УДК 65. 012.7:656.02 **DOI:10.33744/0365-8171-2026-119-383-393**
UDC 65. 012.7:656.02

СИСТЕМАТИЗАЦІЯ ТА ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСИТЕМАХ ЛОГІСТИСНОГО ОБСЛУГОВУВАННЯ

SYSTEMATIZATION AND ASSESSMENT OF INFORMATION SECURITY RISKS IN LOGISTICS SERVICE SYSTEMS

***Добровольська Анна Михайлівна**, кандидат технічних наук, доцент, професор кафедри логістики та проєктного менеджменту, Національний транспортний університет, e-mail: anet_chechet@ukr.net , тел. +380634321538,*

https://orcid.org/0000-0002-5912-0678

***Дерегуз Ігор Андрійович** здобувач PhD, Національний транспортний університет, e-mail: derehuz@ukr.net, тел. +380634321538,*

https://orcid.org/0000-0003-3119-3709

Анотація. У статті розглядаються теоретичні та методичні аспекти оцінювання ризиків інформаційної безпеки в системах логістичного обслуговування, підходи до їх систематизації за рівнями ймовірності та наслідків, а також особливості встановлення причинно-наслідкових зв'язків між вразливостями та загрозами. Відповідно, систематизовано підходи до оцінювання ризиків за рівнями імовірності та впливу на засоби контролю й керування операціями, а також сформовано перелік загрозливих подій, що впливають на досягнення бізнес-цілей транспортних систем. Розроблено механізм управління ризиками інформаційної безпеки, який ґрунтується на категорійній моделі причинно-наслідкових зв'язків між вразливостями та загрозами і передбачає використання матриці наслідків для їх оцінювання та групування.

Запропонований підхід апробовано на прикладі умовного транспортного підприємства «Таксіфай N», для якого визначено причинно-наслідкові зв'язки між загрозами і вразливостями, оцінено рівні ризиків та розроблено програму управління ними. Проведена перевірка узгодженості експертних оцінок (коефіцієнт конкордації 0,86) підтвердила надійність отриманих результатів. Оцінка ефективності впроваджених заходів засвідчила покращення показників управління ризиками (інтегральний показник ефективності – 0,64).

Ключові слова: управління та оцінювання ризиків, управління ризиком в системах логістичного обслуговування, процес оцінювання ризику, систематизація процесу оцінювання ризику, механізму управління ризиками інформаційної безпеки в системах транспортного обслуговування.

Вступ. Актуальність дослідження зумовлена необхідністю підвищення ефективності управління ризиками інформаційної безпеки в системах логістичного обслуговування шляхом розроблення та практичної реалізації механізму їх оцінювання і управління з урахуванням причинно-наслідкових зв'язків між вразливостями та загрозами і впливу їх наслідків на функціонування транспортних систем.

Управління ризиками в системах логістичного управління є складним багатокомпонентним процесом, що охоплює широкий спектр теоретичних і прикладних аспектів, які потребують ґрунтовного опрацювання. Відповідно до методології ISO 31000, процес управління ризиками передбачає послідовну реалізацію таких етапів: визначення сфери застосування, контексту та критеріїв; оцінювання ризиків; їх оброблення; забезпечення збору даних і звітності; моніторинг та перегляд; а також комунікацію і консультації. Водночас етап оцінювання ризиків потребує подальшого вдосконалення, зокрема в частині підвищення об'єктивності результатів. Це може бути досягнуто шляхом систематизації процедур оцінювання ризиків і впровадження ефективного механізму управління ризиками інформаційної безпеки в системах логістичного обслуговування.

Аналіз останніх досліджень і публікацій. Систематизація процесу оцінювання ризиків щодо інформаційної безпеки в системах транспортного обслуговування має базуватися на загальносистемних положеннях управління та оцінювання ризиків, які стосуються: оцінювання стійкості системи й рішень [1], диференціації показників важливості [2], їх мінливості і неточності, що впливає на оцінювання ризику; першочерговості оптимізації надійності [3], врахування чинників навколишнього середовища і соціальних чинників [4], а також розширення основ статистики для інтегрування загроз [5]; прояснення потенційної ролі теорії невизначеності у процесі аналізу ризику [6], концепції надійної його міри [7], особливо у виборі портфелів інфраструктурних проєктів [8]; можливості використання спрощеного підходу для управління ризику [9], методології визначення основних подій в їх оцінюванні [10], обговорення законодавчих когерентних заходів запобігання ризику [11]; питань етики, які пов'язані з прийнятністю ризику з позицій суспільства чи його складових [12], розуміння впливу на ризик бізнес-операції [13].

