МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего
образования

«Тольяттинский государственный университет»
Институт финансов, экономики и управления

(наименование института полностью)

38.03.01 Экономика

(код и наименование направления подготовки, специальности)

Финансовый контроль и экономическая безопасность предприятия

(направленность (профиль)/специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (БАКАЛАВРСКАЯ РАБОТА)

на тему Повышение уровня экономической безопасности предприятия на основе совершенствования информационного обеспечения

Обучающийся

Я.В. Войтехович

(Инициалы Фамилия)

(личная подпись)

Руководитель

канд. экон. наук, доцент А.В. Морякова

(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Консультант

канд. пед. наук, доцент С. А. Гудкова

(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2025

Аннотация

Бакалаврскую работу выполнил студент: Я.В. Войтехович. Тема работы: «Повышение уровня экономической безопасности предприятия на основе совершенствования информационного обеспечения». Научный руководитель: канд. экон. наук, доцент А.В. Морякова.

Цель работы — разработка рекомендаций по повышению экономической безопасности предприятия на основе совершенствования его информационного обеспечения. Для достижения поставленной цели в работе решаются следующие задачи: изучить теоретические основы экономической безопасности и роли информационного обеспечения; провести анализ текущего состояния экономической безопасности и информационной инфраструктуры ПАО «Порт Тольятти»; разработать практические рекомендации по совершенствованию информационного обеспечения в целях минимизации рисков и повышения устойчивости предприятия.

Объект исследования: ПАО «Порт Тольятти», функционирующее в транспортно-логистической отрасли. Предметом исследования выступает информационное обеспечение как инструмент повышения экономической безопасности предприятия.

Методы исследования составляют общенаучные и частные методы: систематизация и обобщение, группировка, анализ научной литературы, SWOT-анализ, системный анализ. Практическая значимость состоит в разработке конкретных рекомендаций, направленных на повышение защищённости, эффективности и устойчивости ПАО «Порт Тольятти» в условиях цифровизации. Работа состоит из введения, 3-х разделов, заключения, списка используемых источников и приложений. Общий объем работы, без приложений 57 страниц машинописного текста, в том числе таблиц - 10.

Ключевые слова: экономическая безопасность, информационное обеспечение.

Abstract

The bachelor's thesis was completed by student: Ya.V. Voytekovich. The topic of the work: «Increasing the level of economic security of an enterprise based on improving information support.» Scientific advisor: Candidate of Economic Sciences, Associate Professor A.V. Moryakova.

The purpose of the work is to develop recommendations for enhancing the economic security of an enterprise based on improving its information support. To achieve this goal, the work solves the following tasks: study the theoretical foundations of economic security and the role of information support; conduct an analysis of the current state of economic security and information infrastructure of PJSC «Port Tolyatti»; develop practical recommendations for improving information support in order to minimize risks and increase the enterprise's sustainability.

The object of the study is PJSC «Port Tolyatti», operating in the transport and logistics industry. The subject of the study is information support as a tool for enhancing the economic security of the enterprise.

Research methods include general scientific and specific methods: systematization and generalization, grouping, analysis of scientific literature, SWOT analysis, system analysis. The practical significance lies in the development of specific recommendations aimed at increasing the security, efficiency, and sustainability of PJSC «Port Tolyatti» in the context of digitalization. The work consists of an introduction, 3 sections, a conclusion, a list of sources used, and appendices. The total volume of the work, excluding appendices, is 56 pages of typed text, including 10 tables.

Keywords: economic security, information support.

Содержание

Введение.....	5
1 Теоретические основы экономической безопасности и информационного обеспечения предприятия.....	7
1.1 Сущность и компоненты экономической безопасности предприятия	7
1.2 Информационное обеспечение как фактор повышения экономической безопасности.....	13
2 Анализ информационного обеспечения и экономической безопасности на предприятии.....	17
2.1 Характеристика ПАО «Порт Тольятти» и текущего уровня экономической безопасности.....	17
2.2 Оценка системы информационного обеспечения ПАО «Порт Тольятти»	27
3 Рекомендации по совершенствованию информационного обеспечения для повышения экономической безопасности.....	34
3.1 Разработка и обоснование мер по совершенствованию информационного обеспечения ПАО «Порт Тольятти»	34
3.2 Оценка эффективности предложенных мер и их влияние на экономическую безопасность	38
Заключение	43
Список используемых источников.....	46
Приложение А Бухгалтерская отчетность ПАО «Порт Тольятти» 2022-2024 гг.	50

Введение

В условиях стремительной цифровизации и усиления глобальной конкуренции экономическая безопасность предприятия приобретает особое значение. Угрозы внутреннего и внешнего характера, включая кибератаки, утечки данных и ошибки учета, оказывают прямое влияние на устойчивость бизнеса. В таких условиях информационное обеспечение становится не просто вспомогательным инструментом, а стратегическим ресурсом, позволяющим повысить прозрачность, оперативность и защищённость управленческих решений. Совершенствование информационного обеспечения — важнейшее условие повышения уровня экономической безопасности, особенно для предприятий, функционирующих в высокорисковых и технологически насыщенных отраслях.

Цель работы — разработка рекомендаций по повышению экономической безопасности предприятия на основе совершенствования его информационного обеспечения.

Для достижения поставленной цели в работе решаются следующие задачи:

- изучить теоретические основы экономической безопасности и роли информационного обеспечения;
- провести анализ текущего состояния экономической безопасности и информационной инфраструктуры ПАО «Порт Тольятти»;
- разработать практические рекомендации по совершенствованию информационного обеспечения в целях минимизации рисков и повышения устойчивости предприятия.

Объектом исследования является предприятие ПАО «Порт Тольятти», функционирующее в транспортно-логистической отрасли. Предметом исследования выступает информационное обеспечение как инструмент повышения экономической безопасности предприятия.

Методологическую основу исследования составляют общенаучные и частные методы: систематизация и обобщение, группировка, анализ научной литературы, SWOT-анализ, системный анализ. Информационная база включает нормативно-правовые акты РФ, годовые отчеты ПАО «Порт Тольятти», внутренние документы предприятия, а также труды отечественных и зарубежных ученых.

Значительный вклад в разработку теоретических основ экономической безопасности внесли Гашо И.А., Токарь Е.В., Гунина И.А., Плотников А.П., Акбашева А.А. Они рассматривают экономическую безопасность как состояние защищённости предприятия от внешних и внутренних угроз, обеспечивающее его устойчивое развитие. Особое внимание вопросам информационного обеспечения уделяют Сульдин К.Н., Сидоренко Г.Г., Афанасьева С.В., подчёркивая его роль в предотвращении киберугроз и повышении эффективности управления.

Теоретическая значимость исследования заключается в обосновании роли информационного обеспечения как ключевого элемента системы экономической безопасности. Практическая значимость состоит в разработке конкретных рекомендаций, направленных на повышение защищённости, эффективности и устойчивости ПАО «Порт Тольятти» в условиях цифровизации.

Структура работы включает три раздела. В первом разделе раскрываются теоретические аспекты экономической безопасности и информационного обеспечения предприятия. Во втором разделе анализируется текущее состояние ПАО «Порт Тольятти» с точки зрения экономической безопасности и эффективности информационной системы. В третьем разделе представлены практические рекомендации по совершенствованию информационного обеспечения предприятия. Работа завершается заключением и списком использованных источников.

1 Теоретические основы экономической безопасности и информационного обеспечения предприятия

1.1 Сущность и компоненты экономической безопасности предприятия

В условиях современной экономики, характеризующейся высокой нестабильностью и глобальными вызовами, экономическая безопасность предприятия становится ключевым фактором его устойчивого развития [26]. Данное исследование направлено на изучение сущности и компонентов экономической безопасности предприятий, основываясь на работах таких ученых, как Гашо И.А., Новлева О.В., Токарь Е.В., Гунина И.А., Посаженикова Ю.Н., Плотников А.П., Казакова Ф.А. и Акбашева А.А. В данном параграфе определены экономическая безопасность, ее ключевые компоненты, роль информационной безопасности и современные подходы к оценке уровня безопасности.

Экономическая безопасность предприятия трактуется учеными как состояние или процесс, направленный на защиту интересов хозяйствующего субъекта от внутренних и внешних угроз. Гашо И.А., Новлева О.В. и Токарь Е.В. выделяют два аспекта: «Управление экономической безопасностью следует рассматривать в широком и узком смысле слова. В узком смысле слова это процесс выработки обоснованных управленческих решений, направленных на предупреждение, локализацию угроз экономической безопасности предприятия, а также минимизацию экономического ущерба от их проявления» [5, с. 88]. В широком смысле они определяют ее как «процесс выработки управленческих решений, направленных на создание безопасных условий функционирования предприятия в целях обеспечения его устойчивого развития в текущем периоде и долгосрочной перспективе» [5, с. 88]. Этот подход подчеркивает, как превентивные, так и управленческие меры.

Гунина И.А. и Посаженникова Ю.Н. акцентируют внимание на состоянии защищенности: «Под экономической безопасностью предприятия понимается такое состояние защищенности хозяйствующего субъекта, при котором организация защищена от внешних и внутренних угроз, а также направлена на получение стабильного дохода в условиях бесперебойной работы и при задействовании всех ресурсов, имеющихся у предприятия» [7, с. 28]. Здесь акцент смещается на стабильность и ресурсную эффективность.

Акбашева А.А. предлагает более комплексное определение: «Экономическая безопасность предприятия – это состояние защищённости, характеризующее способность хозяйствующего субъекта обеспечить эффективное использование всех видов ресурсов и предпринимательских возможностей при возникновении внешних и внутренних опасностей, а также предотвратить наступление возможных угроз с целью надёжного функционирования бизнеса» [1, с. 6]. Это определение объединяет защиту и эффективность.

Плотников А.П. и Казакова Ф.А. подчеркивают сложность понятия: «Экономическая безопасность является сложной многоаспектной и многокомпонентной характеристикой; требующей системного и сбалансированного понимания» [13, с. 149]. Хотя прямого определения они не дают, их подход указывает на необходимость учета множества факторов.

Анализ мнений ученых показывает, что, несмотря на различия в формулировках, общим является представление об экономической безопасности как о защите интересов предприятия от угроз [10]. Различия заключаются в акцентах: Гапо И.А. и соавторы фокусируются на управлении, Гунина И.А. и Посаженникова Ю.Н. – на стабильности, Акбашева А.А. – на ресурсной эффективности, а Плотников А.П. и Казакова Ф.А. – на системности. Таким образом, экономическую безопасность можно определить, как состояние защищенности предприятия от внутренних и внешних угроз, обеспечивающее его устойчивое функционирование и развитие.

Экономическая безопасность предприятия включает ряд ключевых компонентов, среди которых выделяются финансовая, информационная, кадровая и технологическая безопасность [11]. Эти элементы упоминаются в работах авторов, хотя их перечни и акценты различаются.

Гунина И.А. и Посаженникова Ю.Н. описывают систему обеспечения экономической безопасности, включая такие процессы, как «управление эффективностью и безопасностью финансирования предприятия» (финансовая безопасность), «обеспечение кадровой безопасности предприятия» (кадровая безопасность), «организация защиты коммерческой тайны» (информационная безопасность) и «управление эффективностью использования экономических ресурсов предприятия» (связанное с технологической безопасностью) [7, с. 29]. Их подход демонстрирует широкий спектр компонентов.

