Территория новых возможностей. Вестник Владивостокского государственного университета. 2026. Т. 18, № 1. С. 45–61
The Territory of New Opportunities. The Herald of Vladivostok State University. 2026. Vol. 18, № 1. P. 45–61

Научная статья
УДК 658.7
DOI: https://doi.org/10.29039/2949-1258/2026-1/045-061
EDN: https://elibrary.ru/XEWASO

Консолидированная модель измерения корпоративной цифровой ответственности в цепях поставок

Гвилия Наталья Алексеевна
Санкт-Петербургский государственный экономический университет
Санкт-Петербург. Россия

Аннотация. *Цифровая трансформация радикально изменила функционирование цепей поставок, повысив значение данных, алгоритмов и цифровых платформ до ключевых механизмов координации, управления рисками и обеспечения устойчивости. В этих условиях корпоративная цифровая ответственность (КЦО) перестает быть исключительно нормативной или декларативной категорией и приобретает операционное значение, напрямую влияя на надежность и устойчивость логистических систем. Несмотря на рост научного интереса к КЦО, существующие подходы к ее измерению остаются фрагментарными и слабо адаптированными к специфике цепей поставок как распределенных межорганизационных систем. Целью исследования является разработка консолидированной модели измерения корпоративной цифровой ответственности, релевантной для цепей поставок и логистических провайдеров. Методически работа опирается на системный анализ литературы и сравнительную оценку существующих подходов к измерению КЦО, включая клиентоориентированные модели, процессно-ориентированные подходы, модели цифровой зрелости и ESG-ориентированные рамки. На основе выявленных ограничений предлагается консолидированная пятиуровневая модель измерения КЦО, отражающая причинно-следственную логику формирования цифровой ответственности в цепях поставок. Предложенная методика объединяет управляемость цифровых решений, надежность данных и алгоритмов, межорганизационную ответственность за данные, цифровые риски и устойчивость цепей поставок, а также восприятие цифровых решений внешними стейкхолдерами. Для каждого уровня предложены измеримые индикаторы и интегральные индексы, сочетающие количественные метрики и качественные диагностические шкалы. Научная новизна исследования заключается в систематическом переносе логики корпоративной цифровой ответственности в контекст цепей поставок и разработке многоуровневого измерительного подхода, позволяющего рассматривать КЦО как измеримый управленческий феномен, связанный с устойчивостью и управлением цифровыми рисками в логистических системах.*

Ключевые слова**:** *корпоративная логистика, корпоративная социальная ответственность, управление цифровыми рисками, устойчивое развитие, устойчивость цепей поставок, цепи поставок, корпоративная цифровая ответственность, цифровая трансформация, цифровизация, цифровое управление, цифровые технологии, ESG*

Для цитирования: *Гвилия Н.А. Консолидированная модель измерения корпоративной цифровой ответственности в цепях поставок // Территория новых возможностей. Вестник Владивостокского государственного университета. 2026. Т. 18, № 1. С. 45–61. DOI: https://doi.org/10.29039/2949-1258/2026-1/045-061. EDN: https://elibrary.ru/XEWASO*

Original article

Consolidated model for measuring corporate digital responsibility in supply chains

Natalia A. Gviliya
Saint Petersburg State University of Economics
Saint Petersburg. Russia

Abstract. *Digital transformation has fundamentally reshaped supply chains, making data, algorithms, and digital platforms core mechanisms of coordination, risk management, and resilience. In this context, Corporate Digital Responsibility (CDR) is no longer merely a normative or declarative concept but an operational factor that directly affects the reliability and sustainability of logistics systems. Despite the growing academic interest in CDR, existing measurement approaches remain fragmented and poorly adapted to supply chains as distributed and inter-organizational systems. The purpose of this study is to develop a measurement framework for Corporate Digital Responsibility that is applicable to supply chains and logistics providers. Methodologically, the research is based on a systematic literature review and a comparative analysis of existing CDR measurement approaches, including consumer-centric models, process-oriented frameworks, digital maturity models, and ESG-aligned approaches. Based on the identified limitations, the study proposes a consolidated five-level CDR measurement model reflecting the causal logic of how digital responsibility is formed, implemented, and manifested in supply chains. The proposed framework integrates digital governance and accountability, data and algorithm reliability, inter-organizational data responsibility, digital risk and supply chain resilience, and stakeholder perception of digital solutions. For each level, the study introduces measurable indicators and composite indices combining quantitative metrics with qualitative diagnostic scales. The scientific contribution of this research lies in the systematic transfer of Corporate Digital Responsibility logic to the supply chain context and in the development of a multi-level measurement framework that conceptualizes CDR as a measurable managerial phenomenon directly linked to resilience and digital risk management in logistics systems.*

Keywords: *corporate logistics, corporate social responsibility, digital risk management, sustainability, supply chain sustainability, supply chains, corporate digital responsibility, digital transformation, digitalization, digital governance, digital technology, ESG*

For citation*: Gviliya N. A. Consolidated model for measuring corporate digital responsibility in supply chains // The Territory of New Opportunities. The Herald of Vladivostok State University. 2026. Vol. 18, № 1. P. 45–61. DOI: https://doi.org/10.29039/2949-1258/2026-1/045-061. EDN: https://elibrary.ru/XEWASO*

Введение

Современные цепи поставок все больше приобретают характеристики сложных систем, в которых технологические решения тесно переплетены с организационными, институциональными и социальными аспектами. Нарушения в цифровых системах управления, сбои информационных платформ, ошибки алгоритмических решений, искажения данных или недостаточная прозрачность цифровых процессов способны вызывать каскадные эффекты, затрагивающие устойчивость всей логистической сети [1]. В результате цифровые риски перестают быть локальной проблемой отдельных подразделений и становятся фактором системной устойчивости цепей поставок.

