http://www.moderntechno.de/index.php/meit/article/view/meit42-02-021
DOI: 10.30890/2567-5273.2025-42-02-021

IMPROVING SAFETY IN LOGISTICS THROUGH STANDARDIZED PROTOCOLS FOR WORKING WITH COMPLEX EQUIPMENT

Maksym Horbunkov
ORCID: https://orcid.org/0009-0000-8072-7709
Kremenets Taras Shevchenko Regional Academy of Humanities and Pedagogy, Ukraine

Abstract. *In the context of the growth of various types of threats in logistics due to the increase in the level of complexity of transportation of various types of cargo and the development of multimodal transportation, the basic security standards in this area require detailed coverage. The purpose of the article was to study the main security standards in logistics as tools for ensuring protection against threats that arise during the operation of complex equipment. The paper examines the strengths and weaknesses of the developed standards (requirements) for asset security (FSR) of logistics service providers of the Technology Asset Protection Association (TAPA) and the security rules defined by the International Ship and Port Facility Security Code (ISPS Code). Significant differences have been identified in the developed tools for compliance with security and protection against risks of operating complex equipment. The FSR facility security requirements represent generally accepted standards for compliance with three levels of security in agreements between buyers and suppliers of logistics services, acting primarily as a tool for maintaining sustainability in the logistics industry. In turn, the security rules of the ISPS Code define mandatory comprehensive measures for protection against threats that arise in the maritime industry and maritime logistics, providing for the implementation of a comprehensive, integrated approach to security in logistics at the international, national, and regional levels. A proactive approach to security measures, collective responsibility and the development of technical cooperation programs are identified as the main elements that are implemented to support security regulations under the ISPS Code.*

Key words: *logistics security, security regulations, security requirements, standardization, equipment, security risks.*

Introduction

Logistics security or supply chain security management emerged at the beginning of the 21st century as a result of the catastrophic events of September 11, 2001, in the United States [5]. The rise in crime rates in various regions of the world has only reinforced the need for governments and international organizations to develop programs and initiatives for logistics security management and to develop standards and procedures for protection against numerous threats. According to statistics, the largest centers of European crime are the United Kingdom, Germany, France, Italy, and Spain, where in July 2024 alone, thefts of goods worth more than €16 million were recorded. The total financial losses due to crime in Europe are estimated at €549 million in 2023 [10].

Today, some of the most pressing threats to logistics security are the high level of

occupational injuries among workers, the risk of fires due to equipment malfunctions, technical risks and equipment failures due to irregular maintenance, unskilled operation, and cyber threats to new types of equipment.

Standardized protocols for working with complex equipment are defined as one of the key elements of a logistics safety management system. The functional purpose of the protocols is to establish regulatory rules, compliance with which is mandatory to reduce the likelihood of emergencies, minimize the risk of physical injury to employees, the risk of breakdowns of complex equipment, and prevent financial losses in logistics [3]. Standardized protocols are important in terms of cyber protection against cyber threats to automated equipment. In modern industry research, standardized protocols are seen as a tool for systematic management of risks that arise in logistics activities due to non-compliance with the rules for using various types of technical means, covering organizational, technical, and informational aspects of logistics security.

In view of the above, the purpose of the article was to study the basic security standards in logistics as tools for ensuring protection against threats that arise in the process of operating complex equipment.

Input Data and Methods

Considering the purpose of the study and the main objects of research, it was decided to study the main standardized protocols of logistics security in the field of protection against threats that arise during the operation of complex equipment in logistics. The research focuses on security issues in logistics and standardized security protocols of international organizations that define the rules for working with assets in logistics. The following basic security standards (protocols) were selected for analysis: standards (requirements) for the security of assets from various types of risks TAPA Certificates (Technology Asset Protection Association); International Ship and Port Facility Security Code (ISPS Code) – international maritime security rules, including protocols for communication between ships, ports, and authorities to prevent various types of incidents [2, 3].

Taking into account the volume of import and export operations, the volume of

ships in ports and their throughput capacity in different countries around the world [6], as well as the Logistics Performance Index 2023 [9], the study focuses on the experience of the world's leading economies in implementing standardized protocols. Based on official statistical information, five countries were selected for analysis of international requirements and standards, as well as mechanisms for their implementation into national legislation: Singapore, Finland, Denmark, Germany, and the Netherlands (Port of Rotterdam). For each country, the implementation of ISPS into national legislation is described, with a focus on the main communication mechanisms established between ships, port structures, and authorities.

Table 1 – Logistics Performance Index in leading countries, 2023 [9]

№	Economy	LPI Score	LPI Grouped Rank	Customs Score	Infrastructure Score	International Shipments Score	Logistics Competence and Quality Score	Timeliness Score	Tracking and Tracing Score
1	Singapore	4,3	1	4,2	4,6	4,0	4,4	4,3	4,4
2	Finland	4,2	2	4,0	4,2	4,1	4,2	4,3	4,2
3	Denmark	4,1	3	4,1	4,1	3,6	4,1	4,1	4,3
4	Germany	4,1	3	3,9	4,3	3,7	4,2	4,1	4,2
5	Netherlands	4,1	3	3,9	4,2	3,7	4,2	4,0	4,2

The main limitation of the study is the lack of structured quantitative data for a comprehensive analysis of improving safety in logistics through standardized protocols and rules for working with complex equipment. To overcome this limitation, a synthesis of qualitative and quantitative data was used to provide an integrated overview of the issue of ensuring safety in logistics by establishing international rules of operation.