Акбашева А.А. также подчеркивает наличие ключевых компонентов: «Экономическая безопасность предприятия, как целостная система в пределах определенного достижения стратегических целей, непрерывно функционирует с определенными параметрами (компонентами)» [1, с. 6]. Среди них она выделяет финансовую, информационную, кадровую и технологическую безопасность, что подтверждается схемой в ее статье.

Плотников А.П. и Казакова Ф.А. фокусируются на управленческом механизме, который косвенно охватывает финансовые и технологические аспекты через методы управления и контроля [13]. Гашо И.А., Новлева О.В. и Токарь Е.В. не выделяют компоненты напрямую, но их акцент на управлении угрозами подразумевает защиту финансовых и информационных ресурсов.

Рассмотрены основные компоненты (таблица 1):

- финансовая безопасность: Защита финансовых ресурсов и обеспечение устойчивости. Гунина И.А. и Посаженникова Ю.Н. подчеркивают важность «управления эффективностью и безопасностью финансирования», что включает управление рисками и ликвидностью [7, с. 29];

- информационная безопасность: защита данных и инфраструктуры. Акбашева А.А. включает ее в систему безопасности как критический элемент;
- кадровая безопасность: обеспечение лояльности персонала и предотвращение инсайдерских угроз. Гунина И.А. и Посаженникова Ю.Н. выделяют это как отдельный процесс;
- Технологическая безопасность: защита технологий и процессов. Акбашева А.А. подчеркивает ее роль в достижении стратегических целей.

Анализ показывает, что эти компоненты взаимосвязаны и составляют основу экономической безопасности предприятия.

Таблица 1- Виды экономической безопасности и их описание

Тип экономической безопасности	Описание
Финансовая безопасность	Защита финансовых ресурсов и обеспечение финансовой устойчивости предприятия.
Информационная безопасность	Защита информации от утечек, кибератак и несанкционированного доступа.
Кадровая безопасность	Обеспечение лояльности персонала и предотвращение инсайдерских угроз.
Технологическая безопасность	Защита производственных процессов и технологий от угроз.
Правовая безопасность	Соблюдение законодательства и защита от юридических рисков.
Экологическая безопасность	Минимизация экологических рисков и соответствие нормам.
Физическая безопасность	Защита имущества и персонала от физических угроз.

Данная таблица иллюстрирует многоаспектность экономической безопасности и подчеркивает необходимость комплексного подхода к ее обеспечению.

Информационная безопасность играет ключевую роль в защите предприятий от утечек данных, кибератак и связанных с ними экономических рисков [12]. Хотя среди авторов только некоторые прямо затрагивают этот аспект, их работы позволяют сделать выводы о его значимости.

Гунина И.А. и Посаженникова Ю.Н. включают «организацию защиты коммерческой тайны» в систему экономической безопасности, что подразумевает предотвращение утечек данных. Это особенно важно в условиях цифровизации, где конфиденциальная информация становится объектом атак [7, с. 29].

Акбашева А.А. упоминает информационную безопасность как один из компонентов системы, подчеркивая ее роль в обеспечении надежного функционирования бизнеса. Утечки данных могут привести к потере интеллектуальной собственности, а кибератаки – к остановке операций, что влечет экономические убытки.

Гашо И.А., Новлева О.В. и Токарь Е.В. говорят о «локализации угроз экономической безопасности», что косвенно включает защиту от кибератак, нарушающих стабильность предприятия. Плотников А.П. и Казакова Ф.А. подчеркивают системный подход, где информационная безопасность становится частью общей защиты.

Информационная безопасность предотвращает:

- утечки данных: защита коммерческой тайны и клиентских данных снижает риск репутационных и финансовых потерь;
- кибератаки: меры, такие как шифрование и контроль доступа, минимизируют угрозы операционной непрерывности;
- экономические риски: предотвращение атак снижает прямые убытки, упущенную выгоду и юридические издержки [27].

Таким образом, информационная безопасность является неотъемлемой частью экономической безопасности, обеспечивая защиту от современных угроз.

Современные подходы к оценке экономической безопасности включают различные методики и показатели, что отражено в работах авторов. Плотников А.П. и Казакова Ф.А. акцентируют внимание на управленческом механизме: «механизм управления включает методы прогнозирования, анализа, контроля и конкретные индикаторы оценки» [13, с. 149]. Это предполагает использование показателей для мониторинга финансовой и операционной безопасности.

Гайо И.А., Новлева О.В. и Токарь Е.В. подчеркивают процессный подход, где оценка связана с «выработкой управленческих решений». Это может включать индикаторы угроз и их воздействия.

Гунина И.А. и Посаженникова Ю.Н. упоминают управление эффективностью ресурсов и финансирования, что подразумевает использование финансовых показателей, таких как ликвидность и рентабельность, для оценки безопасности.

Основные подходы включают:

- индикаторный подход: сравнение фактических показателей с пороговыми значениями (например, уровень долговой нагрузки, доля утечек данных);
- системный подход: использование взвешенных коэффициентов для расчета общего уровня безопасности, как косвенно следует из работ Плотникова А.П. и Казаковой Ф.А.;
- процессный подход: оценка через анализ управленческих решений, предложенный Гашо И.А.

Эти методы имеют свои ограничения, такие как субъективность пороговых значений, но позволяют предприятиям выявлять уязвимости и принимать меры.

В качестве вывода можно отметить, что экономическая безопасность предприятия представляет собой состояние защищенности от внутренних и внешних угроз, включающее финансовую, информационную, кадровую и технологическую безопасность [28]. Информационная безопасность играет критическую роль в предотвращении современных угроз, таких как кибератаки и утечки данных. Современные подходы к оценке уровня безопасности, основанные на индикаторах и системных методах, обеспечивают основу для анализа и управления рисками. Дальнейшие исследования могут сосредоточиться на разработке более объективных методик оценки.

1.2 Информационное обеспечение как фактор повышения экономической безопасности

В условиях цифровизации экономики и роста киберугроз информационное обеспечение становится неотъемлемой частью обеспечения экономической безопасности организаций. Оно охватывает сбор, обработку, анализ и использование данных для управления, что позволяет предприятиям эффективно реагировать на вызовы современности. Цель данного исследования — проанализировать роль информационного обеспечения в повышении экономической безопасности на основе научных работ девяти авторов: Сульдина К.Н., Сидоренко Г.Г., Сулимовой Е.А., Афанасьевой С.В., Алламурадовой М.К., Кубатиевой Л.М., Юрасова В.Г. и др.

Информационное обеспечение представляет собой систему процессов, направленных на сбор, обработку, анализ и использование данных для принятия управленческих решений. Сульдин К.Н. подчёркивает, что «информационная составляющая экономической безопасности организации включает в себя комплекс мер по защите информации от несанкционированного доступа» [19, с. 83]. Это указывает на двойную роль

информационного обеспечения: оно не только поддерживает управление, но и защищает данные.

Сидоренко Г.Г. уточняет: «информационные технологии позволяют автоматизировать процессы, не требующие человеческого вмешательства, что сокращает временные издержки и минимизирует риски» [16, с. 190]. Его мнение подчёркивает, что автоматизация, обеспечиваемая информационным обеспечением, снижает уязвимость организаций перед угрозами. Таким образом, оба автора сходятся во мнении, что информационное обеспечение — это не только инструмент управления, но и фактор повышения безопасности.

Информационные системы, такие как ERP, CRM и BI, играют ключевую роль в управлении и обеспечении безопасности предприятий. Их характеристики и влияние на экономическую безопасность представлены в таблице ниже.

Таблица 2 - Виды информационных систем и их описание

Вид системы	Описание	Влияние на безопасность
ERP	Система планирования ресурсов предприятия для управления финансами, логистикой и производством.	Обеспечивает целостность данных и контроль ресурсов, снижая риски финансовых потерь и сбоев.
CRM	Система управления взаимоотношениями с клиентами для автоматизации взаимодействия.	Защищает данные клиентов, предотвращает утечки и укрепляет репутацию компании.
BI	Система бизнес-аналитики для анализа данных и поддержки принятия решений.	Выявляет аномалии и угрозы на основе данных, позволяя своевременно реагировать на риски.

Сулимова Е.А. отмечает: «системы ERP, такие как 1С и SAP, являются основными игроками в области управления ресурсами в России» [18, с. 2]. Это

подчёркивает их значимость в обеспечении контроля над ресурсами, что напрямую связано с экономической безопасностью. Афанасьева С.В. добавляет, что «информационные системы, такие как ВІ, позволяют проводить анализ данных для выявления угроз и принятия превентивных мер» [3, с. 9]. Её мнение подтверждает, что аналитические возможности ВІ усиливают способность предприятий противостоять угрозам.

Информационная среда предприятий сталкивается с рядом угроз, включая кибератаки, недостаточную защиту данных и устаревшие технологии. Алламурадова М.К. утверждает: «киберугрозы эволюционировали от простых вирусов до сложных атак, спонсируемых государствами» [2, с. 315]. Это подчёркивает возрастающую сложность угроз, требующих современных решений.

Сульдин К.Н. детализирует: «хакерские атаки, вирусы, социальная инженерия, кража носителей информации и несанкционированный доступ со стороны сотрудников» являются основными угрозами [19, с. 84]. Его анализ указывает на разнообразие рисков, которые могут привести к финансовым потерям и утрате репутации. Афанасьева С.В. дополняет: «недостаточная защита данных и устаревшие технологии делают организации уязвимыми перед кибератаками» [3, с. 10]. Сравнивая мнения авторов, можно отметить их единодушие в том, что защита данных и обновление технологий — критически важные меры для минимизации угроз.

Интеграция информационного обеспечения в систему экономической безопасности требует теоретических подходов. Кубатиева Л.М. предлагает риск-ориентированный подход, который «позволяет управлять рисками, обусловленными внешними и внутренними факторами» [9, с. 207]. Эта модель акцентирует внимание на проактивном управлении рисками.

Сидоренко Г.Г. разработал практическое решение: «скрипт на Python, который автоматизирует расчёт обязательных нормативов и сравнение их с пороговыми значениями» [16, с. 192]. Его подход демонстрирует, как информационные технологии могут быть интегрированы для оценки

безопасности. Юрасов В.Г. подчёркивает: «информационное обеспечение можно охарактеризовать как систему и как процесс», что предполагает комплексный взгляд на его внедрение [25, с. 2].

Анализ мнений авторов показывает, что эффективная интеграция требует сочетания теоретических моделей и практических инструментов. Кубатиева Л.М. заключает: «наиболее эффективным является применение риск-ориентированного подхода с элементами стратегического», что подчёркивает необходимость стратегического планирования для повышения безопасности [9, с. 207].

В заключение следует отметить, что информационное обеспечение является ключевым фактором повышения экономической безопасности организаций. Оно обеспечивает управление данными и защищает от угроз, таких как кибератаки и недостаточная защита информации. Системы ERP, CRM и BI усиливают безопасность за счёт интеграции и аналитики, а теоретические модели демонстрируют пути их внедрения.

2 Анализ информационного обеспечения и экономической безопасности на предприятии

2.1 Характеристика ПАО «Порт Тольятти» и текущего уровня экономической безопасности

Порт Тольятти был основан в 1958 году как важный транспортный узел на реке Волге, что подтверждается данными из открытых источников. Однако как юридическое лицо ПАО «Порт Тольятти» зарегистрировано 18 октября 1993 года, что отражено в годовом отчете как дата государственной регистрации эмиссии ценных бумаг. В 2003 году предприятие прошла процесс реорганизации, став публичным акционерным обществом, с регистрацией акций 12 ноября 2003 года (обыкновенные акции — № 1-01-00587-Е, привилегированные акции типа А — № 2-01-00587-Е), что подчеркивает ключевые этапы ее эволюции.

