-project stage of building a transport system, preliminary advertising of services and enterprise using information and communication technologies. A method based on the OCTAVE model [17] can be used to provide data about the transport system and its components to consumers, to inform consumers about the functioning of transport in real time. At the same time, the formation of understanding and the possibility of categorization of information threats is achieved on the basis of a systemic approach to interrelated processes and the possibility of dividing them into components of activities.

2. With regard to the tasks of formation or operational change of the route system, drawing up traffic schedules and their correction, fare payment and registration of preferential categories of passengers. Expert assessment should be based on the principles of project or activity program security at the stages of their development life cycle with threat modeling according to the OWASP methodology [18]. This allows us to avoid or minimize risks at various stages of development.

3. Regarding the tasks of ensuring unhindered movement of vehicles and safe conditions for the consumption of transport services, logistical management of the transport process, providing technical assistance to vehicles on the line. In this case, a method based on the PASTA model [19] can be used. This model involves the reproduction of threats with a consistent approach to their identification and analysis using a seven-step risk assessment algorithm. It allows us to monitor alignment in business processes and establish appropriate requirements for the decision-making process.

4. For tasks of managing the provision of accompanying and additional transport services to the population and carriers, organization of services for consumers with disabilities. In particular, the CORAS method and model [20] can be used. At the same time, a unified eight-step procedure is used, which provides the opportunity to achieve a cascading effect in determining the individual vulnerability that caused the incident.

Based on the analysis of studies [1–7, 21–24], a categorical model of causal relationships between vulnerabilities and threats in the field of information security was systematized and built (Table 1, Fig. 1).

This model is built according to the directions: hardware, personnel, network, software. For its construction, an analysis method based on the OCTAVE model [17] was used.

Table 1

Categories of vulnerabilities and threats in the field of information security

Categories of vulnerabilities (V_{kj})		Threats (T_{kj})	
1		2	
Hardware (W_i)			
V_{w1}	Susceptibility of hardware to moisture and dust	T_{w1}	Dust, corrosion, icing
V_{w2}	Natural emergencies with hardware	T_{w2}	Earthquake, flood, fire
V_{w3}	Criminal activities, unprotected storage of hardware	T_{w3}	Vandalism, theft of media or documents
V_{w4}	Possibility of uncontrolled copying	T_{w4}	Illegal transfer of information
V_{w5}	Carelessness when replacing or destroying hardware	T_{w5}	Remaining business information and the possibility of its use by competitors
V_{w6}	Improper maintenance of hardware	T_{w6}	Low maintainability of hardware
V_{w7}	Disconnection, susceptibility to changes in power supply	T_{w7}	Failure of the power source and lack of its replacement

Continuation of Table 1

1		2	
Personnel (P_i)			
V_{p1}	Legal regulation of personnel activities	T_{p1}	Violation of contractual relations or legislation
V_{p2}	Inadequate safety training for staff	T_{p2}	Errors in the use of hardware and information
V_{p3}	Lack of mechanisms for monitoring personnel activities	T_{p3}	Unauthorized modification of information
V_{p4}	Uncontrolled work of external personnel	T_{p4}	Theft of media or documents
V_{p5}	Defects in the distribution of responsibilities for access and use of information	T_{p5}	Denial of illegal actions
Information network (N_i)			
V_{n1}	Poor password management in the information network	T_{n1}	Abuse of access rights
V_{n2}	The presence of running services that are not in use	T_{n2}	Illegal data processing
V_{n3}	Imperfect software	T_{n3}	Software failure
V_{n4}	Unsecured lines of communication	T_{n4}	Listening
V_{n5}	Insecure network architecture	T_{n5}	Damage to the information network and resources
V_{n6}	Transmission of passwords in open form	T_{n6}	Remote espionage
V_{n7}	Unsecured connection to a public information network	T_{n7}	Unauthorized use of equipment
Software (S_i)			
V_{s1}	Insufficient software testing	T_{s1}	Distribution of computer viruses
V_{s2}	Improper organization of «exit-exit»	T_{s2}	The possibility of violation of the right of access
V_{s3}	Insufficient number of checks (revisions)	T_{s3}	Software and Access Denials
V_{s4}	Incorrect definition of access conditions	T_{s4}	The possibility of access by third-party users
V_{s5}	Use of unlicensed software	T_{s5}	Data distortion
V_{s6}	Incorrect organizational regulation	T_{s6}	Errors in the use of the software
V_{s7}	Unsafe rebooting of hardware	T_{s7}	Loss of information and software
V_{s8}	Incorrect data	T_{s8}	Error using the software

Note: index k denotes direction, $k\in\{W_i,P_i,N_i,S_i\}$; subscript j denotes the serial number of the vulnerability category and its corresponding threat

