TECHNICAL SCIENCES AND TECHNOLOGIES

DOI: https://doi.org/10.25140/2411-5363-2025-2(40)-207-220
УДК 004.056:656

Олексій Ігорович Трунов[1], Марія Сергіївна Дорош[2]

[1]аспірант, викладач кафедри інформаційних технологій та програмної інженерії
Національний університет «Чернігівська політехніка» (Чернігів, Україна)
E-mail: alexeytrunov1995@gmail.com .**ORCID**: https://orcid.org/0009-0002-0321-2669

[2]доктор технічних наук, професор, професор кафедри інформаційних технологій та програмної інженерії
Національний університет «Чернігівська політехніка» (Чернігів, Україна)
E-mail: m.dorosh@stu.cn.ua. **ORCID**: http://orcid.org/0000-0001-6537-9857
ResearcherID: AAF-2603-2019. **Scopus Author ID**: 56912183600

СИСТЕМАТИЗАЦІЯ ПІДХОДІВ ДО ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТРАНСПОРТНО-ЛОГІСТИЧНИХ ЦЕНТРІВ

Зростання кіберзагроз для транспортно-логістичних центрів (ТЛЦ) вимагає адаптованих підходів до управління ризиками інформаційної безпеки (ІБ). Існуючі методики оцінки ризиків ІБ недостатньо враховують специфіку ТЛЦ (інтеграція IT/OT, унікальні вектори атак та ін.).

Метою статті є систематизація наявних підходів до оцінки ризиків ІБ та визначення їхньої придатності для ризиків інформаційної системи (ІС) ТЛЦ.

На основі аналізу специфіки функціонування ТЛЦ (інтеграція IT/OT, критичність ланцюгів постачання, підвищені ризики воєнного часу) та огляду існуючих досліджень і стандартів, було: ідентифіковано та класифіковано основні категорії ризиків ІБ, характерні для ТЛЦ; проаналізовано поширені методики та стандарти оцінки ризиків ІБ (ISO 2700x, NIST, CORAS, HAZOP, OWASP, FAIR, FMEA, EBIOS та ін.); обґрунтовано доцільність застосування комбінованого, диференційованого підходу до оцінки ризиків, що поєднує використання комплексних фреймворків (NIST, ISO) із застосуванням спеціалізованих методик для окремих напрямків діяльності ТЛЦ; представлено структуровані рекомендації щодо вибору методик оцінки ризиків ІБ відповідно до специфіки ключових функціональних напрямків ТЛЦ.

У результаті дослідження виявлено фрагментарність та недостатню специфічність існуючих рішень. Обґрунтовано гостру потребу розробки інтегрованої, спеціалізованої методики оцінки ризиків ІБ саме для ТЛЦ.

***Ключові слова**: ризик інформаційної безпеки; транспортно-логістичний центр; оцінка ризиків; методика оцінки ризиків; критична інфраструктура.*

Рис.: 1. Табл.: 2. Бібл.: 30.

Актуальність теми дослідження. В умовах нестабільної світової економіки, зумовленою макроекономічною та геополітичною невизначеністю, питання забезпечення ІБ підприємств стає дедалі більш актуальним.

Розвиток інформаційного суспільства створює не лише нові можливості для економічного зростання, але й нові загрози ІБ. На сьогодні підприємства стають більш уразливими до загроз через зростаючу залежність від комп'ютерів, мереж, програм та додатків, соціальних мереж та даних.

Порушення безпеки можуть негативно позначитися на діяльності підприємств та їхніх клієнтах як у фінансовому, так і репутаційному плані. При цьому однією з найважливіших складових забезпечення інформаційної безпеки підприємства є оцінка ризиків ІБ.

За результатами дослідження «Ризик у фокусі на 2025 рік», проведеного Європейською конфедерацією інститутів внутрішнього аудиту (ECIIA) [1], було визначено очікувані ризики, з якими можуть зіткнутися підприємства різних секторів економіки в найближчі 3 роки (рис. 1).

Респонденти дев’ятий рік поспіль першочерговою загрозою вважають кібербезпеку (83 %), а швидко зростаючі цифрові збої за прогнозами, до 2028 року будуть посідати друге місце серед ризиків (72 %). Урядова команда реагування на комп’ютерні надзвичайні події CERT-UA, яка діє при Держспецзв’язку, повідомила, що в Україні у 2024 році було опрацьовано 4315 кіберінцидентів. Це на 69,8 % більше, ніж у 2023 році. Тобто спостерігається стійка тенденція до зростання кібератак передусім на критично важливу інфраструктуру України, зокрема на транспортно-логістичні системи, що забезпечують під час війни постачання військової техніки, гуманітарної допомоги, а також підтримують економічну стабільність [2].

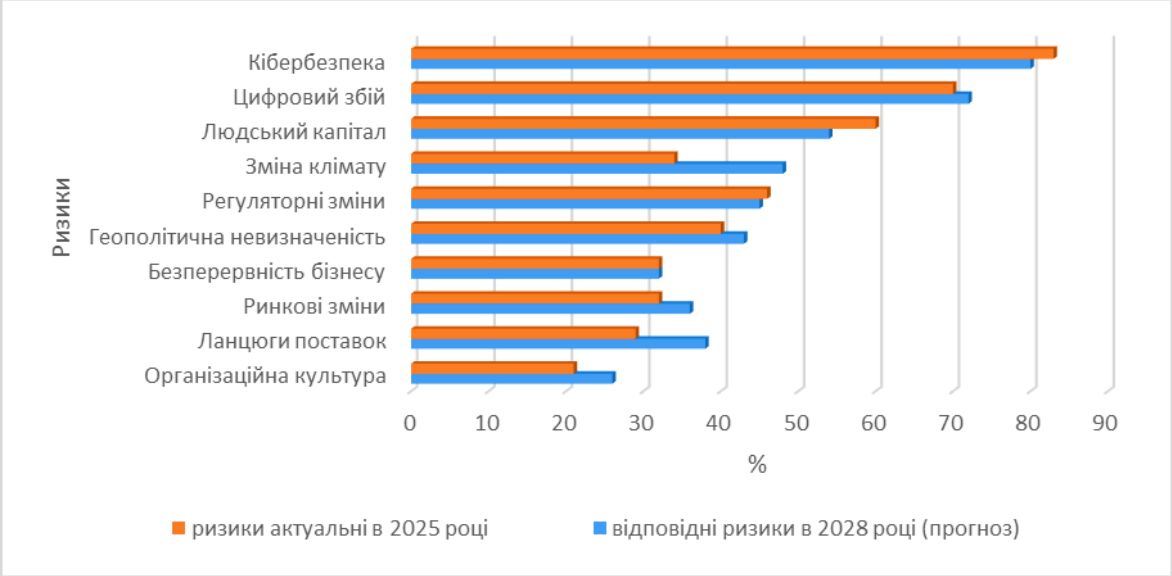

Рис. 1. Найбільші 10 ризиків, з якими можуть зіткнутися підприємства в найближчі 3 роки

Джерело: розроблено авторами.