Main Text

The Transported Asset Protection Association (TAPA) was founded in 1991 to bring together all participants in the supply chain to create the highest standards of sustainability and sustainable logistics. Leading manufacturers and their logistics and transport providers, security and insurance companies, and independent audit bodies [8]. Among the standards developed are Facility Security Requirements (FSR), which define the basic minimum industry rules for the safe storage and transit of assets within

the supply chain. outline the processes and methods for obtaining and maintaining certification for the main facilities of logistics system participants, focusing primarily on distribution centers and warehouses. An analysis of the established mechanism for standardization and certification of facilities in logistics used to provide logistics services indicates the transparency and clarity of the developed processes and methods of standardization. The main strengths of standardization include a high level of expertise through the involvement of specialists in the development of standards and standardization procedures, collegiality in decisions on the development of security requirements, and constant updating of requirements in line with new security threats. A simplified approach to facility certification (one or several facilities at once) is only applicable to the standard security level and means that the applicant must conduct its own minimum-security audit or a "shadow" audit is conducted by TAPA specialists. For the certification of more than three facilities for enhanced and medium security levels, an independent external audit is conducted (Table 2).

Table 2 – Strengths and weaknesses of FSR supply chain facility security standards and requirements

Strengths	Weaknesses
Involvement of professional experts in the logistics industry with significant experience in security to develop standards	The standards were developed by supply chain experts and serve as a tool for self-regulation of security in logistics.
Collegiality in decision-making regarding safety requirements at various logistics facilities	There is a lack of transparent information on the selection of specialists involved in collegial decision-making processes.
Standards are updated in response to new security threats in logistics	Lack of a detailed list of major threats in logistics and their consequences for security
Standards are generally accepted in the logistics industry and are used in security agreements between buyers and suppliers of logistics services.	Standards are recognized as generally accepted at the industry level, between companies, and are therefore not legally defined at the national level (at the government level).
Standards are considered key criteria in selecting partners to comply with various levels of security at logistics facilities.	The complexity of complying with security requirements due to the numerous logistics service providers and subcontractors involved in the supply processes
Compliance with standardization in accordance with the developed security requirements requires passing an external independent security audit, a self-audit for a minimum level of compliance with generally accepted standards.	The complexity of conducting an independent audit and the risks of the quality of the self-audit of logistics service providers

Author's development

In the logistics industry, security standards are widely accepted and used in security agreements between buyers and suppliers of logistics services. At the same time, security requirements recognized at the industry level and between companies are not defined in the national legislation of different countries, which raises the question of their adequacy and relevance for overcoming the most modern types of threats (cyberattacks, fires, emergencies). In the logistics industry, security standards are considered key criteria in selecting partners to comply with various levels of security at logistics facilities. At the same time, the emergence of new types of logistics service providers and subcontractors complicates the practical compliance and selection of suppliers according to the developed security criteria.

Unlike the Facility Security Requirements (FSR) for logistics service providers developed by the Transported Asset Protection Association (TAPA) as a self-regulatory tool in the industry, the International Ship and Port Facility Security Code (ISPS Code) has served as the mandatory basis for comprehensive security in international shipping since July 1, 2004. The mandatory part of the ISPS Code contains detailed port and maritime security requirements that must be complied with by the governments of the countries that are parties to the 1974 International Convention for the Safety of Life at Sea (SOLAS X-2), port authorities, and shipping companies. International maritime security rules contain protocols for communication between ships, ports, and authorities to prevent various types of incidents [2].

Despite international recognition and adoption of the ISPS Code rules in various countries, developing countries face difficulties in implementing standards and problems with compliance due to the generally low or medium level of law enforcement in such states. We consider one of the strongest points to be the application of a proactive approach to security in maritime logistics, as preventive measures are mandatory to protect against existing threats. At the same time, the closed nature of the system for monitoring the implementation of preventive measures does not allow for an assessment of the appropriateness of this approach in practice. When establishing collective responsibility for security in maritime logistics by distributing roles and responsibilities, the approach to protection against threats based on monitoring

compliance with security measures by state control bodies prevails at the national level. In addition, an analysis of the strengths and weaknesses of the Code demonstrates the need to improve the mechanism for collecting and exchanging information on major security threats that may arise from the operation of equipment (Table 3).

