

УДК: 502.131.1

DOI: 10.17586/2310-1172-2025-18-1-60-70

Научная статья

Язык статьи – русский

## Управление цифровой корпоративной ответственностью в контексте устойчивого развития

*Д-р экон. наук, профессор* Силкина Г.Ю. [silkina\\_gyu@spbstu.ru](mailto:silkina_gyu@spbstu.ru)

Пэн Юэ [pen.yu@edu.spbstu.ru](mailto:pen.yu@edu.spbstu.ru)

*Канд. экон. наук, доцент* Ливинцова М.Г. [livintsova\\_mg@spbstu.ru](mailto:livintsova_mg@spbstu.ru)

*Санкт-Петербургский политехнический университет Петра Великого  
195251, Россия, Санкт-Петербург, ул. Политехническая, д. 29, лит. Б*

*Исследование направлено на выявление основных аспектов цифровой корпоративной ответственности и разработку модели для оценки ее влияния на развитие компании. Оно фокусируется на цифровых и управленческих процессах, включая безопасность данных, конфиденциальность, нормативное соответствие и цифровую этику. Предлагается метод оценки цифровой ответственности с помощью количественных показателей, что способствует системному управлению и может улучшить операционную эффективность и рыночный имидж компании. Новизна исследования заключается в предложении интегративного подхода к оценке цифровой ответственности, включающего методы количественного анализа влияния корпоративной цифровой ответственности на устойчивое развитие. Полученные результаты могут стать основой для разработки корпоративных стратегий, направленных на долгосрочное устойчивое развитие, обеспечивая компаниям необходимые инструменты для адаптации в условиях цифровой трансформации и повышения их конкурентоспособности.*

**Ключевые слова:** устойчивое развитие, корпоративная социальная ответственность, цифровая трансформация, цифровая корпоративная ответственность, цифровые технологии.

### Ссылка для цитирования:

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.

Scientific article

Article in Russian

## Digital corporate responsibility management in the context of sustainable development

*D.Sc.* Silkina G.Yu. [silkina\\_gyu@spbstu.ru](mailto:silkina_gyu@spbstu.ru)

Peng Y. [pen.yu@edu.spbstu.ru](mailto:pen.yu@edu.spbstu.ru)

*Ph.D.* Livintsova M.G. [livintsova\\_mg@spbstu.ru](mailto:livintsova_mg@spbstu.ru)

*Peter the Great St. Petersburg Polytechnic University  
195251, Russia, St. Petersburg, Polytechnicheskaya, 29 B*

*The study aims to identify the main aspects of digital corporate responsibility and develop a model for assessing its impact on company development. It focuses on digital and management processes, including data security, privacy, regulatory compliance, and digital ethics. A method for evaluating digital responsibility using quantitative indicators is proposed, which contributes to systematic management and can improve operational efficiency and the market image of the company. The novelty of the research lies in the proposal of an integrative approach to assessing digital responsibility, incorporating methods of quantitative analysis of the impact of digital corporate responsibility on sustainable development. The results obtained can serve as a foundation for developing corporate strategies aimed at*

*long-term sustainable development, providing companies with the necessary tools to adapt to the conditions of digital transformation and enhance their competitiveness.*

**Keywords:** sustainable development, corporate social responsibility, digital transformation, digital corporate responsibility, digital technologies.

**For citation:**

Silkina G.Yu., Peng Y., Livintsova M.G. Digital corporate responsibility management in the context of sustainable development. *Scientific journal NRU ITMO. Series «Economics and Environmental Management»*. 2025. № 1. P. 60–70. DOI: 10.17586/2310-1172-2025-18-1-60-70.

---

## Введение

Концепция устойчивого развития и содержание ее практической реализации в последние десятилетия привлекают внимание ученых-теоретиков и бизнес-сообщества. Появившиеся в 1970-х идеи устойчивого развития концентрируют внимание на обеспечении способности человечества поддерживать свой прогресс в будущем. Само понятие постоянно развивается: сосредоточенная изначально на экологических аспектах концепция достаточно быстро эволюционировала до модели ЗР – People, Planet, Profit (люди, планета, прибыль). С формированием цифровой экономики понятие «корпоративная ответственность» приобретает цифровые составляющие, получает новое звучание, включая аспекты устойчивого развития и вызовы цифровой трансформации. В связи с растущими ожиданиями общества и регуляторов компании должны учитывать влияние своих цифровых операций на общество и окружающую среду. Управление корпоративной цифровой ответственностью помогает минимизировать экологический ущерб, укреплять доверие потребителей и повышать прозрачность бизнеса, способствуя устойчивому будущему.

В современном мире, где информация распространяется мгновенно, а технологии постоянно эволюционируют, корпорации сталкиваются с необходимостью переосмысления своей роли в обществе. Это переосмысление включает в себя не только стремление к прибыльности, но и ответственность перед заинтересованными сторонами: клиентами, сотрудниками и обществом в целом. Таким образом, корпоративная цифровая ответственность становится ключевым элементом стратегического планирования и развития бизнеса.