Згідно із сучасними дослідженнями, централізація логістичної інформації в транспортно-логістичних центрах (ТЛЦ) вимагає підвищеної уваги до питань кібербезпеки. ТЛЦ виконують комплексні функції, включаючи планування, моніторинг та контроль за переміщенням вантажів, забезпечуючи оперативне відображення поточного стану для ухвалення управлінських рішень. Комплексність цих систем, що характеризується багаторівневим доступом та розподілом ресурсів, зумовлює необхідність застосування диверсифікованих підходів до управління та захисту процесів передачі, обробки та зберігання інформації.

В умовах воєнних дій, забезпечення ІБ ТЛЦ набуває критичного значення, оскільки виникають нові ризики, що зачіпають як операційні, так і інформаційні процеси. У цьому контексті, оцінка ризиків ІБ ТЛЦ стає ключовим інструментом для визначення необхідних та достатніх, а також економічно обґрунтованих заходів та засобів захисту інформації. Організація ефективної системи моніторингу ризиків ІБ ТЛЦ є необхідною для превентивного запобігання ризикам ІБ та мінімізації негативних наслідків у разі їх реалізації.

Постановка проблеми. Відсутність адекватної оцінки ризиків для ТЛЦ ускладнює визначення стратегії побудови системи захисту інформації, виділення необхідних ресурсів, ідентифікацію потенційних загроз та вибір пріоритетних контрзаходів [3]. З огляду на це, завдання оцінювання ризиків, пов'язаних із кібератаками на інформаційні системи ТЛЦ, набуває першочергового значення. Нові виклики, що постають перед транспортною та логістичною галузями, зумовлюють необхідність перегляду сучасних підходів до оцінки ризиків ІБ ТЛЦ [4]. Таким чином, науково обґрунтована оцінка ризиків ІБ ТЛЦ є критично важливим елементом забезпечення стабільності та безпеки транспортно-логістичних операцій, особливо в умовах воєнного стану.

Аналіз останніх досліджень і публікацій. Питання оцінки ризику ІБ з кожним роком набуває все більшої актуальності. Зокрема, І. Л. Обертинюк, О. В. Кареліна у статті [5] презентують технологію оцінювання ризиків ІБ для підприємства «Укртелеком» відповідно до вітчизняних нормативних документів та міжнародних стандартів, використовуючи методологію CRAMM. Окремим питанням є економічна оцінка захисту інформації, І. М. Карпович та ін. в роботах [6] та [7] детально досліджують методику оцінки рівня ризиків ІБ та обґрунтування оптимальних витрат на захист інформації. Автори пропонують нові підходи до моделювання заходів безпеки та розробляють методику оцінки ризиків, що

поєднує теорію графів з експертними оцінками. О. Потій та ін. [8] провели докладний аналіз методів оцінки й управління ризиками кібер- і інформаційної безпеки та визначили необхідність адаптації та удосконалення відомих методів шляхом їх логічного поєднання з урахуванням переваг та мінімізації недоліків цих методів. Є. Кузьміних та ін. [9] розглянули оцінку ризиків ІБ з використанням нечіткої логіки, здійснили класифікацію ризиків.

Питанням застосування різних програмних продуктів для оцінки ризиків ІБ присвячені роботи: Х. Разікін, Б. Соевіто [10] – OCTAVE Allegro для компаній роздрібної торгівлі; К. Шмітц, С. Папе [11] – спрощена структура оцінки ризиків безпеки для підтримки прийняття рішень у сфері ІБ (LiSRA); П. Лофт та ін. [12] – Continuous Agile Enterprise Security Architecture Review у 8 доменах (CAESAR8), що підтримує динамічні та цілісні огляди ризиків ІБ в ІТ-проєктах; А. Іршейд та ін. [13] провели порівняльний аналіз методологій управління ІБ ISO 27005, NIST SP 800-30, CRAMM, CORAS, OCTAVE Allegro та COBIT 5, що зосереджений на їхній придатності, гнучкості та здатності залучати різні групи користувачів у контексті хмарних обчислень. Проте запропоновані оцінки не враховують специфіки транспортно-логістичної галузі і ТЛЦ зокрема.

Оцінка ризиків ІБ у транспортній галузі представлена в роботі К. Бернсмед та ін. [14], де розглянуто удосконалення методології оцінки ризиків безпеки SESAR (SecRAM) у сфері управління повітряним рухом. У статті Б. Гюнеш та ін. [15] для чотирьох розроблених сценаріїв кібератаки була застосована методологія оцінки ризику з використанням інтегрованого підходу до управління кібербезпекою з урахуванням фізичних кіберактивів контейнерного порту. У роботі Л. Лян та ін. [16] проаналізовані ризики ІБ компонентів з відкритим вихідним кодом у транспортній галузі та запропоновані заходи щодо їх управління. У дослідженні С. Алфарісі та Н Суранта. [17] застосування OCTAVE Allegro допомогло виявити критичні активи та ризики автопарку. О. Мельниченко та ін. [18] описують процес аналізу, оцінки та управління ризиками ІБ в системах надання транспортних послуг. У роботі систематизовано процес оцінювання ризиків ІБ на транспорті та визначені шляхи попередження та протидії інформаційним загрозам як при проєктуванні, так і при експлуатації систем надання транспортних послуг.

Однак, наголошуючи на істотних здобутках провідних учених в обраному напрямку дослідження, необхідно зауважити, що отримані ними результати вимагають певної систематизації та адаптації до специфіки ТЛЦ у питаннях оцінки ризиків ІБ.

Виділення недосліджених частин загальної проблеми. Незважаючи на підвищення інтересу до питання оцінки ризиків ІБ, методики, що використовуються в наш час, є не достатньо ефективні, оскільки цей процес у більшості транспортних компаній не здійснюється взагалі або здійснюється в окремих підрозділах. Централізований контроль ІБ на підприємствах транспортно-логістичної галузі найчастіше відсутній, що виключає можливість реалізації єдиного та цілісного підходу до управління ризиками у всій організації. У зв'язку з цим у проведеному дослідженні концентрується увага на можливості застосування відомих методологій з урахуванням практичної діяльності ТЛЦ.

Метою статті є систематизація підходів до оцінки ризиків інформаційної безпеки актуальних для ТЛЦ.

Виклад основного матеріалу. Транспортно-логістичні центри є критично важливими об'єктами інфраструктури, що забезпечують переміщення товарів і вантажів. Обробка значних обсягів даних, що включають інформацію про вантажі, транспортні засоби, маршрути, клієнтів та фінансові операції, робить їх особливо вразливими до кіберзагроз [4].

Ризик ІБ для ТЛЦ полягає в можливості пошкодження, знищення або компрометації їхніх інформаційних активів. В умовах військових дій, коли ризики кібератак зростають, забезпечення ІБ ТЛЦ стає першочерговим завданням. Ключовим елементом управління ІБ ТЛЦ є аналіз та керування ризиками. По суті, оцінка ризику визначає ефективність наявних заходів захисту у протидії потенційним інформаційним атакам.

Аналіз специфічних проблем ІБ у сфері транспортної логістики дозволив ідентифікувати та систематизувати основні категорії ризиків для ТЛЦ, які представлено в табл. 1.