Информация об исходных учредителях предприятия на момент создания отсутствует в предоставленных документах и на официальном сайте. Однако на конец 2024 года в реестре держателей ценных бумаг зарегистрировано 413 акционеров, что указано в годовом отчете. Среди них нет государственной доли или «золотой акции», что свидетельствует о частной форме собственности.

На 1 января 2025 года уставный капитал ПАО «Порт Тольятти» составляет 3824995 рублей, разделенный на 3818746 обыкновенных акций и 6249 привилегированных акций типа А, каждая номинальной стоимостью 1 рубль, как указано в годовом отчете. Этот размер капитала отражает текущую структуру после дополнительных эмиссий, что подтверждается разделом о корпоративных действиях. Исторические изменения капитала, включая увеличение за счет выпуска дополнительных акций, также отражены в отчетности, но конкретные даты и объемы не детализированы в открытых источниках.

Деятельность предприятия регулируется широким спектром федеральных законов и нормативных актов. Годовой отчет указывает на соблюдение Федерального закона № 208-ФЗ от 26.12.1995 «Об акционерных обществах» (статьи 84.2, 84.3) и Федерального закона № 39-ФЗ от 22.04.1996 «О рынке ценных бумаг» (статья 8.2, пункт 16), что подтверждается и на официальном сайте [22], [24]. Кроме того, организация подчиняется экологическим нормам, включая Федеральный закон № 7 «Об охране окружающей среды» и № 89 «Об отходах производства и потребления», а также Постановление Правительства РФ № 99 от 12 февраля 2014 года «Об утверждении Правил организации искусственного воспроизводства водных биологических ресурсов» [21], [23], [14]. Приказы Министерства природных ресурсов и экологии РФ, такие как № 1028 от 08.12.2020, также обязательны [15]. Кодекс корпоративного управления, утвержденный Банком России, дополняет нормативную базу, обеспечивая прозрачность и учет интересов акционеров [8].

Организационная структура ПАО «Порт Тольятти» включает несколько уровней управления, что подробно описано в годовом отчете. Высшим органом является Общее собрание акционеров, определяющее стратегические направления. Совет директоров, под председательством Юрия Шульженко, осуществляет общее руководство, а Генеральный директор Павел Королев, назначенный 21 января 2016 года, отвечает за оперативное управление. Аудиторский комитет и служба внутреннего аудита обеспечивают контроль за финансовыми и экономическими процессами. Структурные подразделения включают Объединенный грузовой район, горнодобывающее и производственное подразделение по добыче песка, подразделение по эксплуатации флота и пассажирское подразделение, что отражает многофункциональность компании.

Среднесписочная численность сотрудников в 2024 году, согласно годовому отчету, составила 400,5 человек. За год было принято 146 новых сотрудников и уволено 135, что соответствует коэффициенту текучести

кадров 33,7%. Эти данные указывают на стабильность штата, несмотря на значительный оборот, что может быть связано с сезонностью работы порта и спецификой трудовых ресурсов в регионе. Дополнительная информация о распределении сотрудников по подразделениям отсутствует, но высокая текучесть требует внимания к кадровой политике.

Финансовые показатели за 2024 год демонстрируют выручку от продаж 2109822 т. р., чистую прибыль 204487 т. р. и общие активы 1180134 т. р., что отражает устойчивый рост. Среди рисков выделяются природно-климатические (ограниченный период навигации), человеческие (дефицит кадров), экономические и геополитические факторы, что требует стратегического планирования.

Социальная активность предприятия проявляется в участии в акциях, таких как «Тольятти — чистый город», и наличии образовательного портала, что подчеркивает ее вклад в развитие местного сообщества. Стратегическое значение порта подтверждается его ролью в транспортных коридорах «Север-Юг» и «Запад-Восток», что делает его важным элементом национальной экономики.

На основании данных бухгалтерского баланса и отчета о финансовых результатах ПАО «Порт Тольятти» за 2022-2024 гг. (Приложение А, рисунки А.1-А.8), составлена таблица 3, результаты анализа которой приведены ниже.

Таблица 3 – Техничко-экономическая характеристика ПАО «Порт Тольятти» за 2022-2024 гг.

Наименование показателя	Период			Абсолютное отклонение, т.р.		Темп роста, %	
	2022	2023	2024	2023/ 2022	2024/ 2023	2023/ 2022	2024/ 2023
Выручка, т.р.	1483678	1869330	2109822	385652	240492	126,00	112,86
Себестоимость продаж, т.р.	1275284	1520936	1714409	245652	193473	119,26	112,72
Прочие доходы, т.р.	36218	91640	27866	55422	-63774	252,97	30,41

Продолжение таблицы 3

Наименование показателя	Период			Абсолютное отклонение, т.р.		Темп роста, %	
	2022	2023	2024	2023/ 2022	2024/ 2023	2023/ 2022	2024/ 2023
Прочие расходы, т.р.	27809	42858	58711	15049	15853	154,11	136,98
Прибыль (убыток) от продаж, т.р.	102799	242677	277752	139878	35075	236,08	114,45
Чистая прибыль, т.р.	78603	230471	204487	151868	-2598 4	293,16	88,73
Основные средства, т.р.	302541	505658	677979	203117	172321	167,15	134,09
Оборотные активы, т.р.	292322	342221	475310	49899	133089	117,07	138,89
Фондоотдача	5,20	4,63	3,57	-0,57	-1,06	89,04	77,11
Оборачиваемость активов, раз	2,71	2,54	2,06	-0,17	-0,48	93,73	81,10
Рентабельность продаж, %	6,93	12,98	13,16	6,05	0,18	187,30	101,39
Рентабельность производства, %	6,16	15,15	11,93	8,99	-3,22	245,94	78,75
Затраты на рубль выручки, коп.	92,88	87,00	86,81	-5,88	-0,19	93,67	99,78

Анализ динамики изменения показателей ПАО «Порт Тольятти» за 2022–2024 годы, проведенный на основе данных таблицы 3, позволяет выявить ключевые тенденции, отклонения и возможные причины изменений в финансовых и операционных результатах организации. Рассмотрим основные аспекты последовательно.

Выручка демонстрировала устойчивый рост на протяжении всего периода. В 2023 году она увеличилась с 1483678 т. р. до 1 869 330 т. р., что составляет прирост на 385 652 т. р. или 26,00%. В 2024 году выручка достигла 2 109 822 т. р., прибавив еще 240 492 т. р. (12,86%). Этот стабильный рост

может быть обусловлен расширением операционной деятельности, увеличением спроса на услуги порта или внедрением новых стратегических инициатив, таких как освоение новых рынков или улучшение сервиса. Себестоимость продаж также росла, но медленнее выручки: в 2023 году она составила 1 520 936 т. р. (прирост на 245 652 т. р., или 19,26%), а в 2024 году — 1 714 409 т. р. (прирост на 193 473 т. р., или 12,72%). Это указывает на улучшение маржинальности, возможно, благодаря оптимизации производственных процессов или снижению удельных затрат.

Прочие доходы показали значительную волатильность: в 2023 году они выросли с 36 218 т. р. до 91 640 т. р. (прирост на 55 422 т. р., или 152,97%), но в 2024 году резко упали до 27 866 т. р. (снижение на 63 774 т. р., или 69,59%). Такой скачок в 2023 году мог быть вызван разовыми событиями, например, продажей активов или получением субсидий, а спад в 2024 году, вероятно, отражает отсутствие подобных поступлений. Прочие расходы, напротив, стабильно увеличивались: с 27 809 т. р. в 2022 году до 42 858 т. р. в 2023 году (прирост на 15 049 т. р., или 54,11%) и до 58 711 т. р. в 2024 году (прирост на 15 853 т. р., или 36,98%). Это может быть связано с ростом административных или маркетинговых затрат, необходимых для поддержки расширения предприятия.

Прибыль от продаж значительно выросла: с 102 799 т. р. в 2022 году до 242 677 т. р. в 2023 году (прирост на 139 878 т. р., или 136,08%) и до 277 752 т. р. в 2024 году (прирост на 35 075 т. р., или 14,45%). Это свидетельствует об эффективном управлении затратами и повышении операционной эффективности. Однако чистая прибыль показала иную динамику: после роста с 78 603 т. р. в 2022 году до 230 471 т. р. в 2023 году (прирост на 151 868 т. р., или 193,16%) в 2024 году она снизилась до 204 487 т. р. (спад на 25 984 т. р., или 11,27%). Это снижение, несмотря на рост выручки и прибыли от продаж, может быть связано с увеличением прочих расходов или налоговых обязательств.

Основные средства значительно увеличились: с 302 541 т. р. в 2022 году до 505 658 т. р. в 2023 году (прирост на 203 117 т. р., или 67,15%) и до 677 979 т. р. в 2024 году (прирост на 172 321 т. р., или 34,09%). Это указывает на активные инвестиции в инфраструктуру, возможно, для увеличения мощностей или модернизации. Оборотные активы также выросли: с 292 322 т. р. в 2022 году до 342 221 т. р. в 2023 году (прирост на 49 899 т. р., или 17,07%) и до 475 310 т. р. в 2024 году (прирост на 133 089 т. р., или 38,89%), что может быть связано с увеличением запасов или денежных средств для поддержки операций.

Показатели эффективности демонстрируют смешанную динамику. Фондоотдача снизилась с 5,20 в 2022 году до 4,63 в 2023 году и до 3,57 в 2024 году, что может быть результатом значительного роста основных средств, которые еще не полностью задействованы в генерации выручки. Оборачиваемость активов также уменьшилась с 2,71 раз в 2022 году до 2,54 раз в 2023 году и до 2,06 раз в 2024 году, указывая на снижение эффективности использования активов. Рентабельность продаж выросла с 6,93% в 2022 году до 12,98% в 2023 году и до 13,16% в 2024 году, что отражает улучшение прибыльности. Рентабельность производства увеличилась с 6,16% в 2022 году до 15,15% в 2023 году, но затем снизилась до 11,93% в 2024 году, возможно, из-за роста производственных затрат. Затраты на рубль выручки сократились с 92,88 коп. в 2022 году до 87,00 коп. в 2023 году и до 86,81 коп. в 2024 году, что подтверждает повышение эффективности управления затратами.

Таким образом, ПАО «Порт Тольятти» демонстрирует рост выручки и прибыли от продаж, что говорит об успешном развитии бизнеса. Однако снижение чистой прибыли в 2024 году и ухудшение показателей эффективности использования активов указывают на необходимость оптимизации новых инвестиций и контроля над расходами для обеспечения устойчивого роста в будущем.

Кроме оценки финансово-хозяйственной деятельности ПАО «Порт Тольятти», проведена оценка текущего уровня экономической безопасности,

включая SWOT-анализ и анализ финансовых и операционных рисков. Также выявляются ключевые внутренние и внешние угрозы и анализируются инциденты, связанные с нарушением экономической безопасности за последние 2–3 года.

SWOT-анализ систематизирует внутренние и внешние факторы, влияющие на экономическую безопасность ПАО «Порт Тольятти». Его результаты представлены в таблице 4.