Для эффективного управления корпоративной цифровой ответственностью, компании должны внедрять комплексные подходы, включающие в себя как внутренние процессы, так и взаимодействие с внешним миром. Это означает разработку и внедрение этических кодексов, которые регламентируют использование цифровых технологий, а также активное вовлечение в диалог с общественностью и регулирующими органами. Такие меры способствуют созданию доверительных отношений и укреплению репутации компании в долгосрочной перспективе.

Кроме того, важно отметить, что корпоративная цифровая ответственность не ограничивается только этическими аспектами. Она также включает в себя вопросы обеспечения информационной безопасности, защиты данных и предотвращения цифрового неравенства. Компании должны стремиться к созданию инклюзивных цифровых решений, которые доступны для всех слоев населения, и таким образом способствовать социальному прогрессу и устойчивому развитию.

## Методы анализа

В ходе настоящего исследования использовались следующие методы: анализ литературы, системный анализ, сравнительный анализ и математическое моделирование. Метод анализа литературы позволил систематизировать существующие подходы к корпоративной цифровой ответственности и методологии её оценки. Были исследованы научные работы, касающиеся цифровой трансформации, устойчивого развития и управления рисками, что сформировало теоретическую базу для построения модели. Системный анализ использовался для структурирования ключевых элементов корпоративной цифровой ответственности: цифровая безопасность, конфиденциальность данных, управление рисками и соответствие нормативным требованиям.

При разработке модели оценки корпоративной цифровой ответственности применялся сравнительный анализ, что обеспечило возможность выявления особенностей подходов, используемых в разных отраслях и компаниях. На этапе количественного анализа использовались математические методы, подробно изложенные в книге Королёва А.В. «Экономико-математические методы и моделирование» [Ошибка! Источник ссылки не найден.]. Эти методы позволили преобразовать субъективные показатели, такие как уровень прозрачности и соблюдения этических норм, в цифровые индикаторы, что сделало возможным их объективное измерение. Такой подход способствовал получению точных количественных результатов, которые легли в основу выводов

исследования.

### Обзор литературы

По исследованию Камашевой М.Г., идеи устойчивости зародились в 70-80-е гг. XX века. В 1968 году американский эколог и философ Гаррет Хардин опубликовал эссе под названием «Трагедия общин» [**Ошибка! Источник ссылки не найден.**]. В 1972 году Римский клуб пригласил американских учёных Донеллу Медоуз, Денниса Медоуз, Йоргена Рандерса и Уильяма Беренса III для проведения компьютерного моделирования, целью которого было предсказать возможные последствия при ограниченных ресурсах Земли. Итогом их работы стал доклад «Пределы роста» [**Ошибка! Источник ссылки не найден.**].

В 1987 году Организация Объединенных Наций представила доклад «Наше общее будущее» [**Ошибка! Источник ссылки не найден.**], в котором была обозначена идея устойчивого развития человечества – обеспечение сохранности всего, что необходимо для удовлетворения жизненных потребностей будущих поколений, то есть всего, что мы сами желаем иметь. Концепция устойчивого развития превратилась в международную идеологию и была признана мировым сообществом, начиная с этого отчета.

Среди ключевых аспектов модернизации экономики, где это четко видно, выделяется устойчивое развитие. По данным ООН, Россия повысила свои позиции в мировом рейтинге устойчивого развития и выполнения целей устойчивого развития (ЦУР) с 63-го места (68,9 баллов) в 2018 году до 45-го места (74,1 балла) в 2022 году [**Ошибка! Источник ссылки не найден.**].

Концепция корпоративной социальной ответственности (КСО) восходит к началу 20 века, когда компании начали осознавать свое влияние на общество и окружающую среду. В 1953 году Г. Боуэн в своей книге «Социальная ответственность бизнесмена» предложил концепцию корпоративной социальной ответственности, подчеркивая, что компании должны брать на себя ответственность перед обществом [**Ошибка! Источник ссылки не найден.**].

Корпоративная социальная ответственность играет ключевую роль в современном бизнесе и тесно связана с устойчивым развитием компаний. Кузьмина Е. Ю. отметила, что КСО имеет важное значение в управлении предприятием [**Ошибка! Источник ссылки не найден.**]: сохранение конкурентоспособности и долгосрочных преимуществ; удовлетворение потребностей всех заинтересованных сторон; укрепление имиджа компании и узнаваемости бренда; как основное конкурентное преимущество; финансовая устойчивость и рыночная позиция; социальная и экологическая ответственностью и т.д.

В статье Заводчиковой Т.Б. «Корпоративная социальная ответственность как интегральная составляющая российского бизнеса» [**Ошибка! Источник ссылки не найден.**] автор приводит пропорции ожиданий общества от соблюдения компаниями принципов социальной ответственности и указывает на различные аспекты интеграции социальной ответственности в стратегию бизнеса. Из этих данных мы можем увидеть важность корпоративной социальной ответственности и направления ее приоритетов.