На этом фоне возрастает значение корпоративной цифровой ответственности (КЦО) как элемента устойчивого развития и корпоративного управления. Существенный вклад в формирование исследовательской повестки в области корпоративной цифровой ответственности внесли работы, в которых КЦО рассматривается в контексте устойчивого развития и корпоративного управления.

В данных исследованиях цифровая ответственность концептуализируется как многомерный управленческий конструкт, включающий защиту данных, информационную безопасность, нормативное соответствие, управление цифровыми рисками и цифровую этику. Этот подход позволил систематизировать цифровые аспекты корпоративной ответственности и встроить их в более широкую рамку ESG-логики.

Ускоряющееся развитие цифровых технологий принципиально трансформирует характер корпоративной цифровой ответственности. Масштабирование цифровых решений на уровне распределенных логистических сетей, межорганизационных цепей поставок и платформенных экосистем переводит КЦО из преимущественно нормативной категории в операциональный фактор устойчивости. В этих условиях исследовательский фокус смещается от концептуализации цифровой ответственности к ее операционализации и измерению. Для логистических и инфраструктурных организаций становится критически важным наличие инструментов, позволяющих оценивать фактическую реализацию КЦО и ее влияние на устойчивость цепей поставок, управление рисками и стратегическое планирование [2]. Вместе с тем существующие подходы к измерению цифровой корпоративной ответственности, ориентированные на перцептивные оценки, внутрифирменные практики или агрегированные ESG-индикаторы, не позволяют адекватно отразить ее распределенный, межорганизационный и инфраструктурный характер в цепях поставок, а также зафиксировать связь цифровой ответственности с операционными рисками и устойчивостью логистических систем [3].

Указанное противоречие между практической потребностью в измеримых инструментах КЦО и ограниченной применимостью существующих академических подходов формирует выраженный практико-ориентированный исследовательский разрыв. Практическая повестка, отраженная в отчетах международных организаций и отраслевых аналитических материалах, все более явно указывает на необходимость количественной оценки цифровой ответственности как фактора киберустойчивости, управления данными и алгоритмами, а также интеграции цифровых рисков в ESG-стратегии цепей поставок [4–6]. В то же время академические исследования преимущественно сохраняют концептуальный и ESG-ориентированный фокус, не предлагая сопоставимых и операционально применимых метрик [7].

Настоящее исследование направлено на развитие измерительного подхода к корпоративной цифровой ответственности в условиях цифровой трансформации цепей поставок и логистических систем. *Объектом исследования* выступают цепи поставок и логистические системы как сложные социально-экономические системы. *Предметом исследования* является корпоративная цифровая ответственность как совокупность управленческих практик, процессов и механизмов, связанных с использованием цифровых технологий и данных и влияющих на устойчивость, управляемость рисков и надежность цепей поставок.

Источниковую базу исследования составляют академические публикации по корпоративной цифровой ответственности, устойчивому развитию и управлению цепями поставок, а также отчеты и аналитические материалы международных организаций и профессиональных сообществ, отражающие практическую

повестку цифровой трансформации, управления рисками и устойчивости логистических систем.

Авторская позиция исследования основывается на признании преемственности с существующими концептуальными моделями корпоративной цифровой ответственности, включая подходы, рассматривающие КЦО как элемент устойчивого развития и корпоративного управления. Вместе с тем утверждается, что в условиях зрелой цифровизации данных моделей недостаточно уделяется внимания анализу цепей поставок, где цифровая ответственность носит распределенный, межорганизационный и инфраструктурный характер.

Именно в этом контексте наиболее явно проявляется разрыв между декларативными формами цифровой ответственности и ее фактической реализацией в операционных и межорганизационных процессах. Данный разрыв требует перехода от концептуального осмысления КЦО к разработке многоуровневых измерительных моделей, способных связать управляемость цифровых решений, целостность цифровых процессов, распределение ответственности между участниками цепи и наблюдаемые эффекты для устойчивости логистических систем. Это и является *целью исследования* – разработка и обоснование измерительного подхода к корпоративной цифровой ответственности в цепях поставок, который позволяет рассматривать КЦО не как нормативную или декларативную категорию, а как измеримый управленческий феномен, непосредственно связанный с устойчивостью и надежностью логистических и инфраструктурных систем.

Настоящее исследование носит *методический характер* и направлено на развитие измерительного подхода к корпоративной цифровой ответственности в контексте цепей поставок; основано на проектно-ориентированной исследовательской логике и практико-ориентированной концептуализации, направленной на разработку применимой консолидированной модели измерения КЦО в цепях поставок. Отправной точкой служит выявленный в литературе и практике разрыв между растущей значимостью корпоративной цифровой ответственности для устойчивости цепей поставок и ограниченной применимостью существующих академических подходов к ее измерению. Закрытие данного разрыва требует разработки модели КЦО, способной связать цифровую ответственность с управлением данными, алгоритмической координацией, межорганизационными взаимодействиями и результатами логистической деятельности.

Методически исследование основано на сравнительном анализе четырех существующих подходов к измерению корпоративной цифровой ответственности, их оценке с точки зрения применимости к управлению цепями поставок и последующей интеграции их сильных сторон в консолидированную многоуровневую модель.