Для систематизації процесу оцінювання ризиків інформаційної безпеки системи надання транспортних послуг важливо охарактеризувати відповідні наслідки для кожної вразливості та загрози окремо для кожного активу [14]. При цьому необхідно оцінити імовірність ризику. Серйозність ризику являє собою загальне оцінювання як рівня ймовірності, що подія настане (імовірність), так і впливу події, якщо вона відбудеться (вплив).

Метою статті полягає у систематизації та вдосконаленні підходів до оцінювання ризиків інформаційної безпеки в транспортних логістичних системах шляхом розроблення та практичної реалізації механізму управління ризиками в системах транспортного обслуговування, який базується на встановленні причинно-наслідкових зв'язків між вразливостями та загрозами, оцінюванні ймовірності їх виникнення та рівня наслідків, а також формуванні обґрунтованих заходів реагування на основі матричного підходу.

Викладення основного матеріалу. Потенційна вразливість та/або загроза описується як: майже певна, ймовірна, можлива, малоймовірна, рідкісна (табл. 1) з відповідними рівнями впливу щодо загрозливої події (табл. 2).

Таблиця 1 – Рівні імовірності та їх характеристика, що загрозлива подія настане
Table 1 – Probability levels and their characteristics that a threatening event will occur

Рівні імовірності (I_r)		Характеристика імовірності
$I_{r,1}$	Майже впевнений (визначена)	Очікується у більшості випадків
$I_{r,2}$	Ймовірний	Ймовірно відбудеться у більшості випадків
$I_{r,3}$	Можливий	Може відбутись коли-небудь
$I_{r,4}$	Малоймовірний	Не очікується, але можливо відбудеться коли-небудь
$I_{r,5}$	Рідкісний	Не очікується і може відбутись за певних обставин

Наслідки інциденту інформаційної безпеки в системах транспортного обслуговування визначалися з точки зору втрати конфіденційності, цілісності та доступності. Кількісна оцінка впливу та визначення рівня ризику засновано на NIST SP 800–30, редакція 1 [15].

Таблиця 2 – Рівні впливу загрозливої події, у випадку якщо вона настане
Table 2 – Impact levels of a threatening event, if it occurs

Рівні впливу	Опис впливу
Високий $H_{ir} \in [H_1;H_5]$	Втрата доступності, конфіденційності або цілісності виявляється значною, критичною, та/або негайно впливає на грошові потоки організації, операції, функціональність, юридичні, договірні зобов'язання та/або репутацію
Середній $M_{ir} \in [M_1;M_5]$	Втрата конфіденційності, доступності або цілісності може призвести до витрат та надати середнього або незначного впливу на юридичні, договірні зобов'язання та/або репутацію
Низький $L_{ir} \in [L_1;L_5]$	Втрата конфіденційності, доступності або цілісності не впливає на грошові втрати організації, юридичні, договірні зобов'язання та/або репутацію

Для оцінювання ідентифікованого ризику застосовують шкалу та матрицю рівнів ризику [16]. Підсумкове значення ризику R_i, визначається як добуток оцінки ймовірності реалізації загрози (тобто настання відповідної загрозливої події) на величину наслідків (ефекту), пов'язаних із її виникненням:

$$R_i = G_{Ir,i} \cdot E_{Ir,i}, \tag{1}$$

де $g_{ir,i}$ – рейтинг, наданий ймовірності виникнення i-тої загрози (тобто настання відповідної загрозливої події), як значущість загрози (відповідної загрозливої події);

$E_{ir,i}$ – ефект, пов'язаний із i-ю загрозою (тобто настання відповідної загрозливої події), як значущість загрози (відповідної ризикової події).