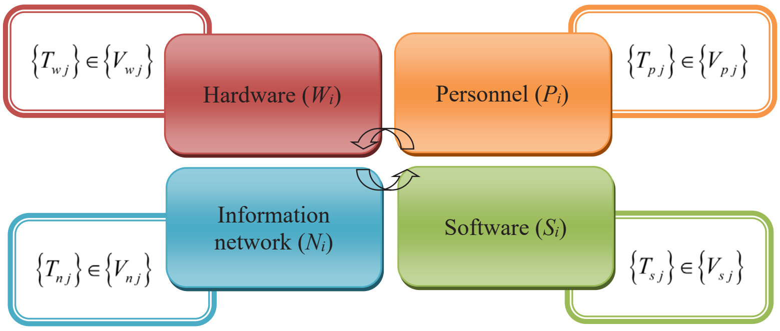
$\{T_{wj}\}\in\{V_{wj}\}$
Hardware (W_i)
Personnel (P_i)
$\{T_{pj}\}\in\{V_{pj}\}$
Information network (N_i)
Software (S_i)
$\{T_{nj}\}\in\{V_{nj}\}$
$\{T_{sj}\}\in\{V_{sj}\}$

Fig. 1. Categorical model of causal relationships between vulnerabilities and threats in the field of information security

5. 2. Systematization of the risk assessment process and development of a methodical approach to their management

The systematization of the risk assessment process should be based on system-wide risk management provisions that relate to:

– assessment of the stability of the system and solutions [25], differentiation of indicators of importance [26], their variability and inaccuracy, which affects the risk assessment;

– priorities of optimizing reliability [27], taking into account environmental and social factors [28], as well as expanding the basis of statistics for the integration of threats [29];

– clarification of the potential role of the theory of uncertainty in the process of risk analysis [30], the concept of a reliable risk measure [31], especially in the selection of portfolios of infrastructure projects [32];

– the possibility of using a simplified approach to risk management [33], the methodology for determining the main events in their assessment [34], the discussion of legislative coherent risk prevention measures [35];

– ethical issues related to the acceptability of risk from the standpoint of society or its constituents [36], understanding the impact on the risk of business operations [37].

To systematize the process of assessing information security risks of transport service delivery systems, it is important to characterize the relevant consequences for each vulnerability and threat separately for each asset [13]. At the same time, it is necessary to assess the probability of risks. The severity of the risk is an overall assessment of both the level of probability that the event will occur (probability) and the impact of the event if it occurs (impact).

Potential vulnerability and/or threat is described as: almost certain, likely, possible, unlikely, rare (Table 2) with corresponding levels of impact (Table 3).

The consequences of a security incident were defined in terms of loss of confidentiality, integrity, and availability. Exposure quantification and risk level determination are based on NIST SP 800–30, Revision 1 [14].

Table 2

Probability levels and their characteristics

Probability levels (I_r)		Probability characteristics
$I_{r,1}$	Almost certain	Expected in most cases
$I_{r,2}$	Probable	Probably will in most cases
$I_{r,3}$	Possible	May happen sometime
$I_{r,4}$	Unlikely	Not expected, but maybe someday
$I_{r,5}$	Rare	Not expected and may occur under certain circumstances

Table 3

Event impact levels

Levels of impact	Description of impact
High $H_{Ir} \in [H_1; H_5]$	The loss of availability, confidentiality, or integrity is significant, critical, and/or immediately affects the organization's cash flows, operations, functionality, legal, contractual obligations, and/or reputation
Medium $M_{Ir} \in [M_1; M_5]$	Loss of confidentiality, availability or integrity may result in costs and moderate or minor impact on legal, contractual obligations and/or reputation
Low $L_{Ir} \in [L_1; L_5]$	Loss of confidentiality, availability or integrity does not affect the organization's monetary losses, legal, contractual obligations and/or reputation

A scale and a risk level matrix were used to measure the recognized risk [24]. The final measure of risk is obtained by multiplying the rating given by the probability of the threat and the effect of the threat:

$$R_i = G_{Ir,i} \cdot E_{Ir,i}, \qquad (1)$$

where $G_{Ir,i}$ is the rating given to the probability of the ith threat, $G_{Ir} \in [0;15]$; $E_{Ir,i}$ – the effect of the ith threat (weight).

Comprehensive risk ratings can be established based on inputs on probability groups and threat exposures. For this purpose, a risk level matrix (Table 4) of size $Y \times X$ is constructed:

$$A = \left(R_{xy}\right)_{x=1,y=1}^{X,Y} = \begin{pmatrix} R_{11} & \ldots & R_{1Y} \\ \ldots & R_{xy} & \ldots \\ R_{X1} & \ldots & R_{XY} \end{pmatrix}, \qquad (2)$$

where x is measured from 1 to X relative to the rating given to the threat impact level (high, medium, low); y is measured from 1 to Y relative to the probability of the threat (almost certain, likely, possible, unlikely, rare).