Клиентоориентированный подход рассматривает корпоративную цифровую ответственность через призму восприятия внешних стейкхолдеров, прежде всего конечных потребителей. В рамках данного направления КЦО операционализируется как латентный конструкт, измеряемый с помощью опросных шкал, отражающих воспринимаемую прозрачность, конфиденциальность, качество цифровых сервисов, механизмы реагирования на инциденты, доступность и инклю-

зивность цифровых решений [8–10]. Методически указанный подход реализуется на основе опросных методов с использованием шкал Лайкерта и стандартных процедур психометрической валидации. Его основное достоинство заключается в высокой измерительной строгости и возможности количественной фиксации социального восприятия цифровой ответственности. В контексте цепей поставок клиентоориентированный подход обладает ограниченной применимостью. Большинство ключевых проявлений цифровой ответственности в логистических системах – управление данными, алгоритмическая координация, распределение цифровых рисков – находятся вне поля прямого потребительского восприятия. В результате метрики клиентоориентированного подхода отражают лишь косвенные эффекты цифровой ответственности и не позволяют анализировать ее как операционный и межорганизационный феномен. В рамках исследования данный подход рассматривается как вспомогательный инструмент валидации внешних эффектов цифровых управленческих решений.

Процессно-ориентированный подход трактует корпоративную цифровую ответственность как совокупность управляемых практик на различных этапах жизненного цикла данных и цифровых технологий. В рамках этого направления КЦО связывается с ответственностью на этапе оцифровки данных (сбор, защита, поддержание качества) и на этапе их использования в аналитических и управленческих решениях [11]. Методически процессно-ориентированный подход опирается на анкетирование лиц, участвующих в управлении процессами, и агрегирование процессных индикаторов, отражающих практики работы с данными и алгоритмами. Его ключевым преимуществом является более высокая операционализация цифровой ответственности по сравнению с перцептивными моделями и возможность увязки КЦО с управленческими процессами. Ограничением указанного подхода в контексте цепей поставок является его преимущественно внутрифирменная направленность. Предлагаемые индикаторы фиксируют управленческие практики отдельных организаций и слабо отражают межорганизационную распределенность цифровой ответственности, платформенную координацию и системные цифровые риски, характерные для логистических сетей.

Методы оценки цифровой зрелости рассматривают корпоративную цифровую ответственность как развивающуюся управленческую способность, формирующуюся поэтапно в процессе цифровой трансформации. В рамках данного подхода акцент делается не на количественных результатах, а на степени формализации и интеграции практик ответственной цифровизации в систему корпоративного управления [12, 13]. Методически оценка цифровой зрелости реализуется через структурированную самооценку и присвоение уровней зрелости, что позволяет диагностировать текущее состояние цифрового управления и формировать дорожные карты развития. Для цепей поставок данный подход ценен своей ориентацией на управляемость сложных цифровых инфраструктур и постепенное развитие практик КЦО. Вместе с тем модели зрелости остаются ориентированными на уровень отдельной организации и не обеспечивают количественной фиксации распределенной цифровой ответственности в межорганизационных цепях поставок. Кроме того, опора на процедуры самооценки огра-

ничивает возможности объективного анализа фактических цифровых взаимодействий между участниками цепи.

ESG-ориентированный подход к оценке КЦО интегрирует корпоративную цифровую ответственность в более широкую систему устойчивого развития, используя прокси-метрики и анализ нефинансовой отчетности. В рамках данного направления цифровизация рассматривается как фактор, влияющий на экологические, социальные и управленческие показатели компаний [14–17]. Методически указанный подход опирается на контент-анализ нефинансовой отчетности и агрегированные показатели устойчивого развития, что обеспечивает институциональную легитимность и регуляторную сопоставимость результатов. Для цепей поставок это особенно важно в контексте требований к прозрачности, должной осмотрительности и управлению рисками. Ограничением ESG-подходов является их неспособность фиксировать корпоративную цифровую ответственность как операционный феномен. Высокий уровень раскрытия информации не обязательно отражает реальное качество цифровых процессов и межорганизационной координации, особенно в сложных логистических системах.

Основная часть

Проведенный анализ подходов к измерению корпоративной цифровой ответственности показывает, что в современной литературе сформировалось несколько методических линий, каждая из которых вносит значимый, но частичный вклад в оценку КЦО. Их сопоставление с задачами управления устойчивыми цепями поставок позволяет выделить три направления, обладающих наибольшей аналитической и практической релевантностью для данного контекста, тогда как четвертое направление выполняет вспомогательную, верификационную функцию.

Процессно-ориентированные подходы формируют операциональную логику КЦО, позволяя разложить цифровую ответственность на управляемые элементы, связанные с жизненным циклом данных и использованием алгоритмических инструментов. Их значимость для цепей поставок обусловлена тем, что координация материальных и информационных потоков все в большей степени осуществляется на основе данных, в то же время их преимущественно внутрифирменный фокус ограничивает анализ распределенной ответственности между участниками цепи.

Модели цифровой зрелости и инструменты внутренней оценки предлагают управленческую рамку диагностики и развития КЦО, трактуя ее как динамическую способность организации. Для цепей поставок они важны ориентацией на управляемость и поэтапное развитие цифровых практик, однако в основном ограничиваются уровнем отдельной организации и недостаточно учитывают сетевой характер цепей поставок.

ESG-ориентированные рамки обеспечивают институциональную легитимность и регуляторную сопоставимость измерения корпоративной цифровой ответственности, позволяя интегрировать КЦО в системы устойчивого развития и нефинансовой отчетности. Вместе с тем они не предназначены для операционного анализа цифровых процессов и механизмов координации в цепях поставок.

Клиентоориентированные методы, основанные на оценке восприятия цифровой ответственности внешними стейкхолдерами, не обладают достаточной операциональной глубиной для анализа цепей поставок и могут рассматриваться лишь как производный уровень, отражающий последствия цифровых управленческих решений. Необходимость перехода к консолидированному подходу обусловлена системными особенностями цепей поставок как распределенных межорганизационных систем. Усиливающаяся платформенность, асимметрия доступа к данным и алгоритмическая координация перераспределяют контроль и ответственность между участниками цепи, тогда как существующие подходы практически не предлагают прямых количественных метрик, применимых к операционным процессам, и не устраняют разрыв между уровнями управления, цифровыми процессами и фактическими результатами.