Повні оцінки чи рейтинги ризику можуть бути встановлені на основі вхідних даних про групи ймовірності та впливу загрози. Для цього будується матриця щодо оцінки (рівня) ризику (табл. 3) розміром $Y \times X$:

$$A = (\mathrm{R_{xy}})_{\mathrm{x=1,y=1}}^{\mathrm{X,Y}} = \begin{pmatrix} \mathrm{R_{11}} & \dots & \mathrm{R_{1Y}} \\ \dots & \mathrm{R_{xy}} & \dots \\ \mathrm{R_{X1}} & \dots & \mathrm{R_{XY}} \end{pmatrix}, \tag{2}$$

де x – вимірюється від 1 до X відносно рейтингу, наданому рівню впливу загрози (тобто відповідної загрозливої події);

y – вимірюється від 1 до Y відносно ймовірності загрози (тобто настання відповідної загрозливої події).

Матриця показує як визначаються загальні рівні ризику чи оцінки ризику. Визначення цих рівнів ризику чи оцінок ризику може бути суб'єктивним. Основа цього пояснення може бути виражена в термінах ймовірності, присвоєної кожному рівню ймовірності загрози (настання загрозливої події), і значення, присвоєного кожному рівню впливу загрози (загрозливої події).

Шкала для оцінки рівнів впливу встановлена у вигляді 15-бальної шкали щодо оцінювання для усіх рівнів впливу загрози (тобто настання відповідної загрозливої події). Відповідно зазначені критерії були засновані на ISO 27005. Шкала оцінок для рівнів ймовірності встановлена у вигляді 5-бальної шкали оцінок: 0,20 – рідкісний**,** 0,40 – малоймовірний, 0,60 – можливий, 0,80 – ймовірний, 1,00 – впевнений (визначений). Обмеження по ризику встановлений на рівні 2,9.

Таблиця 3 – Матриця для визначення оцінок (рівня) ризику А
Table 3 – Matrix for determining risk ratings (levels) A

Рівні впливу загрози	$G_{ir,i}$	Рівні імовірності (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

Матриця визначення оцінок (рівнів) ризику з її рейтингами характеризує рівень ризику, на який можуть наражатися інформаційна система, окрім активів та/або процесів за наявності відомої сприйнятливості та загрози. Для кращого розуміння слід користуватися рівнями наслідків та їх описом (табл. 4, 5).

Матриця наслідків загрози з урахуванням рівня ймовірності її настання представляє собою матриць розміром 5×5, елементи якої подано у вигляді текстових характеристик; її формалізація може бути здійснена за допомогою теоретико-множинного опису:

$$B = \begin{cases} \{I_{r,1}, \dots I_{r,5}\} \\ \{N_{r,1}, \dots N_{r,5}\} \end{cases}, \tag{3}$$

де $I_{r,1}$**…** $I_{r,5}$ – рядки матриці, які відповідають рівням імовірності настання загрози (тобто відповідної загрозливої події),);

$\boldsymbol{N_{r,1}}$… $\boldsymbol{N_{r,5}}$ – стовпчики матриці, які відповідають ступеню тяжкості настання загрози (тобто відповідної загрозливої події), а саме наслідкам.

Отже, функція для реалізації методичного підходу до управління ризиками набуває формалізованого вигляду.:

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

де V_{kj} – категорія j-тої вразливості k-того напряму;
T_{kj} – j-та загроза k-того напряму**;**
R_i – i-тий ризик;
$N_{r,i}$ – ступінь тяжкості настання події (наслідки).

Таблиця 4 – Матриця наслідків загрози (тобто настання відповідної загрозливої події), відповідно до рівня імовірності її настання В.

Table 4 – Matrix of threat consequences (i.e. the occurrence of the relevant threatening event), according to the level of probability of its occurrence B.

Рівень імовірності настання загрозливої події (I_r)	Ступінь тяжкості настання загрозливої події (наслідки), $N_{r,i}$				
	незначна	середня	тяжка форма	підвищена	катастрофічна
$I_{r,1}$	посередній	високий	критичний	критичний	критичний
$I_{r,2}$	посередній	значний	високий	критичний	критичний
$I_{r,3}$	низький	посередній	значний	високий	критичний
$I_{r,4}$	низький	низький	посередній	значний	критичний
$I_{r,5}$	низький	низький	посередній	посередній	високий

Таблиця 5 – Опис рівнів щодо наслідків настання загрозливої події відповідно до рівнів ймовірності за матрицею

Table 5 – Description of levels regarding the consequences of a threatening event according to the probability levels according to the matrix