Таблиця 1 – Основні категорії ризиків ІБ для ТЛЦ

Категорії ризиків ІБ	Типи ризиків ІБ	Характеристика	Приклад реалізації ризику
1	2	3	4
1. Конфіденційність	Несанкціонований доступ до критичних операційних даних (запаси, локації, замовлення, терміни придатності).	Розголошення чутливих даних (маршрути, клієнти, комерційна таємниця, персонал). Ризик цілеспрямованих атак з боку ворожих сил або їхніх агентів для отримання стратегічної інформації.	Через фішинг викрадають детальні плани перевезення гуманітарної допомоги до прифронтових зон.
	Витік даних	Випадкова/навмисна передача даних назовні (помилки, соц. інженерія, інсайдери).	Email зі звітом клієнтів надіслано назовні, перехоплено.
	Прослуховування каналів	Перехоплення даних у каналах зв'язку (особливо радіо, супутник). Ризик перехоплення інформації про переміщення вантажів, особливо військових або гуманітарних.	Перехоплення координат/статусу вантажу з незашифрованого радіоканалу ворожою розвідкою.
2. Цілісність	Пошкодження/ знищення даних	Втрата даних внаслідок кібератак (віруси-шифрувальники, DDoS), фізичних пошкоджень (ракетні удари, диверсії), збоїв в роботі обладнання, перебоїв з електропостачанням, бойових дій або стихійних лих.	Ransomware блокує WMS/TMS; Серверна пошкоджена обстрілом, дані знищено.
	Несанкціонована модифікація/ фальсифікація	Навмисна зміна даних (маршрути, статус вантажу); внесення неправдивої інформації (фіктивні рейси). Ризик внесення неправдивої інформації в системи відстеження вантажів.	Хакери змінюють адресу доставки в TMS; Створення фіктивних перевезень для крадіжки коштів.
3. Доступність	Відмова в обслуговуванні (DoS/DDoS)	Перевантаження систем, недоступність сервісів для користувачів (в т.ч. координовані атаки). Ризик скоординованих атак на критично важливі системи для порушення постачання.	DDoS-атака на клієнтський портал унеможливлює розміщення замовлень.
	Збої обладнання / програмного забезпечення (ПЗ)	Зупинка систем (WMS, TMS, SCM) через техн. проблеми, вразливості ПЗ, невдалі оновлення.	Збій WMS після оновлення зупиняє роботу складу на цілий день, спричиняючи значні затримки.
	Порушення електропостачання або зв'язку	Втрата доступу через проблеми з енергопостачанням, пошкодження інфраструктури (обстріли, диверсії).	Відключення енергії зупиняє всі IT-системи; Втрата зв'язку з ТЗ на маршруті.
4. Автентичність та підзвітність	Підробка особистості (Spoofing)	Видача себе за іншого (користувач, система, орган влади) для доступу/обману.	Фішинг від імені "контролюючого органу" для отримання конфіденційних даних.
	Відмова від дій (Repudiation)	Заперечення виконаних дій через відсутність доказів (логів аудиту), включаючи випадки пошкодження або втрати вантажу.	Водій заперечує отримання інструкцій (без логування) – втрата вантажу.
	Відсутність належного обліку та аудиту	Неможливість відстежити дії користувачів та зміни в системах – ризик зловживань.	Неможливо встановити, хто змінив дані про кількість товару при виявленні розбіжності.

Закінчення табл. 1

1	2	3	4
5. Людський фактор	Помилки персоналу	Ненавмисні дії співробітників – витік даних або збої у роботі систем.	Оператор помилково вводить не той код товару в WMS.
	Інсайдерські загрози	Навмисні зловмисні дії (крадіжка даних, саботаж, зрада, робота на ворога).	Звільнений співробітник видаляє файли; Завербований передає дані про вразливості ворогу.
	Соціальна інженерія	Маніпуляція персоналом для отримання доступу/конфіденційної інформації.	Зловмисник дзвонить співробітнику підтримки, видаючи себе за керівника, і терміново просить пароль до системи, отримуючи таким чином доступ.
	Недостатня обізнаність	Недостатня підготовка персоналу до роботи в умовах воєнних дій або інших кризових ситуацій.	Дзвінок "керівника" з терміновим проханням надати пароль – компрометація доступу.
6. Ланцюги постачальників (SCRM)	Атаки на постачальників/ постачальників	Компрометація систем третіх сторін (партнери, брокери, IT-постачальники) з доступом до даних ТЛЦ.	Злам системи митного брокера – витік даних про міжнародні перевезення ТЛЦ.
	Підробка, модифікація обладнання або ПЗ	Використання контрафактного/модифікованого обладнання/ПЗ з бекдорами/вразливостями.	Мережеве обладнання з «закладкою» від неперевіреного постачальника надає бекдор до мережі.
	Зрив/припинення постачання	Зрив постачання критичного обладнання/ПЗ/послуг (в т.ч. через війну, санкції, банкрутство).	Постачальник ПЗ на окупованій території припиняє підтримку – вразливі системи.
7. Фізична безпека	Несанкціонований фізичний доступ до об'єктів ТЛЦ	Проникнення на об'єкти ТЛЦ для крадіжки обладнання/даних, шпигунства.	Крадіжка ноутбуків з офісу на складі через «сліпі зони» відеоспостереження
	Саботаж, диверсії, воєнні дії	Навмисне пошкодження/знищення інфраструктури ТЛЦ; захоплення/ блокування об'єктів. Ризик захоплення або блокування об'єктів ТЛЦ.	Підрив підстанції/колій, що обслуговують ТЛЦ; Пряме влучання в склад/офіс.
8. Кібертероризм та кібервійна	Цілеспрямовані кібератаки	Кібератаки з боку ворожих сил або терористичних угруповань з метою порушення транспортної інфраструктури. Поширення паніки та підрив економічної стабільності через кібератаки.	Координована атака ворожої держави на системи управління рухом ключових ТЛЦ – транспортний колапс.
	Деструктивні дії в кіберпросторі	Ведення розвідки, саботажу та дезінформаційних кампаній, спрямованих на ТЛЦ, з використанням кіберпростору.	Поширення фейків через соцмережі та зламані сайти про знищення ТЛЦ для паніки.

Джерело: розроблено авторами.

Оцінка ризиків ІБ є найбільш складним і відповідальним етапом процесу управління безпекою, оскільки саме від її результатів залежать подальші дії організації. Методика оцінки ризиків – це систематичний процес ідентифікації, аналізу та оцінювання потенційних ризиків, який включає визначення можливих негативних подій, їхньої ймовірності та потенційних наслідків.

Відомі методики оцінки та аналізу ризиків класифікують за типом оцінки: якісні (використовують описові шкали, наприклад, «високий», «середній», «низький»); кількісні (ризик оцінюється числовим значенням, наприклад, очікуваними річними втратами у грошовому вимірі); гібридні (поєднують якісні та кількісні підходи). Як зазначають Хаджі С., Тан Ц. та Коста Р. С. [19], гібридні моделі, що часто інтегрують методи штучного інтелекту, демонструють високу ефективність в оцінці інформаційних ризиків, оскільки дозволяють враховувати як кількісні показники, так і якісні експертні оцінки. У таких моделях процес оцінки може бути ітеративним: він повторюється доти, доки рівень залишкового ризику після впровадження контрзаходів не досягне прийнятного рівня.