В ответ на эти ограничения в исследовании предлагается пятиуровневая модель корпоративной цифровой ответственности в цепях поставок, отражающая причинно-следственную логику формирования, реализации и проявления КЦО в условиях распределенной цифровизации. Модель исходит из предпосылки, что корпоративная цифровая ответственность не является однородным свойством организации, а формируется на пересечении управленческих механизмов, операционных цифровых процессов, межорганизационной архитектуры данных и наблюдаемых эффектов цифровизации. Выделение пяти уровней обусловлено необходимостью аналитически разделить различные формы проявления цифровой ответственности, не сводя их к единому измерению и одновременно сохраняя их логическую связанность.

Первый уровень (управление цифровыми решениями) отражает институциональные условия корпоративной цифровой ответственности и фиксирует степень управляемости и подотчетности цифровых решений в системе управления цепями поставок. Второй уровень (надежность данных и алгоритмов) описывает операциональное ядро корпоративной цифровой ответственности, связанное с качеством данных, устойчивостью алгоритмических процессов и контролируемостью автоматизированных управленческих решений. Третий уровень (ответственность за данные в цепи поставок) расширяет анализ за пределы отдельной организации и позволяет рассматривать цифровую ответственность как распределенное сетевое свойство цепи поставок, формирующееся в процессе межорганизационного обмена данными и координации цифровых решений. Четвертый уровень (цифровые риски и устойчивость цепей) связывает корпоративную цифровую ответственность с измеримыми результатами функционирования цепей поставок, включая цифрово-обусловленные риски, сбои и способность системы к восстановлению. Пятый уровень (доверие и принятие цифровых решений) выполняет верификационную функцию, отражая социальную легитимность цифровых практик и восприятие цифровых решений внешними стейкхолдерами (табл. 1).

Таким образом, пять уровней модели соответствуют ключевым аналитическим переходам: от управления к процессам, от процессов к межорганизационной архитектуре, от архитектуры к результатам и далее – к социальным эффектам цифровизации. Данное количество уровней является минимально достаточным

для одновременного учета институциональных, операционных, сетевых и результативных аспектов корпоративной цифровой ответственности; позволяет избежать как избыточной детализации, так и чрезмерной агрегации. В совокупности уровни формируют целостную аналитическую рамку, в которой корпоративная цифровая ответственность в цепях поставок может быть как концептуально описана, так и операционализирована через сочетание количественных индексов и качественных диагностических шкал.

Таблица 1

Многоуровневая консолидированная модель измерения корпоративной цифровой ответственности в цепях поставок

Название уровня	Методическая основа	Тип показателей	Что оценивается	Примеры индикаторов / метрик	Показатели в оценке КЦО в цепях поставок
Управление цифровыми решениями	Модели цифровой зрелости и ESG-ориентированные подходы	Качественные + дискретные индексы	Формализация и управляемость цифровой ответственности	Наличие data / AI политик; распределение ответственности за цифровые решения; механизмы контроля алгоритмов; процедуры инцидент-менеджмента	DGML; DGDI; DACI; AOI; DIGS
Надежность данных и алгоритмов	Процессно-ориентированный подход оценки КЦО	Количественные + процессные	Качество и надежность данных и алгоритмических процессов	Качество данных (полнота, точность, своевременность); частота инцидентов, связанных с данными; наличие процедур выявления и контроля искажений; стабильность прогнозных моделей	Доля записей с ошибками; среднее время восстановления после инцидентов, связанных с данными; волатильность ошибки прогнозирования; доля решений, принимаемых с участием человека
Ответственность за данные в цепи поставок	Gap существующих методов + логика УЦП	Количественные + структурные	Распределенная ответственность и архитектура обмена данными	Прозрачность обмена данными; симметрия доступа к данным; общие стандарты данных; платформенная зависимость	Индекс прозрачности данных цепи поставок; показатель асимметрии доступа к данным; доля стандартизированных цифровых интерфейсов

Окончание табл. 1

Название уровня	Методическая основа	Тип показателей	Что оценивается	Примеры индикаторов / метрик	Показатели в оценке КЦО в цепях поставок
Цифровые риски и устойчивость цепей поставок	ESG + управление рисками цепей поставок	Количественные	Эффекты цифровых решений для устойчивости цепей поставок	Сбои, вызванные цифровыми факторами; влияние цифровизации на устойчивость; экологические и социальные эффекты	Доля нарушений в цепи поставок, обусловленных цифровыми причинами; время восстановления после цифровых сбоев; энергоемкость цифровой инфраструктуры; показатели влияния цифровизации на занятость и условия труда
Доверие стейкхолдеров и принятие цифровых решений	Клиентоориентированный подход оценки	Перцептивные (вспомогательные)	Восприятие цифровой ответственности внешними стейкхолдерами	Уровень доверия к цифровым каналам взаимодействия; воспринимаемая прозрачность использования данных; принятие автоматизированных и алгоритмических решений как справедливых и обоснованных; готовность продолжать использование цифровых сервисов и цифровых каналов взаимодействия	Интегральный индекс доверия и принятия цифровых решений

1-й уровень. Управление цифровыми решениями

1-й уровень модели отражает институциональные условия корпоративной цифровой ответственности и характеризует степень управляемости и подотчетности цифровых решений в цепях поставок. На данном уровне цифровая ответственность трактуется как формализованная система управления, обеспечивающая распределение ответственности за цифровые решения и контроль их последствий.

