УДК 338.2:004.94:656

5.2.2. Математические, статистические и инструментальные методы в экономике

ИНТЕГРИРОВАННАЯ МОДЕЛЬ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛОГИСТИЧЕСКИХ СИСТЕМ

Лукьяненко Татьяна Викторовна
Кандидат технических наук, доцент
AuthorID: 810321
Федеральное государственное бюджетное образовательное учреждение высшего образования «Кубанский государственный аграрный университет имени И.Т. Трубилина», Краснодар, Россия

Алашеев Вадим Викторович
Кандидат технических наук, доцент
AuthorID: 903223
Федеральное государственное бюджетное образовательное учреждение высшего образования «Кубанский государственный аграрный университет имени И.Т. Трубилина», Краснодар, Россия

В условиях цифровой трансформации экономики логистические системы сталкиваются с двойным вызовом: необходимостью повышения экономической эффективности и одновременным ростом уязвимости к кибернетическим угрозам. Существующие подходы зачастую рассматривают задачи оптимизации и информационной безопасности изолированно, что снижает общую устойчивость и эффективность цепей поставок. Целью данной работы является разработка и теоретическое обоснование интегрированной модели управления логистическими системами, которая объединяет математические методы оптимизации транспортных процессов с инструментальными и статистическими методами обеспечения информационной и кибернетической безопасности. В статье проанализированы классические и эвристические алгоритмы решения транспортных задач, а также предложены методологические основы для построения подсистемы проактивного мониторинга безопасности, основанной на анализе сигналов и данных в инфокоммуникационной среде. Основным результатом является концептуальная архитектура интегрированной модели, демонстрирующая синергетический эффект от взаимосвязи оптимизационных и защитных контуров управления. Предложенная модель позволяет не только оптимизировать маршруты и распределение ресурсов, но и учитывать риски безопасности в качестве одного из ключевых

UDC 338.2:004.94:656

5.2.2. Mathematical, statistical and instrumental methods in economics

AN INTEGRATED MODEL FOR IMPROVING THE EFFICIENCY AND INFORMATION SECURITY OF LOGISTICS SYSTEMS

Lukyanenko Tatiana Viktorovna
Candidate of Technical Sciences, Associate Professor
AuthorID: 810321
Federal State Budgetary Educational Institution of Higher Education "I.T. Trubilin Kuban State Agrarian University", Krasnodar, Russia

Alasheev Vadim Viktorovich
Candidate of Technical Sciences, Associate Professor
AuthorID: 903223
Federal State Budgetary Educational Institution of Higher Education "I.T. Trubilin Kuban State Agrarian University", Krasnodar, Russia

In the context of the digital transformation of the economy, logistics systems face a double challenge: the need to increase economic efficiency and simultaneously increase vulnerability to cyber threats. Existing approaches often consider optimization and information security tasks in isolation, which reduces the overall stability and efficiency of supply chains. The purpose of this work is to develop and theoretically substantiate an integrated management model for logistics systems that combines mathematical methods for optimizing transport processes with instrumental and statistical methods for ensuring information and cybernetic security. The article analyzes classical and heuristic algorithms for solving transport problems, as well as offers methodological foundations for building a subsystem of proactive safety monitoring based on the analysis of signals and data in the infocommunication environment. The main result is the conceptual architecture of the integrated model, demonstrating the synergetic effect of the interconnection of optimization and protective control circuits. The proposed model allows not only to optimize routes and resource allocation, but also to take into account security risks as one of the key optimization parameters, which contributes to increasing the fault tolerance and competitiveness of logistics companies in the modern digital economy

параметров оптимизации, что способствует повышению отказоустойчивости и конкурентоспособности логистических компаний в современной цифровой экономике

Ключевые слова: ЛОГИСТИКА, ОПТИМИЗАЦИЯ, ТРАНСПОРТНАЯ ЗАДАЧА, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, КИБЕРБЕЗОПАСНОСТЬ, МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ, ИНСТРУМЕНТАЛЬНЫЕ МЕТОДЫ, ЦИФРОВАЯ ЭКОНОМИКА, УПРАВЛЕНИЕ ЦЕПЯМИ ПОСТАВОК, ИНТЕГРИРОВАННАЯ МОДЕЛЬ

Keywords: LOGISTICS, OPTIMIZATION, TRANSPORT TASK, INFORMATION SECURITY, CYBERSECURITY, MATHEMATICAL MODELING, INSTRUMENTAL METHODS, DIGITAL ECONOMY, SUPPLY CHAIN MANAGEMENT, INTEGRATED MODEL

http://dx.doi.org/10.21515/1990-4665-212-018

Введение (Introduction)

Современная мировая экономика характеризуется глубокой цифровизацией и усложнением хозяйственных связей, что выводит логистику и управление [4] цепями поставок на первый план в качестве ключевого фактора конкурентоспособности предприятий и целых отраслей. Глобализация рынков, стремительный рост электронной коммерции и повышение требований клиентов к скорости и качеству доставки товаров формируют запрос на создание высокоэффективных, гибких и адаптивных логистических систем. Главным стремлением компаний, занимающихся грузоперевозками, является минимизация расходов при сохранении высокой производительности, и именно в этом контексте эффективное управление маршрутами играет центральную роль.