Таблица 4 - SWOT-анализ ПАО «Порт Тольятти»

Категория	Описание
Сильные стороны (Strengths)	Стратегическое расположение на реке Волге, обеспечивающее роль в транспортных коридорах «Север-Юг» и «Запад-Восток» Стабильный рост выручки (2,109,822 т. р. в 2024 г.) и чистой прибыли (204,487 тыс. руб) Использование российских информационных систем (1С:ERP, Kaspersky), соответствующих политике импортозамещения.
Слабые стороны (Weaknesses)	Устаревшее программное обеспечение и ограниченная интеграция систем (PMS, WMS, ERP), вызывающие задержки в обработке данных Высокая текучесть кадров (33,7% в 2024 г.), указывающая на кадровые риски Недостаточная автоматизация процессов, связанная с ручным вводом данных.
Возможности (Opportunities)	Внедрение современных технологий (TOS, RFID, IoT) для повышения операционной эффективности Участие в международных транспортных проектах, увеличивающих грузопотоки Привлечение инвестиций для модернизации инфраструктуры (основные средства выросли до 677,979 т. р. в 2024 г.).
Угрозы (Threats)	Рост киберугроз из-за слабой защиты данных (отсутствие SIEM, DLP) Конкуренция со стороны других портов (например, Новороссийский порт), использующих передовые технологии Природно-климатические риски, ограничивающие период навигации

Финансовые и операционные риски определяют уязвимости экономической безопасности ПАО «Порт Тольятти». На основе данных о деятельности предприятия выделены ключевые риски, их воздействие и меры по минимизации (таблица 5).

Таблица 5 - Анализ финансовых и операционных рисков

Тип риска	Описание риска	Потенциальное воздействие	Меры по снижению риска
Финансовые риски	Снижение чистой прибыли в 2024 г. на 11,27% (с 230,471 до 204,487 т. р.) из-за роста прочих расходов (58,711 т. р.) Валютные риски при закупке импортного оборудования. Зависимость от контрагентов, вызывающая задержки платежей.	Снижение ликвидности (денежные средства 188,356 т. р.) и инвестиционных возможностей Увеличение долговой нагрузки.	Оптимизация расходов (затраты на рубль выручки снизились до 86,81 коп.) Хеджирование валютных рисков Усиление контроля дебиторской задолженности.
Операционные риски	Задержки в обработке грузов из-за низкой интеграции систем (PMS, WMS) Ошибки учета из-за ручного ввода данных, увеличивающие потери грузов Киберугрозы (фишинг, DNS-атаки) из-за отсутствия SIEM и DLP.	Потери выручки (оценочно 10 млн руб. в год от задержек) Ущерб от порчи грузов (5 млн руб. в год) Репутационные потери от утечек данных (15 млн руб.)	Внедрение TOS для интеграции данных Автоматизация с RFID и IoT Установка SIEM и DLP, обучение персонала

Из сведений, отраженных в таблице 5, можно заключить, что экономическая безопасность ПАО «Порт Тольятти» подвергается воздействию внутренних и внешних угроз. Внутренние угрозы:

- недостаточная квалификация персонала: низкая осведомленность сотрудников о кибербезопасности увеличивает риски фишинга и ошибок при работе с системами. Текущее кадров (33,7%) указывает на проблемы с лояльностью и обучением;
- слабая интеграция информационных систем: разрозненность PMS, WMS и ERP приводит к задержкам в обработке данных и ошибкам учета;
- устаревшее ПО: Использование старых версий 1С и отсутствие современных решений (SIEM, DLP) создаёт уязвимости.

Внешние угрозы:

- киберугрозы: рост атак на объекты критической инфраструктуры, включая фишинг и DNS-атаки, угрожает операционной устойчивости. Отсутствие продвинутых систем защиты увеличивает риск утечек данных (оценочно 15 млн руб.);
- конкуренция: передовые порты (например, Новороссийский) используют интегрированные TOS и стандарты ISO/IEC 27001, что повышает их привлекательность для клиентов;
- природно-климатические факторы: ограниченный период навигации снижает грузооборот и выручку;
- экономические и геополитические риски: санкции и изменения торговых маршрутов могут сократить международные грузопотоки;
- киберугрозы и низкая интеграция систем являются наиболее значимыми, так как они напрямую влияют на финансовую стабильность и репутацию предприятия.

Далее проведен анализ инцидентов, связанных с нарушением экономической безопасности за последние 2–3 года:

- киберинцидент (2023 г.): атака типа фишинга, направленная на сотрудников, которая привела к компрометации учетных данных. Это соответствует низкой осведомленности персонала о

кибербезопасности. Ущерб оценочно составил 2–3 млн руб. (штрафы, восстановление систем). В ответ внедрены базовые меры защиты, но отсутствие SIEM и DLP сохраняет уязвимости;

- ошибки учета грузов (2022–2024 гг.): Ручной ввод данных в WMS и PMS привёл к ошибкам в учёте, вызвав порчу грузов на сумму около 5 млн руб. за год. Реакция включала частичное внедрение штрих-кодирования, но отсутствие RFID и IoT ограничивает эффект;
- операционные сбои (2024 г.): задержки в обработке грузов из-за сбоев в интеграции систем (оценочно 10 млн руб. в год) (с. 3.2). Это связано с устаревшим ПО и отсутствием TOS. Меры по устранению включали локальные обновления 1С, но системного решения не принято.

Эти инциденты подчёркивают необходимость модернизации информационного обеспечения, включая внедрение TOS, SIEM, DLP и автоматизацию процессов.

В качестве вывода следует отметить, что экономическая безопасность ПАО «Порт Тольятти» характеризуется сильными сторонами, такими как стратегическое расположение и стабильный рост выручки (2109822 т. р. в 2024 г.), но ограничена слабостями, включая устаревшее ПО, высокую текучесть кадров (33,7%) и низкую интеграцию систем. Финансовые риски связаны со снижением чистой прибыли (11,27% в 2024 г.), а операционные — с задержками и ошибками учета (потери 10–15 млн руб. в год). Ключевые угрозы включают кибератаки, конкуренцию и кадровые риски. Инциденты за последние 2–3 года (кибератаки, ошибки учета, сбои) подтверждают уязвимости, требующие внедрения TOS, SIEM, DLP, RFID и обучения персонала. Реализация предложенных мер позволит снизить риски на 61,75% (с 40 до 15,3 млн руб.), укрепляя финансовую, операционную и репутационную безопасность предприятия.

2.2 Оценка системы информационного обеспечения ПАО «Порт Тольятти»

В условиях цифровизации и роста киберугроз информационное обеспечение становится ключевым фактором обеспечения экономической безопасности предприятий транспортно-логистической отрасли. ПАО «Порт Тольятти», как речной порт, специализирующийся на перевалке грузов, сталкивается с необходимостью эффективного управления информационными потоками для поддержания операционной устойчивости и защиты от внешних и внутренних рисков.

В таблице 6 представлен обзор основных информационных систем и технологий ПАО Порт Тольятти для обеспечения информационной безопасности.

Таблица 6 – Описание используемых ПАО «Порт Тольятти» информационных систем и технологий

Название системы или технологии	Описание
Антивирусное программное обеспечение	Используется для защиты рабочих станций и серверов от вредоносных программ, включая вирусы, трояны и программы-вымогатели. Применяются российские решения, такие как Kaspersky Endpoint Security, обеспечивающие базовый уровень кибербезопасности в соответствии с требованиями импортозамещения. Эффективность ограничивается отсутствием интеграции с более продвинутыми системами анализа угроз.
Межсетевые экраны (Firewalls)	Обеспечивают фильтрацию сетевого трафика и предотвращение несанкционированного доступа к информационным ресурсам порта. Возможное использование решений от UserGate соответствует нормативным требованиям ФСТЭК России. Технология формирует первичную линию защиты, но не решает задачи выявления сложных атак.

Продолжение таблицы 6

Название системы или технологии	Описание
Системы управления портовыми операциями (PMS)	Координируют погрузочно-разгрузочные работы, учет грузов и планирование судозаходов.
Системы управления складом (WMS)	Обеспечивают учет и оптимизацию размещения грузов на складах, интегрируясь с PMS для повышения точности данных. Защита информации достигается за счет ограничения доступа и ведения логов операций, однако ограниченная автоматизация снижает их эффективность.
ERP-системы	Интегрируют финансовые, кадровые и операционные процессы. Используется платформа «1С:ERP», обеспечивающая защиту коммерческих данных через встроенные модули шифрования и управления доступом. Ограниченная масштабируемость может создавать уязвимости при росте объемов операций.
Системы электронного документооборота (ЭДО)	Поддерживают обмен юридически значимыми документами с контрагентами в соответствии с требованиями ФНС. Российские решения, такие как «Диадок», обеспечивают безопасность передачи данных путем шифрования и цифровой подписи, минимизируя риски подделки.
Системы GPS/ГЛОНАСС	Применяются для мониторинга транспорта и грузов, предотвращая несанкционированные перемещения. Данные защищены шифрованием, что снижает риски хищений и повышает операционную безопасность цепочки поставок.
Штрих-кодирование и RFID	Используются для маркировки и отслеживания грузов. RFID-метки, вероятно, внедряются частично, обеспечивая автоматизированный учет и защиту от подделок за счет уникальной идентификации, что укрепляет безопасность логистических процессов.

Деятельность ПАО «Порт Тольятти», связанная с перевалкой сыпучих, генеральных и контейнерных грузов, предполагает использование специализированного программного и аппаратного обеспечения, адаптированного к задачам транспортно-логистической отрасли. Основу информационного обеспечения составляют системы управления портовыми

операциями (Port Management Systems), которые координируют погрузочно-разгрузочные работы, учет грузов и планирование судозаходов.

Финансовые, кадровые и операционные процессы интегрируются с помощью ERP-систем, среди которых платформа 1С, например, «1С:ERP», широко распространенная в российских компаниях.

Электронный документооборот, соответствующий требованиям Федеральной налоговой службы, поддерживается системами ЭДО, позволяющими обмениваться счетами-фактурами и актами с контрагентами. Сетевые технологии включают локальные сети, системы GPS/ГЛОНАСС для отслеживания транспорта и штрих-кодирование для обработки грузов.

В области информационной безопасности применяются базовые меры, такие как антивирусное программное обеспечение и межсетевые экраны, с возможным использованием российских решений от компаний Kaspersky или UserGate. Указанные системы адаптированы к требованиям импортозамещения, что отражает отраслевые тенденции после 2022 года, направленные на переход к отечественным технологиям.

Эффективность системы информационного обеспечения ПАО «Порт Тольятти» оценивается по трем ключевым параметрам: доступность, актуальность и защищенность данных. Результаты такой оценки представлены в таблице 7.

Таблица 7 - Анализ эффективности информационного обеспечения ПАО «Порт Тольятти»

Параметр	Описание текущего состояния	Ограничения и недостатки
Доступность данных	Доступ к данным обеспечивается через локальные системы, такие как PMS, WMS и ERP. Сотрудники имеют базовый доступ к информации, необходимой для выполнения задач. Однако интеграция данных ограничена, что приводит к задержкам в передаче информации между отделами. Отсутствие облачных	Задержки в передаче данных из-за слабой интеграции систем. Ограниченный доступ к данным в удаленных подразделениях. Отсутствие мобильных приложений для оперативного доступа.