The matrix shows how the overall risk levels are determined. Determining these risk levels or assessments can be subjective. The basis of this explanation can be expressed in terms of the probability assigned to each level of threat probability and the value assigned to each level of exposure.

The rating scale for the levels of influence is established as a 15-point rating scale for all levels of influence. These criteria were based on ISO 27005. The rating scale for the probability levels is set as a 5-point rating scale: 0.20 – rare, 0.40 – unlikely, 0.60 – possible, 0.80 – likely, 1.00 – assured. The risk limit is set at 2.9.

Table 4

Risk determination matrix A

Levels of impact	$G_{Ir,i}$	Probability levels (I_r)				
		$I_{r,5}$	$I_{r,4}$	$I_{r,3}$	$I_{r,2}$	$I_{r,1}$
		$E_{Ir,i}$				
		0.2	0.4	0.6	0.8	1.0
H_5	15	3	6	9	12	15
H_4	14	2.8	5.6	8.4	11.2	14
H_3	13	2.6	5.2	7.8	10.4	13
H_2	12	2.4	4.8	7.2	9.6	12
H_1	11	2.2	4.4	6.6	8.8	11
M_5	10	2	4	6.0	8.0	10
M_4	9	1.8	3.6	5.4	7.2	9
M_3	8	1.6	3.2	4.8	6.4	8
M_2	7	1.4	2.8	4.2	5.6	7
M_1	6	1.2	2.4	3.6	4.8	6
L_5	5	1	2.0	3.0	4.0	5
L_4	4	0.8	1.6	2.4	3.2	4
L_3	3	0.6	1.2	1.8	2.4	3
L_2	2	0.4	0.8	1.2	1.6	2
L_1	1	0.2	0.4	0.6	0.8	1

The matrix of risk levels with its ratings characterizes the level of risk to which an information system, asset and/or process may be exposed in the presence of a known vulnerability and threat. For a better understanding, you should use the levels of consequences and their description (Tables 5, 6).

Table 5

Matrix of the consequences of an event according to the level of probability of its occurrence *B*

Level of probability (I_r)	The severity of the event (consequences), $N_{r,i}$				
	Negligible	Medium	Heavy form	Increased	Catastrophic
$I_{r,1}$	Average	High	Critical	Critical	Critical
$I_{r,2}$	Average	Considerable	High	Critical	Critical
$I_{r,3}$	Low	Average	Considerable	High	Critical
$I_{r,4}$	Low	Low	Average	Considerable	Critical
$I_{r,5}$	Low	Low	Average	Average	High

Table 6

Description of the levels of consequences according to the levels of probability according to the matrix

The level of consequences	Description
Critical	Extreme risk – requires in-depth research, management planning
High	High risk – urgent risk response is required
Considerable	Significant risk – requires management attention
Average	Medium risk – one needs to carry out the division of responsibility
Low	Low risk – consider it an everyday occurrence

The matrix of the consequences of an event according to the level of probability of its occurrence is a 5×5 matrix with elements in the form of text values, which can be written using a set-theoretic description:

$$B=\begin{cases}\left\{I_{r,1},\ldots I_{r,5}\right\};\\ \left\{N_{r,1},\ldots N_{r,5}\right\},\end{cases} \qquad (3)$$

where $I_{r,1}$...$I_{r,5}$ are rows of the matrix that correspond to the levels of probability of the occurrence of the event; $N_{r,1}$...$N_{r,5}$ – columns of the matrix that correspond to the degree of severity of the occurrence of the event (consequences).

Thus, the function of applying a methodical risk management approach will tale a formalized form:

$$f\left(R'\right)=\left\{\sum V_{kj},\sum T_{kj},\sum R_i,\sum N_{r,i}\right\}\rightarrow \min, \qquad (4)$$

where V_{kj} is the j-th vulnerability category of the k-th direction; T_{kj} is the j-th threat of the kth direction; R_i – i-th risk; $N_{r,i}$ is the degree of severity of the occurrence of the event (consequences).

Risk management in logistics support extends to the field of transport services [38]. There are four levels of risk management mechanisms: acceptance (low level of consequences), reduction (medium level), transfer (significant level) and removal (high or critical level). The conceptual scheme of risk management of a motor vehicle enterprise according to the proposed approach is shown in Fig. 2.