Для достижения этих целей компании активно внедряют современные информационные технологии: системы управления складом (WMS) и транспортом (TMS), технологии интернета вещей (IoT) для отслеживания грузов в реальном времени, облачные платформы для обработки данных и искусственный интеллект (ИИ) для прогнозирования спроса и автоматизации планирования. Эти технологии позволяют существенно повысить прозрачность и управляемость логистических процессов, сократить издержки и оптимизировать использование ресурсов.

Однако по мере усложнения технологической инфраструктуры логистические системы становятся все более уязвимыми для нового класса угроз. Информационные системы, управляющие материальными потоками, содержат критически важные данные: сведения о грузах, маршрутах, клиентах, финансовую информацию. Их интеграция с общемировым информационным пространством делает их привлекательной целью для кибернетических атак. Появление новейших проводных и беспроводных сетевых технологий привело к созданию глобальной международной инфокоммуникационной системы, которая используется совместно государством, корпорациями, а также террористическими и преступными группировками. Угрозы варьируются от несанкционированного доступа к данным и их хищения до полного выведения из строя элементов информационно-телекоммуникационной сети [7], что может привести к параличу всей цепи поставок и колоссальным финансовым и репутационным потерям.

Анализ научной литературы показывает, что проблемы оптимизации логистических процессов и обеспечения их информационной безопасности чаще всего исследуются в рамках разных научных дисциплин и практических подходов. С одной стороны, в области исследования операций и экономики разрабатываются сложные математические модели и алгоритмы для решения транспортных задач, оптимизации запасов и размещения складов. С другой стороны, специалисты по кибербезопасности фокусируются на защите IT-инфраструктуры [3], разработке средств обнаружения вторжений и защите данных. Этот разрыв приводит к тому, что решения, оптимальные с точки зрения математики (например, самый короткий маршрут), могут быть крайне рискованными с точки зрения безопасности (например, пролегать через зону с незащищенной связью). Отсутствие комплексного подхода, который бы рассматривал эффективность и безопасность как взаимосвязанные и

взаимозависимые параметры, является существенным пробелом в современной теории и практике управления логистикой.

Целью настоящей статьи является разработка и теоретическое обоснование интегрированной модели управления логистическими системами, которая органично сочетает математические, статистические и инструментальные методы для одновременного решения задач оптимизации и обеспечения информационной безопасности. Мы исходим из гипотезы, что только синергетический подход, при котором параметры безопасности включаются в целевую функцию оптимизационных моделей, а результаты оптимизации, в свою очередь, определяют приоритеты для систем защиты [6], способен обеспечить долгосрочную устойчивость и подлинную экономическую эффективность современных цепей поставок.

Для достижения поставленной цели в статье решаются следующие задачи:

1. Систематизация и анализ математических методов и алгоритмов, применяемых для оптимизации грузоперевозок.
2. Исследование современных угроз информационной безопасности в логистике и разработка концепции инструментально-статистических методов их обнаружения и нейтрализации.
3. Построение концептуальной архитектуры интегрированной модели, описывающей взаимосвязи между подсистемами оптимизации и безопасности.
4. Обоснование практической значимости и потенциальных преимуществ предложенной модели для предприятий логистической отрасли.

Статья имеет следующую структуру. В разделе «Методы» подробно рассматриваются два ключевых блока: математические методы оптимизации и инструментально-статистические методы обеспечения безопасности. В разделе «Результаты» представлена разработанная

интегрированная модель, описаны ее основные компоненты и принципы их взаимодействия. Раздел «Обсуждение» посвящен интерпретации полученных результатов, их сопоставлению с существующими подходами, а также анализу практических импликаций и ограничений модели. В заключении подводятся итоги исследования и намечаются направления для дальнейшей научной работы.

Методы (Methods)

Для построения комплексной модели управления логистическими системами необходимо использовать синтез методологических подходов из различных областей знаний: математического программирования, теории графов, теории информации, статистики и радиотехники. В данном разделе мы последовательно рассмотрим две группы методов, составляющих фундамент предлагаемой интегрированной модели.

2.1. Математические методы оптимизации логистических процессов

Основой для повышения экономической эффективности грузоперевозок является математическая оптимизация. Большинство логистических задач, связанных с транспортировкой, могут быть формализованы в терминах теории графов, где города или склады представляются вершинами графа (V), а возможные пути перемещения – ребрами (A) [2].

