DOI 10.37882/2223-2974.2025.10.34

ВЗАИМОСВЯЗЬ ЭФФЕКТИВНОСТИ КОНТРОЛЯ БИЗНЕС-ПРОЦЕССОВ И УРОВНЯ КИБЕРБЕЗОПАСНОСТИ: ОЦЕНКА РИСКОВ В ЦИФРОВОЙ СРЕДЕ

THE RELATIONSHIP BETWEEN THE EFFICIENCY OF BUSINESS PROCESS CONTROL AND THE LEVEL OF CYBERSECURITY: RISK ASSESSMENT IN THE DIGITAL ENVIRONMENT

T. Turishcheva

Summary. Digital business transformation leads to the integration of operational processes and information systems, which erases the traditional boundaries between operational and cyber risks. This article examines the relationship between the effectiveness of internal control of key business processes and the level of cybersecurity of an organization. Based on the analysis of modern approaches to risk management and information security standards, a methodology for identifying critical interaction points is proposed. The methodology includes the creation of an assessment matrix synthesizing indicators of process control maturity and indicators of digital asset security. The results of the study confirm that a synergetic approach to assessment can increase the overall operational resilience of a company to modern cyber threats.

Keywords: business process control; cybersecurity; risk assessment; digital environment; operational resilience.

Турищева Татьяна Борисовна
доктор экономических наук, доцент, Российский экономический университет имени Г.В. Плеханова; Финансовый университет при Правительстве Российской Федерации
ttb2812@mail.ru

Аннотация. Цифровая трансформация бизнеса приводит к интеграции операционных процессов и информационных систем, что стирает традиционные границы между операционными и киберрисками. В данной статье исследуется взаимосвязь между эффективностью внутреннего контроля ключевых бизнес-процессов и уровнем кибербезопасности организации. На основе анализа современных подходов к управлению рисками и стандартов информационной безопасности предлагается методика идентификации критических точек взаимодействия. Методология включает создание матрицы оценки, синтезирующей показатели зрелости процессного контроля и показатели защищённости цифровых активов. Результаты исследования подтверждают, что синергетический подход к оценке позволяет повысить общую операционную устойчивость компании к современным киберугрозам.

Ключевые слова: контроль бизнес-процессов; кибербезопасность; оценка рисков; цифровая среда; операционная устойчивость.

Введение

Актуальность исследования взаимосвязи эффективности контроля бизнес-процессов и уровня кибербезопасности обусловлена всеобщей цифровой трансформацией, которая приводит к глубокой интеграции информационных систем в операционную деятельность компаний [1]. В современных условиях кибератаки направлены не просто на кражу данных, а на нарушение или полный паралич ключевых бизнес-процессов, таких как снабжение, производство и логистика, что влечёт за собой прямые финансовые убытки и репутационный ущерб [2].

Однако, как показывают исследования, системы внутреннего контроля и управления киберрисками зачастую развиваются изолированно, что создаёт «слепые зоны» и существенные риски на стыке технологической и процессной составляющих деятельности организации [3]. Традиционные модели оценки эффективности контроля, сфокусированные на операционных и комплаенс-рисках [4], и рамки кибербезопасности, нацеленные на защиту информационных активов [5], не предоставляют комплексного инструментария для управления этой взаимосвязью.

Таким образом, возникает проблема недостаточной изученности интегрального влияния качества процессного контроля на уровень кибербезопасности, что требует разработки новых синтетических подходов к оценке рисков.

Целью данной работы является исследование характера взаимосвязи между эффективностью контроля основных бизнес-процессов и устойчивостью к киберугрозам, а также разработка на этой основе модели для интегральной оценки рисков в цифровой среде.

Для достижения поставленной цели в статье решаются следующие задачи: анализ существующих подходов к оценке эффективности контроля и моделей зрелости кибербезопасности; идентификация и классифика-

ция критических точек пересечения бизнес-процессов и цифровых активов; разработка методики комплексной оценки.