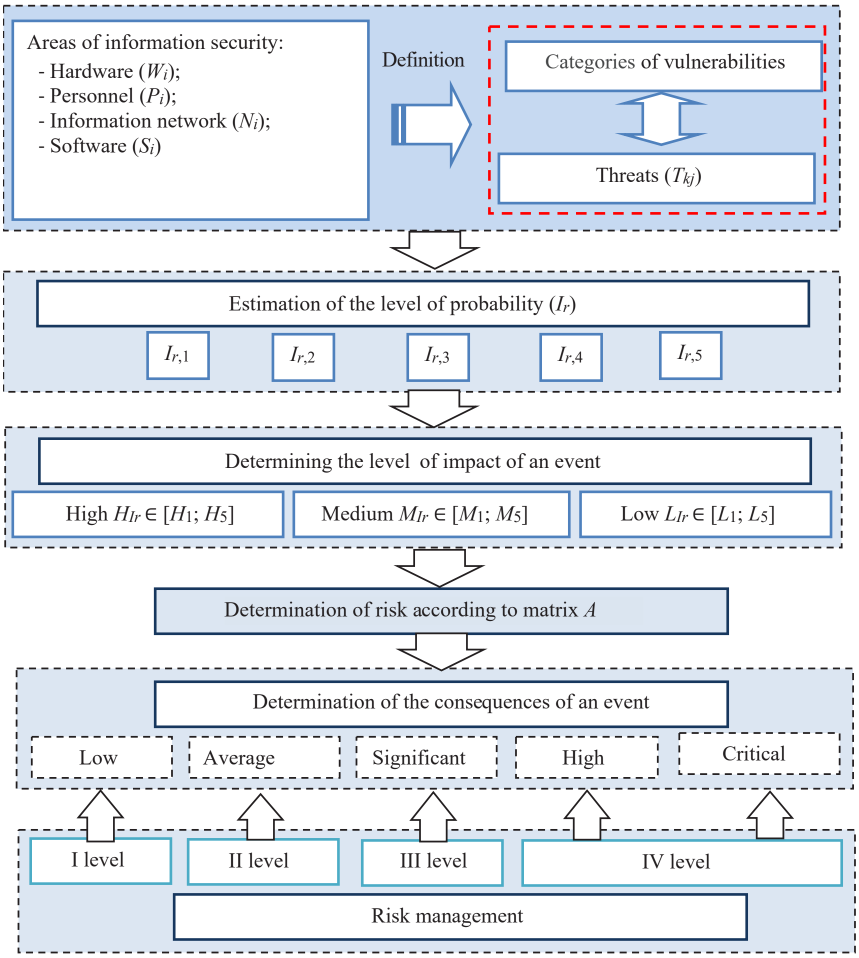
Areas of information security:
- Hardware (W_i);
- Personnel (P_i);
- Information network (N_i);
- Software (S_i)
Definition
Categories of vulnerabilities
Threats (T_{kj})
Estimation of the level of probability (I_r)
$I_{r,1}$
$I_{r,2}$
$I_{r,3}$
$I_{r,4}$
$I_{r,5}$
Determining the level of impact of an event
High $H_{Ir} \in [H_1; H_5]$
Medium $M_{Ir} \in [M_1; M_5]$
Low $L_{Ir} \in [L_1; L_5]$
Determination of risk according to matrix A
Determination of the consequences of an event
Low
Average
Significant
High
Critical
I level
II level
III level
IV level
Risk management

Fig. 2. Conceptual scheme of risk management of a motor transport enterprise

At the first level, risk-taking should be reserved for low-priority risks where other options for action would cost more than the potential impact. In order to reduce the risk identified, all risks should include a recommendation for controls and alternative solutions according to NIS2.

At the second level, risk mitigation involves minimizing the probability and/or consequences of risk-threats and vulnerabilities. Preventive measures against a risk are always more effective than repairing the damage caused by an identified risk.

At the third level, risk transfer involves transferring the negative effect of a threat or vulnerability. Transferring risk to third parties (vendors) does not eliminate the threat or vulnerability. The other party will be responsible for handling the relevant risk.

At the last level, risk prevention involves changing aspects of common business processes or system architecture to eliminate threats – preventing the risk by stopping the associated business activity. The provisions of NIS2 can be applied to plan and develop future controls to eliminate the identified risk.

5. 3. Verifying the devised methodical approach to information security risk management

Based on the expert method, all possible threats were considered for each asset of the conditional transport company «Taxifay N». The company's income for 2022 was 2 million 713 thousand monetary units, the value of the company's assets was 1 million 150 thousand monetary units. The company «Taxifay N» provides services for searching, ordering, and paying for trips by car, motorcycle, and electric scooter through the mobile application Bolt (Estonia) in Ukraine. That is, the communication system enables the collection, search, processing and forwarding of information.