2.1.1. Точные методы

Точные методы гарантируют нахождение глобально оптимального решения, однако их вычислительная сложность, как правило, экспоненциально растет с увеличением размерности задачи, что ограничивает их применение на практике для крупных транспортных сетей.

- **Линейное программирование (ЛП)**. Методы ЛП предоставляют математические инструменты для оптимизации

линейных функций при линейных ограничениях и широко применяются в логистике. Классическая транспортная задача формулируется как задача ЛП, где требуется минимизировать суммарные затраты на перевозку товаров от поставщиков к потребителям при соблюдении ограничений на объемы поставок и потребности. Метод ветвей и границ, также относящийся к точным алгоритмам, часто используется для решения задач комбинаторной оптимизации, таких как задача коммивояжера (TSP). Его суть заключается в рекурсивном разбиении множества решений на подмножества и отсечении тех из них, которые заведомо не содержат оптимального решения.

- **Динамическое программирование**. Этот подход применяется для задач, которые можно разбить на последовательность более простых подзадач. Алгоритм Хелда-Карпа для решения TSP является классическим примером применения динамического программирования, однако его сложность $O(n^2 2^n)$ также делает его неприменимым для больших n.

2.1.2. Неточные (эвристические) методы

В случаях, когда точное решение задачи невозможно найти за приемлемое время, применяются неточные (приближенные) алгоритмы. Они не гарантируют оптимальности найденного решения, но позволяют получить «достаточно хорошее» решение с гораздо меньшими вычислительными затратами.

- **Алгоритм Кристофидеса**. Предназначен для решения метрической задачи коммивояжера и относится к 2-приближенному классу. Он гарантирует, что найденный маршрут будет не более чем в 1.5 раза длиннее оптимального. Алгоритм включает построение минимального остовного дерева, нахождение совершенного

паросочетания для вершин нечетной степени и построение эйлерова цикла.

- **Алгоритм Кернигана-Лина**. Является высокоэффективным итерационным методом для улучшения уже существующего маршрута. На каждом шаге алгоритм пытается улучшить гамильтонов цикл путем обмена парами ребер. Несмотря на сложность реализации, практика показала, что данный подход существенно улучшает компромисс между трудоемкостью и качеством решения.
- **Метод Гюйгенса**. Этот метод представляет собой математический подход, основанный на принципе Гюйгенса, и используется для определения оптимального расположения логистического центра (склада) с целью минимизации времени доставки груза до всех потребителей. В отличие от дискретных моделей, он переходит к непрерывной постановке задачи, что позволяет более точно описывать реальные процессы.

Для практического применения в рамках интегрированной модели целесообразно использовать гибридный подход, сочетающий различные методы. Например, стратегические задачи (размещение складов) могут решаться с помощью метода Гюйгенса, в то время как тактические задачи (ежедневная маршрутизация) – с помощью быстрых эвристических алгоритмов с последующей локальной оптимизацией методами ЛП для отдельных кластеров.

2.2. Инструментальные и статистические методы обеспечения информационной безопасности

Информационная безопасность в логистике – это состояние защищенности данных и инфраструктуры, при котором обеспечиваются их конфиденциальность, целостность и доступность. Учитывая активное использование беспроводных технологий (GPS/ГЛОНАСС, сотовая связь,

RFID, NFC), риски несанкционированного доступа и перехвата информации значительно возрастают.

2.2.1. Концепция проактивного инструментального мониторинга

Традиционные методы защиты (межсетевые экраны, антивирусы) являются необходимыми, но недостаточными. Мы предлагаем концепцию проактивного инструментального мониторинга, основанную на методологии, разработанной для обнаружения несанкционированно установленных электронных устройств (НУОЭУ) [8]. Суть подхода заключается в постоянном контроле физической и информационной среды на предмет аномалий, которые могут свидетельствовать о наличии угрозы.

Методология включает следующие этапы:

1. **Формирование эталонной сигнатуры.** На начальном этапе создается база данных (БД) спектральных характеристик всех легитимных радиоэлектронных и информационных сигналов в контролируемой зоне (например, на складе, в транспортном средстве). Для каждого сигнала запоминаются его параметры: частота, мощность, тип модуляции и т.д..
2. **Непрерывный мониторинг.** С помощью специализированных аппаратно-программных комплексов (анализаторов спектра, сетевых сканеров) производится постоянное сканирование среды.
3. **Сравнение и обнаружение аномалий.** Полученные в реальном времени данные сравниваются с эталонной БД. Появление нового, ранее не зарегистрированного сигнала или значительное изменение параметров известного сигнала классифицируется как аномалия.
4. **Идентификация и реагирование.** Каждая аномалия подвергается дополнительному анализу для определения ее природы. Например, проверяется условие гармонической связи

частот (Ufh1 > U1(2f1) > U1(3f1)), что характерно для многих подслушивающих устройств. В случае подтверждения угрозы система генерирует сигнал тревоги и инициирует протоколы реагирования.

