

Научная статья

Статья в открытом доступе

УДК 65.01

doi: 10.30987/2658-6436-2026-1-81-86

ПРОГНОЗИРОВАНИЕ ТЕХНОЛОГИЧЕСКИХ И ЭКОНОМИЧЕСКИХ РИСКОВ В ЦИФРОВОЙ СРЕДЕ ПРЕДПРИЯТИЯ С ЦЕЛЬЮ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ РАСПРЕДЕЛЕНИЯ РЕСУРСОВ

Антон Олегович Попов

Институт конструкторско-технологической информатики Российской академии наук,
г. Москва, Россия

kraz12345@mail.ru

Аннотация. Проводится исследование проблематики потребности в сквозном анализе бизнес- и технологических рисков как взаимосвязанных категорий при оценке достоверности данных предприятия. Цель исследования в обосновании важности сквозной аналитики бизнес- и технологических рисков при построении системы управления рисками, идентификации и оценки влияния рисков связанных с искажением данных предприятия. Применены такие методы, как системный анализ, моделирование и осмысление возможных путей управления рисками, тестирование в рабочей среде. Результаты исследования применимы в разных отраслях деятельности современных предприятий, в которых ключевым аспектом деятельности выступает цифровые платформы в условиях постоянного развития цифровой среды предприятия.

Ключевые слова: прогнозирование, управление, риски, модели, информация, безопасность, данные, предприятия, сквозной анализ

Для цитирования: Попов А.О. Прогнозирование технологических и экономических рисков в цифровой среде предприятия с целью повышения эффективности распределения ресурсов // Автоматизация и моделирование в проектировании и управлении. 2026. №1 (31). С. 81-86. doi: 10.30987/2658-6436-2026-1-81-86.

Original article

Open Access Article

FORECASTING TECHNOLOGICAL AND ECONOMIC RISKS IN THE DIGITAL ENVIRONMENT OF ENTERPRISES FOR IMPROVING RESOURCE ALLOCATION EFFICIENCY

Anton O. Popov

Institute for Design-Technological Informatics of the Russian Academy of Sciences, Moscow, Russia

kraz12345@mail.ru

Abstract. The study investigates the issue of the need for integrated analysis of business and technological risks as interconnected categories when assessing the reliability of enterprise data. The research aims to justify the importance of integrated analytics of business and technological risks in constructing a risk management system, identifying and assessing the impact of risks related to distortions in enterprise data. The work employs such methods as systemic analysis, modelling, reasoning of possible ways of risk management, and testing in a working environment. The research results are applicable in different sectors of modern enterprises where digital platforms serve as a key aspect of operations amidst the continuous development of the enterprise's digital environment.

Keywords: forecasting, management, risks, models, information, security, data, enterprises, integrated analysis

For citation: Popov A.O. Forecasting Technological and Economic Risks in the Digital Environment of Enterprises for Improving Resource Allocation Efficiency. Automation and modeling in design and management, 2026, no. 1 (31). pp. 81-86. doi: 10.30987/2658-6436-2026-1-81-86.

Введение

Цифровая трансформация является неотъемлемой частью современного предприятия, являясь средством повышения конкурентоспособности и адаптации к требованиям рынка в условиях постоянного научно-технического прогресса. Важным аспектом деятельности является информационный поток, обеспечивающий жизнедеятельность любой системы предприятия. Быстрый рост объема данных в информационном потоке, имеющих высокую критичную значимость для предприятия, является критическим фактором при принятии эффективных управленческих решений. В условиях постоянной цифровой трансформации и роста процессов как количественно, так и по составу этапов появляется необходимость приоритизации управления рисками искажения данных на основе совокупности факторов, учитывающих сложность и взаимосвязанность этих рисков в целях повышения эффективности деятельности предприятия при ограниченных ресурсах.