Information and communication technologies are used by «Taxifay N» not only in the process of receiving and executing the order but also at the preparatory stage based on photocopies of the relevant documents. In particular, in the taxi sector, this applies to the admission of candidate drivers (executives) based on age, driving experience, citizenship, and the presence of a smartphone. Cars are checked by brand, term of use, appearance, availability of insurance documents, with the right to apply Bolt symbols. To connect to the server, the presence of a bank card for non-cash payments is checked.

Later, the risks were specified with the involvement of 10 experts using the example of the taxi service system in the city. To determine the probability of events and risks that can cause potential damage to the company's information systems, an analysis was conducted based on the OCTAVE model (Table 1). The corresponding weighted expert assessment of the level of impact and the level of probability of occurrence of the event was evaluated according to matrices (Tables 4, 5) and given in Table 7.

Table 7

Assessment of threats, levels of their probability and consequences for Taxify N

Threats		Expert score	Probability levels	Levels of consequences relative to levels of risk R_i	The severity of the event (consequences)
T_{p2}	Errors in the use of hardware and information	H_5	$I_{r,2}$	High, R_i=12	Heavy form
T_{w3}	Vandalism, theft of hardware, media or documents	H_4	$I_{r,2}$	High, R_i=11.2	Heavy form
T_{w4}	Illegal transfer of information	H_3	$I_{r,3}$	High, R_i=7.8	Increased
T_{n1}	Abuse of access rights	H_2	$I_{r,3}$	High, R_i=7.2	Increased
T_{w5}	Remains of information are not destroyed, the possibility of its unauthorized use	H_1	$I_{r,3}$	High, R_i=6.6	Increased
T_{p2}	Distribution of computer viruses	M_5	$I_{r,2}$	Average, R_i=8.0	Insignificant
T_{n5}	Damage to the information network and software	M_4	$I_{r,2}$	Average, R_i=7.2	Insignificant
T_{p3}	Unauthorized modification of information	M_3	$I_{r,3}$	Average, R_i=4.8	Average
T_{n4}	Listening	M_2	$I_{r,3}$	Average, R_i=4.2	Average
T_{n6}	Remote espionage	M_1	$I_{r,4}$	Low, R_i=2.4	Average
T_{s4}	The possibility of access by third parties	L_5	$I_{r,2}$	Considerable, R_i=4.0	Average
T_{s3}	Software and Access Denials	L_4	$I_{r,4}$	Low, R_i=2.4	Insignificant
T_{s6}	Errors in the use of the software	L_3	$I_{r,3}$	Low, R_i=1.2	Insignificant
T_{n7}	Unauthorized use of equipment	L_2	$I_{r,4}$	Low, R_i=0.8	Insignificant
T_{s2}	Possibility of violation of access rules	L_1	$I_{r,5}$	Low, R_i=0.2	Insignificant

Consistency of experts' opinions regarding the impact of loss of confidentiality, integrity and availability of information was assessed using the concordance method, which is described in detail in study [39]. The value of the concordance coefficient of W=0.86 confirms the reliability of the obtained results.

The risk assessment criteria were established to ensure a common understanding of security measures that would minimize potential exposure to an acceptable level according to ISO 31000.

According to the conducted risk assessment, a risk management and mitigation program was developed in 2023 for the motor vehicle enterprise «Taxifai N» according to the devised methodical approach of information security risk management. According to the proposed «Taxify N» program, it is recommended at the first level for threats T_{n6}, T_{s3}, T_{s6}, T_{n7}, T_{s2} to accept the identified risk. At the second level, for threats T_{p2}, T_{n5}, T_{p3}, T_{n4} «Taxify N» is proposed to plan and develop future controls to eliminate the identified risk. At the third level for the T_{s4} threat, «Taxify N» should consider all options for transferring the identified risk to other organizations (for example, insurance companies). At the last level of risk prevention for threats T_{p2}, T_{w3}, T_{w4}, T_{n1}, T_{w5}, it is recommended to choose the appropriate control objectives in order to reduce the identified risks and minimize the potential impact on the information systems of «Taxify N» in accordance with the rules of the annex to ISO/IEC 27001.

The results of comparing the economic activity of the enterprise before the introduction of the program in 2022 and according to the results of the program in 2023 were evaluated using economic efficiency analysis (CEA). This approach is based on a comparison of performance indicators for different years of the company's activity:

$$F=\frac{C_{t1}-C_{t2}}{E_{t2}-E_{t1}}=\frac{\Delta C}{\Delta E}, \qquad (5)$$

where C is the gross costs of the enterprise; E – gross revenues of the enterprise; t_1 – the period before the introduction of the information security risk management program; t_2 – the period based on the results of the information security risk management program.

The criterion for the effectiveness of the measures is the value of the F indicator greater than zero. For the company «Taxifay N», this indicator was 0.64, which indicates the effectiveness of the proposed program.