У світовій практиці існує значна кількість стандартів та методологій оцінки ризиків ІБ (наприклад, OCTAVE Allegro, FRAP, FAIR, CRAMM, CORAS). Міжнародні стандарти, зокрема серії ISO/IEC 27000 (зокрема, ISO/IEC 27005:2022), слугують основою для побудови систем управління ІБ (СУІБ) у багатьох організаціях, включно з ТЛЦ. Водночас сфера кібербезпеки в Україні динамічно розвивається. Зокрема, відзначимо розробку методичних рекомендацій Національним банком України (НБУ), щодо СУІБ та оцінки ризиків для фінансового сектору, які можуть слугувати орієнтиром і для інших критично важливих галузей [20].

При виборі методик оцінки ризиків ІБ для ТЛЦ в Україні необхідно враховувати специфіку галузі: тісну інтеграцію інформаційних та операційних технологій (IT/OT), критичну важливість ланцюгів постачання та постійно високий рівень загроз, особливо в умовах військових дій (цілеспрямовані атаки, DDoS, руйнівне ПЗ, дезінформація). Актуальними залишаються виклики щодо уніфікації галузевих підходів та адаптації міжнародних стандартів.

Аналіз сучасних методологій та стандартів дозволив обґрунтувати вибір найбільш релевантних підходів для ТЛЦ. Ключовими є комплексні фреймворки, що забезпечують системне управління ІБ:

– стандарти NIST (CSF, RMF, SP 800-161) [21] надають надійну основу для комплексної програми ІБ, управління ризиками життєвого циклу систем (IT/OT) та ризиками ланцюга постачання (SCRM). Мають дуже високу придатність для ТЛЦ як критичної інфраструктури, хоча й вимагають ресурсів для впровадження;

– міжнародні стандарти ISO/IEC 27001:2022 [22] та ISO/IEC 27005:2022 [23]: Визначають вимоги до Системи Управління Інформаційною Безпекою (СУІБ) та процес управління ризиками ІБ. Мають високу придатність, демонструють зрілість ІБ партнерам, дозволяючи гнучко обирати методи оцінки. Впровадження СУІБ є ресурсоємним.

Ці фундаментальні підходи доцільно доповнювати спеціалізованими методиками для поглибленого аналізу конкретних аспектів діяльності ТЛЦ:

– CORAS (гібридна) для моделювання складних IT/OT систем [24];

– HAZOP (Cyber HAZOP) (якісна) для аналізу безпеки та безперебійності систем OT (АСУТП, SCADA) [25];

– Threat Modeling / PASTA (якісна) для проактивного виявлення загроз під час розробки/модифікації систем та API [26];

– OWASP (гібридна) для оцінки безпеки вебдодатків та API (надає практичні інструменти та підтримується активною спільнотою) [27];

– FAIR (кількісна) для фінансової оцінки ризику [28];

– FMEA (якісна) для аналізу відмов критичних систем (WMS, контроль доступу) [29];

– EBIOS (якісна) для аналізу ризиків в екосистемі (партнери, постачальники) та сценаріїв навмисних загроз [30].

Зауважимо, що вибір методики оцінки ризиків впливає на формування стратегії виявлення атак. Наприклад, аналіз станів систем (FMEA, HAZOP) обґрунтовує впровадження моніторингу аномалій стану для IT/OT систем, тоді як моделювання загроз (PASTA, Threat Modeling) чи аналіз специфікацій (OWASP) вказують на пріоритетність сигнатурних, специфікаційних чи евристичних методів для захисту вебінтерфейсів та API.

Для досягнення ефективного управління ризиками та адекватного виявлення атак у складних умовах функціонування ТЛЦ рекомендується застосування синергетичного, комбінованого підходу. Це передбачає використання визнаного комплексного фреймворку (NIST або ISO) як базової структури, яка доповнюється спеціалізованими методиками для поглибленого аналізу ключових областей ризику. Такий підхід дозволяє сформувати комплексну, адаптовану та ризикоорієнтовану систему виявлення атак та реагування на них.

При цьому важливо враховувати аспект вартості та доступності: більшість стандартів та методологій надають документацію безкоштовно (NIST, ISO 27005, OWASP, EBIOS), однак їх ефективне впровадження, використання спеціалізованих інструментів (ПЗ), залучення експертів та навчання потребують фінансових та часових ресурсів. Оптимізація витрат може бути досягнута шляхом збалансованого поєднання безкоштовних ресурсів із платними, але більш спеціалізованими рішеннями та експертною підтримкою.

Вибір методики(ик) оцінки ризиків ІБ є ключовим питанням для формування подальшої стратегії виявлення кібератак та визначає загальний рівень кіберстійкості ТЛЦ. Оптимальним є диференційований підхід, що враховує специфіку конкретних напрямків діяльності ТЛЦ (управління складом, транспортуванням, клієнтським сервісом тощо). Найкращі результати демонструє саме комбінація фундаментальних фреймворків (ISO 27005/NIST RMF) зі спеціалізованими інструментами та техніками, цілеспрямовано застосованими.

Систематизований вибір рекомендованих методик оцінки ризиків, диференційованих за ключовими напрямками діяльності ТЛЦ, представлено в табл. 2.

Таблиця 2 – Рекомендовані методики оцінки ризиків залежно від напрямку діяльності ТЛЦ

Напрямок діяльності ТЛЦ та відповідні послуги	Можливі ризики ІБ	Методики оцінки ризиків ІБ
1	2	3
1. Управління складом: приймання, розміщення, крос-докінг; Управління запасами (IoT, RFID), AS/RS; внутрішній транспорт (AGV, конвеєри); облік та звітність (Big Data, AI); відвантаження, комплектація (pick-by-voice/light/vision), повернення; Інтеграція (API) з e-commerce; Хмарні/гібридні WMS)	Несанкціонований доступ до критичних операційних даних (запаси, локації, замовлення, терміни придатності).	EBIOS: Аналіз бізнес-ризиків та сценаріїв несанкціонованого доступу. Threat Modeling: Моделювання векторів доступу (інтерфейси, персонал, вразливості). NIST RMF: Оцінка ризиків для визначення необхідних контролів доступу.
	Кібератаки (Ransomware, DDoS, злам акаунтів) на системи WMS/ASRS, що призводять до зупинки операцій, втрати даних.	Threat Modeling (STRIDE, PASTA): Проактивний аналіз архітектури та векторів атак (API, IoT, оператори). FMEA / HAZOP: Аналіз відмов та операційних небезпек в OT компонентах (ASRS, AGV, конвеєри), у т.ч. спровокованих кібератаками.
	Втрата або пошкодження цілісності операційних даних (запаси, замовлення) через збої, помилки, людський фактор, кібератаки.	FAIR: Кількісна оцінка фінансових наслідків втрати/недоступності даних. NIST RMF: Загальна оцінка ризиків порушення цілісності даних. НБУ: Для оцінки фінансової стійкості та відповідності регуляторним вимогам.
	Неправомірні маніпуляції даними в WMS (кількість, якість, статус) з метою шахрайства, крадіжки, саботажу.	FMEA: Аналіз потенційних відмов процесів обліку та контролю. EBIOS – оцінка ризиків, пов'язаних із неадекватним контролем доступу та розмежуванням повноважень
2. *Управління транспортуванням:* планування маршрутів (AI/ML); відстеження вантажів (GPS, IoT, телематика); Управління автопарком; інтеграція (API) з біржами; Мобільні додатки для водіїв; АСУР на території; е-документообіг (митниця); доставка «останньої милі» (дрони, роботи).	Компрометація систем телематики (GPS/IoT), вкл. спуфінг/джамінг: невірне відстеження, зрив графіків, крадіжки.	ORAS: Моделювання ризиків у складних соціотехнічних системах (взаємодія GPS/IoT та людини). Threat Modeling: Аналіз специфічних векторів атак (спуфінг, джамінг).