Рівень наслідків настання загрозливої події	Опис
Критичний	Надзвичайний ризик – потрібне глибоке дослідження, планування
Високий	Високий ризик – потрібне термінове реагування на ризик
Значний	Значний ризик – потрібна увага керівництва
Посередній	Посередній ризик – потрібно здійснити розподіл відповідальності
Низький	Низький ризик – вважати повсякденною подією

Управління ризиками в логістичному забезпеченні розповсюджується на сферу транспортного обслуговування [17]. До механізмів управління ризиком слід віднести чотири рівні: прийняття (низькій рівень наслідків), зменшення (посередній рівень наслідків), передача (значний рівень наслідків) і видалення (високий або критичний рівень наслідків). Управління ризиками інформаційної безпеки в організації перевізника автомобільного транспорту в контексті рівнів управління ризиками можна представити наступним чином.

При роботі з ризиками першого рівня необхідно зарезервувати прийняття ризику для таких низькопріоритетних ризиків, коли інші варіанти заходів коштуватимуть більше, ніж потенційний вплив настання загрозливої події. Для того щоб знизити виявлений ризик усі ризики повинні включати рекомендацію щодо засобів контролю та альтернативних рішень згідно із NIS2.

При роботі з ризиками другого рівня пом'якшення ризику передбачає мінімізацію ймовірності і/або наслідків настання загрозливих подій або вразливостей. Запобіжні заходи проти ризику розглядаються ефективніші, ніж відновлення шкоди, заподіяної виявленим ризиком.

При роботі з ризиками третього рівня передбачається перенесення (передача) ризику, що передбачає перенесення негативного ефекту від загрозливої події або вразливості. Передача ризику третій стороні назовні не усуває настання загрозливої події або вразливості. Інша сторона нестиме відповідальність за опрацювання відповідного ризику.

При роботі з ризиками четвертого рівня запобігання ризику передбачає зміну аспектів спільних бізнес-процесів або системної архітектури для усунення загрозливих подій – запобігання ризику

шляхом припинення пов'язаної з ним ділової активності. Для планування і розроблення майбутніх засобів контролю для усунення виявленого ризику можна застосовувати положення Директиву ЄС про кібербезпеку (NIS2).

Пропонований механізм управління ризиками інформаційної безпеки в системах транспортного обслуговування базується на моделі OCTAVE із подальшим удосконаленням, узгоджуючись із міжнародними стандартами управління ризиками [18]. Зазначене дозволяє реалізовувати ефективний експертний підхід при оцінюванні та управлінні ризиками. Реалізацію даного методу можна представити в рамках проходження наступних етапів:

На першому етапі встановлюється причинно-наслідкові зв'язківи між вразливостями та загрозами і оцінювання їх імовірності. На другому етапі здійснюється аналіз інформаційної системи та визначення впливу загрозливої події. На третьому етапі проводиться оцінювання рівня ризику на основі ймовірності та впливу загрозливої події. На четвертому етапі визначаються можливі наслідки загрозливих подій. На п'ятому етапі формуються рекомендації щодо рівнів управління ризиками (прийняття, зниження, передача або уникнення ризику).

Розглянемо умови щодо реалізації механізму управління ризиками інформаційної безпеки в системах транспортного обслуговування. Ефективність розробленого механізму управління ризиками інформаційної безпеки в системах транспортного обслуговування була оцінена експертним методом на прикладі автотранспортної компанії «Таксіфай N». Відповідна зважена оцінка експертів рівня впливу ризикових подій та рівня ймовірності настання ризикових подій була оцінена із використанням матриць, наведеними в табл. 3, 4, та представлена у табл. 6.