6. Discussion of results of verifying the devised methodical approach to information security risk management

The devised methodical approach to information security risk management is based on the use of the OCTAVE model with further improvement in accordance with international risk management standards. This makes it possible to implement an effective expert approach to risk assessment and management. At the first stage, a categorical model of causal relationships between vulnerabilities and threats was built (Table 1, Fig. 1). Subsequently, the process of assessing information security risks of transport service provision systems is systematized by using probability levels (Table 2) and event impact levels (Table 3). A matrix of risk levels (2) with its ratings was constructed (Table 4). It is proposed to carry out further risk assessment according to the matrix of consequences of the event (3) according to the level of probability of its occurrence (Table 5). The application of a methodological approach to risk management is represented in the form of objective function (4) and a conceptual scheme (Fig. 2). Unlike [12, 13], in which the basis is the determination of cause-and-effect relationships between vulnerabilities and threats to information security, the devised methodical approach includes further risk assessment based on the event's consequences matrix. This makes it possible to develop an effective information security risk management program based on a conceptual scheme (Fig. 2).

The effectiveness of the devised methodical approach was evaluated by the expert method using an example of the taxi company «Taxifai N» (Table 7). After establishing cause-and-effect relationships between vulnerabilities and threats to information security, an assessment of the probability of the occurrence of a potential danger was performed. The threat probability (threat level) was described as the probable occurrence of the event. When determining the likelihood of a threat, «Taxify N» took into account the causes of the threat, possible susceptibility, and available controls. At the second stage, the analysis of the threat to the information system included the analysis of vulnerabilities related to the «Taxify N» environment – the assessment of vulnerability levels for the threat scenario. As a result of the assessment, it was established that 5 risks have a high level of consequences, 4 – medium, 1 – significant, 5 – low. The determined degree of severity of the occurrence of the event (consequences) for «Taxify N» for 2 threats has a severe form, for 3 threats – increased, for 6 threats – minor, for 4 threats – medium. For each group of threats with corresponding consequences, measures were developed to manage information security risks of the enterprise, which were included in the corresponding program.

The results of the expert risk assessment analysis were statistically processed using the concordance method. The calculated concordance coefficient was $W=0.86$, which testifies to a high level of consistency of experts' opinions.

The effectiveness of the measures was assessed by the non-negativity of the effectiveness coefficient. For this motor vehicle enterprise, this indicator was 0.64, which indicates the effectiveness of the implemented program of measures to manage information security risks.

Limitations in using the devised methodical approach for assessing information risks are that it is focused only on motor vehicle enterprises. The disadvantages of this approach are that in the process of its implementation there may be certain obstacles associated with the implementation of ISO 27001 since it requires the full support of employees. The further development of this study consists in expanding the list of threats and categories of vulnerabilities, depending on the characteristics of the economic activity of various enterprises.

In the future, it is planned to test the devised methodological approach at enterprises of another type of activity or sector. This will make it possible to expand the list of threats and categories of vulnerabilities, depending on the specificity of the economic activity of various enterprises.

7. Conclusions

1. Categorization of cause-and-effect relationships between vulnerabilities and threats to information security of transport service provision systems has been carried out. The categorical model built can be considered a form of genetic interconnection of phenomena and processes of their functioning and development since one phenomenon (cause) in the presence of certain conditions necessarily generates, determines a positive or negative consequence. It is recommended to use a risk-oriented approach, which involves the process of identifying requirements for information security of service provision systems, that is, identifying vulnerabilities and related threats.

2. We have systematized the process of assessing information security risks in the systems of providing transport services according to the levels of their probability and impact on the means of control and management of operations. At the same time, a list of events that can prevent or delay the achievement of business goals of a specific system of providing transport services to the population has been compiled. A methodical approach to information security risk management of transport service provision systems has been devised, which involves four levels: acceptance, reduction, transfer, and removal of risks. A matrix of risk levels with its subsequent rating has been built. It is proposed to carry out a final risk assessment based on the event consequences matrix. This approach will make it possible to devise risk management measures for information security of transport service provision systems in accordance with groups of consequences.

3. The possibilities of using our methodical approach were assessed by an expert method using an example of the conditional motor vehicle company «Taxifay N». Cause-and-effect relationships between vulnerabilities and threats to information security were established, and the probability of occurrence of potential dangers was assessed. The results of the assessment showed that 5 risks have a high level of consequences, 4 – moderate, 1 – significant, 5 – low. A risk management program was proposed for Taxify N, which included measures for each group of identified threats. The experts' assessments were checked for consistency using the concordance method, with an estimated coefficient of 0.86. The evaluation of the effectiveness of the information security risk management of «Taxifay N» based on the results of the implementation of the program indicates the improvement of the resulting indicators. In particular, the efficiency criterion of the proposed measures has a positive value of 0.64.