Продовження табл. 2

1	2	3
	Несанкціонований доступ до конфіденційних логістичних даних (маршрути, графіки, клієнти, водії).	EBIOS: Ідентифікація цінних логістичних даних та аналіз загроз їх конфіденційності.
	Кібератаки на TMS та інтегровані платформи: збої в плануванні, комунікації, обміні даними.	Threat Modeling: Аналіз загроз та вразливостей архітектури TMS та інтеграційних API.
	Зловмисне втручання або технічний збій АСУР / AGV / дронів на території ТЛЦ	HAZOP: Детальний аналіз потенційних відхилень та небезпечних наслідків у роботі систем управління рухом. FMEA: Аналіз відмов компонентів АСУР/AGV/дронів. НБУ: Оцінка операційних ризиків, що можуть мати фінансові наслідки.
	Ризики компрометації даних при обміні з партнерами (митниця, перевізники) через незахищені канали або вразливості їхніх систем.	CORAS: Аналіз ризиків інформаційної взаємодії між організаціями, моделювання довіри. NIST SP 800-161: Управління ризиками ланцюга постачання (SCRM), включаючи партнерів
3. Управління ланцюгами постачання (SCM): прогнозування попиту (AI/ML); автоматизація замовлень (EDI, API); end-to-end visibility (IoT, Blockchain); інтеграція (API) з постачальниками; аналітика SCM (ризики, стійкість).	Атаки на інтерфейси обміну даними (API, EDI) з партнерами (MitM, ін'єкції, проблеми автентифікації).	OWASP (API Security Top 10): Ідентифікація та оцінка технічних вразливостей API. Threat Modeling: Аналіз векторів атак на протоколи та інтерфейси обміну..
	Несанкціонований доступ до стратегічної комерційної інформації SCM (постачальники, ціни, обсяги, контракти).	EBIOS: Оцінка критичності активів SCM та аналіз загроз їх конфіденційності.
	Каскадний ефект від кібератак на партнерів (Supply Chain Attack), що впливає на власні операції, дані, репутацію.	NIST SP 800-161: Комплексне управління ризиками SCRM. MAGERIT: Аналіз залежностей між активами та процесами, включаючи зовнішні системи. CORAS: Моделювання поширення ризиків у ланцюгу постачання.
	Ризики, пов'язані з безпекою даних у хмарних провайдерів та інших сторонніх постачальників IT-послуг (SaaS, PaaS).	NIST RMF / SP 800-161: Структуроване управління ризиками третіх сторін.
4. Клієнтський сервіс: онлайн-портали (замовлення, відстеження); мобільні додатки; Чат-боти, вірт. асистенти (AI); персоналізовані пропозиції; інтеграція з CRM	Компрометація облікових записів клієнтів (Account Takeover), доступ до PII та історії взаємодії.	OWASP (Top 10, ASVS, Mobile): Ідентифікація вразливостей веб/мобільних додатків. Threat Modeling: Загальний аналіз загроз для процесів автентифікації та управління сесіями. NIST SP 800-63: Оцінка ризиків, пов'язаних з цифровою ідентичністю та автентифікацією.
	Витік комерційної інформації (замовлення, платежі) через вразливості порталів/додатків, помилки конфігурації.	OWASP (Top 10, ASVS, Mobile): Ідентифікація технічних вразливостей, що призводять до витоків. EBIOS: Оцінка ризиків розголошення конфіденційної клієнтської інформації.
	Кібератаки на клієнтські інтерфейси (дефейс, DDoS, XSS, CSRF).	OWASP: Оцінка захищеності від специфічних вебатак, рекомендації Secure SDLC.

Закінчення табл. 2

1	2	3
	Соціальна інженерія (фішинг, вішинг), спрямована на клієнтів для викрадення даних або шахрайства.	EBIOS: Аналіз сценаріїв соціальної інженерії та їх потенційного впливу. NIST SP 800-63 / SP 800-50: Оцінка ризиків, пов'язаних з процесами ідентифікації та ефективністю програм обізнаності.
5. Внутрішні операції: хмарні сервіси (IaaS, PaaS, SaaS); СЕД; RPA; Політики віддаленої роботи, BYOD; корпоративні мобільні пристрої (MDM/EMM).	Несанкціонований доступ до корпоративної мережі та критичних внутрішніх систем (ERP, фінанси, HR).	ISO 27005: Основа для управління ризиками ІБ в рамках СУІБ. NIST RMF: Комплексне управління ризиками для федеральних та критичних систем. Threat Modeling: Ідентифікація векторів проникнення.
	Витік внутрішньої конфіденційної інформації (дані співробітників, фінанси, комерційна таємниця, IP).	NIST RMF: Управління ризиками конфіденційних даних.
	Кібератаки на ключові елементи IT-інфраструктури (сервери, СЗД, мережа), вкл. DoS, експлуатація вразливостей.	IT-Grundschutz: Деталізовані каталоги базових заходів безпеки ("будівельні блоки"). FMEA / HAZOP: Аналіз відмов для критичних компонентів інфраструктури.
	Зараження систем шкідливим ПЗ (віруси, трояни, ransomware) через фішинг, USB, вразливості, інсайдерів.	Threat Modeling: Аналіз та моделювання векторів розповсюдження шкідливого ПЗ. NIST CSF: Комплексний фреймворк, що включає захист від шкідливого ПЗ (Protect, Detect).

Джерело: розроблено авторами.

Представлений підхід, що систематизує рекомендовані методики та стандарти оцінки ризиків ІБ відповідно до ключових напрямів діяльності ТЛЦ, є важливим кроком до структурованого управління безпекою. Таке розбиття на функціональні напрямки допомагає систематизувати аналіз та забезпечує повніше охоплення потенційних проблемних зон. Запропонована структура може слугувати відправною точкою для ТЛЦ будь-якого розміру, однак вона не є догматичною і повинна гнучко адаптуватися під унікальні умови конкретного логістичного центру (специфічні послуги, технології, регуляторні вимоги, наявні ресурси, рівень ризик-апетиту).

Попри переваги структурованого підходу та можливість комбінування методик, їх застосування в контексті ТЛЦ виявляє певні суттєві обмеження:

– стандартні методи часто фокусуються на оцінці ризиків окремих компонентів, недостатньо враховуючи кумулятивні наслідки та системні взаємозв'язки у тісно інтегрованому IT/OT ландшафті ТЛЦ. Атаки можуть експлуатувати вразливості на стиках систем, призводячи до каскадних ефектів, які важко передбачити при ізольованій оцінці;

– методики загального призначення не завжди повною мірою враховують унікальну специфіку логістичних операцій (критичність своєчасності, фізична взаємодія з товарами, складні ланцюги постачання, специфічні OT/ICS системи);

– істотним практичним недоліком багатьох методик є високі вимоги до ресурсів: необхідність залучення експертів з глибокими знаннями в ІБ та логістиці, а також значні витрати на підтримку та актуалізацію процесів оцінки й баз знань.