2.2.2. Статистические методы и алгоритмы классификации

Для автоматизации процесса идентификации угроз предлагается использовать статистические методы и алгоритмы машинного обучения. Разработанный алгоритм идентификации многопараметрических объектов может быть адаптирован для нужд логистической безопасности.

Процесс идентификации можно представить в виде следующей последовательности действий (рис. 4 в):

1. **Нормировка параметров.** Измеренные параметры обнаруженного аномального сигнала (объекта) нормируются для приведения их к единому масштабу.
2. **Вычисление «центра тяжести».** Для совокупности параметров вычисляется обобщенный показатель – «центр тяжести».
3. **Поэтапное сравнение.** Вычисленный центр тяжести последовательно сравнивается с предварительно рассчитанными эталонными центрами тяжести для известных классов угроз (например, «GPS-глушилка», «неавторизованная Wi-Fi точка доступа», «RFID-скиммер»). Сравнение идет от общего к частному: сначала определяется класс угрозы, затем подкласс и конкретный тип.
4. **Принятие решения.** Принадлежность объекта к тому или иному классу определяется по минимальному отклонению его параметров от эталонных.

Такой подход, основанный на теории распознавания образов, позволяет с высокой вероятностью и в автоматическом режиме

классифицировать угрозы, снижая нагрузку на оператора и сокращая время реакции. Совокупность инструментального мониторинга и статистической классификации формирует надежную подсистему обеспечения безопасности, способную противостоять современным кибернетическим и техническим угрозам.

Результаты (Results)

На основе проанализированных в предыдущем разделе методов нами была разработана концептуальная архитектура **Интегрированной Оптимизационно-Защитной Модели (ИОЗМ)** для управления логистическими системами. Данная модель представляет собой многоуровневую систему, в которой подсистемы экономической оптимизации и информационной безопасности функционируют не изолированно, а в тесной взаимосвязи, обмениваясь данными и управляющими воздействиями.

3.1. Архитектура Интегрированной Модели

Общая архитектура ИОЗМ представлена на Рисунке 1. Она состоит из трех ключевых компонентов: Оптимизационной подсистемы, Подсистемы безопасности и Интеграционного ядра.

Рисунок 1. Блок-схема архитектуры Интегрированной Оптимизационно-Защитной Модели (ИОЗМ)

(Примечание: Ниже представлено текстовое описание блок-схемы)

- **Входные данные:** Заказы клиентов, данные о транспортных средствах, состояние дорожной сети, стоимость ресурсов (топливо, труд), нормативы безопасности, данные мониторинга.
- **Блок 1: Подсистема безопасности**
  - **Модуль 1.1:** Инструментальный мониторинг (сканирование радиоэфира, сетевого трафика).

- **Модуль 1.2:** Статистический анализ и идентификация угроз (сравнение с БД сигнатур, классификация аномалий).
- **Выход:** Карта рисков (оценка уровня угрозы для маршрутов, узлов, каналов связи), оперативные оповещения.

- **Блок 2: Интеграционное ядро**
  - **Модуль 2.1:** Анализ рисков и формирование ограничений (преобразование карты рисков в весовые коэффициенты и ограничения для оптимизационной модели).
  - **Модуль 2.2:** Динамическая корректировка планов (обработка оперативных оповещений и передача команд на перепланирование).
- **Блок 3: Оптимизационная подсистема**
  - **Модуль 3.1:** Стратегическое планирование (размещение складов, распределение парка ТС).
  - **Модуль 3.2:** Тактическое планирование (построение маршрутов, графиков).
  - **Алгоритмический блок:** Гибридные алгоритмы (ЛП, эвристики).
- **Выходные данные:** Оптимизированные и безопасные маршруты, графики движения, распределение ресурсов, отчеты.
- **Обратная связь:** Данные о выполнении планов и фактических маршрутах поступают на вход для анализа и корректировки моделей.

3.2. Функционирование компонентов модели

3.2.1. Оптимизационная подсистема

Данная подсистема решает классические задачи логистики, но с важным дополнением: она учитывает параметры безопасности, поступающие из Интеграционного ядра.

- **Вход:** Массив заказов, характеристики транспортных средств, графовая модель дорожной сети, стоимостные параметры (цена топлива, амортизация), а также весовые коэффициенты рисков для каждого ребра (дороги) и вершины (склада) графа.
- **Процесс:** На стратегическом уровне (например, раз в год) с помощью методов типа Гюйгенса определяется оптимальное расположение хабов с учетом долгосрочных прогнозов рисков. На тактическом уровне (ежедневно) запускается гибридный алгоритм маршрутизации. Целевая функция минимизирует не просто расстояние или стоимость, а совокупный взвешенный показатель:
  - $C\_total = w1 * Cost\_fuel + w2 * Cost\_time + w3 * Cost\_risk$

  где $Cost\_risk$ – это функция, рассчитанная на основе карты рисков. Маршруты через зоны с высоким уровнем киберугроз или риском работы технических средств разведки получают высокий «штраф».
- **Выход:** Набор маршрутных листов и графиков, которые являются не только экономически эффективными, но и проложены с учетом минимизации рисков безопасности.

