Standard. Formal vote, CLC/TC 9X.
4. ДСТУ IEC/TR 61000-5-6:2012. Електромагнітна сумісність. Частина 5-6. Настанови щодо встановлення устаткування та притлумлення завад. Зменшення зовнішнього електромагнітного впливу (IEC/TR 61000-5-6:2002, IDT).
5. IEC 61000-5-6:2024. Electromagnetic compatibility (EMC) – Part 5-6: Mitigation of external EM influences.
6. Кустов В. Ф., Єлізаренко А. О. Нормування і вплив завад поїзного радіозв'язку 2,13 і 2,15 МГц на порти живлення електронних пристроїв СЦБ рівнів SIL 3/4. Зб. наук. пр. УкрДУЗТ. 2026. Вип. 216. С. 289–314. DOI: 10.18664/1994-7852.216.2026.362481.
7. Кустов В. Ф., Прилипко А. А. Вплив вологості на деградацію елементів захисту і параметри каналів проникнення завад: загрози для електромагнітної сумісності і функціональної безпеки систем залізничної автоматики. Інформаційно-керуючі системи на залізничному транспорті. 2025. № 2. С. 144–158.
8. IEC 61000-4-36:2020. Electromagnetic compatibility (EMC) – Part 4-36: IEMI immunity test methods for equipment and systems.
9. Heddebaut M. et al. Mitigation Techniques to Reduce the Vulnerability of Railway Signaling to Radiated Intentional EMI Emitted From a Train. IEEE Trans. Electromagn. Compat. 2017. Vol. 59, No. 3. P. 845–852. DOI: 10.1109/TEMC.2016.2635259.

УДК 656.025.4:004.056

Бойко Андрій Григорович,

аспірант кафедри транспортних технологій Харківського національного автомобільно-дорожнього університету

КЛАСТЕРИЗАЦІЯ ТРАНСПОРТНО-ЛОГІСТИЧНИХ ЦЕНТРІВ У МОДЕЛЯХ КІБЕРСТІЙКОГО УПРАВЛІННЯ ДОСТАВКОЮ ЗАПАСНИХ ЧАСТИН

Анотація. Запропоновано концептуальну модель управління технологією доставки запасних частин на основі динамічної кластеризації транспортно-логістичних центрів. Модель поєднує прогнозування попиту, оцінювання ресурсів центрів і контроль достовірності інформації про замовлення та запаси. Обґрунтовано розділення логістичної кластеризації та перевірки інформаційної надійності, що дає змогу зберігати економічний зміст групування й обмежувати використання непідтверджених даних. Визначено критерій вибору технології доставки, умови переходу до резервного режиму та порядок сценарної перевірки. Очікуване практичне значення полягає у підтримці узгоджених рішень щодо поповнення запасів, консолідації відправлень і перенаправлення замовлень за зміни попиту та порушення інформаційного обміну.

Ключові слова: запасні частини, транспортно-логістичний центр, кластеризація,

динамічний попит, кіберстійкість, управління доставкою.

Управління доставкою запасних частин потребує узгодження наявності товарів, терміновості замовлень і можливостей транспортно-логістичних центрів (ТЛЦ). Нерівномірний попит за окремими номенклатурними позиціями ускладнює вибір періодичності поповнення та розміру партій. Для переривчастого попиту метод TSB передбачає оновлення ймовірності виникнення попиту в кожному періоді, що дозволяє враховувати тривалу відсутність замовлень [1]. Проте прогноз сам по собі не визначає, через який центр і за якою технологією доцільно виконувати доставку.

Додатковим обмеженням є залежність управлінських рішень від цифрового обміну між системами обліку замовлень, складського та транспортного управління. Несанкціонована зміна залишків, дублювання заявок або недоступність каналів зв’язку можуть спричинити помилкове перенаправлення вантажопотоків. Тому під кіберстійкістю управління доставкою у цьому дослідженні розуміємо здатність підтримувати прийнятний рівень обслуговування під час порушення інформаційного обміну та відновлювати узгоджені дані після інциденту.