Рост цифровизации на предприятиях приводит, в том числе, к росту технологических сбоев, уязвимостей и ошибок, в частности исходящих от работников предприятий, приводящих к искажению данных, принятию несвоевременных решений и нерелевантному стратегическому планированию, оказывающих влияние на эффективность деятельности предприятия. Для снижения степени расхождения данных и более эффективного управления предприятием необходима оценка рисков в целях выявления наиболее критичных, ввиду чего особую актуальность приобретает сквозной анализ бизнес- и технологических рисков как взаимосвязанных категорий, включающих не только процессы внутри компании, но и взаимодействие с внешней средой. При такой сложности и взаимосвязанности рисков возникает необходимость в формировании единого подхода к идентификации, оценке и управлению, основанного на интеграции бизнес-процессов и их технологической оснастки, что, в свою очередь, требует глубокого осмысления роли информации и рисков ее искажения при оценке эффективности деятельности предприятия.

Также в рамках взаимодействия бизнес-процессов и информационно-технологических систем (ИТ-систем) необходимо согласованное управление рисками, при котором технологические риски оцениваются так же оказывающими влияние, как и риски в бизнес-процессах: снижение доверия, упущенная выгода, репутационные потери, материальные потери, что означает необходимость для предприятия в комплексной методике, оценивающей оценку ущербов риска и факторы их возникновения по цепочке процесса и его технологической оснастке.

В текущее время по причине высокого уровня цифровизации развитых предприятий допустимо обозначить важность разработки инструментов для сквозного анализа и оценки рисков, позволяющих повысить точность оценки влияния, основанных на данных мониторинга распределенных систем, разработанных и описанных ранее процессов и реализации цифровых инструментов для обеспечения жизнедеятельности процессов, а также использовании искусственного интеллекта при оценке рисков и их потенциального негативного влияния в целях проведения объективной оценки эффективности деятельности предприятия.

В связи с вышесказанным потребность создания системы сквозного анализа продиктована требованиями к точности данных, интеграционно-архитектурными решениями и необходимостью своевременной адаптации при управлении предприятием.

Наибольшую актуальность имеют превентивные процедуры в целях анализа и снижения возможных рисков на основе накопившегося опыта предприятия. Предложенный подход позволяет определить узкие места в процессах, приводящих к возникновению рисков искажения данных, на стыке бизнес-требований и технологической реализации, что непосредственно влияет на построении системы управления рисками.

Наиболее распространенные подходы к управлению рисками не включают комплексно-сквозное проведение оценки рисков, и не обеспечивают точной оценки потенциальной реализации рисков. Подход, основанный на интеграции сквозного анализа,

покрывающего весь жизненный цикл процесса, позволяет наиболее точно оценивать «узкие» места процесса, и выстраивать устойчивое и адаптивное цифровое окружение предприятия.

В условиях ограниченности ресурсов предприятия при приоритизации процессов для анализа рисков необходимо основываться на обязательной материальной оценке. При планировании деятельности предприятия критически важно определить и выразить потенциальный финансовый ущерб для предприятия как с позиции сокращения убытков реализации рисков искажения данных, так и с позиции обоснованности ранжирования приоритетов деятельности, что позволяет оценить ресурсы и внимание в наиболее уязвимых процессах, обеспечивая устойчивое управление бизнес-моделью при постоянной цифровизации.

Цель исследования в подробном рассмотрении возможности и обосновании важности применения сквозного подхода для выявления потенциальных рисков искажения данных на предприятии.

В соответствии с целью сформулированы следующие задачи:

- проанализировать современные практики сквозного анализа при определении рисков;
- провести сквозной анализ процесса в рабочей среде предприятия;
- оценить эффективность сквозного анализа бизнес- и технологических рисков, сформулировать рекомендации по внедрению, сформулировать вывод.