3.2.2. Подсистема безопасности

Эта подсистема работает в непрерывном режиме, обеспечивая информационную осведомленность о состоянии защищенности логистической инфраструктуры.

- **Вход:** Потоки данных от сенсоров: анализаторов спектра на складах и в автомобилях, систем обнаружения вторжений (IDS) в корпоративной сети, данных от IoT-устройств.
- **Процесс:** Модуль инструментального мониторинга в реальном времени собирает данные и выявляет аномалии. Модуль статистического анализа, используя методы распознавания образов,

классифицирует эти аномалии и определяет их уровень опасности. Например, обнаружение мощного неидентифицированного сигнала в УКВ-диапазоне рядом с контейнером с ценным грузом будет классифицировано как угроза высокого уровня.

- **Выход:** Два типа данных. Во-первых, **карта рисков** – динамически обновляемая матрица, где для каждого элемента логистической сети (участок дороги, склад, канал связи [5]) указан текущий интегральный уровень угрозы. Эта карта передается в Интеграционное ядро для использования в плановой оптимизации. Во-вторых, **оперативные оповещения** о критических инцидентах, требующих немедленной реакции.

3.2.3. Интеграционное ядро

Это центральный элемент модели, обеспечивающий синергию между оптимизацией и безопасностью.

- **Процесс 1: Плановое взаимодействие.** Ядро регулярно (например, раз в час) получает обновленную карту рисков от Подсистемы безопасности. Оно преобразует эти качественные и количественные оценки в конкретные параметры для Оптимизационной подсистемы: весовые коэффициенты для целевой функции, запреты на использование определенных маршрутов или технологий связи.
- **Процесс 2: Оперативное взаимодействие.** При получении оперативного оповещения (например, «Обнаружена попытка взлома бортового компьютера на автомобиле №Х»), ядро инициирует экстренный протокол. Оно может отдать команду Оптимизационной подсистеме на немедленное перестроение маршрута для данного автомобиля, передать команду на переключение на резервный защищенный канал связи и уведомить службу безопасности.

3.3. Пример работы модели (сценарий)

Рассмотрим гипотетический сценарий. Логистическая компания перевозит партию дорогостоящей электроники.

1. **Планирование:** ИОЗМ строит маршрут. Стандартный, самый короткий путь пролегает через участок с неустойчивым и незащищенным покрытием сотовой связи. Подсистема безопасности присваивает этому участку высокий коэффициент риска. В результате Оптимизационная подсистема выбирает альтернативный, немного более длинный, но более безопасный маршрут, использующий стабильную спутниковую связь.
2. **Исполнение:** Во время движения грузовика Подсистема безопасности фиксирует попытку GPS-спуфинга (подмены координат).
3. **Реагирование:** Генерируется оперативное оповещение. Интеграционное ядро блокирует передачу неверных данных в систему управления, информирует водителя и службу безопасности, а Оптимизационная подсистема предлагает ближайший безопасный пункт для остановки и проверки.

Этот сценарий демонстрирует, как интеграция двух подсистем позволяет предотвратить инцидент, который при изолированном подходе мог бы привести к угону транспортного средства или потере груза. Модель обеспечивает переход от реактивного к проактивному управлению рисками, встраивая безопасность в саму ткань бизнес-процессов.

Обсуждение (Discussion)

Представленная в работе Интегрированная Оптимизационно-Защитная Модель (ИОЗМ) является концептуальным шагом к созданию нового поколения систем управления логистикой, отвечающих вызовам цифровой экономики. В данном разделе мы обсудим значимость полученных результатов, их место в контексте существующих

исследований, а также практические аспекты и ограничения предложенного подхода.

4.1. Интерпретация результатов и теоретическая значимость

Ключевой результат работы – это теоретическое обоснование необходимости и возможности синергетического объединения двух традиционно разделенных областей: экономической оптимизации и информационной безопасности. Мы утверждаем, что в современных условиях понятие «оптимальный маршрут» или «эффективная цепь поставок» теряет смысл, если оно не включает в себя оценку рисков безопасности. Маршрут, математически оптимальный по критерию времени и затрат, но пролегающий через зону высокого риска кибератак, в действительности является экономически субоптимальным, поскольку математическое ожидание потерь может многократно превысить экономию от сокращения пути.