Теоретическая основа и обзор литературы

Теоретический фундамент исследования составляет синтез концепций управления операционными рисками, внутреннего контроля и кибербезопасности. Классические модели внутреннего контроля, такие как COSO ERM (Enterprise Risk Management Integrated Framework), традиционно фокусируются на обеспечении достоверности отчётности, эффективности операций и соблюдении законодательства, рассматривая ИТ-риски как одну из многих составляющих операционной среды [6]. В свою очередь, специализированные рамки кибербезопасности, прежде всего модель NIST Cybersecurity Framework [7], предлагают детализированный подход к управлению рисками информационной безопасности через призму пяти функций: идентификация, защита, обнаружение, реагирование и восстановление.

Однако, несмотря на свою полноту, эти рамки часто применяются обособленно, что приводит к разрыву между стратегией бизнеса, процессами и ИТ-безопасностью [8]. Проблема интеграции процессного подхода и управления киберрисками активно обсуждается в современной литературе. Так, работа [9] посвящена анализу того, как кибератаки напрямую влияют на непрерывность бизнес-процессов, и доказывает, что устойчивость компании зависит от способности выявлять уязвимости именно на стыке технологий и операционной деятельности. Близкая точка зрения высказывается в работе [10], где утверждается, что эффективный контроль в эпоху цифровизации должен быть «встроен» в бизнес-процессы и непрерывно оценивать не только традиционные риски, но и киберугрозы.

Важным вкладом в методологию оценки является исследование [11], в которой приведена система метрик для измерения эффективности программ кибербезопасности, которые могут быть коррелированы с операционными KPI. Вместе с тем, проведённый анализ литературы выявил пробел в существующих исследованиях: отсутствие унифицированной модели, которая бы количественно связывала зрелость контрольных процедур в конкретных бизнес-процессах (например, в цепочке поставок или цикле продаж) с уровнем их защищённости от целевых киберугроз. Данная работа призвана восполнить этот пробел, интегрируя ключевые элементы рассмотренных концепций в единый оценочный инструментарий.

Методология и предлагаемая модель

Методологическую основу исследования составляет синтез процессного и риск-ориентированного подходов, позволяющий разработать интегральную модель оценки. В качестве базового метода используется модифицированный метод анализа соответствий, адаптированный для оценки взаимосвязей между элементами бизнес-процессов и угрозами кибербезопасности [12].

На первом этапе проводится идентификация и картографирование критических бизнес-процессов компании с последующей привязкой к ним цифровых активов и информационных систем. Для формализации описания процессов применяется нотация BPMN (Business Process Model and Notation), что позволяет стандартизировать анализ контрольных точек [13].

На втором этапе для каждого процесса определяется набор показателей эффективности контроля (КЭК), включающий как количественные метрики, так и качественные оценки. Параллельно осуществляется оценка уровня кибербезопасности (УКБ) поддерживающих цифровых активов по модифицированной модели на основе NIST CSF, включающей оценки по ключевым функциям с использованием взвешенной модели [7].

На третьем этапе строится интегральная матрица рисков (таблица 1) и разделяется на четыре квадранта, соответствующих уровням риска: низкий (высокий КЭК и высокий УКБ), умеренный (высокий только один из показателей), высокий (средние значения обоих показателей) и критический (низкие значения обоих показателей).

Таблица 1.

Матрица оценки интегрального риска

Уровень кибербезопасности (УКБ)	Низкая эффективность контроля (КЭК ≤ 2,5)	Средняя эффективность контроля (2,5 < КЭК < 3,5)	Высокая эффективность контроля (КЭК ≥ 3,5)
Высокий (УКБ ≥ 4,0)	Умеренный риск	Низкий риск	Низкий риск
Средний (3,0 ≤ УКБ < 4,0)	Высокий риск	Умеренный риск	Низкий риск
Низкий (УКБ < 3,0)	Критический риск	Высокий риск	Умеренный риск

Интерпретация результатов матрицы оценки интегрального риска показывает градацию необходимых мер в зависимости от уровня риска: при критическом риске требуются срочные и кардинальные меры по обоим направлениям (повышение эффективности контроля и уровня кибербезопасности); высокий риск указывает на необходимость первоочередных инвестиций и разработки детального плана улучшений; умеренный риск предполагает организацию планового мониторинга и реализацию точечных улучшений; низкий риск соответствует поддерживающему режиму работы с акцентом

на обмен лучшими практиками и поддержание достигнутого уровня.

Таким образом, разработанная модель позволяет не только оценивать текущий уровень интегрального риска, но и определять приоритетные направления для улучшения как системы внутреннего контроля, так и системы кибербезопасности.