Методология исследования

В условиях постоянной цифровой трансформации предприятия одной из ключевых задач в целях обеспечения устойчивости и эффективности деятельности предприятия является управление рисками искажения данных. Основой управленческих решений являются данные в информационных потоках жизненных циклов процессов предприятия, требующих сквозного анализа ввиду связанности отдельных компонентов как бизнес, так и технологических процессов. Необходимо анализировать процесс, учитывая все оказывающие влияние факторы, и взаимосвязь между влияющими факторами.

Одним из наиболее эффективных подходов является комплексная методология, основанная на принципах сквозного процессного подхода, и управления рисками на основе материальности. Разработка и внедрение единого подхода по идентификации, оценки и управлению рисками искажения данных в цифровую среду предприятия позволит системно, унифицировано, полно и своевременно выявлять, оценивать и приоритизировать риски искажения данных, принимая во внимание материальную оценку процесса в рамках предприятия с целью оптимального распределения ограниченных ресурсов.

Комплексный подход анализа рисков, основанный на изучении всех этапов жизненного цикла процессов, а также взаимодействии с внешней средой, позволяет выявить все цепочки процессов с потенциальной потерей качества данных, учитывая взаимосвязь технологических и бизнес-рисков. Для получения достоверной оценки о рисках искажения данных необходимо рассматривать бизнес-процессы в совокупности с их техническими компонентами, такими как базы данных, системы контроля доступа и прочее.

Большая часть современных предприятий совмещает в цифровой среде гибридное решение, где часть функционала реализована через технологические инструменты, разработанные самим предприятием, часть функционала реализована через платформы планирования ресурсов, что, в свою очередь, затрудняет унифицировать единый подход к анализу рисков. Основным инструментом, вне зависимости от реализации, является постоянный мониторинг метрик бизнес-процессов и технологического состояния цифрового окружения предприятия, что также формирует базу для дальнейшего превентивного предотвращения рисков, однако использование искусственного интеллекта еще не интегрировано в процесс оценки рисков. Все этапы жизненного цикла процессов анализируются на основании стандартов в области безопасности данных, включающие следующие факторы: источник данных, интеграция при передаче данных между процессами

и системами, методы обработки и хранения, уровни доступа и возможные уязвимости, участие сотрудников и влияние человеческого фактора.

Оценка рисков базируется на источниках, критериях, методах оценки. Источниками могут являться как бизнес-риски, связанные с организационными процессами, ошибками сотрудников, нарушениями стандартов и процедур, так и технологические риски, связанные с проблемами с оборудованием, ошибками интеграции, управлением доступа и прочего. Основными критериями выступают вероятность возникновения, основанная на цифровом следе жизненного цикла процесса, в частности предшествующих реализации рисков факторам, и потенциальный ущерб в материальном выражении, состоящий из финансовых потерь, состоящих как из прямых убытков, так и репутационных потерях и упущенной выгоде. Повсеместно применяется матрица оценки рисков, а в целях оценки рисков используются качественные и количественные критерии, основанные на экспертных оценках, свершившихся инцидентах, анализе событий и прогнозировании. При оценке технологических рисков можно выделить матрицу общих информационно технологических контролей, обеспечивающих поддержания стабильности цифровой среды, и также позволяющей оценивать степень зрелости контроля рисков путем осуществления сквозного анализа между уязвимостями в технологическом слое и бизнес-рисками. Материальность при оценке реализации рисков рассчитывается на основе законодательства, релевантной судебной практики, исторических данных с учетом изменений.

Приоритизация основывается на совокупности факторов, а именно на оценке материальности и вероятности реализации риска как на факторах, наиболее ясно отражающих потенциальное влияние при дальнейшем стратегическом планировании. При большом количестве процессов при планировании приоритетов используются различные диаграммы.