Table 3 – Strengths and weaknesses of the International Ship and Port Facility Security Code (ISPS Code)

Strengths	Weaknesses
Internationally defined and accepted maritime safety rules integrated into national legislation	The difficulty of implementing rules, especially in developing countries with low levels of law enforcement
Application of a proactive approach to security in maritime logistics – mandatory preventive security measures are defined	Closed system for monitoring preventive measures to promote maritime safety
Collective responsibility for maritime safety, distribution of roles and responsibilities at the international, national, and regional levels	At the national level, the prevailing approach is focused on monitoring compliance with safety standards and regulations.
A mechanism for collecting and exchanging information in the field of security is provided for.	Limited data and information on major security threats arising from operational risks, insufficient staff qualifications, security violations, etc.
A methodology for assessing security risks is provided for the development of plans and procedures for protection against threats.	The complexity of combining risk assessment results at the international, national, and regional levels due to differences in the implementation of safety rules in different countries
The principle of proportionality to the security measures taken by different parties is provided for.	Many countries are limited in their ability to implement security measures due to restrictions in adopting security standards and regulations as a result of a shortage of human resources and the need to improve institutional support.

Author's development

The complexity of combining risk assessment results at the international, national, and regional levels due to differences in the implementation of safety rules in different countries limits detailed studies of existing risks and the development of measures to eliminate them. Many countries are limited in their ability to implement safety measures due to restrictions in the adoption of safety standards and rules as a result of a shortage of human resources and the need to improve institutional support. One way to address this problem is through the implementation of technical cooperation programs, which provide financial, material, technical, and human resources support from various sources: the Technical Cooperation Fund, multilateral donor trust funds, and financial support based on bilateral agreements between different governments [3].

In Singapore, Finland, Denmark, Germany, and the Netherlands (Port of Rotterdam), the security rules and the ISPS Code are integrated into national legislation, but different mechanisms have been created to implement security measures in the industry. In Singapore, the Maritime and Port Authority of Singapore defines the ISPS Code as a set of security measures that include training of human resources and the creation of a national security plan [4]. A similar mechanism for compliance with international security rules has been established in Denmark, where the Danish Maritime Authority is responsible for security in the industry [7]. In France, the Finnish Transport and Communications Agency Traficom is the body responsible for implementing security rules, focusing on developing a national security plan for the industry based on risk assessment [1].

Conclusions

The rules for ensuring security in logistics and supply chains discussed above demonstrate different approaches to choosing tools for strengthening protection against the risks associated with the operation of complex equipment on a global, national, and regional scale. Developed by the Transported Asset Protection Association (TAPA), are used as a self-regulation tool in the logistics industry, based on standardization and certification of facilities and a fairly simplified approach to protecting against risks associated with the use of equipment and machinery for the provision of logistics services. Facility security requirements are largely focused on supporting the sustainability of equipment in the provision of logistics services. In contrast, the mandatory rules established under the International Ship and Port Facility Security Code (ISPS Code) provide for a more comprehensive integrated approach to maritime logistics security, including a proactive approach to preventive security measures and technical support for the implementation of rules in different countries. A closed system for monitoring preventive measures to promote maritime security, limited data and information on major security threats arising from operational risks, insufficient staff qualifications, and security violations make it difficult to quantitatively measure the impact of standardized rules on improving security in logistics. The international safety standards and rules that have been established are important for national

regulation and protection against threats arising from the operation of ships and equipment in the process of transporting and supplying cargo.

References:

1. Finnish Transport and Communications Agency TraficomTraficom, 2004. Maritime security [WWW Document]. URL https://www.traficom.fi/en/transport/maritime/shipping-companies-and-shippers/maritime-security

2. International maritime organization, n.d. SOLAS XI-2 and the International Ship and Port Facility (ISPS) Code [WWW Document]. URL https://www.imo.org/en/ourwork/security/pages/solas-xi-2%20isps%20code.aspx

3. International maritime organization, n.d. Integrated Technical Cooperation Programme (ITCP) [WWW Document]. URL https://www.imo.org/en/ourwork/technicalcooperation/pages/itcp.aspx

4. Maritime & Port Authority of Singapore (MPA), n.d. International Ship and Port Facility Security (ISPS) Code [WWW Document]. URL https://www.mpa.gov.sg/port-marine-ops/port-safety-security/safety@sea-singapore/safety-resources/port-security/international-ship-and-port-facility-security-(isps)-code

5. Mora Lozano, P.E., Montoya-Torres, J.R., 2024. Global Supply Chains Made Visible through Logistics Security Management. Logistics 8, 6. https://doi.org/10.3390/logistics8010006

6. OECD, n.d. Monitoring Maritime Trade: The OECD AIS Vessel Tracking Dashboard [WWW Document]. URL https://www.oecd.org/en/data/dashboards/monitoring-maritime-trade-the-oecd-ais-vessel-tracking-dashboard.html

7. The Danish Maritime Authority, n.d. Maritime security - ISPS.The Danish maritime security regulations [WWW Document]. URL https://www.dma.dk/safety-at-sea/ship-safety/maritime-security-isps-

8. The Transported Asset Protection Association, n.d. About The Transported

Asset Protection Association (TAPA). URL https://tapa-apac.org/mission-vision/

9. The World Bank, n.d. Logistics Performance Index (LPI). Supply chain tracking data, LPI 2023 [WWW Document]. URL https://lpi.worldbank.org/postal

10. Underhill, E., 2025. Logistics Security: Protecting the Supply Chain. Titan Secur. Eur. URL https://www.titansecurityeurope.com/logistics-security-protecting-the-supply-chain/