Теоретическая новизна ИОЗМ заключается в предложении механизма такой интеграции через **Интеграционное ядро**. Оно выступает в роли транслятора, переводящего данные из области безопасности (уровни угроз, аномалии) на язык экономики и математики (весовые коэффициенты, ограничения, штрафы в целевой функции). Это позволяет рассматривать безопасность не как накладные расходы или отдельную сервисную функцию, а как один из фундаментальных ресурсов, которым необходимо управлять наравне с финансами, временем и материальными активами.

4.2. Сопоставление с существующими подходами

Существующие научные работы и коммерческие системы управления логистикой, как правило, демонстрируют высокую степень проработки либо в области оптимизации, либо в области безопасности. Системы TMS (Transportation Management System) содержат мощные алгоритмы маршрутизации, но вопросы кибербезопасности в них обычно

сводятся к базовым мерам защиты самой платформы. С другой стороны, решения класса SIEM (Security Information and Event Management) способны агрегировать и анализировать события безопасности, но они не имеют инструментов для прямого влияния на логистические бизнес-процессы.

ИОЗМ предлагает мост между этими двумя мирами. В отличие от существующих подходов, наша модель позволяет системе управления транспортом динамически реагировать на изменение ландшафта угроз, а системе безопасности – фокусировать свои ресурсы на наиболее критичных с точки зрения логистики участках и объектах. Этот двунаправленный обмен информацией является принципиальным отличием и преимуществом предложенной архитектуры.

4.3. Практические импликации и перспективы внедрения

Внедрение ИОЗМ на предприятии способно принести значительные практические выгоды:

- **Повышение устойчивости бизнеса:** Снижение вероятности срыва поставок из-за киберинцидентов, хищения грузов или информации.
- **Снижение совокупных потерь:** Модель позволяет минимизировать не только прямые затраты (топливо, время), но и косвенные, связанные с рисками безопасности.
- **Повышение конкурентоспособности:** Возможность предлагать клиентам услуги повышенной надежности и безопасности, что особенно важно для перевозки ценных, опасных или чувствительных грузов.

Однако внедрение такой комплексной системы сопряжено с рядом вызовов. Во-первых, это требует значительных инвестиций в как в программное обеспечение, так и в аппаратные средства (сенсоры, анализаторы спектра). Во-вторых, для эксплуатации и развития ИОЗМ

необходимы междисциплинарные команды специалистов, включающие логистов, математиков-программистов и экспертов по кибербезопасности, что соответствует современным требованиям к компетенциям в условиях цифровой экономики [1]. В-третьих, потребуется разработка и стандартизация протоколов взаимодействия между различными технологическими системами (TMS, WMS, IoT-платформы, системы мониторинга).

4.4. Ограничения модели и направления будущих исследований

Следует признать, что представленная в данной статье модель носит концептуальный характер. Ее практическая реализация требует дальнейших глубоких исследований в нескольких направлениях:

1. **Разработка алгоритмического обеспечения:** Необходимо создать конкретные гибридные алгоритмы для Оптимизационной подсистемы, способные эффективно работать с динамически изменяющимися весовыми коэффициентами рисков.
2. **Применение машинного обучения:** Подсистему безопасности можно существенно усилить за счет внедрения моделей машинного обучения (ML) и искусственного интеллекта (AI) для предиктивного анализа угроз. Нейронные сети могут обучаться на исторических данных об инцидентах для выявления скрытых закономерностей и прогнозирования будущих атак.
3. **Количественная оценка эффективности:** Требуется разработка методики для количественной оценки экономического эффекта от внедрения ИОЗМ. Это можно сделать с помощью имитационного моделирования, сравнивая показатели работы стандартной логистической системы и системы под управлением ИОЗМ в различных сценариях кибератак.

4. **Исследование человеческого фактора:** Модель в текущем виде фокусируется на технологических аспектах. Важным направлением является интеграция в модель человеческого фактора, включая оценку психофизиологического состояния операторов и водителей как одного из элементов общей системы безопасности.

Несмотря на эти ограничения, мы уверены, что предложенный интегрированный подход задает верный вектор развития для интеллектуальных систем управления в логистике.

Заключение (Conclusion)

В настоящей статье было проведено комплексное исследование, направленное на решение одной из наиболее актуальных проблем современной логистики – разрыва между задачами повышения экономической эффективности и обеспечения информационной безопасности. Анализ показал, что по мере проникновения цифровых технологий в управление цепями поставок, эти две задачи становятся неразрывно связанными, и игнорирование одной из них неизбежно ведет к потерям в другой.

Основным вкладом данной работы является разработка концептуальной архитектуры **Интегрированной Оптимизационно-Защитной Модели (ИОЗМ)**. Предложенная модель формализует и структурирует взаимодействие между Оптимизационной подсистемой, основанной на математических методах решения транспортных задач, и Подсистемой безопасности, использующей инструментальные и статистические методы для проактивного мониторинга угроз. Центральным элементом модели выступает Интеграционное ядро, которое обеспечивает синергию двух подсистем, позволяя учитывать риски безопасности в качестве параметров оптимизации и, наоборот, корректировать логистические планы в ответ на возникающие угрозы в реальном времени.