В качестве примера возьмем часть рабочей матрицы общих контролей предприятия с вероятностью наступления и рассчитанной материальностью, где УР-вероятность реализации рисков по степени градации, где 1 – наименее вероятный, 5 – наиболее вероятный:

Категория	Контроль	Описание и цель	УР	Материальность (оценка ущерба)	Обоснование / Пример
Контроль доступа	Контроль избыточных прав доступа к базам данных	Проверка наличия у пользователей минимально необходимого уровня доступа	4	8 000 000 Р	Утечка персональных данных, санкции регулятора, компенсации клиентам, репутационные потери
Контроль изменений	Контроль согласования и тестирования изменений	Исключение внедрения непроверенных изменений, способных вызвать сбой	2	2 500 000 Р	Сбой сервиса из-за ошибки в коде, простой, ручное восстановление, недоступность услуг
Интегр. управление	Контроль корректности интеграции между сервисами	Обеспечение стабильной передачи данных между модулями, системами, микросервисами	3	4 500 000 Р	Потеря/искажение данных при синхронизации, сбой бизнес-процесса, повторная обработка
Контроль ввода данных	Контроль ошибок ввода данных оператором (ручной ввод)	Проверка достоверности и полноты ручного ввода информации	5	3 000 000 Р	Ошибка при вводе суммы, ИНН, реквизитов, дат – может повлечь штрафы, двойную оплату, искажение отчетности
Контроль ввода данных	Контроль точности сканирования штрих-кодов	Обеспечение точного автоматизированного ввода информации без участия оператора	1	1 000 000 Р	Ошибка сканирования → неверный товар/дата → потери, штрафы, возвраты

Также для примера возьмем часть поэтапно описанного процесса «выполнение заказа клиента»:

1) этап: регистрация заказа. Участники: менеджер по продажам, клиент. ИТ-системы: система управления клиентами, веб-портал. Данные на входе: данные клиента, номенклатура, количество, цена. Данные на выходе: заказ клиента;

2) этап: проверка наличия и резервирование товара. Участники: система (автоматически), складской работник. ИТ-системы: складская система, центральная система. Данные на входе: заказ клиента. Данные на выходе: заказ со статусом «товар зарезервирован»;

3) этап: отгрузка товара. Участники: кладовщик, водитель. ИТ-системы: складская система, транспортная система, сканеры штрих-кодов. Данные на входе: заказ для отгрузки. Данные на выходе: факт отгрузки, обновленные остатки на складе;

4) этап: выставление счета и учет дебиторской задолженности. Участники: система (автоматически), бухгалтер. ИТ-системы: центральная система, система электронного документооборота (СЭД). Данные на входе: данные об отгрузке. Данные на выходе: счет-фактура, проводки в бухгалтерии.

Идентифицируем и опишем риски по матрице выше:

Точка процесса	Описание риска	Природа риска	Возможная причина
Сканирование штрих-кода	Не отсканирована одна из позиций. Фактически отгружено 10 шт., в систему внесено 9 шт.	Операционный	Человеческая ошибка, спешка
Интеграция складская система → центральная система	Сбой передачи данных. Факт отгрузки не попал в центральную систему, счет не сформирован.	Технологический	Сбой программного интерфейса приложения, сетевые проблемы
Ручной ввод данных	Кладовщик вручную вводит номер заказа, ошибается в одной цифре. Отгрузка приписана другому заказу.	Операционный / технологический	Отсутствие контроля ввода, нет сканирования

В том числе более подробно рассмотрим риски интеграции систем:

- бизнес-требование: счет должен быть сформирован автоматически в день отгрузки;
- технологическая реализация: интеграция складской системы с центральной системой через программный интерфейс складской системы;

- риск искажения: если в запросе программного интерфейса от складской системы не передается обязательное поле «дата-время отгрузки с часовым поясом», складская система может присвоить псевдослучайную дату, что приведет к искажению данных для управленческой отчетности (отгрузки одного дня попадут в другой). Это классический «стыковой» риск, который не увидит ни бизнес-аналитик, ни ИТ-специалист по отдельности.

Проведенное исследование реализовано для сквозного анализа рисков предприятия и оценки материальности с целью обоснования такого подхода.