Ці виявлені обмеження – ризик фрагментарної оцінки, недостатнє врахування системних ефектів та специфіки логістики, високі вимоги до експертизи та ресурсів – вказують на те, що навіть комбінація існуючих стандартних методик може бути недостатньою для адекватного управління ризиками ІБ у сучасних ТЛЦ. Це обґрунтовує нагальну необхідність розробки власної, спеціалізованої методики оцінки ризиків ІБ, цілеспрямо-

вано створеної для транспортно-логістичних центрів. Така методика має інтегрувати сильні сторони існуючих підходів, але водночас бути адаптованою до специфіки галузі, враховувати системні взаємозв'язки та бути більш ефективною і менш ресурсоємною в реальних умовах функціонування ТЛЦ.

Отже, спеціалізована методика оцінки ризиків ІБ для ТЛЦ має базуватися на динамічній моделі, що передбачає: адаптацію до специфіки та загроз різних типів ТЛЦ; гнучкий вибір заходів безпеки з урахуванням логістичної інфраструктури; застосування релевантних підходів для компонентів IT/OT систем та бізнес-процесів; швидке оновлення баз знань про загрози для підтримки актуальності оцінки; динамічне моделювання для прогнозування еволюції ризиків та забезпечення проактивного управління ІБ.

Висновки. Забезпечення інформаційної безпеки транспортно-логістичних центрів набуває критичного значення в умовах зростання кіберзагроз, особливо під час воєнних дій, враховуючи їхню роль у підтримці економіки та національної безпеки. Проте аналіз стану досліджень виявив недостатню увагу до специфіки ризиків ІБ саме в цій галузі.

У роботі вирішено завдання систематизації підходів до оцінки ризиків ІБ, актуальних саме для ТЛЦ. На основі аналізу специфіки функціонування ТЛЦ (інтеграція IT/OT, критичність ланцюгів постачання, підвищені ризики воєнного часу) та огляду існуючих досліджень і стандартів, було: ідентифіковано та класифіковано основні категорії ризиків ІБ, характерні для ТЛЦ; проаналізовано поширені методики та стандарти оцінки ризиків ІБ (ISO 2700x, NIST, CORAS, HAZOP, OWASP, FAIR, FMEA, EBIOS та ін.); обґрунтовано доцільність застосування комбінованого, диференційованого підходу до оцінки ризиків, що поєднує використання комплексних фреймворків (NIST, ISO) із застосуванням спеціалізованих методик для окремих напрямків діяльності ТЛЦ; представлено структуровані рекомендації щодо вибору методик оцінки ризиків ІБ відповідно до специфіки ключових функціональних напрямків ТЛЦ.

Запропонований диференційований підхід та систематизація методик надають практичну основу для ТЛЦ при виборі та впровадженні найбільш адекватних інструментів управління ризиками ІБ в поточних умовах, дозволяючи структурувати цей процес та оптимізувати використання ресурсів.

Однак, незважаючи на переваги структурованого застосування існуючих методик, виявлено їхні суттєві недоліки для комплексного аналізу ТЛЦ: недостатній облік системних взаємозв'язків та кумулятивних ефектів, обмежене врахування специфіки логістичних операцій та високі вимоги до ресурсів. Зважаючи на виявлені обмеження та унікальну складність і критичність ТЛЦ, зроблено висновок про обґрунтовану необхідність розробки нової, комплексної та адаптованої методики оцінки ризиків інформаційної безпеки, спеціально призначеної для транспортно-логістичних центрів.

Список використаних джерел

1. European Confederation of Institutes of Internal Auditing (ECIIA). (2024). Risk in Focus 2025: Hot topics for internal auditors. https://www.eciia.eu/2024/09/risk-in-focus-2025-hot-topics-for-internal-auditors.

2. Державна служба спеціального зв’язку та захисту інформації України. (n.d.). CERT-UA минулого року опрацювала 4315 кіберінцидентів. https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv.

3. Trunov, O., Skiter, I., Dorosh, M., Trunova, E., Voitsekhovska, M. (2024). Modeling of the Information Security Risk of a Transport and Logistics Center Based on Fuzzy Analytic Hierarchy Process. In: Kazymyr, V., et al. Mathematical Modeling and Simulation of Systems. MODS 2023. Lecture Notes in Networks and Systems, vol 1091. Springer, Cham. https://doi.org/10.1007/978-3-031-67348-1_23.

4. Трунов, О. І., Дорош, М. С. (2023). Системи забезпечення інформаційної безпеки для транспортно-логістичних центрів. Математичне та імітаційне моделювання систем. МОДС 2022: тези доповідей Сімнадцятої міжнародної науково-практичної (С. 7-10). http://ir.stu.cn.ua/handle/123456789/26927.

5. Обертинюк, І. Л., Кареліна, О.В. (2018). Технології оцінки ризиків інформаційної безпеки відповідно до вітчизняних нормативних документів та міжнародних стандартів. Актуальні задачі сучасних технологій : зб. тез доповідей міжнар. наук.-техн. конф. Молодих учених та студентів, (С. 132-134). https://m.tntu.edu.ua/storage/pages/00000742/Book-2-2018.pdf.

6. Карпович, І. М., Гладка, О. М., Наконечна, Ю. А. (2020). Аналіз ризиків безпеки інформаційної системи ІТ-підприємства. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки, 31*(70), 5, 69–74. https://doi.org/10.32838/2663-5941/2020.5/12.

7. Карпович, І., Гладка, О., Бухало, Ю. (2021). Технології моделювання і оцінки ризиків інформаційної безпеки. *Технічні науки та технології,* (1(23)), 62–68. https://doi.org/10.25140/2411-5363-2021-1(23)-62-68.

8. Потій, О., Горбенко, Ю., Замула, О. та Ісірова, К. (2021). Аналіз методів оцінки і управління ризиками кібер-і інформаційної безпеки. *Радіотехника,* (206), 5-24. https://doi.org/10.30837/rt.2021.3.206.01.

9. Kuzminykh, I., Ghita, B., Sokolov, V., & Bakhshi, T. (2021). Information security risk assessment. *Encyclopedia,* 1(3), 602–617. https://doi.org/10.3390/encyclopedia1030050.

10. Razikin, K., Soewito, B. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. *Egyptian Informatics Journal, 23*(3), 383–404. https://doi.org/10.1016/j.eij.2022.03.001.

11. Schmitz, C., Pape, S. (2020). LiSRA: Lightweight security risk assessment for decision support in information security. *Computers & Security*, Article 101656. https://doi.org/10.1016/j.cose.2019.101656.

12. Loft, P., He, Y., Yevseyeva, I., Wagner, I. (2022). CAESAR8: an agile enterprise architecture approach to managing information security risks. *Computers & Security,* 122, Article 102877. https://doi.org/10.1016/j.cose.2022.102877.

13. Irsheida, A., Murada, A., AlNajdawia, M., Qusefa A. (2022). Information security risk management models forcloud hosted systems: A comparative study. *Procedia Computer Science,* 204, 205–217. https://doi.org/10.1016/j.procs.2022.08.025.