Мета дослідження: розробити концептуальні положення моделі вибору технології доставки запасних частин, яка використовує кластеризацію ТЛЦ за логістичними характеристиками та враховує достовірність інформації в умовах динамічної зміни попиту. Об’єктом є процес доставки запасних частин через мережу ТЛЦ; предметом – залежності між складом кластерів, параметрами доставки та обмеженнями інформаційної надійності.

Одиницею групування пропонується визначити ТЛЦ, а не окремий товар чи замовлення. Для кожного центру в ковзному часовому вікні формують вектор ознак: інтенсивність і варіативність попиту, частку

термінових замовлень, тривалість виконання доставки, завантаження складських і транспортних ресурсів, а також доступність резервних напрямків. Попит доцільно агрегувати за однорідними товарними групами зі збереженням окремих прогнозів для критичних запасних частин. Це запобігає приховуванню дефіциту важливої номенклатури за загальними показниками центру.

Перед групуванням ознаки очищують від підтверджених помилок і масштабують за параметрами навчальної вибірки. Кластерний аналіз використовується як інструмент виявлення структури даних; вибір алгоритму залежить від характеру ознак і форми груп [2]. Як базовий варіант пропонується k-medoids, у якому представником кластера є реальний центр. Кількість кластерів обирають за поєднанням силуетного коефіцієнта, стійкості групування на послідовних часових вікнах та придатності кластерів для прийняття технологічних рішень.

У моделі передбачається перевірка можливості виділення трьох типів центрів: зі стабільним потоком, із мінливим попитом і значною часткою термінових заявок, а також із переважно переривчастим попитом. Це робоча гіпотеза щодо інтерпретації груп, а не заздалегідь встановлений результат кластеризації. Для першого типу оцінюють регулярні консолідовані відправлення, для другого – частіше поповнення й гнучке перенаправлення, для третього – централізоване зберігання частини асортименту з адресною доставкою. Остаточний вибір визначається витратами та обмеженнями сервісу.

Перевірку даних пропонується виконувати окремим контуром до їх передавання у прогнозну та оптимізаційну моделі. Ризикові ознаки охоплюють порушення послідовності повідомлень, неузгодженість замовлень і складських операцій, втрату підтвердження джерела та перевищення допустимої давності записів. Підхід узгоджується із загальним принципом управління кіберризиками NIST CSF 2.0 [3];

конкретні логістичні правила перевірки є авторською пропозицією.

Для центру встановлюють один із режимів: штатний, обмеженої довіри або резервний. У штатному режимі використовують перевірені поточні дані. За обмеженої довіри критичні зміни залишків і термінові заявки потребують додаткового підтвердження. У резервному режимі застосовують останній узгоджений стан запасів із коригуванням на документально підтверджені операції, знижують доступну для обіцянки кількість товару та погоджують перенаправлення з відповідальною особою. Різкий попит не вважається доказом кібератаки: його необхідно зіставляти з незалежними відомостями про замовлення та фактичне відвантаження.

Модель управління доставкою. Вектор керування u охоплює призначення замовлень центрам, обсяги поповнення, періодичність відправлень і вибір між прямою та консолідованою доставкою. Пропонується мінімізувати очікувані сукупні витрати на горизонті планування

$$J(u) = E\left[C_{\text{тр}}(u) + C_{\text{зб}}(u) + C_{\text{деф}}(u) + C_{\text{зап}}(u) + C_{\text{відн}}(u)\right] \rightarrow min, \quad (1)$$

де $C_{\text{тр}}$ – транспортні витрати; $C_{\text{зб}}$ – витрати зберігання; $C_{\text{деф}}$ – втрати від незадоволеного попиту; $C_{\text{зап}}$ – штрафи за запізнення виконаних замовлень; $C_{\text{відн}}$ – витрати відновлення та резервних операцій. Усі складові виражаються у грошових одиницях за однаковий горизонт, а математичне сподівання оцінюється за сценаріями попиту й інформаційних порушень. Втрати від дефіциту та запізнення розмежовують, щоб уникнути подвійного обліку.