Корпоративная цифровая ответственность (КЦО) – это новое понятие, возникшее на основе корпоративной социальной ответственности в контексте цифровой трансформации, и оно отражает социальную ответственность компаний в области цифровых активов. В статье «Корпоративная социальная ответственность в контексте цифровой трансформации» упоминается, что корпоративная цифровая ответственность появилась в результате развития и применения цифровых технологий. Она расширяет рамки ответственности компании, учитывая этические возможности и проблемы, возникающие в процессе цифровизации. Согласно содержанию статьи, корпоративная цифровая ответственность может быть понята как обязательства компании в продвижении технологического развития и использовании технологий для привлечения граждан и предоставления услуг.

В статье «Стратегии устойчивого развития бизнеса в условиях цифровой экономики» Шайдуллин А. Ф. указывает на процесс цифровой трансформации бизнес-процессов, отмечая, что цифровая трансформация приводит к увеличению производительности компании почти на 32%. Цифровая трансформация также повышает конкурентоспособность предприятий, в среднем компании получают прирост доходов на 37% благодаря цифровой трансформации. Автор считает, что в таких условиях управление корпоративной социальной ответственностью, особенно в области цифровой ответственности, становится особенно важным. В новом рынке цифровой экономики существуют как возможности, так и вызовы; эффективное использование цифровой трансформации, развитие цифровых управленческих способностей и реализация социальной ответственности позволят компаниям занять выгодные позиции.

На фоне быстрого расширения глобального рынка цифровой безопасности компаниям необходимо уделять больше внимания цифровой ответственности, что не только связано с репутацией компании, но и является ключом к достижению долгосрочных стратегических целей. Создание совершенной системы цифровой ответственности делает компании конкурентоспособными. Ниже представлена информация, опубликованная организацией Precedence Research, о размере, доле и тенденциях рынка кибербезопасности с 2024 по 2034 год.

Данные показывают, что доля рынка цифровой безопасности для предприятий ежегодно увеличивается, и к 2034 году она достигнет 878 миллионов долларов. Эта тенденция указывает на то, что важность цифровой ответственности для предприятий будет расти из года в год.

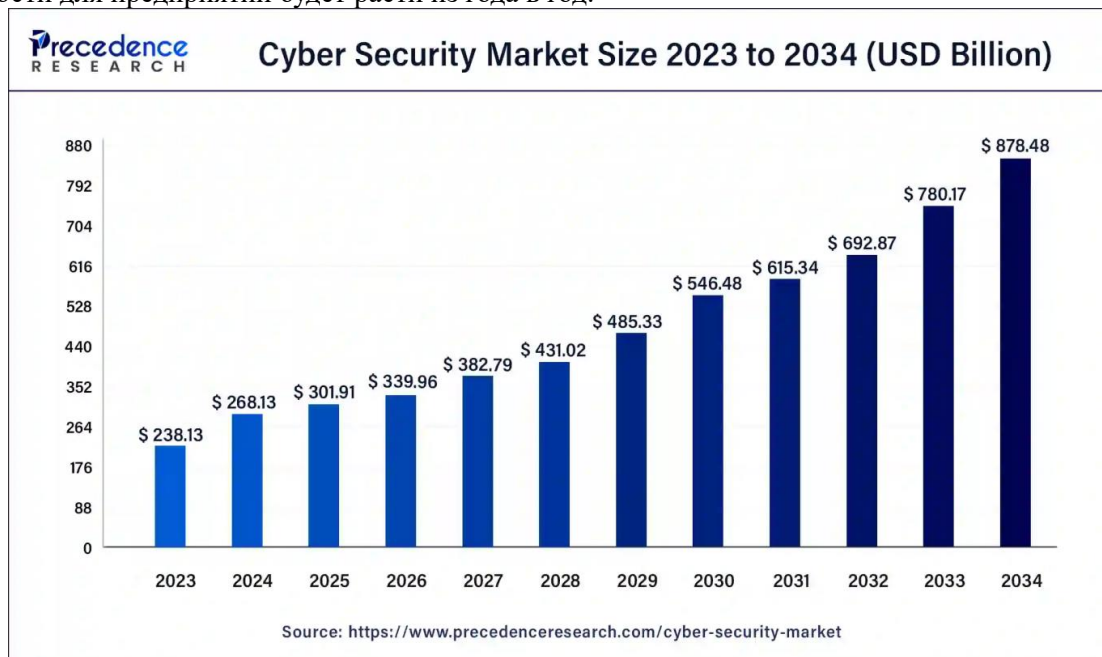


Рис. 1. Размер, доля и тенденции рынка кибербезопасности с 2024 по 2034 год

### Необходимость и содержание управления цифровой ответственностью

Анализ исследований Гвилия Н.А. [**Ошибка! Источник ссылки не найден.**], Арнаутовой В.А. [**Ошибка! Источник ссылки не найден.**], Плешко ЕА. и других приводят к выводу о том, что цифровая ответственность компаний включает следующие аспекты.