14. Bernsmed, K., Bour, G., Lundgren, M., Bergström, E. (2022). An evaluation of practitioners' perceptions of a security risk assessment methodology in air traffic management projects. *Journal of Air Transport Management*, 102, 102223. https://doi.org/10.1016/j.jairtraman.2022.102223.

15. Gunes, B., Kayisoglu, G., Bolat, P. (2021). Cyber security risk assessment for seaports: A case study of a container port. Computers & Security, 103, 102196, https://doi.org/10.1016/j.cose.2021.102196.

16. Liang, L., Wu, X., Deng J., Lv, X. (2022). Research on risk analysis and governance measures of open-source components of information system in transportation industry. *Procedia Computer Science, 208*, 106-110. https://doi.org/10.1016/j.procs.2022.10.017.

17. Alfarisi, S., Surantha, N. (2022). Risk assessment in fleet management system using OCTAVE allegro. *Bulletin of Electrical Engineering and Informatics, 11*(1), 530–540. https://doi.org/10.11591/eei.v11i1.3241.

18. 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. https://doi.org/10.15587/1729-4061.2024.298144.

19. 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

20. Національний банк України. (2011, 3 березня). Щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України: 1 Лист № 24-112/365. Верховна Рада України. https://zakon.rada.gov.ua/laws/show/v0365500-11#Text.

21. NIST SP 800-37 Rev. 2. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (2018). https://doi.org/10.6028/NIST.SP.800-37r2.

22. International Organization for Standardization & International Electrotechnical Commission. (2022). Information security, cybersecurity and privacy protection – Guidance on managing information security risks (ISO/IEC 27005:2022). https://cdn.standards.iteh.ai/samples/80585/7bca93ac16fd426a9bc717cadc9284d9/ISO-IEC-27005-2022.pdf.

23. International Organization for Standardization & International Electrotechnical Commission. (2022). Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO/IEC 27001:2022).

24. Lund, M. S., Stølen, K., & Vraalsen, F. (2011). Model-Driven Risk Analysis: The CORAS Approach. Springer. https://doi.org/10.1007/978-3-642-12323-8.

25. International Electrotechnical Commission. (2016). Hazard and operability studies (HAZOP studies) – Application guide (IEC 61882:2016).

26. UcedaVélez, T., & Morana, M. M. (2015). Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. Wiley.

27. OWASP Foundation. (n.d.). OWASP Foundation | Open Source Foundation for Application Security. https://owasp.org.

28. Freund, J., & Jones, J. (2014). Measuring and Managing Information Risk: A FAIR Approach. Butterworth-Heinemann.

29. International Electrotechnical Commission. (2018). Failure modes and effects analysis (FMEA and FMECA) (IEC 60812:2018).

30. Agence nationale de la sécurité des systèmes d'information (ANSSI). (2018). EBIOS Risk Manager – The method. https://www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method.

References

1. European Confederation of Institutes of Internal Auditing (ECIIA). (2024). Risk in Focus 2025: Hot topics for internal auditors. https://www.eciia.eu/2024/09/risk-in-focus-2025-hot-topics-for-internal-auditors.

2. Derzhavna sluzhba spetsialnoho zv'iazku ta zakhystu informatsii Ukrainy [State Service of Special Communications and Information Protection of Ukraine]. CERT-UA mynuloho roku opratsiuvala 4315 kiberintsydentiv [CERT-UA processed 4315 cyber incidents last year]. https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv.

3. Trunov, O., Skiter, I., Dorosh, M., Trunova, E., & Voitsekhovska, M. (2024). Modeling of the information security risk of a transport and logistics center based on fuzzy analytic hierarchy process. In V. Kazymyr et al. (Eds.), *Mathematical modeling and simulation of systems. MODS 2023. Lecture Notes in Networks and Systems* (Vol. 1091). Springer, Cham. https://doi.org/10.1007/978-3-031-67348-1_23.

4. Trunov, O. I., & Dorosh, M. S. (2023). Systemy zabezpechennia informatsiinoi bezpeky dlia transportno-lohistychnykh tsentriv [Information security systems for transport and logistics centers]. In *Matematychne ta imitatsiine modeliuvannia system. MODS 2022: tezy dopovidei Simnadtsiatoi mizhnarodnoi naukovo-praktychnoi konferentsii – Mathematical and simulation modeling of systems. MODS 2022: Abstracts of the Seventeenth International Scientific and Practical Conference* (pp. 7-10). *Chernihiv Polytechnic National University*. http://ir.stu.cn.ua/handle/123456789/26927.

5. Obertyniuk, I. L., & Karelina, O. V. (2018). Tekhnolohii otsinky ryzykiv informatsiinoi bezpeky vidpovidno do vitchyznianykh normatyvnykh dokumentiv ta mizhnarodnykh standartiv [Information security risk assessment technologies according to domestic regulations and international standards]. In *Aktualni zadachi suchasnykh tekhnolohii: zb. tez dopovidei mizhnar. nauk.-tekhn. konf. Molodykh uchenykh ta studentiv – Current problems of modern technologies: Collection of abstracts of the international scientific and technical conference of young scientists and students*, (pp. 132-134). *Ternopil Ivan Puluj National Technical University*. https://m.tntu.edu.ua/storage/pages/00000742/Book-2-2018.pdf.

6. Karpovych, I. M., Hladka, O. M., & Nakonechna, Yu. A. (2020). Analiz ryzykiv bezpeky informatsiinoi systemy IT-pidpryiemstva [Analysis of security risks of the information system of an IT enterprise]. *Vcheni zapysky Tavriiskoho natsionalnoho universytetu imeni V. I. Vernadskoho. Seriia: Tekhnichni nauky – Scientific Notes of V. I. Vernadsky Taurida National University. Series: Technical Sciences, 31(70), 5, 69–74.* https://doi.org/10.32838/2663-5941/2020.5/12

7. Karpovych, I., Hladka, O., & Bukhalo, Yu. (2021). Tekhnolohii modeliuvannia i otsinky ryzykiv informatsiinoi bezpeky [Technologies for modeling and assessment of information security risks]. *Tekhnichni nauky ta tekhnolohii – Technical Sciences and Technologies*, (1(23)), 62–68. https://doi.org/10.25140/2411-5363-2021-1(23)-62-68.

8. Potii, O., Horbenko, Yu., Zamula, O., & Isirova, K. (2021). Analyz metodov otsenky y upravlenyia kyberryskamy y ynformatsyonnoi bezopasnostiu [Analysis of methods for assessing and managing cyber risks and information security]. *Radyotekhnyka – Radio Engineering,* (206), 5–24. https://doi.org/10.30837/rt.2021.3.206.01.

9. Kuzminykh, I., Ghita, B., Sokolov, V., & Bakhshi, T. (2021). Information security risk assessment. *Encyclopedia, 1*(3), 602–617. https://doi.org/10.3390/encyclopedia1030050.

10. Razikin, K., Soewito, B. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. *Egyptian Informatics Journal, 23*(3), 383–404. https://doi.org/10.1016/j.eij.2022.03.001.

11. Schmitz, C., Pape, S. (2020). LiSRA: Lightweight security risk assessment for decision support in information security. *Computers & Security,* 101656. https://doi.org/10.1016/j.cose.2019.101656.