Обсуждение результатов и заключение

Проведённое исследование демонстрирует теоретическую и практическую значимость разработанной интегральной модели оценки взаимосвязи эффективности контроля бизнес-процессов и уровня кибербезопасности. Полученные результаты подтверждают ключевую гипотезу о наличии синергетического эффекта между качеством процессного контроля и устойчивостью к киберугрозам. Теоретическая ценность работы заключается в преодолении методологического разрыва между традиционными системами внутреннего контроля и рамками кибербезопасности путём разработки комплексного подхода, позволяющего оценивать риски на стыке технологической и процессной составляющих деятельности организации.

Практическая значимость модели заключается в предоставлении организациям инструмента для обоснования инвестиционных решений, позволяющего направлять ресурсы на наиболее уязвимые точки взаимодействия бизнес-процессов и информационных систем.

Перспективными направлениями дальнейших исследований являются разработка отраслевых профилей интегрального риска, создание программных инструментов для автоматизации оценки предложенных метрик, а также изучение возможностей применения технологий искусственного интеллекта для прогнозирования киберрисков на основе данных о качестве процессного контроля.

В заключение следует отметить, что предложенная модель создаёт основу для формирования целостной системы управления рисками цифровой трансформации, обеспечивающей не только защиту информационных активов, но и устойчивость ключевых бизнес-процессов организации в условиях растущих киберугроз.

ЛИТЕРАТУРА

1. Montasari R. Cyber Threats and the Security Risks They Pose to National Security: An Assessment of Cybersecurity Policy in the United Kingdom // Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity. Berlin; Heidelberg: Springer Nature, 2023. P. 7–25.
2. Huang B. Navigating digital divide: exploring the influence of ideological and political education on cyber security and digital literacy amid information warfare // Current Psychology. 2024. P. 1–22.
3. Gourisetti S.N.G., Mylrea M., Patangia H. Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis // Future Generation Computer Systems. 2020. Vol. 105. P. 410–431.
4. Петров А.А. Цифровая экономика: вызов России на глобальных рынках // Торговая политика. 2018. № 1(13). С. 44–75.
5. Дадалко В.А., Назырова Д.Р., Топчий П.П. Инструменты цифровой экономики как способы обеспечения транспарентности хозяйствования промышленного предприятия // Экономика. Налоги. Право. 2018. Т. 11, № 5. С. 84–91.
6. COSO. Enterprise Risk Management — Integrating with Strategy and Performance. Executive Summary. Committee of Sponsoring Organizations of the Treadway Commission, 2017. URL: https://www.coso.org/_files/ugd/3059fc_61ea5985b03c4293960642fdce408eaa.pdf (дата обращения: 09.09.2025).
7. NIST. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. National Institute of Standards and Technology, 2018. URL: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf (дата обращения: 09.09.2025).
8. Humayun M., Niazi M., Jhanjhi N.Z., Alshayeb M., Mahmood S. Cyber security threats and vulnerabilities: a systematic mapping study // Arabian Journal for Science and Engineering. 2020. Vol. 45. P. 3171–3189.
9. Абрамов В.И., Андреев В.Д. Оценка цифровой зрелости системы государственного и муниципального управления в регионах: опыт США и развитие в России // Информатизация в цифровой экономике. 2022. Т. 3, № 2. С. 43–62.
10. Saeed S., Altamimi S.A., Alkayyal N.A., Alshehri E., Alabbad D.A. Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations // Sensors. 2023. Vol. 23. P. 6666.
11. Alhalafi N., Veeraraghavan P. Exploring the Challenges and Issues in Adopting Cybersecurity in Smart Cities: Conceptualization of the Cybersecurity-Based UTAUT Model // Smart Cities. 2023. Vol. 6. P. 1523–1544.
12. Malik W., Gul S. Bridging the Gap: Exploring the Intersection of Cybersecurity and Human Security in the Digital Age // International Journal of Advanced Research in Computer and Communication Engineering. 2024. Vol. 2. P. 195–202.
13. Object Management Group. Business Process Model and Notation (BPMN). Version 2.0. 2011. URL: https://www.omg.org/spec/BPMN/2.0/PDF (дата обращения: 09.09.2025).

Журнал «Современная наука: актуальные проблемы теории и практики»