**Цифровая безопасность.** Компании в цифровую эпоху несут ответственность за обеспечение безопасности своих информационных систем и данных. Они обязаны принимать эффективные меры для предотвращения несанкционированного доступа и утечек данных, чтобы защитить конфиденциальность пользователей и корпоративные секреты, а также поддерживать интересы и доверие всех сторон.

**Юридическая ответственность.** Компании должны строго соблюдать все применимые законы и нормативные акты, обеспечивая законность и соответствие своих цифровых действий, чтобы избежать юридических санкций за правонарушения и нести соответствующую юридическую ответственность.

**Ответственность за раскрытие информации.** Компании обязаны раскрывать общественности и заинтересованным сторонам правдивую, точную и полную информацию о своих цифровых действиях, чтобы обеспечить прозрачность информации, позволяя всем сторонам принимать обоснованные решения, и нести ответственность за ненадлежащее раскрытие информации.

**Управление цифровыми рисками.** Компании должны уделять внимание управлению рисками цифровой экономики и цифровых активов, проводить детальную оценку рисков для обеспечения устойчивого развития своего цифрового бизнеса.

**Ответственность за использование цифровых ресурсов.** Компании при использовании и разработке цифровых ресурсов должны учитывать принципы устойчивого развития, разумно распределять ресурсы, снижать негативное воздействие на окружающую среду и обеспечивать долгосрочную доступность и устойчивость цифровых ресурсов.

**Ответственность за инновации в цифровых технологиях.** Компании должны активно продвигать инновации в цифровых технологиях, увеличивать инвестиции в исследования и разработки, а также развивать профессиональные кадры, чтобы сохранять лидирующие позиции в отрасли.

**Ответственность за удовлетворение цифровых потребностей общества.** Компании должны активно реагировать на ожидания общества в отношении цифровых технологий, предоставляя высококачественные цифровые продукты и услуги через инновации и технологический прогресс, удовлетворяя потребности общества в цифровых технологиях и способствуя цифровой трансформации и прогрессу.

**Этическая ответственность в цифровой сфере.** Компании, осуществляя цифровую деятельность, должны

следовать этическим нормам, предотвращая злоупотребление технологиями и этические риски, неся ответственность за нарушения этических норм, чтобы гарантировать, что технологические инновации приносят пользу обществу, а не становятся источником социальных проблем.

Внедрение цифровой ответственности имеет решающее значение для достижения целей устойчивого развития. Это не только помогает компаниям оставаться на переднем крае технологических инноваций, но и способствует социальной инклюзии и охране окружающей среды. Анализ важности корпоративной цифровой ответственности в управлении устойчивым развитием предприятий представлен в таблице 1.

Таблица 1

**Основные аспекты корпоративной цифровой ответственности**

Важность	Описание
Обеспечение безопасного использования цифровых технологий	Цифровая ответственность бизнеса требует от компаний обеспечения безопасности технологий и защиты человеческой безопасности при использовании цифровых технологий, чтобы избежать причинения вреда как отдельным лицам, так и обществу
Содействие устойчивому социальному и экономическому развитию	Цифровая ответственность бизнеса требует от компаний обеспечения безопасности технологий и защиты человеческой безопасности при использовании цифровых технологий, чтобы избежать причинения вреда как отдельным лицам, так и обществу
Поддержание репутации компании и ценности бренда	Практика цифровой ответственности бизнеса способствует улучшению социального имиджа компании, укреплению доверия со стороны потребителей и инвесторов, что, в свою очередь, помогает поддерживать репутацию и ценность бренда компании
Управление рисками	Цифровая ответственность бизнеса требует от компаний выявления и управления рисками, связанными с цифровыми технологиями, включая безопасность данных и защиту конфиденциальности, что помогает снизить потенциальные юридические и репутационные риски
Стимулирование инноваций и конкурентных преимуществ	Принятие цифровой ответственности предприятия может способствовать инновациям, позволяя компаниям разрабатывать цифровые продукты и услуги, соответствующие социальным потребностям, что открывает новые рыночные возможности и конкурентные преимущества
Управление отношениями с заинтересованными сторонами	Цифровая ответственность предприятия помогает устанавливать и поддерживать хорошие отношения с заинтересованными сторонами, включая клиентов, поставщиков, сообщества и государственные органы, что имеет решающее значение для долгосрочного успеха компании
Стимулирование практик устойчивого развития внутри компании	Цифровая ответственность требует от предприятий внедрения принципов устойчивого развития в их внутреннее управление, таких как этическое поведение и уважение прав человека, что способствует формированию культуры устойчивого развития внутри компании

Для более четкого понимания ключевых элементов управления цифровой ответственностью, представлена таблица, в которой описаны основные требования к управлению в этой области.