Оценка осуществляется на основе совокупности ключевых механизмов цифрового управления, включая политику управления данными и AI, распределение ролей и ответственности, процедуры контроля алгоритмов и управления

цифровыми инцидентами. Для агрегирования указанных характеристик используется интегральный индекс управления цифровыми решениями, позволяющий формализовать институциональную готовность цепей поставок к реализации корпоративной цифровой ответственности и обеспечить сопоставимость результатов во времени и между организациями.

Для агрегирования показателей уровня «Управление цифровыми решениями» в рамках предлагаемой модели используется интегральный индекс цифрового управления и подотчетности, рассчитываемый как взвешенная сумма нормализованных компонент:

$$DGAI = w_1 \cdot DGML + w_2 \cdot DGDI + w_3 \cdot DACI + w_4 \cdot AOI + w_5 \cdot DIGS ,$$

где DGML (Digital Governance Maturity Level) – уровень зрелости системы цифрового управления; DGDI (Digital Governance Disclosure Index) – индекс формализации и раскрытия информации о цифровом управлении; DACI (Digital Accountability Clarity Index) – показатель четкости распределения ответственности за цифровые решения; AOI (Algorithm Oversight Index) – индекс наличия и регулярности механизмов контроля алгоритмических решений; DIGS (Digital Incident Governance Score) – показатель зрелости процедур управления цифровыми инцидентами; w_i – веса соответствующих компонент.

Компоненты индекса могут иметь различную измерительную природу. Часть показателей (в частности, уровни зрелости и наличие формализованных процедур) носит порядковый характер и предварительно нормализуется, например в интервале [0; 1], что обеспечивает сопоставимость с количественными компонентами и возможность агрегирования в единый индекс.

Выбор весов w_i может осуществляться двумя методически допустимыми способами. В базовой конфигурации допускается использование равных весов, что обеспечивает нейтральность агрегирования и делает индекс пригодным для сравнительного анализа между организациями и во времени при отсутствии приоритетов. В более продвинутых сценариях веса могут определяться экспертным методом, отражающим контекстные особенности цепей поставок, степень цифровой зрелости и профиль рисков. Экспертная калибровка весов может осуществляться, например, с использованием процедур экспертного опроса, парных сравнений или Delphi-метода.

2-й уровень. Надежность данных и алгоритмов

2-й уровень модели направлен на оценку операционной надежности процессов работы с данными и алгоритмическими системами в цепях поставок. В отличие от уровня управления цифровыми решениями, фиксирующего институциональные условия ответственности, данный уровень отражает фактическое качество и устойчивость цифровых процессов, обеспечивающих координацию цепей поставок. Корпоративная цифровая ответственность на 2-м уровне трактуется как способность организации обеспечивать корректность, устойчивость и управляемость процессов сбора, обработки и использования данных, а также алгоритмических механизмов принятия решений. Поскольку именно данные и алгоритмы лежат в основе планирования, диспетчеризации и синхронизации

потоков в цепях поставок, их надежность является ключевым условием ответственного цифрового управления.

Оценка осуществляется на основе количественных и процессных показателей. Базовым измерением выступает качество данных, которое характеризуется показателями полноты, корректности и своевременности. Оно может оцениваться через долю записей с ошибками, уровень пропусков в данных и среднюю задержку обновления информации относительно операционных процессов.

Вторым измерением является частота и управляемость цифровых инцидентов, включая ошибки данных и сбои алгоритмов. Для их оценки используется показатель среднего времени восстановления после инцидентов, позволяющий количественно зафиксировать устойчивость цифровых процессов и способность минимизировать их операционные последствия.

Отдельное измерение связано с контролем алгоритмических решений. Оно включает показатели наличия и регулярности проверок алгоритмических искажений, а также долю управленческих решений, принимаемых с участием человека. Эти показатели отражают степень сохранения управленческой ответственности в условиях автоматизации.

Дополнительным параметром надежности алгоритмических процессов является стабильность прогнозных моделей, оцениваемая через вариативность ошибок прогнозирования. Высокая изменчивость ошибок интерпретируется как признак повышенных цифровых рисков и ограниченной предсказуемости алгоритмических решений.

Для агрегирования указанных характеристик используется интегральный индекс надежности данных и алгоритмов, объединяющий нормализованные показатели качества данных, управляемости инцидентов, контроля алгоритмов и стабильности моделей. Значения данного индекса позволяют сопоставлять уровень операционной цифровой ответственности во времени и между различными участниками цепей поставок и служат эмпирической основой для анализа связи цифровых процессов с устойчивостью цепей поставок.

3-й уровень. Ответственность за данные в цепи поставок

3-й уровень направлен на оценку распределенной ответственности за данные и цифровые решения в межорганизационном пространстве цепи поставок. В отличие от предыдущих уровней, ориентированных на внутрифирменное управление и операционные процессы, данный уровень рассматривает корпоративную цифровую ответственность как сетевое свойство, формирующееся в результате взаимодействия нескольких участников, связанных общими цифровыми инфраструктурами и потоками данных.

Цифровая ответственность на 3-м уровне трактуется как характеристика архитектуры обмена данными между участниками цепи поставок, определяющая распределение цифрового контроля, рисков и подотчетности. Объектом оценки становятся не внутренние процедуры отдельных организаций, а параметры межфирменных цифровых взаимодействий, через которые осуществляется координация материальных и информационных потоков.

Ключевым измерением является прозрачность межорганизационного обмена данными, отражающая степень доступности информации о происхождении, качестве и использовании данных для различных участников цепи поставок. В операциональном выражении прозрачность может оцениваться через долю процессов, по которым данные доступны более чем одному участнику цепи, а также через степень формализации правил доступа и использования данных. На основе этих параметров может рассчитываться индекс прозрачности данных цепи поставок, позволяющий выявлять скрытые информационные асимметрии и зоны концентрации цифровых рисков.