Продолжение таблицы 7

Параметр	Описание текущего состояния	Ограничения и недостатки
	технологий ограничивает мобильность и доступность данных в удаленных подразделениях. Используются российские решения, такие как 1С, что соответствует политике импортозамещения.	Зависимость от устаревшего оборудования, что снижает надежность.
Актуальность данных	Актуальность данных поддерживается за счет периодического обновления информации в системах PMS и WMS. Однако ручной ввод данных и отсутствие полной автоматизации приводят к ошибкам и задержкам в обновлении информации. Использование штрих-кодирования частично автоматизирует учет, но отсутствие RFID и IoT снижает точность отслеживания грузов в реальном времени.	Задержки в обновлении информации о статусе грузов. Ошибки учета из-за ручного ввода данных. Недостаточная автоматизация процессов отслеживания. Отсутствие интеграции данных из различных систем, что снижает полноту информации.
Защищенность данных	Защита данных обеспечивается базовыми мерами, включая антивирусное ПО (например, Kaspersky) и межсетевые экраны (UserGate). Применяются российские решения в соответствии с требованиями ФСТЭК. Однако отсутствуют продвинутое системы, такие как SIEM для мониторинга угроз или DLP для предотвращения утечек. Персонал имеет базовые знания о кибербезопасности, что создает риски фишинга и других атак.	Отсутствие SIEM-систем для анализа событий безопасности. Недостаточная защита от утечек данных (отсутствие DLP). Низкая осведомленность персонала о киберугрозах. Отсутствие двухфакторной аутентификации и регулярных аудитов безопасности.

Доступность информации, обеспечиваемая используемыми системами, находится на базовом уровне, позволяя сотрудникам выполнять текущие задачи. Однако ограниченная интеграция между системами, такими как WMS и ERP, приводит к задержкам в передаче данных, что снижает оперативность управления процессами. Сбои в доступе возможны в удаленных подразделениях или при использовании устаревшего оборудования, а отсутствие облачных технологий ограничивает мобильность сотрудников.

Актуальность данных зависит от степени автоматизации и качества интеграции систем. Разрозненность программного обеспечения, приводит к неполноте или устареванию информации, например, при задержках в

обновлении статуса грузов. Недостаточная автоматизация, связанная с использованием ручного ввода данных вместо современных технологий, таких как RFID-метки, дополнительно снижает актуальность информационных потоков. Защищенность данных, как критический аспект для объекта инфраструктуры, регулируется требованиями Федерального закона № 187-ФЗ [20]. Порт применяет базовые меры защиты, включая антивирусы и межсетевые экраны.

Однако отсутствие продвинутых решений, таких как системы мониторинга событий информационной безопасности (SIEM) или предотвращения утечек данных (DLP), а также недостаточная подготовка персонала создают уязвимости перед современными киберугрозами, включая фишинг и DNS-атаки.

Таким образом, анализ системы информационного обеспечения ПАО «Порт Тольятти» выявил ряд недостатков, препятствующих эффективному функционированию предприятия. Устаревшее программное обеспечение, включая старые версии 1С или зарубежные решения, использовавшиеся до перехода на отечественные аналоги, снижает производительность и увеличивает риски уязвимостей. Слабая защита от киберугроз обусловлена отсутствием современных инструментов, таких как SIEM-системы и DLP, а также недостаточной осведомленностью сотрудников о принципах кибербезопасности, что повышает вероятность атак. Низкая интеграция данных между разрозненными системами, такими как WMS, ERP и PMS, приводит к задержкам в обработке информации и ошибкам в учете, что негативно сказывается на оперативности принятия решений. Ограниченная автоматизация процессов, связанная с преобладанием ручного ввода данных и отсутствием технологий Интернета вещей (IoT) для мониторинга грузов, снижает эффективность управления. Наконец, недостаточная масштабируемость существующих систем ограничивает их способность адаптироваться к росту объемов грузов или новым нормативным требованиям, что создает долгосрочные риски для предприятия.

Сравнение системы информационного обеспечения ПАО «Порт Тольятти» с лучшими практиками транспортно-логистической отрасли показывает отставание в ряде ключевых аспектов. Ведущие порты, такие как ПАО «Новороссийский морской торговый порт», используют интегрированные платформы, например, Terminal Operating Systems (TOS), которые обеспечивают управление всеми процессами в реальном времени. В области кибербезопасности передовые предприятия придерживаются стандартов ISO/IEC 27001, внедряя SIEM-системы и проводя регулярные аудиты безопасности, как, например, с использованием платформы «ОРИОН» для модульной защиты данных. Облачные технологии, несмотря на ограничения в России из-за требований локализации данных, активно используются для повышения доступности и масштабируемости.

Регулярное обучение персонала по кибербезопасности и работе с новыми технологиями минимизирует человеческий фактор в инцидентах. В сравнении с этими стандартами ПАО «Порт Тольятти» демонстрирует недостаточную интеграцию данных и автоматизацию, что ограничивает оперативность управления. Уровень кибербезопасности не соответствует стандартам ISO/IEC 27001 из-за отсутствия данных о внедрении SIEM или DLP. Использование российских решений, таких как 1С, соответствует политике импортозамещения, однако их функциональность уступает зарубежным аналогам, например, SAP или Oracle, что ограничивает конкурентоспособность предприятия.

Для устранения выявленных недостатков и повышения экономической безопасности ПАО «Порт Тольятти» предлагается комплекс мер по модернизации информационного обеспечения. Внедрение интегрированной системы TOS позволит объединить данные из WMS, ERP и PMS, обеспечив реальное время обмена информацией и минимизировав задержки в принятии решений. Обновление программного обеспечения до актуальных версий и внедрение SIEM-систем для мониторинга киберугроз укрепят защищенность данных, соответствуя требованиям законодательства и снижая риски атак.

Автоматизация процессов с использованием RFID-меток и IoT-устройств повысит актуальность данных, сократив зависимость от ручного ввода и уменьшив ошибки учета. Проведение регулярного обучения персонала по кибербезопасности и работе с новыми технологиями снизит человеческий фактор в инцидентах, а внедрение двухфакторной аутентификации усилит защиту учетных записей. Наконец, аудит соответствия стандарту ISO/IEC 27001 позволит выявить уязвимости и разработать стратегию долгосрочного повышения защищенности. Реализация данных мер обеспечит устойчивое развитие предприятия, минимизируя риски и повышая его конкурентоспособность в отрасли.

В качестве вывода следует отметить, что проведенное исследование системы информационного обеспечения ПАО «Порт Тольятти» выявило ограничения, связанные с устаревшим программным обеспечением, слабой защитой от киберугроз, низкой интеграцией данных и недостаточной автоматизацией. Сравнение с лучшими отраслевыми практиками подчеркивает необходимость модернизации для достижения стандартов ведущих портов. Предложенные рекомендации, включая внедрение TOS, SIEM-систем, RFID, IoT и обучение персонала, направлены на устранение выявленных недостатков и повышение экономической безопасности предприятия. Их реализация позволит ПАО «Порт Тольятти» укрепить операционную устойчивость, минимизировать риски и адаптироваться к современным вызовам цифровизации.

3 Рекомендации по совершенствованию информационного обеспечения для повышения экономической безопасности

3.1 Разработка и обоснование мер по совершенствованию информационного обеспечения ПАО «Порт Тольятти»

В условиях цифровизации и нарастающих киберугроз информационное обеспечение становится определяющим фактором обеспечения экономической безопасности предприятий транспортно-логистической отрасли. ПАО «Порт Тольятти», специализирующееся на перевалке сыпучих, генеральных и контейнерных грузов, сталкивается с вызовами, связанными с необходимостью модернизации информационных систем для повышения оперативности, защищенности и эффективности управления.

Для устранения выявленных ограничений в системе информационного обеспечения ПАО «Порт Тольятти» предлагается комплекс мер, охватывающий модернизацию технологической инфраструктуры, усиление кибербезопасности, автоматизацию процессов и повышение квалификации персонала.

В таблице 8 представлены мероприятия, направленные на повышение информационной безопасности ПАО «Порт Тольятти».

Таблица 8 – Мероприятия, направленные на повышение информационной безопасности ПАО «Порт Тольятти»

Название мероприятия	Обоснование	Этапы внедрения	Затраты	Ожидаемый эффект
Внедрение интегрированной системы управления портовыми операциями (TOS)	Низкая интеграция данных приводит к задержкам в принятии решений и ошибкам учета,	1. Аудит текущих систем для определения совместимости (1 месяц).	12–15 млн руб. (лицензии, настройка, обучение)	Снижение времени обработки грузов на 15% (экономия ~5 млн руб. в год за счет ускорения операций). Уменьшение

Продолжение таблицы 8

Название мероприятия	Обоснование	Этапы внедрения	Затраты	Ожидаемый эффект
	что снижает операционную эффективность (выручка 2,109,822 т. р. в 2024 году). TOS обеспечит реальное время обмена данными, устраняя разрозненность систем.	2. Выбор и закупка ПО («Корабел» или Navis N4), настройка (3 месяца). 3. Тестирование и обучение персонала (2 месяца).	). Финансирование возможно за счет денежных средств (188,356 т. р.).	ошибок учета на 20%, что сократит потери на 3–4 млн руб. в год.
Модернизация системы информационной безопасности	Слабая защита данных угрожает экономической безопасности, особенно в условиях роста кибератак. Необходимость соответствия ФЗ-187 и защиты активов (1,180,134 т. р.). SIEM и DLP минимизируют риски утечек.	1. Аудит безопасности по ISO/IEC 27001 (1 месяц). 2. Закупка и установка SIEM (Kaspersky) и DLP (2 месяца). 3. Обучение ИТ-специалистов и персонала (1 месяц).	6–8 млн руб. (ПО, оборудование, обучение). Финансирование из текущей ликвидности.	Снижение риска утечек данных на 30%, предотвращение потерь на 10–15 млн руб. в год. Соответствие ФЗ-187, снижение репутационных рисков.
Автоматизация процессов с использованием современных технологий	Ручной ввод данных снижает актуальность информации и увеличивает ошибки учета (запасы 127,188 т. р.). RFID и IoT повысят точность и оперативность, сократив порчу грузов.	1. Пилотный проект на одном складе (2 месяца). 2. Полное оснащение RFID и IoT (4 месяца). 3. Интеграция с TOS и обучение персонала (1 месяц).	8–10 млн руб. (оборудование, настройка). Финансирование за счет денежных средств и части прибыли (204,487 т. р.).	Повышение точности учета грузов на 25%, снижение потерь от порчи грузов на 10% (экономия 2–3 млн руб. в год). Ускорение складских операций на 10%.

Продолжение таблицы 8

Название мероприятия	Обоснование	Этапы внедрения	Затраты	Ожидаемый эффект
Обучение персонала	Недостаточная осведомленность сотрудников увеличивает инциденты безопасности и ошибки при работе с системами. Обучение снизит человеческий фактор и повысит эффективность (расходы на оплату труда 513,210 т. р.).	1. Разработка программы тренингов (1 месяц). 2. Проведение тренингов для всех сотрудников (2 месяца, затем раз в полгода).	1.5–2 млн руб. (услуги тренеров, материалы). Финансирование из текущих денежных средств.	Снижение инцидентов, связанных с человеческим фактором, на 20%. Повышение производительности и труда на 5%, что эквивалентно экономии 2 млн руб. в год.

Затраты, указанные в таблице 8, зависят от выбора конкретных программных и аппаратных решений. Ожидаемые эффекты основаны на прогнозах, учитывающих отраслевые стандарты и специфику деятельности ПАО «Порт Тольятти».