Таблица 2

**Ключевые элементы управления цифровой ответственностью**

Элемент	Цифровая безопасность	Методы контроля	Показатели оценки
Цифровая безопасность	Защита цифровых активов компании (таких как данные, системы и сети) с помощью многоуровневых механизмов от несанкционированного доступа, кибератак, утечек данных и других инцидентов безопасности	<ul style="list-style-type: none"> <li>- Внедрение многофакторной аутентификации и политики использования сложных паролей</li> <li>- Регулярное проведение сканирования уязвимостей и тестирования на проникновение</li> <li>- Применение новых технологий шифрования и распределенного хранения данных</li> </ul>	<ul style="list-style-type: none"> <li>- Количество инцидентов утечки данных</li> <li>- Уровень обнаружения уязвимостей системы</li> <li>- Процент успешного прохождения тестов на проникновение</li> </ul>
Раскрытие информации	Публикация для заинтересованных сторон цифровых политик, соответствия нормативным требованиям и мер управления информацией для обеспечения прозрачности и своевременности коммуникации, что способствует укреплению доверия	<ul style="list-style-type: none"> <li>- Регулярный выпуск отчетов о раскрытии информации, соответствующих международным стандартам</li> <li>- Открытая публикация информации об управлении данными и защите конфиденциальности</li> <li>- Соблюдение региональных и международных законов и нормативных требований</li> </ul>	<ul style="list-style-type: none"> <li>- Оценка соответствия отчетов стандартам раскрытия</li> <li>- Частота ежегодных раскрытий</li> <li>- Удовлетворенность заинтересованных сторон обратной связью</li> </ul>
Конфиденциальность данных	Защита персональных данных пользователей и клиентов, соблюдение принципов минимизации данных и конфиденциальности, обеспечение безопасности и соответствия требованиям конфиденциальности.	<ul style="list-style-type: none"> <li>- Проведение оценок влияния на конфиденциальность и оценок влияния на защиту данных</li> <li>- Полный охват данных шифрованием</li> <li>- Введение стратегии классификации и контроля доступа к данным</li> </ul>	<ul style="list-style-type: none"> <li>- Количество случаев утечки данных</li> <li>- Доля зашифрованных персональных данных</li> </ul>
Соответствие требованиям	Соблюдение отраслевых, региональных и международных правовых норм (таких как GDPR, ССРА и др.) для обеспечения законности и соблюдения цифровых операций компании.	<ul style="list-style-type: none"> <li>- Регулярные внутренние и сторонние аудиты соответствия требованиям</li> <li>- Проведение обучения сотрудников по вопросам соответствия и повышения осведомленности</li> <li>- Разработка процессов управления и проверки соблюдения нормативных требований</li> </ul>	<ul style="list-style-type: none"> <li>- Количество нарушений, выявленных аудитом</li> <li>- Процент сотрудников, успешно прошедших тесты по знанию норм</li> <li>- Скорость реакции на изменения в законодательстве</li> </ul>
Управление рисками	Систематическое выявление, оценка и управление цифровыми рисками, предотвращение киберугроз, утечек данных и сбоев в системе.	<ul style="list-style-type: none"> <li>- Внедрение структуры управления рисками (например, COSO или ISO 31000)</li> <li>- Регулярное обновление и тестирование планов реагирования на риски</li> </ul>	<ul style="list-style-type: none"> <li>- Время реагирования на инциденты</li> <li>- Оценка эффективности мер по контролю рисков</li> <li>- Снижение числа инцидентов в год</li> </ul>

		- Проведение тренировок по управлению непрерывностью бизнеса	
--	--	--	--

Окончание табл. 2

Элемент	Цифровая безопасность	Методы контроля	Показатели оценки
Непрерывный мониторинг	Круглосуточный мониторинг цифровой среды компании для выявления и анализа подозрительных действий, обеспечение быстрого обнаружения и реакции на угрозы.	- Развертывание системы управления информационной безопасностью и событиями - Организация 24/7 центра по обнаружению угроз - Регулярный пересмотр и обновление политики мониторинга	- Среднее время реакции на инциденты - Уровень обнаружения инцидентов безопасности - Оценка соответствия стандартам проверки журналов
Обучение сотрудников	Повышение осведомленности и навыков сотрудников в области защиты данных и цифровой ответственности для снижения риска ошибок и внутренних угроз.	- Регулярные тренинги по кибербезопасности и навыкам в этой сфере - Проведение учений по предотвращению атак - Введение системы поощрений и наказаний в сфере цифровой безопасности	- Охват сотрудников обучением - Уровень успешного обнаружения атак - Средний балл по тестам знаний после обучения
Способность к цифровым инновациям	Повышение конкурентоспособности компании в цифровой трансформации за счет реализации инновационных проектов и инвестиций в НИОКР.	- Увеличение бюджета на исследования и разработки - Создание лабораторий для инноваций и команд цифровых разработок - Регулярная оценка хода инновационных проектов и успешности преобразования их в реальные результаты	- Количество проектов цифровых инноваций - Вклад дохода от технологических инноваций - Процент успешной трансформации инновационных результатов

Эти элементы представляют собой основы, на которых строится управление цифровой ответственностью. Они позволяют компаниям адаптироваться к современным требованиям, минимизируя риски и укрепляя свой имидж.