Вторым измерением выступает симметрия доступа к данным, отражающая баланс возможностей использования цифровой информации между ключевыми участниками цепи поставок. Для ее оценки используется показатель асимметрии доступа, соотносящий объем и глубину доступа к данным у различных акторов. Высокие значения асимметрии интерпретируются как признак концентрации цифрового контроля и ответственности, характерной для платформенных конфигураций цепей поставок.

Третье измерение связано со стандартизированностью цифровых интерфейсов и данных, отражающей степень согласованности форматов, протоколов и правил обмена информацией между участниками цепи. В качестве количественного показателя используется доля стандартизированных цифровых интерфейсов в общем объеме межорганизационных цифровых взаимодействий. Низкий уровень стандартизации усиливает зависимость участников от отдельных узлов и снижает распределенность цифровой ответственности.

Отдельным параметром оценки является платформенная зависимость, характеризующая степень концентрации цифрового управления и координации в цепи поставок. Она отражает, в какой мере обмен данными и алгоритмическая координация опосредованы доминирующими цифровыми платформами, и позволяет оценить уязвимость цепи поставок к односторонним изменениям правил доступа и цифровых условий взаимодействия.

Совокупность указанных параметров формирует основу для расчета интегральных показателей межорганизационной цифровой ответственности, включая индекс прозрачности данных цепи поставок, показатель асимметрии доступа и долю стандартизированных цифровых интерфейсов. Использование данных индексов позволяет перейти от описания межфирменных цифровых связей к количественной оценке распределенной цифровой ответственности и выявить структурные источники цифровых рисков в цепях поставок.

Роль данного уровня в общей архитектуре заключается в обеспечении связи между внутрифирменной цифровой ответственностью и устойчивостью цепи поставок как целостной системы. Учет межорганизационной архитектуры данных позволяет анализировать корпоративную цифровую ответственность не как сумму индивидуальных практик, а как свойство всей цепи поставок, без чего ее измерение остается методически неполным.

4-й уровень. Цифровые риски и устойчивость цепей

4-й уровень направлен на оценку фактических последствий цифровых решений для устойчивости и надежности цепей поставок. В отличие от предыдущих уровней, фиксирующих управляемость, операционную целостность и межорганизационную архитектуру цифровой ответственности, данный уровень фокусируется на результатах: на том, как цифровизация влияет на риски, сбои и восстановительные способности цепей поставок.

Корпоративная цифровая ответственность на 4-м уровне трактуется как способность цепи поставок ограничивать негативные последствия цифровых решений и контролировать системные цифровые риски. Объектом оценки становится влияние цифровых технологий – алгоритмического планирования, автоматизации, платформенных решений и цифровой инфраструктуры – на устойчивость цепи поставок в целом.

Ключевым измерением выступает доля сбоев, вызванных цифровыми факторами. Данный показатель позволяет выделить нарушения, связанные с ошибками данных, сбоями алгоритмов, отказами цифровых платформ или некорректными автоматизированными решениями; рассчитывается как доля цифровообусловленных сбоев в общем числе зарегистрированных нарушений за анализируемый период.

Вторым важным измерением является способность цепи поставок к восстановлению после цифровых сбоев, оцениваемая через показатели времени восстановления. Эти показатели отражают совокупный эффект технической устойчивости цифровых систем и эффективности управленческих и межорганизационных механизмов реагирования. Сокращение времени восстановления интерпретируется как индикатор более высокой цифровой ответственности.

Дополнительные измерения связаны с экологическими и социальными эффектами цифровизации. Экологическое измерение включает показатели энергоемкости цифровой инфраструктуры, отражающие влияние вычислительных и телекоммуникационных ресурсов на устойчивое развитие. Социальное измерение охватывает эффекты автоматизации, включая изменение структуры занятости, перераспределение функций между человеком и цифровыми системами и трансформацию требований к квалификации персонала.

Для агрегирования указанных характеристик используется интегральный индекс цифровых рисков и устойчивости цепей, объединяющий нормализованные показатели цифровообусловленных сбоев, времени восстановления, экологической интенсивности цифровой инфраструктуры и социальных эффектов автоматизации. Применение данного индекса позволяет установить количественную связь между корпоративной цифровой ответственностью и устойчивостью цепей поставок и завершает причинно-следственную логику, связывая цифровое управление и процессы с наблюдаемыми результатами функционирования цепей поставок.

5-й уровень. Доверие и принятие цифровых решений

5-й уровень направлен на оценку восприятия и принятия цифровых решений внешними стейкхолдерами, прежде всего клиентами и пользователями логистических и инфраструктурных сервисов. В отличие от предыдущих уровней,

ориентированных на управляемость, операционные процессы, сетевую архитектуру и результативные эффекты цифровизации, данный уровень фиксирует производные социальные эффекты корпоративной цифровой ответственности, проявляющиеся на стороне внешних участников цепей поставок.

Цифровая ответственность на 5-м уровне трактуется как степень доверия к цифровым решениям и их социальной легитимности, отражающая согласованность между внутренними цифровыми практиками и внешним восприятием. Объектом анализа становятся не сами цифровые процессы, а их отражение в опыте взаимодействия клиентов и партнеров с цепью поставок в целом.

Оценка осуществляется на основе перцептивных показателей, включающих уровень доверия к цифровым сервисам, воспринимаемую прозрачность обработки данных и принятие автоматизированных и алгоритмических решений как справедливых и обоснованных. Для формализации данных характеристик используется интегральный индекс доверия и принятия цифровых решений (Digital Trust & Acceptance Index), агрегирующий нормализованные результаты опросных шкал восприятия.