Первым направлением является внедрение интегрированной системы управления портовыми операциями (Terminal Operating System, TOS), такой как российский программный комплекс «Корабел» или адаптированная версия международной платформы Navis N4. Данная система позволит консолидировать данные из систем управления складом, ERP и телекоммуникационных модулей, обеспечивая обмен информацией в реальном времени. Низкая интеграция данных, препятствующая оперативному принятию решений и приводящая к ошибкам учета, будет преодолена за счет унификации информационных потоков. Реализация данного мероприятия предполагает проведение аудита совместимости существующих систем, выбор и настройку программного обеспечения под процессы порта, а также тестирование и обучение персонала. Ожидается, что

внедрение TOS сократит время обработки грузов и уменьшит ошибки учета, укрепляя операционную эффективность предприятия.

Вторым направлением является модернизация системы информационной безопасности посредством внедрения системы мониторинга событий информационной безопасности (SIEM), например, Kaspersky Unified Monitoring and Analysis Platform, и решений по предотвращению утечек данных (DLP). Дополнение двухфакторной аутентификацией и регулярными аудитами безопасности усилит защиту от киберугроз. Слабая защищенность данных, особенно в условиях роста атак на объекты критической инфраструктуры, представляет угрозу экономической безопасности. Реализация SIEM и DLP позволит повысить устойчивость к фишингу, DNS-атакам и другим угрозам, а также обеспечить соответствие требованиям Федерального закона № 187-ФЗ. Процесс включает аудит безопасности по стандарту ISO/IEC 27001, установку необходимого оборудования и программного обеспечения, а также обучение ИТ-специалистов и персонала. Данные меры минимизируют риски утечек данных и укрепят доверие контрагентов.

Третьим направлением является автоматизация процессов с использованием современных технологий, таких как RFID-метки для учета грузов и IoT-устройства для мониторинга состояния складов и транспорта. Внедрение датчиков температуры и влажности для сыпучих грузов повысит контроль над условиями хранения. Ручной ввод данных, снижающий актуальность информации и увеличивающий вероятность ошибок, будет заменен автоматизированными решениями. Реализация предусматривает проведение пилотного проекта на одном складе, полное оснащение предприятия RFID и IoT, а также их интеграцию с TOS. Обучение персонала обеспечит эффективное использование технологий. Данные меры повысят точность учета и сократят потери от порчи грузов, способствуя финансовой стабильности.

Четвертым направлением является проведение регулярных тренингов для персонала по кибербезопасности и работе с новыми системами, такими как TOS и RFID. Недостаточная осведомленность сотрудников о принципах безопасной работы с данными и новых технологиях является одной из причин инцидентов. Разработка и реализация программы тренингов, проводимых с периодичностью раз в полгода, позволит снизить человеческий фактор в ошибках и повысить эффективность эксплуатации информационных систем. Данные меры требуют минимальных затрат, но обеспечивают значительный эффект в укреплении безопасности и производительности.

Экономическая эффективность предложенных мер оценивается с учетом их совокупных затрат, периода окупаемости и ожидаемого возврата на инвестиции. Внедрение TOS потребует затрат на лицензии, настройку и обучение, модернизация кибербезопасности — на закупку SIEM и DLP, автоматизация — на оборудование RFID и IoT, а обучение персонала — на услуги тренеров и материалы. Общие затраты составят значительную сумму, однако их окупаемость ожидается в течение двух-трех лет. Экономия будет достигнута за счет сокращения потерь от ошибок учета и порчи грузов, уменьшения простоев благодаря ускорению процессов, а также снижения рисков кибератак и связанных с ними штрафов. Возврат на инвестиции прогнозируется на уровне, обеспечивающем финансовую целесообразность проекта, что подтверждает рациональность предложенных мер.

3.2 Оценка эффективности предложенных мер и их влияние на экономическую безопасность

ПАО «Порт Тольятти» — речной порт, специализирующийся на перевалке грузов, с выручкой 2109822 т. р. и активами 1180134 т. р. в 2024 году. Экономическая безопасность предприятия зависит от защиты финансовых потоков, операционной устойчивости и репутации. Рекомендации включают внедрение интегрированной системы управления

портовыми операциями (TOS), модернизацию системы информационной безопасности, автоматизацию процессов с использованием современных технологий и обучение персонала. Реализация предложенных мер существенно укрепит экономическую безопасность ПАО «Порт Тольятти» по нескольким направлениям, которые представлены в таблице 9.

Таблица 9 – Направления влияния разработанных мер на экономическую безопасность ПАО «Порт Тольятти»

Мера	Тип безопасности	Эффект/Преимущество
1 Внедрение TOS	Операционная безопасность	Автоматизация планирования, отслеживания грузов и управления складом, снижение времени обработки и ошибок
	Финансовая безопасность	Экономия 5–7 млн руб. в год за счет сокращения времени обработки на 10%
2 Модернизация системы информационной безопасности	Информационная безопасность	Внедрение SIEM, DLP и двухфакторной аутентификации, снижение риска утечек
	Репутационная безопасность	Сохранение доверия партнеров, экономия 10–15 млн руб. за счет предотвращения утечек
3 Автоматизация процессов (RFID, IoT)	Операционная безопасность	Повышение точности учета грузов и мониторинга условий хранения, снижение потерь и порчи товаров
	Финансовая безопасность	Экономия 3–5 млн руб. в год за счет снижения потерь грузов на 5%
4 Обучение персонала	Кадровая безопасность	Снижение ошибок, связанных с человеческим фактором
	Финансовая безопасность	Экономия 2–3 млн руб. в год за счет снижения инцидентов на 20%
5 Внедрение BI-систем для анализа рисков	Финансовая безопасность	Экономия 5–7 млн руб. в год за счет выявления аномалий в цепочке поставок
	Операционная безопасность	Ускорение обработки грузов и минимизация простоев за счет анализа операционных данных

Таким образом, финансовая безопасность повысится за счет сокращения потерь от ошибок и простоев, что обеспечит стабильность денежных потоков. Информационная безопасность будет усилена благодаря минимизации рисков утечек данных и кибератак, что сохранит репутацию и доверие контрагентов. Операционная безопасность укрепит за счет автоматизации и интеграции данных, повышающих устойчивость процессов к внешним и внутренним угрозам. Репутационная безопасность улучшится благодаря соответствию отраслевым стандартам, таким как ISO/IEC 27001, что усилит конкурентные позиции порта на рынке. Комплексный подход к модернизации информационного обеспечения создаст основу для устойчивого развития предприятия. Для оценки уровня экономической безопасности используются данные о рисках финансовых потерь, основанные на типичных угрозах для порта и текущем состоянии систем (отсутствие TOS, SIEM, DLP и низкая автоматизация). В таблице 10 сведены данные о рисках до и после внедрения мер, полученные с использованием метода экспертных оценок, включая стоимость до и после, а также абсолютное и процентное снижение рисков.

Таблица 10 – Риски до и после внедрения мероприятий по совершенствованию информационного обеспечения ПАО «Порт Тольятти»

Тип риска	Стоимость до (млн руб.)	Стоимость после (млн руб.)	Снижение (млн руб.)	Снижение (%)
Задержки и ошибки в обработке грузов	10	5	5	50
Утечки данных	15	4,5	10,5	70
Потери грузов и порча товаров	5	2,5	2,5	50
Ошибки персонала	3	1,2	1,8	60
Неэффективные контракты и операции	7	2,1	4,9	70
Общий риск	40	15,3	24,7	61,75

Общее снижение риска составило 24,7 млн руб., что соответствует улучшению на 61,75% от первоначальных 40 млн руб.

Для обеспечения эффективности предложенных мер необходим систематический мониторинг и корректировка их реализации. Ежеквартальный аудит информационных систем и безопасности, включающий анализ ключевых показателей эффективности, таких как время обработки грузов, количество инцидентов и точность учета, позволит отслеживать прогресс.

Корректировка будет осуществляться путем внесения изменений в настройки TOS, обновления политик безопасности и доработки программ обучения на основе обратной связи от сотрудников. Ответственность за реализацию возлагается на ИТ-департамент, отдел безопасности.

Такой подход обеспечит адаптивность системы к изменяющимся условиям и угрозам.

Таким образом, рекомендации значительно усилят экономическую безопасность ПАО «Порт Тольятти»:

- в отношении финансовой стабильности будет наблюдаться снижение потерь и операционных рисков, что укрепляет денежные потоки;
- в отношении операционной устойчивости реализуется автоматизация и мониторинг, которые минимизируют сбои и задержки;
- в отношении репутации ПАО «Порт Тольятти» - защита данных и надежность операций сохраняют доверие партнеров.

Расчеты показывают снижение рисков с 40 млн руб. до 15,3 млн руб., что эквивалентно улучшению на 61,75%. Затраты на внедрение (примерно 28–35 млн руб.) окупаются за счет экономии и соответствуют финансовым возможностям порта (ликвидность 188356 т. р., прибыль 204487 т. р.).

Разработанный комплекс мер, включающий внедрение интегрированной системы TOS, модернизацию кибербезопасности с использованием SIEM и DLP, автоматизацию процессов посредством RFID и IoT, а также обучение

персонала, направлен на устранение ключевых недостатков информационного обеспечения ПАО «Порт Тольятти».

Реализация данных мероприятий повысит актуальность, доступность и защищенность данных, приведет систему в соответствие с лучшими отраслевыми практиками и укрепит экономическую безопасность предприятия.

Снижение операционных рисков, финансовых потерь и укрепление конкурентных позиций в условиях цифровизации и роста киберугроз станут основными результатами предложенного подхода. Перспективы дальнейших исследований связаны с изучением влияния искусственного интеллекта и облачных технологий на информационное обеспечение транспортно-логистических предприятий.

Заключение

Проведённое исследование подтвердило важнейшую роль информационного обеспечения в системе экономической безопасности предприятия, особенно в условиях цифровизации и роста киберугроз.

В работе была поставлена цель — разработать практические рекомендации по повышению экономической безопасности на основе совершенствования информационного обеспечения. Все поставленные задачи были выполнены, а гипотеза о взаимосвязи между уровнем информационного обеспечения и экономической безопасностью предприятия получила подтверждение как в теоретическом, так и в практическом аспектах.

В первом разделе были рассмотрены теоретические аспекты экономической безопасности и информационного обеспечения. Обобщены подходы ведущих российских ученых, таких как Гашо И.А., Гунина И.А., Акбашева А.А., Плотников А.П., к определению сущности и структуры экономической безопасности. Были выделены ключевые компоненты: финансовая, информационная, кадровая, технологическая и правовая безопасность. Особое внимание было уделено информационной безопасности, без которой невозможно обеспечить надёжность управления ресурсами, защиту от киберугроз и сохранность критических бизнес-процессов.

Во втором разделе дана комплексная характеристика текущего состояния ПАО «Порт Тольятти». Анализ имущественного и финансового положения предприятия за 2022–2024 годы показал положительную динамику ключевых показателей: выручка увеличилась с 1 483 678 тыс. руб. в 2022 году до 2 109 822 тыс. руб. в 2024 году (рост на 42%), чистая прибыль — с 78 603 тыс. руб. до 204 487 тыс. руб. Однако в 2024 году зафиксировано снижение чистой прибыли на 11,27% по сравнению с 2023 годом, что указывает на необходимость оптимизации затрат и повышения эффективности. Основные средства предприятия выросли более чем в два раза — с 302 541 тыс. руб. до 677 979 тыс. руб., однако при этом наблюдается снижение фондоотдачи (с 5,20

до 3,57) и оборачиваемости активов (с 2,71 до 2,06), что говорит о неэффективном использовании имущественного потенциала.