### Составляющие и оценка цифровой ответственности

Ссылаясь на методы, описанные в книге «Экономико-математические методы и моделирование» [Ошибка! Источник ссылки не найден.3] компания должна учитывать свои реальные условия при разработке показателей оценки и методов оценки для каждого элемента, используя показатели оценки из таблицы 2 выше для оценки выполнения каждого элемента.

Например, элемент цифровой безопасности можно оценить следующими методами (табл. 3).

Таблица 3

### Оценка элемента «цифровая безопасность»

Показатели оценки	Цель	Вес	Формула расчета показателя
Количество инцидентов утечки данных	0	0,4	$\max(0, 100 - \frac{(\text{Фактическое значение} - \text{цель})}{2} \times 100)$

Уровень обнаружения уязвимостей системы	95%	0,3	$\min(100, \frac{\text{Фактическое значение}}{\text{Цель}} \times 100)$
Процент успешного прохождения тестов на проникновение	90%	0,3	$\min(100, \frac{\text{Фактическое значение}}{\text{Цель}} \times 100)$

$$C_{\text{Цифровая безопасность}} = 0,4 \times C_{\text{Утечка данных}} + 0,3 \times C_{\text{Обнаружения уязвимостей системы}} + 0,3 \times C_{\text{Прохождения тестов}}$$

Этот алгоритм количественно обрабатывает несколько оценочных показателей цифровых элементов безопасности, что позволяет получить оценку этого элемента в диапазоне от 0 до 100. Компания может в зависимости от конкретной ситуации разрабатывать различные формулы оценки и использовать разные целевые значения для проведения оценки.

После завершения оценки алгоритма соответствующих элементов необходимо распределить веса для каждого элемента, суммировать оценки по всем проектам и получить общий балл выполнения цифровой ответственности компании. При установлении целевого балла следует учитывать средние показатели по отрасли, вычислить балл на уровне отрасли и сравнить его с баллом компании. Если у компании есть соответствующие потребности, можно повысить балл, который будет служить целевым объектом, чтобы достичь сравнимого значения, соответствующего потребностям компании.

Обобщения данных о выполнении цифровой ответственности нескольких компаний [14, 15], обосновывает следующее распределение весов:

- цифровая безопасность – 0, 2;
- раскрытие информации – 0, 15;
- конфиденциальность данных – 0,2;
- соответствие требованиям – 0,15;
- управление рисками – 0,1;
- постоянный мониторинг – 0,1;
- обучение сотрудников – 0,05;
- способности к цифровым инновациям – 0,05.

Компания может немного скорректировать веса в зависимости от своих реальных потребностей.

После завершения оценки компания может создать визуальный отчет в виде радарной диаграммы.

Примером может служить китайская компания IPСВА (ООО Шэньчжэньская компания Шоухэн Текнолоджи) [Ошибка! Источник ссылки не найден.], основным направлением которой является проектирование, производство и взлом печатных плат. Согласно данным, предоставленным менеджерами и результатам анализа соответствующих подразделений компании, после обработки данных была составлена таблица 4.

Таблица 4

#### Результатов оценки компании

Элемент	Вес	Оценка	Цель
Цифровая безопасность	0,2	87,45	80
Раскрытие информации	0,15	65,40	70
Конфиденциальность данных	0,2	89,34	70
Соответствие требованиям	0,15	73,23	80
Управление рисками	0,1	44,87	75
Постоянный мониторинг	0,1	89,86	70
Обучение сотрудников	0,05	91,34	75
Способности к цифровым инновациям	0,05	67,57	75

Компания получила окончательную оценку: Сумма(Оценка × Вес) = 77.57; целевая оценка составила: 74.5. Оценка компании выше целевой оценки, выполнение цифровых обязательств компанией находится на



хорошем уровне.

Сформирована следующая диаграмма (рис. 2).



Рис. 2. Визуализация результатов оценки: радиальная диаграмма

На диаграмме можно наглядно увидеть, что компания хорошо справляется с такими аспектами, как Цифровая безопасность, Конфиденциальность данных, Постоянный мониторинг и Обучение сотрудников. Однако в таких областях, как Раскрытие информации, Соответствие требованиям и Способности к цифровым инновациям, показатели ниже среднего уровня, а в Управлении рисками ситуация худшая. В будущем компании следует скорректировать свою стратегию в области устойчивого развития и управления цифровой ответственностью, уделяя особое внимание недостаткам в нескольких аспектах, а также провести дальнейший анализ и исправление в области Управления рисками.