В состав индекса могут входить следующие компоненты: уровень доверия к цифровым каналам взаимодействия, восприятие прозрачности использования данных, принятие автоматизированных решений в операционных процессах, готовность продолжать использование цифровых сервисов.

Агрегирование показателей осуществляется по взвешенной или равновзвешенной схеме в зависимости от исследовательских целей и доступности данных. Полученное значение индекса интерпретируется не как самостоятельная мера операционной цифровой ответственности, а как индикатор социальной валидности цифровых решений.

Роль 5-го уровня в общей архитектуре рамки носит вспомогательный и проверочный характер. Он используется для сопоставления значений индексов предыдущих уровней с их внешними проявлениями. Расхождение между высокими значениями показателей управляемости, надежности данных и межорганизационной ответственности и низкими значениями индекса доверия может свидетельствовать о коммуникационных разрывах, недостаточной прозрачности или социально значимых эффектах цифровизации, не учтенных в управленческих решениях.

Таким образом, уровень доверия и принятия цифровых решений замыкает консолидированная модель измерения КЦО, обеспечивая обратную связь между операциональной цифровой ответственностью и ее социальной легитимностью, при этом операциональный анализ не подменяется перцептивными оценками.

В совокупности представленные пять уровней образуют целостную многоуровневую модель корпоративной цифровой ответственности в цепях поставок, позволяющую перейти от нормативных и декларативных представлений о цифровой ответственности к ее операциональному, измеримому и сопоставимому анализу.

Заключение

Проведенное исследование вносит вклад в развитие теории корпоративной цифровой ответственности за счет перехода от преимущественно нормативного и концептуального понимания КЦО к ее операционализации как измеримого

управленческого феномена в цепях поставок. В работе обосновано рассмотрение цепей поставок как сложных социально-экономических систем, в которых корпоративная цифровая ответственность формируется не на уровне отдельной организации, а как распределенное сетевое свойство, возникающее в результате взаимодействия цифровых решений, данных и алгоритмов нескольких участников. Показано, что существующие подходы к измерению КЦО – потребительские, внутрифирменные и ESG-ориентированные – не позволяют адекватно зафиксировать данную распределенность и эффекты цифровой ответственности в логистических системах.

Научная новизна исследования заключается в разработке и обосновании многоуровневой модели измерения корпоративной цифровой ответственности в цепях поставок, интегрирующей управляемость цифровых решений, процессную целостность, межорганизационную архитектуру данных и результативные эффекты цифровизации. Предложенный автором подход позволяет связать корпоративную цифровую ответственность с устойчивостью, управлением цифровыми рисками и надежностью цепей поставок на основе сопоставимых индикаторов и интегральных показателей. Тем самым корпоративная цифровая ответственность впервые системно представлена как объект количественного анализа и управленческого воздействия в масштабных и высокоцифровизированных логистических и инфраструктурных системах.

Список источников

1. Гвилия Н. А. Развитие цифровых экосистем корпораций на основе интернета логистики (IoL) // Вестник Ростовского государственного экономического университета (РИНХ). 2021. № 1 (73). С. 74–81.
2. Щербаков В. В., Гвилия Н. А. Драйверы клиентоориентированности корпоративной транспортной логистики // Телескоп: журнал социологических и маркетинговых исследований. 2021. № 1. С. 145–149. DOI: 10.51692/1994-3776_2021_1_145
3. Силкина Г. Ю., Пэн Юэ, Ливинцова М. Г. Управление цифровой корпоративной ответственностью в контексте устойчивого развития // Научный журнал НИУ ИТМО. Серия: Экономика и экологический менеджмент. 2025. № 1. С. 60–70. DOI: 10.17586/2310-1172-2025-18-1-60-70
4. OECD. Global Forum on Digital Security for Prosperity. OECD; 10–11 July 2024. Swiss Grand Hotel, Seoul, Korea. Hybrid event. URL: https://www.oecd-events.org/e/global-forum-digital-security-for-prosperity (дата обращения: 20.12.2025).
5. OECD. Recommendation of the Council on Digital Security Risk Management. OECD/LEGAL/0479. Adopted 26 Sep. 2022. URL: https://legalinstruments.oecd.org/en/-instruments/OECD-LEGAL-0479 (дата обращения: 21.01.2026).
6. World Economic Forum. Global Cybersecurity Outlook 2025. URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/ (дата обращения: 20.01.2026).
7. Гвилия Н. А. Концепция корпоративной цифровой ответственности в управлении мезологистическими системами // Вестник Астраханского государственного технического университета. Серия: Экономика. 2021. № 3. С. 88–101.
8. Asa Romeo Asa, Johanna Pangeiko Nautwima. Corporate digital responsibility and consumer trust: a signaling theory perspective // Cogent Business & Management. 2025. Т. 13, № 1. URL: 10.1080/23311975.2025.2607753