Conflicts of interest

The authors declare that they have no conflicts of interest in relation to the current study, including financial, personal, authorship, or any other, that could affect the study and the results reported in this paper.

Funding

The study was conducted without financial support.

Data availability

The data will be provided upon reasonable request.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the current work.

References

1. Ferdman, G. (2020). The essence of the concept of transport safety: public administration aspect. Law and Public Administration, 2, 231–236. https://doi.org/10.32840/pdu.2020.2.34
2. Semeryanova, N., Mordvinov, A. (2019). Information security in the field of transport services. E3S Web of Conferences, 135, 04072. https://doi.org/10.1051/e3sconf/201913504072

3. Tubis, A. (2018). Risk Assessment in Road Transport – Strategic and Business Approach. Journal of KONBiN, 45 (1), 305–324. https://doi.org/10.2478/jok-2018-0016
4. Chow, A. H. F., Kuo, Y.-H., Angeloudis, P., Bell, M. G. H. (2020). Dynamic modelling and optimisation of transportation systems in the connected era. Transportmetrica B: Transport Dynamics, 10 (1), 801–802. https://doi.org/10.1080/21680566.2020.1851312
5. Ersoy, P., Tanyeri, M. (2021). Risk management tools in the road transportation industry with mediation and moderation analysis. Scientific Journal of Logistics, 17 (4), 555–567. Available at: https://www.logforum.net/pdf/17_4_8_21.pdf
6. Vagiokas, N., Zacharias, C. (2021). Tool for Analyzing the Risks in Dangerous Goods Transportation. OALib, 08 (05), 1–22. https://doi.org/10.4236/oalib.1107373
7. Cheung, K.-F., Bell, M. G. H. (2021). Attacker–defender model against quantal response adversaries for cyber security in logistics management: An introductory study. European Journal of Operational Research, 291 (2), 471–481. https://doi.org/10.1016/j.ejor.2019.10.019
8. Wu, P.-J., Chaipiyaphan, P. (2019). Diagnosis of delivery vulnerability in a logistics system for logistics risk management. The International Journal of Logistics Management, 31 (1), 43–58. https://doi.org/10.1108/ijlm-02-2019-0069
9. Fan, H., Li, G., Sun, H., Cheng, T. C. E. (2017). An information processing perspective on supply chain risk management: Antecedents, mechanism, and consequences. International Journal of Production Economics, 185, 63–75. https://doi.org/10.1016/j.ijpe.2016.11.015
10. Mohamed, I. B., Labarthe, O., Bouchery, Y., Klibi, W., Stauffer, G. (2023). Multi-echelon Urban Distribution Networks. The Routledge Handbook of Urban Logistics, 208–224. https://doi.org/10.4324/9781003241478-19
11. Tang, C. S., Yang, S. A., Wu, J. (2019). Financing Suppliers under Performance Risk. Foundations and Trends® in Technology, Information and Operations Management, 12 (2-3), 135–151. https://doi.org/10.1561/0200000091
12. Aven, T. (2015). On the allegations that small risks are treated out of proportion to their importance. Reliability Engineering & System Safety, 140, 116–121. https://doi.org/10.1016/j.ress.2015.04.001
13. Andersson, A., Hedström, K., Karlsson, F. (2022). Standardizing information security – a structurational analysis. Information & Management, 59 (3), 103623. https://doi.org/10.1016/j.im.2022.103623
14. The NIST Cybersecurity Framework 2.0 (2023). National Institute of Standards and Technology. https://doi.org/10.6028/nist.cswp.29.ipd
15. Pizzi, G. (2020). Cybersecurity and its integration with safety for transport systems: not a formal fulfillment but an actual commitment. Transportation Research Procedia, 45, 250–257. https://doi.org/10.1016/j.trpro.2020.03.014
16. Bélanger, F., Collignon, S., Enget, K., Negangard, E. (2017). Determinants of early conformance with information security policies. Information & Management, 54 (7), 887–901. https://doi.org/10.1016/j.im.2017.01.003
17. Caralli, R. A., Stevens, J. F., Young, L. R. Wilson, W. R. (2007). Introducing OCTAVE Allegro: Improving the information security risk assessment process. https://doi.org/10.1184/R1/6574790.v1
18. Threat Modeling. OWASP. Available at: https://owasp.org/www-community/Threat_Modeling
19. Shameli-Sendi, A., Aghababaei-Barzegar, R., Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). Computers & Security, 57, 14–30. https://doi.org/10.1016/j.cose.2015.11.001
20. Haji, S., Tan, Q., Costa, R. S. (2019). A Hybrid Model for Information Security Risk Assessment. International Journal of Advanced Trends in Computer Science and Engineering, 8 (1.1), 100–106. https://doi.org/10.30534/ijatcse/2019/1981.12019
21. van Ginkel, K. C. H., Dottori, F., Alfieri, L., Feyen, L., Koks, E. E. (2021). Flood risk assessment of the European road network. Natural Hazards and Earth System Sciences, 21 (3), 1011–1027. https://doi.org/10.5194/nhess-21-1011-2021
22. Abrahamsen, E. B., Aven, T. (2012). Why risk acceptance criteria need to be defined by the authorities and not the industry? Reliability Engineering & System Safety, 105, 47–50. https://doi.org/10.1016/j.ress.2011.11.004
23. Aven, T. (2014). The Concept of Antifragility and its Implications for the Practice of Risk Analysis. Risk Analysis, 35 (3), 476–483. https://doi.org/10.1111/risa.12279
24. Kitsios, F., Chatzidimitriou, E., Kamariotou, M. (2022). Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry. Sustainability, 14 (3), 1269. https://doi.org/10.3390/su14031269
25. Smerichevskyi, S., Mykhalchenko, O., Poberezhna, Z., Kryvovyazyuk, I. (2023). Devising a systematic approach to the implementation of innovative technologies to provide the stability of transportation enterprises. Eastern-European Journal of Enterprise Technologies, 3 (13 (123)), 6–18. https://doi.org/10.15587/1729-4061.2023.279100
26. Floreale, G., Baraldi, P., Lu, X., Rossetti, P., Zio, E. (2024). Sensitivity analysis by differential importance measure for unsupervised fault diagnostics. Reliability Engineering & System Safety, 243, 109846. https://doi.org/10.1016/j.ress.2023.109846
27. Coit, D. W., Zio, E. (2019). The evolution of system reliability optimization. Reliability Engineering & System Safety, 192, 106259. https://doi.org/10.1016/j.ress.2018.09.008
28. Sultana, S., Salon, D., Kuby, M. (2021). Transportation sustainability in the urban context: a comprehensive review. Geographic Perspectives on Urban Sustainability, 13–42. https://doi.org/10.4324/9781003130185-2
29. Shahjee, D., Ware, N. (2022). Integrated Network and Security Operation Center: A Systematic Analysis. IEEE Access, 10, 27881–27898. https://doi.org/10.1109/access.2022.3157738