### Заключение

В данном исследовании применен комплексный подход к оценке влияния цифровой ответственности компании на устойчивое развитие, охватывающий такие процессы управления, как обеспечение безопасности данных, защита конфиденциальности, соблюдение нормативных требований и цифровая этика. С помощью методов количественного анализа предложена модель для оценки влияния цифровой ответственности, что способствует систематизации управления и повышению операционной эффективности и рыночного имиджа компании.

Научный результат работы заключается в разработке метода оценки цифровой ответственности, который включает количественный подход для измерения её влияния на устойчивое развитие. Эти результаты предоставляют инструменты для формирования долгосрочной стратегии устойчивого развития компании, что помогает повысить конкурентоспособность в условиях цифровой трансформации.

### Литература

1. Королев АВ. Экономико-математические методы и моделирование [J]. М.: Юрайт, 2017. URL: <https://publications.hse.ru/pubs/share/folder/inbly3btur/202051943.pdf>.
2. Камашева, М.Г. Концепция устойчивого развития: история и определение понятия // Инновации. Наука. Образование. 2021. № 37. С. 1786–1792.
3. Преодолевая пределы роста. Основные положения доклада для Римского клуба: монография / под ред. В.А. Садовниченко. – Москва: Издательство Московского университета, 2023. – 99 с. ISBN 978-5-19-011875-9.
4. Наше общее будущее: Доклад Международной комиссии по окружающей среде и развитию (МКОСР) / United Nations. 1987. 247 с.
5. The Sustainable Development Goals Report 2022. New York, NY: United Nations, 2022. 68 p. [Электронный ресурс]: <https://unstats.un.org/sdgs/report/2022/The-Sustainable-Development-GoalsReport-2022.pdf> (дата обращения: 06.01.2023).

6. *Благов Ю.Е.* Генезис концепции корпоративной социальной ответственности // Вестник Санкт-Петербургского университета. Менеджмент. 2006. № 2.
7. *Кузьмина Е.Ю.* Значение корпоративной социальной ответственности в современной организации для ее устойчивого развития // Актуальные проблемы развития экономики и управления в современных условиях : сборник материалов III Международной научно-практической конференции, Москва, 27–28 октября 2020 года / Негосударственное образовательное частное учреждение высшего образования «Московский экономический институт». – Москва: Негосударственное образовательное частное учреждение высшего образования "Московский экономический институт", 2020. – С. 420–424.
8. *Заводчикова Т.Б.* Корпоративная социальная ответственность как интегральная составляющая российского бизнеса // Вестник Самарского университета. Экономика и управление. 2024. № 15(3). С. 102–112.
9. *Анисифоров А.Б.* Важнейшие проблемы, возникающие в ходе цифровой трансформации предприятий, и подходы к их решению // Экономика и экологический менеджмент. 2024. № 3.
10. Precedenceresearch. Cyber Security Market Size, Share, and Trends 2024 to 2034. <https://www.precedenceresearch.com/cyber-security-market>.
11. *Гвилия Н.А.* Концепция корпоративной цифровой ответственности в управлении мезологистическими системами // Вестник АГТУ. Серия: Экономика. 2021. № 3. С. 88–101. DOI: 10.24143/2073-5537-2021-3-88-101
12. *Арнаутова В.А., Камшилов С.Г.* Трансформация форм социальной ответственности бизнеса в цифровой экономике // Научное пространство современной молодежи: приоритетные задачи и инновационные решения : Сборник статей участников III Всероссийской молодежной научно-практической конференции VI Уральского вернисажа науки и бизнеса, Международного научного культурно-образовательного форума, Челябинск, 07–08 апреля 2022 года / Под общей редакцией Е.П. Велихова, отв. за выпуск О.А. Хэгай. – Челябинск: Челябинский государственный университет, 2022. С. 8–10.
13. *Плешко Е.А., Силкина Г.Ю.* Корпоративная цифровая ответственность в контексте цифровой трансформации. Сборник трудов всероссийской научно-практической и учебно-методической конференции Том. Ч. 2. С. 78–82.
14. Выпуск отчета о корпоративной социальной ответственности промышленной отрасли Китая за 2023 год. Сборник корпоративных отчетов. URL: <http://web.shanghuibao.net/index/information/show/id/2515.html>.
15. Архив отчетов о корпоративной ответственности. URL: <https://esgnews.com/ru/день/отчет-о-корпоративной-ответственности/>.
16. Официальный информационный сайт компании ООО Шэньчжэньская компания Шоухэн Текнолоджи. <https://www.ipcba.com/company-certificate>.