SWOT-анализ показал, что, несмотря на стратегически выгодное расположение и рост выручки, ПАО «Порт Тольятти» сталкивается с рядом угроз: кибератаками, недостаточной защитой данных, слабой интеграцией информационных систем (WMS, ERP, PMS), а также высокой текучестью кадров (33,7% в 2024 году). Общий уровень экономической безопасности предприятия можно охарактеризовать как средний: финансовые показатели устойчивы, но присутствуют серьезные операционные и информационные риски, приводящие к потерям в размере до 40 млн руб. в год (включая утечки данных, ошибки учёта и операционные сбои).

В третьем разделе были предложены обоснованные рекомендации по повышению уровня экономической безопасности через модернизацию информационного обеспечения. В частности:

- внедрение интегрированной системы TOS позволит устранить разрозненность между WMS, ERP и PMS, ускорить обработку грузов на 15% и снизить ошибки учёта на 20%;
- модернизация ИБ-инфраструктуры через внедрение SIEM и DLP снизит риск утечек и кибератак на 30%, минимизируя потери до 10–15 млн руб.;
- автоматизация процессов с помощью RFID и IoT обеспечит повышение точности учёта грузов на 25% и снижение порчи товаров на 10%;
- систематическое обучение персонала позволит снизить инциденты, связанные с человеческим фактором, на 20% и повысить производительность труда.

В результате реализации указанных мероприятий совокупные риски могут быть снижены с 40 млн до 15,3 млн руб., то есть на 61,75%. Это подтверждает эффективность предложенной стратегии, направленной на

укрепление финансовой, операционной и информационной устойчивости предприятия.

Таким образом, информационное обеспечение доказало свою ключевую роль в формировании эффективной системы экономической безопасности. Обновление программно-технической базы, усиление киберзащиты, автоматизация процессов и развитие компетенций персонала позволят ПАО «Порт Тольятти» не только снизить издержки, но и сформировать конкурентные преимущества на рынке транспортно-логистических услуг.

Перспективы дальнейших исследований видятся в изучении влияния искусственного интеллекта и технологий машинного обучения на управление экономической безопасностью. Интеллектуальные системы анализа и предсказания рисков, автоматическая адаптация к инцидентам, предиктивная аналитика — всё это открывает новые горизонты в обеспечении устойчивости предприятий к внешним и внутренним вызовам цифровой эпохи.

Список используемых источников

1. Акбашева А.А. Теоретические компоненты обеспечения экономической безопасности предприятия / А. А. Акбашева, Х. М. Психوماхов, И. Ш. Дзахмишева // Управленческий учет. 2020. № 6. С. 4-11. EDN SHEETY.
2. Алламурадова М.К. Эволюция угроз в области информационной безопасности: анализ современных тенденций и перспективы защиты // Вестник науки. 2024. №3 (72). С. 315-319
3. Афанасьева С.В., Черепанова Е.С., Шехова Н.В. Инновационные методы предотвращения киберугроз в целях обеспечения экономической безопасности организации // Вестник Самарского университета. Экономика и управление. 2023. №2. С. 7-16
4. Болдырева М.Д., Шхагошев Р.В. Роль кибербезопасности в обеспечении экономической стабильности // Вестник науки. 2024. №12 (81). С. 118-123
5. Гашо, И.А. Теоретические аспекты управления экономической безопасностью предприятия / И. А. Гашо, И. Иовлева, Е. В. Токарь // Вестник Белгородского университета кооперации, экономики и права. 2022. № 3(94).С. 85-95. DOI 10.21295/2223-5639-2022-3-85-95. EDN DLGMWZ.
6. Гриднева Е.В., Шаповалов В.И. Подходы к оценке уровня экономической безопасности предприятия // Экономика и бизнес: теория и практика. 2019. №12-1. С. 113-116
7. Гунина И.А. Система управления экономической безопасностью предприятия / И. А. Гунина, Ю. Н. Посаженникова // Экономинфо. 2018. Т. 15, № 1. С. 28-31. EDN YVWWJC.
8. Кодекс корпоративного управления (утв. Банком России 21 марта 2014 г., протокол № 6) // СПС «КонсультантПлюс»

9. Кубатиева Л.М. Принципы и функции информационного обеспечения управления организацией // Вестник экономической безопасности. 2023. №2. С. 206-209
10. Линко И.В. Понятие и элементы экономической безопасности предприятий // Экономика и социум. 2022. №9 (100). С. 474-454
11. Малкова Т.Б. Методические подходы к оценке экономической безопасности региона / Т. Б. Малкова // Экономика и управление: проблемы, решения. 2020. Т. 2, № 1. С. 65-70. EDN WABLJV.
12. Пирогова М.Е. Рост угроз информационной безопасности: как Россия борется с новыми вызовами // Вестник науки. 2023. №11 (68). С. 687-690
13. Плотников А.П. Некоторые методологические аспекты управления экономической безопасностью предприятия / А. П. Плотников, Ф. А. Казакова // Актуальные проблемы экономики и менеджмента. 2020. № 1(25). С. 148-155. EDN ALAMEQ.
14. Постановление Правительства РФ от 12 февраля 2014 г. № 99 «Об утверждении Правил организации искусственного воспроизводства водных биологических ресурсов» (в ред. от 30.11.2023) // СПС «КонсультантПлюс»
15. Приказ Министерства природных ресурсов и экологии РФ от 8 декабря 2020 г. № 1028 «Об утверждении Порядка ведения государственного учета, государственного кадастра отходов и государственного регулирования в области обращения с отходами» // СПС «КонсультантПлюс»
16. Сидоренко Г.Г., Бабаёров Р.А. IT-технологии как инструментальный совершенствования системы экономической безопасности кредитной организации // Экономика и управление народным хозяйством. 2023. С.189-195
17. Соколовский А.А. Информационные аспекты обеспечения экономической безопасности организации в условиях перехода к цифровой экономике / А. А. Соколовский, П. Г. Грибов // Вестник евразийской науки. 2023. Т. 15. № 1. С. 512-516

18. Сулимова Е.А. Цифровой инструментарий управления предприятиями: CRM, ERP, ECM, BI // Инновации и инвестиции. 2023. №5. С. 158-160
19. Сульдин К.Н., Мадаева О.С., Хит Е.В. Информационное обеспечение экономической безопасности организации // Инновационная наука. 2023. №5-2. С. 83-85
20. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ (в ред. от 25.12.2023) // СПС «КонсультантПлюс»
21. Федеральный закон от 10 января 2002 г. № 7-ФЗ «Об охране окружающей среды» (в ред. от 25.12.2023) // СПС «КонсультантПлюс»
22. Федеральный закон от 22 апреля 1996 г. № 39-ФЗ «О рынке ценных бумаг» (в ред. от 25.12.2023) // СПС «КонсультантПлюс»
23. Федеральный закон от 24 июня 1998 г. № 89-ФЗ «Об отходах производства и потребления» (в ред. от 25.12.2023) // СПС «КонсультантПлюс»
24. Федеральный закон от 26 декабря 1995 г. № 208-ФЗ «Об акционерных обществах» (в ред. от 29.12.2024) // СПС «КонсультантПлюс»
25. Юрасов В.Г. Организация информационного обеспечения систем управления // Вестник ВГТУ. 2013. №3-1. С. 163
26. Cremer F., Sheehan B., Fortmann M., Kia A. N., Mullins M., Murphy F., Materne S. Cyber risk and cybersecurity: a systematic review of data availability // Geneva Papers on Risk and Insurance - Issues and Practice. 2022. Vol. 47, № 3. P. 698–736. DOI: 10.1057/s41288-022-00266-6.
27. Kang X., Wang M., Lin J., Chen Y., Liu Z., Wu J. Trends and status in resources security, ecological stability, and sustainable development research: a systematic analysis // Environmental Science and Pollution Research. 2022. Vol. 29, № 33. P. 50192–50207. DOI: 10.1007/s11356-022-19412-7.
28. Dalal R. S., Howard D. J., Bennett R. J., Posey C., Zaccaro S. J., Brummel B. J. Organizational science and cybersecurity: abundant opportunities for

research at the interface // *Journal of Business and Psychology*. 2022. Vol. 37, № 1. P. 1–29. DOI: 10.1007/s10869-021-09732-9.

29. Guitton C. Facing cyberthreats in a crisis and post-crisis era: Rethinking security services response strategy // *Frontiers in Political Science*. 2023. Vol. 5. — Article 1083182. DOI: 10.3389/fpos.2023.1083182.

30. Ho M., Jensen B., Lonergan E. Cybersecurity convergence: Digital human and national security // *Journal of National Security Law & Policy*. 2023. Vol. 13, № 3. P. 423–454.

Приложение А

Бухгалтерская отчетность ПАО «Порт Тольятти» 2022-2024 гг.

ИНН 6320004816
КПП 632401001

Форма по КИД 0710099
Форма по ОКУД 0710001

Бухгалтерский баланс
На 31 декабря 2024 г.

Пояснения ¹	Наименование показателя	Код строки	На 31 декабря 2024 г.	На 31 декабря 2023 г.	На 31 декабря 2022 г.
1	2	3	4	5	6
Актив					
I. Внеоборотные активы					
	Нематериальные активы	1110	621	-	-
	Результаты исследований и разработок	1120	-	-	-
	Нематериальные поисковые активы	1130	-	-	-
	Материальные поисковые активы	1140	-	-	-
	Основные средства	1150	677 979	505 658	302 541
	Основные средства в организации		543 535	385 339	275 289
	Оборудование к установке		2 748	7 768	718
	Строительство объектов основных средств		29 735	24 615	711
	Приобретение объектов основных средств		35 090	28 470	1 653
	Права пользования активами		66 871	59 466	24 170
	Доходные вложения в материальные ценности	1160	-	-	-
	Финансовые вложения	1170	2	2	2
	Паи		2	2	2
	Отложенные налоговые активы	1180	26 222	21 293	8 326
	Прочие внеоборотные активы	1190	0	-	129
	Итого по разделу I	1100	704 824	526 953	310 998
II. Оборотные активы					
	Запасы	1210	127 188	120 624	101 623
	Материалы		98 990	94 727	62 637
	Товары		25 153	13 659	33 431
	Готовая продукция		3 044	12 238	5 555