30. Dubois, D. (2010). Representation, Propagation, and Decision Issues in Risk Analysis Under Incomplete Probabilistic Information. Risk Analysis, 30 (3), 361–368. https://doi.org/10.1111/j.1539-6924.2010.01359.x
31. Fertis, A., Baes, M., Lüthi, H.-J. (2012). Robust risk management. European Journal of Operational Research, 222 (3), 663–672. https://doi.org/10.1016/j.ejor.2012.03.036
32. Joshi, N. N., Lambert, J. H. (2011). Diversification of infrastructure projects for emergent and unknown non-systematic risks. Journal of Risk Research, 14 (6), 717–733. https://doi.org/10.1080/13669877.2011.553733
33. Maselli, G., Macchiaroli, M. (2020). Tolerability and Acceptability of the Risk for Projects in the Civil Sector. Smart Innovation, Systems and Technologies, 686–695. https://doi.org/10.1007/978-3-030-48279-4_64
34. Reinert, J. M., Apostolakis, G. E. (2006). Including model uncertainty in risk-informed decision making. Annals of Nuclear Energy, 33 (4), 354–369. https://doi.org/10.1016/j.anucene.2005.11.010
35. Shapiro, A. (2013). On Kusuoka Representation of Law Invariant Risk Measures. Mathematics of Operations Research, 38 (1), 142–152. https://doi.org/10.1287/moor.1120.0563
36. Vanem, E. (2012). Ethics and fundamental principles of risk acceptance criteria. Safety Science, 50 (4), 958–967. https://doi.org/10.1016/j.ssci.2011.12.030
37. Zsidisin, G. A. (2003). A grounded definition of supply risk. Journal of Purchasing and Supply Management, 9 (5-6), 217–224. https://doi.org/10.1016/j.pursup.2003.07.002
38. Melnichenko, O., Ignatenko, O., Dmytrychenko, A., Dereguz, I. (2023). Logistics management of the system for providing transportation services to the population: anti-crisis aspect. The National Transport University Bulletin, 1 (55). https://doi.org/10.33744/2308-6645-2023-1-55-200-210
39. Khrutba, V., Kharchenko, A., Khrutba, Y., Kolbasin, M., Tsybulskyi, V., Silantieva, I., Lysak, R. (2022). Applying a design mindset to develop a prototype of an electronic service for assessing the impact on the environment. Eastern-European Journal of Enterprise Technologies, 4 (2 (118)), 6–15. https://doi.org/10.15587/1729-4061.2022.262356