#### References

1. Korolev AV. Ekonomiko-matematicheskie metody i modelirovanie [J]. M.: Yurait, 2017. URL: <https://publications.hse.ru/pubs/share/folder/inbly3btur/202051943.pdf>.
2. Kamasheva, M.G. Kontsepsiya ustoichivogo razvitiya: istoriya i opredelenie ponyatiya // *Innovatsii. Nauka. Obrazovanie*. 2021. № 37. P. 1786–1792.
3. Preodolevaya predely rosta. Osnovnye polozheniya doklada dlya Rimskogo kluba: monografiya / pod red. V.A. Sadovnichego. – Moskva: Izdatel'stvo Moskovskogo universiteta, 2023. – 99 s. ISBN 978-5-19-011875-9.
4. Nashe obshchee budushchee: Doklad Mezhdunarodnoi komissii po okruzhayushchei srede i razvitiyu (MKOSR) / United Nations. 1987. 247 s.
5. The Sustainable Development Goals Report 2022. New York, NY: United Nations, 2022. 68 p. [Elektronnyi resurs]: <https://unstats.un.org/sdgs/report/2022/The-Sustainable-Development-GoalsReport-2022.pdf> (data obrashcheniya: 06.01.2023).
6. Blagov Yu.E. Genezis kontsepsii korporativnoi sotsial'noi otvetstvennosti // *Vestnik Sankt-Peterburgskogo universiteta. Menedzhment*. 2006. № 2.
7. Kuz'mina E.Yu. Znachenie korporativnoi sotsial'noi otvetstvennosti v sovremennoi organizatsii dlya ee ustoichivogo razvitiya // Aktual'nye problemy razvitiya ekonomiki i upravleniya v sovremennykh usloviyakh : sbornik materialov III Mezhdunarodnoi nauchno-prakticheskoi konferentsii, Moskva, 27–28 oktyabrya 2020 goda / Negosudarstvennoe obrazovatel'noe chastnoe uchrezhdenie vysshego obrazovaniya «Moskovskii ekonomicheskii institut». – Moskva: Negosudarstvennoe obrazovatel'noe chastnoe uchrezhdenie vysshego obrazovaniya "Moskovskii ekonomicheskii institut", 2020. – S. 420–424.
8. Zavadchikova T.B. Korporativnaya sotsial'naya otvetstvennost' kak integral'naya sostavlyayushchaya rossiiskogo biznesa // *Vestnik Samarskogo universiteta. Ekonomika i upravlenie*. 2024. № 15(3). S. 102–112.

9. Anisiforov A.B. Vazhneishie problemy, vznikayushchie v khode tsifrovoi transformatsii predpriyatii, i podkhody k ikh resheniyu // *Ekonomika i ekologicheskii menedzhment*. 2024. № 3.
10. Precedenceresearch. Cyber Security Market Size, Share, and Trends 2024 to 2034. <https://www.precedenceresearch.com/cyber-security-market>.
11. Gviliya N.A. Kontsepsiya korporativnoi tsifrovoi otvetstvennosti v upravlenii mezologisticheskimi sistemami // *Vestnik AGTU. Seriya: Ekonomika*. 2021. № 3. S. 88–101. DOI: 10.24143/2073-5537-2021-3-88-101
12. Arnautova, V.A., Kamshilov S.G. Transformatsiya form sotsial'noi otvetstvennosti biznesa v tsifrovoi ekonomike // Nauchnoe prostranstvo sovremennoi molodezhi: prioritetye zadachi i innovatsionnye resheniya : Sbornik statei uchastnikov III Vserossiiskoi molodezhnoi nauchno-prakticheskoi konferentsii VI Ural'skogo vernisazha nauki i biznesa, Mezhdunarodnogo nauchnogo kul'turno-obrazovatel'nogo foruma, Chelyabinsk, 07–08 aprelya 2022 goda / Pod obshechi redaktsiei E.P. Velikhova, otv. za vypusk O.A. Khegai. – Chelyabinsk: Chelyabinskii gosudarstvennyi universitet, 2022. S. 8–10.
13. Pleshko E.A., Silkina G.Yu. Korporativnaya tsifrovaya otvetstvennost' v kontekste tsifrovoi transformatsii. Sbornik trudov vserossiiskoi nauchno-prakticheskoi i uchebno-metodicheskoi konferentsii Tom. Ch. 2. S. 78–82.
14. Vypusk otcheta o korporativnoi sotsial'noi otvetstvennosti promyshlennoi otrasli Kitaya za 2023 god. Sbornik korporativnykh otchetov. URL: <http://web.shanghuibao.net/index/information/show/id/2515.html>.
15. Arkhiv otchetov o korporativnoi otvetstvennosti. URL: <https://esgnews.com/ru/den'/otchet-o-korporativnoi-otvetstvennosti/>.
16. Ofitsial'nyi informatsionnyi sait kompanii OOO Shen'chzhen'skaya kompaniya Shoukhen Teknologzhi. <https://www.ipcba.com/company-certificate>.

Статья поступила в редакцию 14.01.2025

Принята к публикации 27.02.2025

Received 14.01.2025

Accepted for publication 27.02.2025