12. Loft, P., He, Y., Yevseyeva, I., Wagner, I. (2022). CAESAR8: an agile enterprise architecture approach to managing information security risks. *Computers & Security, 122,* 102877. https://doi.org/10.1016/j.cose.2022.102877.

13. Irsheida, A., Murada, A., AlNajdawia, M., Qusefa, A. (2022). Information security risk management models forcloud hosted systems: A comparative study. *Procedia Computer Science, 204*, 205–217. https://doi.org/10.1016/j.procs.2022.08.025.

14. Bernsmed, K., Bour, G., Lundgren, M., Bergström, E. (2022). An evaluation of practitioners' perceptions of a security risk assessment methodology in air traffic management projects. *Journal of Air Transport Management, 102*, 102223. https://doi.org/10.1016/j.jairtraman.2022.102223.

15. Gunes, B., Kayisoglu, G., Bolat, P. (2021). Cyber security risk assessment for seaports: A case study of a container port. *Computers & Security, 103,* 102196, https://doi.org/10.1016/j.cose.2021.102196.

16. Liang, L., Wu, X., Deng, J., Lv, X. (2022). Research on risk analysis and governance measures of open-source components of information system in transportation industry. *Procedia Computer Science, 208*, 106-110. DOI: 10.1016/j.procs.2022.10.017.

17. Alfarisi, S., Surantha, N. (2022). Risk assessment in fleet management system using OCTAVE allegro. *Bulletin of Electrical Engineering and Informatics, 11*(1), 530–540. https://doi.org/10.11591/eei.v11i1.3241.

18. 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. https://doi.org/10.15587/1729-4061.2024.298144.

19. 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.

20. National Bank of Ukraine. (2011, March 3). Shchodo vprovadzhennia systemy upravlinnia informatsiinoiu bezpekoiu ta metodyky otsinky ryzykiv vidpovidno do standartiv Natsionalnoho banku Ukrainy: Lyst № 24-112/365 [Regarding the implementation of the information security management system and risk assessment methodology in accordance with the standards of the National Bank of Ukraine: Letter No. 24-112/365]. *Verkhovna Rada of Ukraine*. https://zakon.rada.gov.ua/laws/show/v0365500-11#Text.

21. NIST SP 800-37 Rev. 2. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (2018). https://doi.org/10.6028/NIST.SP.800-37r2.

22. International Organization for Standardization & International Electrotechnical Commission. (2022). Information security, cybersecurity and privacy protection — Guidance on managing information security risks (ISO/IEC 27005:2022). https://cdn.standards.iteh.ai/samples/80585/7bca93ac16fd426a9bc717cadc9284d9/ISO-IEC-27005-2022.pdf.

23. International Organization for Standardization & International Electrotechnical Commission. (2022). *Information security, cybersecurity and privacy protection – Information security management systems – Requirements* (ISO/IEC 27001:2022).

24. Lund, M. S., Stølen, K., & Vraalsen, F. (2011). Model-Driven Risk Analysis: The CORAS Approach. Springer. https://doi.org/10.1007/978-3-642-12323-8

25. International Electrotechnical Commission. (2016). Hazard and operability studies (HAZOP studies) – Application guide (IEC 61882:2016).

26. UcedaVélez, T., & Morana, M. M. (2015). Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. Wiley.

27. *OWASP Foundation*. (n.d.). OWASP Foundation. Open Source Foundation for Application Security. https://owasp.org.

28. Freund, J., & Jones, J. (2014). Measuring and Managing Information Risk: A FAIR Approach. Butterworth-Heinemann.

29. *International Electrotechnical Commission*. (2018). Failure modes and effects analysis (FMEA and FMECA) (IEC 60812:2018).

30. *Agence nationale de la sécurité des systèmes d'information* (ANSSI). (2018). EBIOS Risk Manager – The method. https://www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method.

Отримано 05.05.2025

UDC 004.056:656

Trunov Oleksii[1], Dorosh Mariia[2]

[1]PhD student, Lecturer at the Department of Information Technology and Software Engineering
E-mail: alexeytrunov1995@gmail.com. **ORCID**: https://orcid.org/0009-0002-0321-2669

[2]Doctor of Technical Sciences, Professor, Professor of the Department of Information Technologies and Software Engineering
Chernihiv Polytechnic National University (Chernihiv, Ukraine)
E-mail: m.dorosh@stu.cn.ua. **ORCID**: http://orcid.org/0000-0001-6537-9857
ResearcherID: AAF-2603-2019. **Scopus Author ID**: 56912183600

SYSTEMATIZATION OF APPROACHES TO THE INFORMATION SECURITY RISK ASSESSMENT OF TRANSPORTATION AND LOGISTICS CENTERS

Relevance of the study is driven by significant and constant growth of cyber threats to critical infrastructure, in particular to transport and logistics centers (TLCs), which are key nodes in global supply chains. Attacks on TLCs lead to serious consequences, namely: financial losses, disruption of logistics, and data compromise. This creates urgent need for effective approaches to information security (IS) risk management adapted to the specifics of the TLC. Existing methods for assessing IS risks do not sufficiently take into account unique operational processes, integrated IT and OT systems, and technological landscape of TLCs, which jeopardizes their sustainability.

The main problem addressed in this study is fragmentation of knowledge and insufficient adaptation of existing IS risk assessment methodologies to the specific conditions of TLCs. General approaches do not take into account unique attack vectors (via WMS, TMS), specific IT/OT vulnerabilities (SCADA), and cascading effects on physical operations. This mismatch makes it difficult to build effective cyber defense, which is critical for the sustainability of operations and data protection.

The purpose of the article is to comprehensively systematize existing approaches to assessing IS risks, identify their advantages/disadvantages, and determine their relevance to TLCs.

The study analyzed scientific works, standards and practices, which confirmed insufficient coverage of the specifics of TLCs' IS. The categories of security risks for TLCs are systematized. Risk assessment methodologies (FAIR, EBIOS, NIST, ISO/IEC 27005:2023, etc.) are classified and compared, their suitability for TLC is assessed, and advantages, disadvantages, and difficulties of adaptation are identified. The use of the combined, multi-level approach to selection of methods is proposed.

The scientific novelty lies in development of classification and systematization of modern methods of assessing IS risks for TLC, as well as in the analysis of relationships between risk assessment methods, attack detection methods and approaches to their implementation in the context of TLC. This forms the knowledge base for making informed decisions by the TLC management on IS management. Practical value is possibility of improving the cybersecurity of TLCs through implementation of the recommended combined approach. At the same time, limitations of existing methods have been identified, including: fragmentation, insufficient consideration of the specifics of TLCs (especially IT/OT convergence) and potential resource intensity.

Conclusions confirm achievement of the goal and substantiate urgent need for further research to develop the integrated, specialized methodology for assessing IS risks specifically for TLCs.

***Keywords**: information security risk; transport and logistics center; risk assessment; risk assessment methodology; critical infrastructure.*

Fig.: 1. Table: 4. References:30.

Трунов О. І., Дорош М. С. Систематизація підходів до оцінки ризиків інформаційної безпеки транспортно-логістичних центрів. *Технічні науки та технології.* 2025. № 2(40). С. 207-220. DOI: https://doi.org/10.25140/2411-5363-2025-2(40)-207-220.