Таблиця 6 – Оцінювання загроз (загрозливих подій), рівнів їх ймовірності та наслідків для організації перевізника «Таксіфай N»

Table 6 – Assessment of threats (threat events), their probability levels and consequences for the organization of the carrier "Taxify N"

Загроза (загрозлива подія)		Оцінка експертів	Рівень ймовірності	Рівень наслідків відносно рівня ризику, R_i	Ступінь тяжкості настання загрозливої події (наслідки)
1	2	3	4	5	6
T_{p2}	Помилки у використані апаратних засобів та інформації	H_5	$I_{r,2}$	Високий, R_i = 12	Тяжка форма
T_{w3}	Вандалізм, крадіжка апаратних засобів, носіїв інформації чи документів	H_4	$I_{r,2}$	Високий, R_i = 11,2	Тяжка форма
T_{w4}	Протиправна передача інформації	H_3	$I_{r,3}$	Високий, R_i = 7,8	Підвищена
T_{n1}	Зловживання правом доступу	H_2	$I_{r,3}$	Високий, R_i =7,2	Підвищена
T_{w5}	Не знищені залишки інформації, можливість її несанкціонованого використання	H_1	$I_{r,3}$	Високий, R_i = 6,6	Підвищена
T_{p2}	Розповсюдження комп'ютерних вірусів	M_5	$I_{r,2}$	Посередній, R_i = 8,0	Незначна

Продовження таблиці 6
Continuation of table 6

1	2	3	4	5	6
T_{n5}	Нанесення шкоди інформаційній мережі та програмному забезпеченні	M_4	$I_{r,2}$	Посередній, R_i = 7,2	Незначна
T_{p3}	Несанкціонована модифікація інформації	M_3	$I_{r,3}$	Посередній, R_i = 4,8	Середня
T_{n4}	Прослуховування	M_2	$I_{r,3}$	Посередній, R_i = 4,2	Середня
T_{n6}	Віддалене шпигунство	M_1	$I_{r,4}$	Низький, R_i = 2,4	Середня
T_{s4}	Можливість доступу сторонніх осіб	L_5	$I_{r,2}$	Значний, R_i = 4,0	Середня
T_{s3}	Відмови програмного забезпечення та доступу	L_4	$I_{r,4}$	Низький, R_i = 2,4	Незначна
T_{s6}	Помилки у використанні програмного забезпечення	L_3	$I_{r,3}$	Низький, R_i = 1,2	Незначна
T_{n7}	Несанкціоноване використання обладнання	L_2	$I_{r,4}$	Низький, R_i = 0,8	Незначна
T_{s2}	Можливість порушення правил доступу	L_1	$I_{r,5}$	Низький, R_i = 0,2	Незначна

Узгодженість думок експертів щодо впливу втрати конфіденційності, цілісності та доступності інформації була оцінена за методом конкордації, який детально описаний в дослідженні [19]. Значення коефіцієнта конкордації в W=0,86 підтверджує достовірність отриманих результатів.

Критерії оцінки ризику були встановлені для забезпечення загального розуміння заходів безпеки, які мінімізували б потенційний вплив до прийнятного рівня згідно з ISO 31000.

Відповідно до проведеної оцінки ризиків у відповідності до концептуальних засад управління ризиками інформаційної безпеки в системах транспортного обслуговування для організації перевізника автомобільного транспорту «Таксіфай N» у 2023 році було розроблено програму управління та пом'якшення ризиків. Згідно запропонованої програми «Таксіфай N» рекомендовано на першому рівні для загроз T_{n6}, T_{s3}, T_{s6}, T_{n7}, T_{s2} прийняти виявлений ризик. На другому рівні для загроз T_{p2}, T_{n5}, T_{p3}, T_{n4} «Таксіфай N» запропоновано виконати планування та розроблення майбутніх засобів контролю для усунення виявленого ризику. На третьому рівні для загрози T_{s4} «Таксіфай N» має розглянути всі варіанти передачі виявленого ризику іншим організаціям (наприклад, страховим). На останньому рівні запобігання ризику для загроз T_{p2}, T_{w3}, T_{w4}, T_{n1}, T_{w5} рекомендовано обрати відповідні цілі контролю, щоб знизити виявлені ризики та звести до мінімуму потенційний вплив на інформаційні системи «Таксіфай N» відповідно до правил додатку до ISO/IEC 27001.

Результати порівняння економічної діяльності організації до введення програми у 2022 р. та за результатами дії програми у 2023 р. були оцінені за допомогою аналізу економічної ефективності (CEA). Цей підхід ґрунтується на порівнянні показників ефективності різних років діяльності організації:

$$F = \frac{C_{t_1} - C_{t_2}}{E_{t_2} - E_{t_1}} = \frac{\Delta C}{\Delta E} \quad , \tag{5}$$

де C – валові витрати організації;

E – валові доходи організації;
t_1 – період до введення програми управління ризиками інформаційної безпеки;
t_2 – період за результатами дії програми управління ризиками інформаційної безпеки.