Результаты исследования и обсуждение

По результатам проведения сквозного анализа и оценки рисков они были идентифицированы и оценены для дальнейшей эффективной разработки мер по снижению выявленных угроз. Важным аспектом результатов является выявленная высокая степень взаимосвязанности факторов бизнес- и технологических рисков при взаимодействии бизнес-процессов с информационной средой, ранее не обнаруживаемая при изоляционном рассмотрении.

Также внедрение принципов сквозной аналитики положительно повлияло на:

- 1) повышение достоверности данных по причине выявления возможных «узких» мест на этапах всего процесса;

- 2) ввиду системности и унификации процесса сократилось время на идентификацию и оценку рисков;

- 3) создана основа для количественной аналитики путем перевода инцидентов в материальность;
- 4) создана основа для дальнейшей интеграции искусственного интеллекта в процесс определения и оценки рисков.

Выводы

По результатам исследования подтверждена необходимость применения сквозного анализа при оценке рисков и планировании мероприятий и разработке технологий по снижению влияния рисков. Предложенный подход позволяет повысить качество данных, улучшить достоверность текущего состояния цифровой среды, повысить эффективность за счет более эффективного распределения человеческих ресурсов. Полученные результаты подтверждают применимость подхода в условиях масштабируемой и динамически изменяющейся информационной среды предприятия.

Список источников:

1. Попов А.О., Карлова Т.В., Шептунов С.А. Оценка достоверности данных электронной среды предприятия на основе моделей и алгоритмов интеллектуальной поддержки документооборота как ключевой фактор обеспечения эффективного управления предприятием // Автоматизация и моделирование в проектировании и управлении. – 2024. – №1 (23). – С. 65-72.
2. Баранова О.В. Аудит информационных систем // Вестник финансовой Академии. – 2009. – С. 58-60.
3. Анисимов В.Г., Зегжда П.Д., Супрун А.Ф. Риск-ориентированный подход к организации контроля в подсистемах обеспечения безопасности информационных систем // Проблемы информационной безопасности. Компьютерные системы. – 2016. – № 3. – С. 61-67.
4. Горбунов В.Л., Файзуллина А.И. Предикивный анализ информационных потоков в системах информационной безопасности телекоммуникационных комплексов // Проблемы информационной безопасности. Компьютерные системы. – 2024. – № 4. – С. 140-151.

References:

1. Popov A.O., Karlova T.V., Sheptunov S.A. Assessing the Reliability of Data in the Enterprise Electronic Environment Based on Models and Algorithms for Intelligent Document Management Support as a Key Factor for Effective Enterprise Management. Automation and Modeling in Design and Management. 2024;1(23):65-72.
2. Baranova O.V. Auditing Information Systems. Vestnik finansovoj akademii. 2009; 58-60.
3. Anisimov V.G., Zegzhda P.D., Suprun A.F. The Risk-Based Method for Organization of Monitoring in Information Systems Security Facilities. Problems of Information Security. Computer Systems. 2016;(3): 61-67.
4. Gorbunov V.L., Fayzullina A.I. Predictive Analysis of Information Flows in Information Security Systems of Telecommunications Complexes. Problems of Information Security. Computer Systems. 2024;(4):140-151.

Информация об авторах:

Попов Антон Олегович
аспирант Института конструкторско-технологической информатики Российской академии наук

Information about the authors:

Popov Anton Olegovich
Postgraduate Student of the Institute for Design-Technological Informatics of the Russian Academy of Sciences

Статья поступила в редакцию 02.10.2025; одобрена после рецензирования 01.11.2025; принята к публикации 14.11.2025.

The article was submitted 02.10.2025; approved after reviewing 01.11.2025; accepted for publication 14.11.2025.

Рецензент – Малаханов А.А., кандидат технических наук, доцент, Брянский государственный технический университет.

Reviewer – Malakhanov A.A., Candidate of Technical Sciences, Associate Professor, Bryansk State Technical University.