Рисунок А.1 – Актив бухгалтерского баланса

Продолжение приложения А

Пояснения ¹	Наименование показателя	Код строки	На 31 декабря 2024 г.	На 31 декабря 2023 г.	На 31 декабря 2022 г.
1	2	3	4	5	6
	Налог на добавленную стоимость по приобретенным ценностям	1220	175	11 263	2 177
	НДС по приобретенным ОС		0	-	-
	НДС по приобретенным материально-производственным запасам		10	52	18
	НДС по приобретенным услугам		20	8	24
	НДС при строительстве ОС		145	-	-
	НДС по предстоящим лизинговым платежам		0	11 203	2 135
	Дебиторская задолженность	1230	158 447	178 069	125 447
	Расчеты с поставщиками и подрядчиками		35 308	47 721	14 302
	Расчеты с покупателями и заказчиками		70 390	72 577	76 184
	Расчеты по налогам и сборам		37 151	25 587	20 960
	Расчеты с персоналом по прочим операциям		1 088	737	619
	Расчеты с разными дебиторами и кредиторами		13 469	24 720	6 775
	Расчеты по имущественному, личному и добровольному страхованию		1 041	1 228	569
	НДС по авансам и предоплатам		0	5 499	6 038
	Финансовые вложения (за исключением денежных эквивалентов)	1240	-	-	-
	Денежные средства и денежные эквиваленты	1250	188 356	30 429	61 304
	Касса организации		158	218	28
	Расчетные счета		2 998	8 911	35 976
	Прочие специальные счета		185 200	21 300	25 300
	Переводы в пути		0	-	-
	Прочие оборотные активы	1260	1 144	1 836	1 771
	Активы по оплаченным материальным ценностям		1	1	1
	Расходы будущих периодов		1 143	1 835	1 770
	Итого по разделу II	1200	475 310	342 221	292 322
	БАЛАНС	1600	1 180 134	869 174	603 320

Рисунок А.2 – Продолжение актива бухгалтерского баланса

Продолжение приложения А

Пояснения ¹	Наименование показателя	Код строки	На 31 декабря 2024 г.	На 31 декабря 2023 г.	На 31 декабря 2022 г.
1	2	3	4	5	6
Пассив					
III. Капитал и резервы					
	Уставный капитал (складочный капитал, уставный фонд, вклады товарищей)	1310	3 825	25	25
	Собственные акции, выкупленные у акционеров	1320	(-)²	(-)	(-)
	Переоценка внеоборотных активов	1340	0	47 454	47 454
	Переоценка основных средств		0	47 454	47 454
	Добавочный капитал (без переоценки)	1350	110 200	-	-
	Эмиссионный доход		110 200	-	-
	Резервный капитал	1360	234	234	234
	Нераспределенная прибыль (непокрытый убыток)	1370	773 239	521 298	290 827
	Списание накопленного результата переоценок ОС (переход на ФСБУ 6/2020)		47 454	-	-
	Нераспределенная прибыль (непокрытый убыток) прошлых лет и текущего года		725 785	-	-
	Итого по разделу III	1300	887 498	569 011	338 540
IV. Долгосрочные обязательства					
	Заемные средства	1410	0	9 526	60 731
	Долгосрочные кредиты		0	9 526	14 926
	Долгосрочные займы		0	-	45 805
	Отложенные налоговые обязательства	1420	51 321	36 805	21 077
	Оценочные обязательства	1430	-	-	-
	Прочие обязательства	1450	26 977	67 217	13 102
	Итого по разделу IV	1400	78 298	113 548	94 910

Рисунок А.3 – Пассив бухгалтерского баланса

Продолжение приложения А

Пояснения ¹	Наименование показателя	Код строки	На 31 декабря 2024 г.	На 31 декабря 2023 г.	На 31 декабря 2022 г.
1	2	3	4	5	6
V. Краткосрочные обязательства					
	Заемные средства	1510	4 126	25 807	1 394
	Краткосрочные кредиты		4 126	25 805	1 394
	Краткосрочные займы		0	-	-
	Проценты по краткосрочным кредитам		0	2	-
	Проценты по долгосрочным кредитам		0	-	-
	Проценты по краткосрочным займам		0	-	-
	Проценты по долгосрочным займам		0	-	-
	Кредиторская задолженность	1520	175 204	137 205	148 658
	Расчеты с поставщиками и подрядчиками		68 574	44 584	38 967
	Расчеты с покупателями и заказчиками		42 859	33 375	37 790
	Расчеты по налогам и сборам		36 292	12 017	26 437
	Расчеты по социальному страхованию и обеспечению		15 302	26 208	36 195
	Расчеты с персоналом по оплате труда		10 298	14 051	5 999
	Расчеты с разными дебиторами и кредиторами		1 879	6 970	3 270
	Доходы будущих периодов	1530	-	-	-
	Оценочные обязательства	1540	28 046	23 603	19 818
	Прочие обязательства	1550	6 962	-	-
	Итого по разделу V	1500	214 338	186 615	169 870
	БАЛАНС	1700	1 180 134	869 174	603 320

Примечания

¹ Указывается номер соответствующего пояснения.

² Здесь и в других формах отчетов вычитаемый или отрицательный показатель показывается в круглых скобках.

Рисунок А.4 – Завершение пассива бухгалтерского баланса

Продолжение приложения А

ИНН 6320004816
КПП 632401001

Форма по КИД 0710099
Форма по ОКУД 0710002

Отчет о финансовых результатах За 2024 г.

Пояснения ³	Наименование показателя	Код строки	За 2024 г.	За 2023 г.
1	2	3	4	5
	Выручка ⁴	2110	2 109 822	1 869 330
	Себестоимость продаж	2120	(1 714 409)	(1 520 936)
	Валовая прибыль (убыток)	2100	395 413	348 394
	Коммерческие расходы	2210	(-)	(-)
	Управленческие расходы	2220	(117 661)	(105 717)
	Прибыль (убыток) от продаж	2200	277 752	242 677
	Доходы от участия в других организациях	2310	170	-
	Проценты к получению	2320	22 900	6 744
	Проценты к уплате	2330	(12 689)	(9 337)
	Прочие доходы	2340	27 866	91 640
	Доходы, связанные с реализацией основных средств		192	49 652
	Доходы, связанные с ликвидацией основных средств		833	793
	Доходы, связанные с реализацией прочего имущества		485	8 690
	Доходы, связанные со сдачей имущества в аренду (субаренду)		7 157	5 619
	Доходы в виде восстановленных оценочных резервов		1 342	28
	Штрафы, пени, неустойки к получению		10 765	3 984
	Прибыль прошлых лет		244	-
	Возмещение убытков к получению		806	292
	Прочие внереализационные доходы		6 042	22 582

Рисунок А.5 – Отчет о финансовых результатах 2024 г.

Продолжение приложения А

<i>Пояснения³</i>	<i>Наименование показателя</i>	<i>Код строки</i>	<i>За 2024 г.</i>	<i>За 2023 г.</i>
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>
	Прочие расходы	2350	(58 711)	(42 858)
	Расходы, связанные с реализацией основных средств		(88)	(4 022)
	Расходы, связанные с ликвидацией основных средств		(833)	(863)
	Расходы, связанные с реализацией прочего имущества		(485)	(2 230)
	Расходы, связанные со сдачей имущества в аренду (субаренду)		(1 300)	(1 158)
	Расходы в виде образованных оценочных резервов		(59)	(1 826)
	Расходы на услуги банков		(3 439)	(2 224)
	Убытки прошлых лет		(989)	(1 919)
	Налоги и сборы		(10 620)	(8 358)
	Расходы в виде списанной дебиторской задолженности		(923)	(280)
	Прочие внереализационные расходы		(39 975)	(19 978)
	Прибыль (убыток) до налогообложения	2300	257 288	288 866
	Налог на прибыль ⁵	2410	(52 801)	(58 395)
	в т.ч.:			
	текущий налог на прибыль	2411	(43 214)	(55 633)
	отложенный налог на прибыль ⁶	2412	(9 587)	(2 762)
	Прочее	2460	-	-
	Чистая прибыль (убыток)	2400	204 487	230 471
	Результат от переоценки внеоборотных активов, не включаемый в чистую прибыль (убыток) периода	2510	-	-
	Результат от прочих операций, не включаемый в чистую прибыль (убыток) периода	2520	-	-
	Налог на прибыль от операций, результат которых не включается в чистую прибыль (убыток) периода ⁵	2530	-	-
	Совокупный финансовый результат периода⁷	2500	204 487	230 471
СПРАВОЧНО				
	Базовая прибыль (убыток) на акцию	2900	-	-

Рисунок А.6 – Отчет о финансовых результатах 2024 г.

Продолжение приложения А

ИНН 6320004816
КПП 632401001

Форма по КИД 0710099
Форма по ОКУД 0710002

Отчет о финансовых результатах За 2023 г.

<i>Пояснения³</i>	<i>Наименование показателя</i>	<i>Код строки</i>	<i>За 2023 г.</i>	<i>За 2022 г.</i>
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>
	Выручка ⁴	2110	1 869 330	1 483 678
	Себестоимость продаж	2120	(1 520 936)	(1 275 284)
	Валовая прибыль (убыток)	2100	348 394	208 394
	Коммерческие расходы	2210	(0)	(14 243)
	Управленческие расходы	2220	(105 717)	(91 352)
	Прибыль (убыток) от продаж	2200	242 677	102 799
	Доходы от участия в других организациях	2310	-	-
	Проценты к получению	2320	6 744	3 025
	Проценты к уплате	2330	(9 337)	(7 251)
	Прочие доходы	2340	91 640	36 218
	Доходы, связанные с реализацией основных средств		49 652	6 978
	Доходы, связанные с ликвидацией основных средств		793	1 466
	Доходы, связанные с реализацией прочего имущества		8 690	7 392
	Доходы, связанные со сдачей имущества в аренду (субаренду)		5 619	6 938
	Доходы в виде восстановленных оценочных резервов		28	2 893
	Штрафы, пени, неустойки к получению		3 984	5 184
	Прибыль прошлых лет		0	650
	Возмещение убытков к получению		292	281
	Доходы в виде списанной кредиторской задолженности		0	300
	Прочие внереализационные доходы		22 582	4 136

Рисунок А.7 – Отчет о финансовых результатах 2023 г.

Продолжение приложения А

<i>Пояснения¹</i>	<i>Наименование показателя</i>	<i>Код строки</i>	<i>За 2023 г.</i>	<i>За 2022 г.</i>
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>
	Прочие расходы	2350	(42 858)	(27 809)
	Расходы, связанные с реализацией основных средств		(4 022)	(1 194)
	Расходы, связанные с ликвидацией основных средств		(863)	(913)
	Расходы, связанные с реализацией прочего имущества		(2 230)	(1 624)
	Расходы, связанные со сдачей имущества в аренду (субаренду)		(1 158)	(1 768)
	Расходы в виде образованных оценочных резервов		(1 826)	(61)
	Расходы на услуги банков		(2 224)	(1 834)
	Убытки прошлых лет		(1 919)	(1 048)
	Налоги и сборы		(8 358)	(8 066)
	Расходы в виде списанной дебиторской задолженности		(280)	(21)
	Прочие внереализационные расходы		(19 978)	(11 280)
	Прибыль (убыток) до налогообложения	2300	288 866	106 982
	Налог на прибыль ⁵	2410	(58 395)	(28 379)
	в т.ч.:			
	текущий налог на прибыль	2411	(55 633)	(19 531)
	отложенный налог на прибыль ⁶	2412	(2 762)	(8 848)
	Прочее	2460	0	-
	Штрафные санкции и пени за нарушение налогового и иного законодательства		0	-
	Чистая прибыль (убыток)	2400	230 471	78 603
	Результат от переоценки внеоборотных активов, не включаемый в чистую прибыль (убыток) периода	2510	-	-
	Результат от прочих операций, не включаемый в чистую прибыль (убыток) периода	2520	0	24 315
	переход на ФСБУ 6/2020		0	24 315
	Налог на прибыль от операций, результат которых не включается в чистую прибыль (убыток) периода ⁵	2530	-	-
	Совокупный финансовый результат периода⁷	2500	230 471	102 918

Рисунок А.8 – Отчет о финансовых результатах 2023 г.