Критерієм ефективності заходів є значення показника *F* більше від 0. Для організації «Таксіфай N» цей показник склав 0,64, що свідчить про ефективність запропонованої програми.

Висновок. Систематизовано процес оцінювання ризиків інформаційної безпеки в системах транспортного обслуговування за рівнями імовірності та впливу на засоби контролю й керування операціями. Сформовано перелік загрозливих подій, що можуть перешкоджати досягненню бізнес-цілей систем надання транспортних послуг, зокрема міського громадського транспорту. Запропоновано механізм управління ризиками інформаційної безпеки, який ґрунтується на категорійній моделі причинно-наслідкових зв'язків між вразливостями та загрозами й передбачає систематизацію оцінювання ризиків із підсумковим визначенням за матрицею наслідків. Відповідно, це дозволяє формувати заходи управління ризиками відповідно до груп наслідків; реалізація методу передбачає п'ять етапів. За обмеження до використання розробленого механізму виступає те, що у процесі його реалізації можуть виникнути певні перешкоди, які пов'язані із впровадженням ISO 27001, оскільки це портребує певної підтримки персоналу організації.

Таким чином, можливості використання запропонованого механізму управління ризиками інформаційної безпеки в системах транспортного обслуговування були оцінені експертним методом на прикладі умовної компанії перевізника автомобільного транспорту «Таксіфай N». Встановлено причинно-наслідкові зв'язки між вразливостями та загрозами (загрозливими подіями) в сфері інформаційної безпеки та виконана оцінка ймовірності виникнення потенційних загрозливих подій. Результати оцінювання засвідчили, що 5 ризиків мають високий рівень наслідків, 4 – посередній, 1 – значний, 5 – низький. Для «Таксіфай N» була запропонована програма управління ризиками, яка включала заходи для кожної групи виявлених загрозливих подій. Оцінки експертів були перевірені на узгодженість за методом конкордації, із розрахунковим коефіцієнтом в 0,86. Здійснена оцінка ефективності управління ризиками інформаційної безпеки для компанії перевізника автомобільного транспорту «Таксіфай N» за результатами впровадження свідчить про покращення результуючих показників. Зокрема, критерій ефективності щодо запропонованих і впроваджених відповідно до вищезгадуваної програми заходів має позитивне значення та складає 0,64.

Перелік посилань

1. Smerichevskyi, S., Mykhalchenko, O., Poberezhna, Z., Kryvovyazyuk, I. (2023). Devising a systematic approach to the implemen-tation 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

2. 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

3. 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

4. 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

5. 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

6. 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

7. Fertis, A., Baes, M., Lthi, 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

8. Joshi, N. N., Lambert, J. H. (2011). Diversification of infrastructure projects for emergent and unknown non-systematic risks. Jour-nal of Risk Research, 14 (6), 717–733. https://doi.org/10.1080/13669877.2011.553733.

9. 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

10. 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

11. 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

12. 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

13. 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

14. Andersson, A., Hedstrm, K., Karlsson, F. (2022). Standardizing information security – a structurational analysis. Informa-tion & Management, 59 (3), 103623. https://doi.org/10.1016/j.im.2022.103623

15. The NIST Cybersecurity Framework 2.0 (2023). National Institute of Standards and Technology. https://doi.org/10.6028/nist.cswp.29.ipd

16. 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

17. Мельниченко, О.І., Ігнатенко, О.С., Дмитриченко А.М. (2023). Логістичне управління системою надання транспортних послуг населенню: антикризовий аспект. *Вісник Національного транспортного університету*. Серія «Технічні науки», Випуск 1 (55), С.200–210. https://doi.org/10.33744/2308-6645-2023-1-55-200-210

18. Добровольська А., Добровольський О., Дерегуз І. Розробка науково-методичного підходу до систематизації процесу оцінювання ризику в системах логістичного обслуговування // *Multidisciplinární mezinárodní vědecký magazín "Věda a perspektivy" je registrován v České republice.* Státní registrační číslo u Ministerstva kultury ČR: E 24142. № 9(52) 2025. str. 185-196. https://doi.org/10.52058/2695-1592-2025-9(52)-185-196