9. Fazli M. Measuring the scale development and validation of corporate digital responsibility from a consumer perspective // Digital Economy and Sustainable Development. 2025. URL: https://doi.org/10.1007/s44265-025-00067-4
10. Scale development and validation of corporate digital responsibility: A consumer perspective / P. Yang, C. Ji, C. Prentice [et al.] // International Journal of Consumer Studies. 2025. DOI: 10.1111/ijcs.70023
11. Cheng C., Zhang M. Conceptualizing Corporate Digital Responsibility: A Digital Technology Development Perspective // Sustainability. 2023. Vol. 15, No. 3, Art. 2319. DOI: 10.3390/su15032319
12. Carl K., Hauer M., Arnold T. Are We Still on Track with Our Responsibility Strategy? // Introducing an Internal Assessment of Corporate Digital Responsibility Engagement. 2024. P. 1573–1585. URL: https://doi.org/10.18420/inf2024_137
13. Rugeviciute A., Courboulay V. Empowering Organizations for Sustainable Digitalization: a Corporate Digital Responsibility Maturity Model Approach //10th International Conference on ICT for Sustainability (ICT4S). 2024. P. 87–98. URL: https://doi.org/10.1109/ict4s64576.2024.00018
14. Jawad Abbas. When and how corporate digital responsibility contributes to a firm's reputation in society: Scale development and structural analysis // Technology in Society. 2026. No. 84. URL: 10.1016/j.techsoc.2025.103067
15. Corporate digital responsibility / L. Lobschat, B. Mueller, F. Eggers [et al.] // Journal of Business Research. 2021. Vol. 122. P. 875–888. DOI: 10.1016/j.jbusres.2019.10.006
16. Merbecks U. Corporate digital responsibility (CDR) in Germany: background and first empirical evidence from DAX 30 companies in 2020 // J Bus Econ. 2024. № 94. P. 1025–1049. URL: https://doi.org/10.1007/s11573-023-01148-6
17. Mueller B. Corporate Digital Responsibility // Bus Inf Syst Eng. 2022. № 64. P. 689–700. URL: https://doi.org/10.1007/s12599-022-00760-0

References

1. Gviliya N. A. Development of Digital Ecosystems of Corporations Based on the Internet of Logistics (IoL). *Bulletin of the Rostov State University of Economics (RINH).* 2021; 1 (73): 74–81.
2. Shcherbakov V. V., Gviliya N. A. Drivers of corporate transport logistics customer orientation. *Telescope: Journal of Sociological and Marketing Research*. 2021; (1): 145–149. DOI: 10.51692/1994-3776_2021_1_145
3. Silkina G. Yu., Pen Yue, Livintsova M. G. Managing digital corporate responsibility in the context of sustainable development. *Scientific Journal of NRU ITMO. Series: Economics and Environmental Management.* 2025; (1): 60–70. DOI: 10.17586/2310-1172-2025-18-1-60-70
4. OECD. Global Forum on Digital Security for Prosperity. OECD, 2024. July 10–11, Swiss Grand Hotel, Seoul, Republic of Korea. Hybrid event. URL: https://www.oecd-events.org/e/global-forum-digital-security-for-prosperity (accessed date: 2012.2025).
5. OECD. Recommendation of the Council on Digital Security Risk Management. OECD/LEGAL/0479. Adopted 26 September 2022. URL: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0479 (accessed date: 21.01.2026).
6. World Economic Forum. Global Cybersecurity Outlook 2025. World Economic Forum, 2025. URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/ (accessed date: 20.01.2026).

7. Gviliya N. A. The concept of corporate digital responsibility in the management of mesological systems. *Bulletin of the Astrakhan Gos. tech. University. Series: Economics*. 2021; (3): 88–101. DOI: 10.24143/2073-5537-2021-3-88-101
8. Asa Romeo Asa, Johanna Pangeiko Nautwima. Corporate digital responsibility and consumer trust: a signaling theory perspective. *Cogent Business & Management*. 2025; 13 (1). URL: 10.1080/23311975.2025.2607753
9. Fazli M. (2025). Measuring the scale development and validation of corporate digital responsibility from a consumer perspective. *Digital Economy and Sustainable Development*. 2025. URL: https://doi.org/10.1007/s44265-025-00067-4
10. Scale development and validation of corporate digital responsibility: A consumer perspective / P. Yang, C. Ji, C. Prentice [et al.]. *International Journal of Consumer Studies.* 2025. DOI: 10.1111/ijcs.70023
11. Cheng C., Zhang M. Conceptualizing Corporate Digital Responsibility: A Digital Technology Development Perspective. *Sustainability*. 2023; 15 (3 (2319)). DOI: 10.3390/su15032319
12. Carl K., Hauer M., Arnold T. Are We Still on Track with Our Responsibility Strategy? *Introducing an Internal Assessment of Corporate Digital Responsibility Engagement*. 2024: 1573–1585. URL: https://doi.org/10.18420/inf2024_137
13. Rugeviciute A., Courboulay V. (2024). Empowering Organizations for Sustainable Digitalization: a Corporate Digital Responsibility Maturity Model Approach. *10th International Conference on ICT for Sustainability (ICT4S).* 2024: 87–98. URL: https://doi.org/10.1109/ict4s64576.2024.00018
14. Jawad Abbas. When and how corporate digital responsibility contributes to a firm's reputation in society: Scale development and structural analysis. *Technology in Society*. 2026; (84). URL: 10.1016/j.techsoc.2025.103067
15. Corporate digital responsibility / L. Lobschat, B. Mueller, F. Eggers [et al.]. *Journal of Business Research*. 2021; (122): 875–888. DOI: 10.1016/j.jbusres.2019.10.006
16. Merbecks U. Corporate digital responsibility (CDR) in Germany: background and first empirical evidence from DAX 30 companies in 2020. *J Bus Econ.* 2024; (94): 1025–1049. URL: https://doi.org/10.1007/s11573-023-01148-6
17. Mueller B. Corporate Digital Responsibility. *Bus Inf Syst Eng.* 2022; (64): 689–700. URL: https://doi.org/10.1007/s12599-022-00760-0

Информация об авторе:

Гвилия Наталья Алексеевна, д-р экон. наук, профессор каф. логистики и управления цепями поставок, ФГБОУ ВО «Санкт-Петербургский государственный экономический университет», Санкт-Петербург, natagvi@mail.ru

DOI: https://doi.org/10.29039/2949-1258/2026-1/045-061
EDN: https://elibrary.ru/XEWASO

Дата поступления:	Одобрена после рецензирования:	Принята к публикации:
04.02.2026	12.02.2026	16.02.2026