Обмеження моделі забезпечують баланс запасів за кожною позицією, невід’ємність залишків, пропускну спроможність центрів і вантажомісткість автомобілів. Для критичних замовлень встановлюють

мінімальну частку своєчасного виконання. Призначення замовлень центрам із непідтвердженим станом ресурсів обмежують або дозволяють лише після погодження. Належність до кластера задає набір технологій для порівняння, але не скасовує перевірки фактичної транспортної доступності та наявності потрібної деталі.

Перерахунок плану виконують на ковзному горизонті після оновлення прогнозу. Повторну кластеризацію запускають за стійкого відхилення логістичних ознак від базового профілю. Порушення довіри до даних насамперед змінює режим керування, а не належність центру до кластера. Для уникнення частих перемикань задають мінімальну тривалість режиму та враховують витрати перепланування. Порогові значення необхідно калібрувати на історичних даних мережі.

Перевірка та очікуваний результат. Доцільно порівняти три стратегії: фіксований розподіл замовлень; адаптивну кластеризацію без контролю інформаційної надійності; запропоновану модель із резервними режимами. Усім стратегіям задають однакові початкові запаси, ресурси та реалізації попиту. Сценарії охоплюють сезонне зростання, локальний стрибок замовлень, недоступність інформаційної системи одного центру та спотворення повідомлень про залишки. Змінні витрати й результати порівнюють за повторними імітаційними прогонами з довірчими інтервалами.

Показниками оцінювання визначено сукупні витрати на виконане замовлення, частку своєчасних доставок, частоту дефіциту, кількість перепризначень і час відновлення узгодженого плану. Доцільність моделі підтверджуватиметься зменшенням витрат за збереження встановленого рівня сервісу або підвищенням сервісу в межах погодженого бюджету. Числове оцінювання ефекту є завданням подальших досліджень.

Запропоновано поєднати логістичну кластеризацію ТЛЦ, прогнозування попиту та контроль інформаційної надійності в єдиному

контурі управління доставкою запасних частин. Основне положення підходу полягає у розділенні зміни логістичного профілю центру й тимчасової втрати довіри до його даних. Це створює основу для вибору технології доставки та переходу до резервного режиму за цифрових порушень. Подальша робота передбачає параметризацію моделі на даних реальної мережі та сценарну оцінку її результативності.

Список використаних джерел

1. Teunter R. H., Syntetos A. A., Babai M. Z. Intermittent demand: Linking forecasting to inventory obsolescence. European Journal of Operational Research. 2011. Vol. 214, no. 3. P. 606–615. DOI: https://doi.org/10.1016/j.ejor.2011.05.018.
2. Jain A. K. Data clustering: 50 years beyond K-means. Pattern Recognition Letters. 2010. Vol. 31, no. 8. P. 651–666. DOI: https://doi.org/10.1016/j.patrec.2009.09.011.
3. Pascoe C., Quinn S., Scarfone K. The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg : National Institute of Standards and Technology, 2024. NIST CSWP 29. DOI: https://doi.org/10.6028/NIST.CSWP.29.

УДК 004.056:004.89:656.05

Гавриленко Аліна Олександрівна,

здобувачка 2 курсу магістратури Харківського національного автомобільно-дорожнього університету

КІБЕРЗАХИСТ ІНФОРМАЦІЇ В ІНТЕЛЕКТУАЛЬНИХ ТРАНСПОРТНИХ СИСТЕМАХ

Анотація. У роботі розглянуто питання кіберзахисту інформації в інтелектуальних транспортних системах в умовах цифровізації транспортної галузі. Визначено основні кіберзагрози, пов’язані з використанням інтернету речей, бездротових мереж і взаємопов’язаних інформаційних систем. Розглянуто багаторівневий підхід до захисту інформації, застосування методів автентифікації, шифрування та виявлення аномалій. Особливу увагу приділено використанню математичних моделей для оцінювання ризиків кібератак і своєчасного реагування на потенційні загрози. Обґрунтовано важливість комплексного підходу до забезпечення кібербезпеки для підвищення надійності та стійкості інтелектуальних транспортних систем.

Ключові слова: інтелектуальні транспортні системи, кібербезпека, кіберзахист