19. Khrutba, V., Kharchenko, A., Khrutba, Y., Kolbasin, M., Tsybulskyi, V., Silantieva, I., & Lysak, R. 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*, 2022. Vol. 4. No. 2 (118), P. 6-15. https://doi.org/10.15587/1729-4061.2022.262356

SYSTEMATIZATION AND ASSESSMENT OF INFORMATION SECURITY RISKS IN LOGISTICS SERVICE SYSTEMS

Dobrovolska Anna. M, Ph.D., associate professor, National Transport University, Professor of Department of Logistics and Project Management, e-mail: anet_chechet@ukr.net, tel. +380634321538, https://orcid.org/0000-0002-5912-0678

Derehuz Igor, A., PhD candidate, National Transport University, Department of Logistics and Project Management, Kyiv, Ukraine, derehuz@ukr.net, http://orcid.org/0000- 0003-3119-3709

Summary.

The relevance of the study is due to the need to increase the effectiveness of information security risk management in logistics service systems by developing and practical implementation of a mechanism for their

assessment and management, taking into account the cause-and-effect relationships between vulnerabilities and threats and the impact of their consequences on the functioning of transport systems.

The purpose of the article is to systematize and improve approaches to assessing information security risks in transport logistics systems by developing and practical implementation of a risk management mechanism in transport service systems, which is based on establishing cause-and-effect relationships between vulnerabilities and threats, assessing the probability of their occurrence and the level of consequences, as well as forming justified response measures based on a matrix approach.

The article considers theoretical and methodological aspects of assessing information security risks in logistics service systems, approaches to their systematization by levels of probability and consequences, as well as the features of establishing cause-and-effect relationships between vulnerabilities and threats.

A mechanism for managing information security risks in logistics service systems is proposed, which is based on a categorical model of relationships between threats and vulnerabilities, involves the use of a matrix of consequences for assessing risks and developing justified measures to minimize them, and is also tested on the example of a transport enterprise. Based on the results of the assessment, the distribution of risks by significance levels is determined and response measures are developed. The effectiveness of the proposed approach is confirmed by the consistency of expert assessments and the improvement of the integral indicator of risk management effectiveness.

Key words: risk management and assessment, risk management in logistics service systems, risk assessment process, systematization of the risk assessment process, information security risk management mechanism in transport service systems.

References

1. Smerichevskyi, S., Mykhalchenko, O., Poberezhna, Z., Kryvovyazyuk, I. (2023). Devising a systematic approach to the implemen-tation 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

2. 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

3. 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

4. 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

5. 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

6. 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

7. Fertis, A., Baes, M., Lthi, 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

8. 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.

9. 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

10. 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

11. Shapiro, A. (2013). On Kusuoka Representation of Law Invariant Risk Measures. M*athematics of Operations Research,* 38 (1), 142–152. https://doi.org/10.1287/moor.1120.0563

12. 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

13. 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

14. Andersson, A., Hedstrm, K., Karlsson, F. (2022). Standardizing information security – a structurational analysis. *Information & Management,* 59 (3), 103623. https://doi.org/10.1016/j.im.2022.103623

15. The NIST Cybersecurity Framework 2.0 (2023). National Institute of Standards and Technology. https://doi.org/10.6028/nist.cswp.29.ipd

16. 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

17. Melnichenko, O., Ignatenko, O., Dmytrychenko, A., Dereguz, I. (2023). Logistics management of the system for providing transpor-tation 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 [in Ukrainian]

18. Dobrovolska A., Dobrovolskiy O., Derehuz I. Development of a scientific-methodical approach to the systematization of the risk assessment process in logistics service systems // *Multidisciplinární mezinárodní vědecký magazín "Věda a perspektivy" je registrován v České republice.* Státní registrační číslo u Ministerstva kultury ČR: E 24142. № 9(52) 2025. str. 185-196. https://doi.org/10.52058/2695-1592-2025-9(52)-185-196

19. Khrutba, V., Kharchenko, A., Khrutba, Y., Kolbasin, M., Tsybulskyi, V., Silantieva, I., & Lysak, R. 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*, 2022. Vol. 4. No. 2 (118), P. 6-15. https://doi.org/10.15587/1729-4061.2022.262356

Дата надходження до редакції 10.02.2026.
Дата прийняття статті після рецензування 21.02.2026.