На основе вышеизложенного мы можем обоснованно предположить, что такой интегрированный подход позволяет перейти от традиционного, реактивного управления инцидентами к проактивному управлению совокупными рисками, что является ключевым фактором для построения по-настоящему информационно защищенных, отказоустойчивых и эффективных логистических систем.

Дальнейшее развитие предложенных идей лежит в плоскости практической реализации и верификации модели. Это включает в себя разработку конкретных программных алгоритмов, в том числе с применением технологий искусственного интеллекта, а также проведение масштабного имитационного моделирования для количественной оценки преимуществ интегрированного подхода. Постоянное совершенствование методов и алгоритмов оптимизации и защиты в рамках единой концепции позволит логистическим компаниям не только успешно противостоять вызовам цифровой эпохи, но и использовать их для получения решающих конкурентных преимуществ.

Список использованных источников

1. Лукьяненко, Т. В. Ключевые компетенции цифровой экономики / Т. В. Лукьяненко // Цифровые технологии в аграрном образовании : Сборник статей по материалам учебно-методической конференции, Краснодар, 01 марта – 30 2022 года / Отв. за выпуск Д.С. Лилякова. – Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2022. – С. 144-145. – EDN XWIQDI.

2. Чубенко, Д. А. Методы и алгоритмы оптимизации грузоперевозок / Д. А. Чубенко, Т. В. Лукьяненко // Инновационное развитие техники и технологий в промышленности : Сборник материалов Всероссийской научной конференции молодых исследователей с международным участием, Москва, 16 апреля 2024 года. – Москва: Российский государственный университет им. А.Н. Косыгина (Технологии. Дизайн. Искусство), 2024. – С. 264-269. – EDN MSEZVW.

3. Мамлеев, Э. С. Особенности и проблемы использования современных IT-технологий в логистике и обработки информации с их помощью / Э. С. Мамлеев, Т. В. Лукьяненко // Информационное общество: современное состояние и перспективы развития : СБОРНИК МАТЕРИАЛОВ XVII МЕЖДУНАРОДНОГО ФОРУМА, Краснодар, 16–20 июня 2025 года. – Краснодар: ФГБОУ ВО «Кубанский государственный аграрный университет имени И. Т. Трубилина», 2025. – С. 18-20. – EDN WFCLST.

4. Хыбыртов, А. Р. Проблемы современных информационных технологий логистического управления и пути их решения / А. Р. Хыбыртов, Т. В. Лукьяненко // Информационное общество: современное состояние и перспективы развития : СБОРНИК МАТЕРИАЛОВ XVII МЕЖДУНАРОДНОГО ФОРУМА, Краснодар, 16–20 июня 2025 года. – Краснодар: ФГБОУ ВО «Кубанский государственный аграрный университет имени И. Т. Трубилина», 2025. – С. 51-53. – EDN EEDHMS.

5. Гартман, Д. С. Компьютерные системы связи и их анализ / Д. С. Гартман, В. В. Алашеев // Тенденции развития науки и образования. – 2024. – № 105-14. – С. 174-176. – DOI 10.18411/trnio-01-2024-735. – EDN OQZSEX.

6. Алашеев, В. В. Средства и способы защиты информационных ресурсов / В. В. Алашеев, Е. М. Хорольский // Актуальные аспекты развития гражданской авиации (Авиатранс-2024) : Материалы XIII международной научно-практической конференции, приуроченной к 55-летию со дня основания Ростовского филиала МГТУ ГА, Ростов-на-Дону, 21 июня 2024 года. – Ростов-на-Дону: Московский государственный технический университет гражданской авиации, 2024. – С. 256-264. – EDN HNUYQM.

7. Алашеев, В. В. Кибернетические воздействия на информационно-телекоммуникационные сети связи / В. В. Алашеев, Е. М. Хорольский // Актуальные аспекты развития гражданской авиации (Авиатранс-2025) : Материалы XIV Всероссийской научно-практической конференции, Ростов-на-Дону, 16–21 июня 2025 года. – Ростов-на-Дону: Московский государственный технический университет гражданской авиации, 2025. – С. 130-134. – EDN AODAMK.

8. Алашеев, В. В. К вопросу обнаружения несанкционированно установленных электронных устройств / В. В. Алашеев // Актуальные аспекты развития гражданской авиации (Авиатранс-2025) : Материалы XIV Всероссийской научно-практической конференции, Ростов-на-Дону, 16–21 июня 2025 года. – Ростов-на-Дону: Московский государственный технический университет гражданской авиации, 2025. – С. 232-237. – EDN USJRJT.

Spisok ispol`zovanny`x istochnikov

1. Luk`yanenko, T. V. Klyuchevy`e kompetencii cifrovoj e`konomiki / T. V. Luk`yanenko // Cifrovy`e texnologii v agrarnom obrazovanii : Sbornik statej po materialam uchebno-metodicheskoj konferencii, Krasnodar, 01 marta – 30 2022 goda / Otv. za vy`pusk D.S. Lilyakova. – Krasnodar: Kubanskij gosudarstvenny`j agrarny`j universitet imeni I.T. Trubilina, 2022. – S. 144-145. – EDN XWIQDI.

2. Chubenko, D. A. Metody` i algoritmy` optimizacii gruzoperevozok / D. A. Chubenko, T. V. Luk`yanenko // Innovacionnoe razvitie texniki i texnologij v promy`shlennosti : Sbornik materialov Vserossijskoj nauchnoj konferencii molody`x issledovatelej s mezhdunarodny`m uchastiem, Moskva, 16 aprelya 2024 goda. – Moskva: Rossijskij gosudarstvenny`j universitet im. A.N. Kosy`gina (Texnologii. Dizajn. Iskusstvo), 2024. – S. 264-269. – EDN MSEZVW.

3. Mamleev, E`. S. Osobennosti i problemy` ispol`zovaniya sovremenny`x IT-texnologij v logistike i obrabotki informacii s ix pomoshh`yu / E`. S. Mamleev, T. V. Luk`yanenko // Informacionnoe obshhestvo: sovremennoe sostoyanie i perspektivy` razvitiya : SBORNIK MATERIALOV XVII MEZhDUNARODNOGO FORUMA, Krasnodar, 16–20 iyunya 2025 goda. – Krasnodar: FGBOU VO «Kubanskij gosudarstvenny`j agrarny`j universitet imeni I. T. Trubilina», 2025. – S. 18-20. – EDN WFCLST.

4. Xy`by`rtov, A. R. Problemy` sovremenny`x informacionny`x texnologij logisticheskogo upravleniya i puti ix resheniya / A. R. Xy`by`rtov, T. V. Luk`yanenko // Informacionnoe obshhestvo: sovremennoe sostoyanie i perspektivy` razvitiya : SBORNIK

MATERIALOV XVII MEZhDUNARODNOGO FORUMA, Krasnodar, 16–20 iyunya 2025 goda. – Krasnodar: FGBOU VO «Kubanskij gosudarstvenny`j agrarny`j universitet imeni I. T. Trubilina», 2025. – S. 51-53. – EDN EEDHMS.

5. Gartman, D. S. Komp`yuterny`e sistemy` svyazi i ix analiz / D. S. Gartman, V. V. Alasheev // Tendencii razvitiya nauki i obrazovaniya. – 2024. – № 105-14. – S. 174-176. – DOI 10.18411/trnio-01-2024-735. – EDN OQZSEX.

6. Alasheev, V. V. Sredstva i sposoby` zashhity` informacionny`x resursov / V. V. Alasheev, E. M. Xorol`skij // Aktual`ny`e aspekty` razvitiya grazhdanskoj aviacii (Aviatrans-2024) : Materialy` XIII mezhdunarodnoj nauchno-prakticheskoj konferencii, priurochennoj k 55-letiyu so dnya osnovaniya Rostovskogo filiala MGTU GA, Rostov-na-Donu, 21 iyunya 2024 goda. – Rostov-na-Donu: Moskovskij gosudarstvenny`j texnicheskij universitet grazhdanskoj aviacii, 2024. – S. 256-264. – EDN HNUYQM.

7. Alasheev, V. V. Kiberneticheskie vozdejstviya na informacionno-telekommunikacionny`e seti svyazi / V. V. Alasheev, E. M. Xorol`skij // Aktual`ny`e aspekty` razvitiya grazhdanskoj aviacii (Aviatrans-2025) : Materialy` XIV Vserossijskoj nauchno-prakticheskoj konferencii, Rostov-na-Donu, 16–21 iyunya 2025 goda. – Rostov-na-Donu: Moskovskij gosudarstvenny`j texnicheskij universitet grazhdanskoj aviacii, 2025. – S. 130-134. – EDN AODAMK.

8. Alasheev, V. V. K voprosu obnaruzheniya nesankcionirovanno ustanovlenny`x e`lektronny`x ustrojstv / V. V. Alasheev // Aktual`ny`e aspekty` razvitiya grazhdanskoj aviacii (Aviatrans-2025) : Materialy` XIV Vserossijskoj nauchno-prakticheskoj konferencii, Rostov-na-Donu, 16–21 iyunya 2025 goda. – Rostov-na-Donu: Moskovskij gosudarstvenny`j texnicheskij universitet grazhdanskoj aviacii, 2025. – S. 232-237. – EDN USJRJT.