

Д. В. Санников¹

¹ Югорский государственный университет, г. Ханты-Мансийск, Россия

Правовые и экономические риски цифровых экосистем университетов: системный анализ и управление

Санников Дмитрий Васильевич, кандидат экономических наук, доцент центра образовательного инжиниринга, Югорский государственный университет
E-mail: dvsannikov@yandex.ru
ORCID: <http://orcid.org/0000-0002-0820-2737>
Web of Science Researcher ID: OKR-6790-2025
Scopus Author ID: 58825314700
eLIBRARY SPIN-код: 8569-7816

Аннотация

Цель: проведение системного анализа комплекса правовых и экономических рисков, возникающих в процессе формирования и функционирования цифровых экосистем университетов, и разработка на его основе модели управления данными рисками.

Методы: исследование базируется на методологии системного анализа и синтеза. Используются методы сравнительного правового и экономического анализа, концептуального моделирования, а также контент-анализ массива научной литературы (более 40 источников).

Результаты: выявлена и классифицирована система взаимосвязанных рисков, структурированная по трем уровням: 1) микроуровень (внутриэкосистемный): риски кибербезопасности, нарушения прав на интеллектуальную собственность и персональные данные, коррупционные риски при закупках ИТ-решений; 2) мезоуровень (экосистемный): риски неэффективного управления (проектные, коммуникационные, культурные), правовой неопределенности регулирования цифровых платформ и сервисов; 3) макроуровень (внешний): риски, связанные с геополитической ситуацией (санкции, ограничение доступа к технологиям и R & D), а также с глобальными вызовами (цифровое неравенство, этика ИИ). На основе выявленной системы рисков разработана интегративная трехконтурная модель управления, включающая: 1) превентивный контур (правовой комплаенс и регуляторный каркас); 2) оперативный контур (проектное управление и инструменты мониторинга); 3) стратегический контур (формирование «цифровой экосистемы доверия», развитие культуры и этики).

Научная новизна: впервые цифровая экосистема университета исследуется как целостный социотехнический объект, обладающий свойствами сложной системы, с позиции комплексного выявления и управления кросс-дисциплинарными рисками на стыке экономики, права и криминологии. Предложена интеграция концепции «цифровой экосистемы доверия» с аппаратом системной экономической теории и проектным управлением.

Практическая значимость: разработанные выводы и предложения могут быть использованы в рамках управления вузами для реализации принципов цифровых преобразований, создания систем управления рисками и соблюдения требований, а также законодателей для формирования сбалансированного правового поля, стимулирующего инновации в высшей школе при обеспечении безопасности и прав субъектов.

Ключевые слова:

экономическая теория, цифровая экосистема университета, правовые риски, экономические риски, системный анализ, управление рисками, кибербезопасность, интеллектуальная собственность, проектное управление, транзакционные издержки, цифровая трансформация

Как цитировать статью: Санников, Д. В. (2026). Правовые и экономические риски цифровых экосистем университетов: системный анализ и управление. *Russian Journal of Economics and Law*, 20(1), 48–63. <https://doi.org/10.21202/2782-2923.2026.1.48-63>

Scientific article

D. V. Sannikov¹

¹ Yugra State University, Khanty-Mansiysk, Russia

Legal and economic risks of digital ecosystems of universities: system analysis and management

Dmitry V. Sannikov, Cand. Sci. (Economics), Associate Professor at the Center for Educational Engineering, Yugra State University
E-mail: dvsannikov@yandex.ru
ORCID: <http://orcid.org/0000-0002-0820-2737>
Web of Science Researcher ID: OKR-6790-2025
Scopus Author ID: 58825314700
eLIBRARY SPIN-code: 8569-7816

Abstract

Objective: to systematically analyze the complex of legal and economic risks arising in the formation and functioning of digital ecosystems of universities, and to develop a risk management model based on this analysis.

Methods: the research uses the methodology of system analysis and synthesis and such methods as comparative legal and economic analysis, conceptual modeling, as well as content analysis of the scientific literature (more than 40 sources).

Results: the author identified and classified a system of interrelated risks, structured at three levels: 1) micro-level (intra-ecosystem): cybersecurity risks, violations of intellectual property and personal data rights, corruption risks in the procurement of IT solutions; 2) meso-level (ecosystem): risks of ineffective management (project, communication, cultural), legal uncertainty in regulating digital platforms and services; and 3) macro-level (external): risks related to the geopolitical situation (sanctions, restrictions on access to technology and R&D) and global challenges (digital inequality, AI ethics). Based on the identified system, an integrative three-contour management model was developed, including: 1) preventive contour (legal compliance and regulatory framework); 2) operational contour (project management and monitoring tools); and 3) strategic contour (forming a “digital ecosystem of trust”, developing culture and ethics).

Scientific novelty: for the first time, a university’s digital ecosystem is studied as an integral sociotechnical object with the properties of a complex system, in terms of comprehensive identification and management of cross-disciplinary risks at the intersection of economics, law and criminology. The author proposes integrating the concept of a “digital ecosystem of trust” with the apparatus of systemic economic theory and project management.

Practical significance: the conclusions and proposals can be used in university management to implement the digital transformation principles, create risk management and compliance systems, and in legislation to form a balanced legal framework that stimulates innovation in higher education while ensuring the safety and rights of subjects.

Keywords:

economic theory, university digital ecosystem, legal risks, economic risks, system analysis, risk management, cybersecurity, intellectual property, project management, transaction costs, digital transformation

For citation: Sannikov, D. V. (2026). Legal and economic risks of digital ecosystems of universities: system analysis and management. *Russian Journal of Economics and Law*, 20(1), 48–63. (In Russ.). <https://doi.org/10.21202/2782-2923.2026.1.48-63>

Введение

Современный университет претерпевает фундаментальную трансформацию, превращаясь из традиционного образовательного учреждения в открытую сетевую, цифровую экосистему (Reichert, 2019; Kozirog et al., 2022; Санников, 2024; Дорошенко, Шеломенцев, 2017). Этот переход детерминирован глобальными трендами: четвертой промышленной революцией (Индустрия 4.0), экспоненциальным ростом объема данных, повсеместным проникновением искусственного интеллекта (далее – ИИ) и необходимостью формирования «экономики знаний». В этих условиях цифровая экосистема становится не просто технологической инфраструктурой, а ключевым активом и новой организационной парадигмой университета, определяющей его конкурентоспособность, устойчивость и способность выполнять свою миссию (Григорьев и др., 2020; Anvari et al., n.d.).

Как и любая сложная социотехническая система, цифровая экосистема университета генерирует не только очевидные преимущества, такие как снижение транзакционных издержек, персонализация образования, рост операционной эффективности и открытие новых возможностей для исследований (Санников, Ширинкина, 2023а; Barykin et al., 2020), но и порождает комплекс новых, слабо изученных и системно взаимосвязанных рисков. Эти риски имеют междисциплинарную природу, находясь на стыке экономики, права, криминологии и управления.

С одной стороны, стремительная цифровизация опережает развитие нормативно-правовой базы, создавая правовые вакуумы и зоны неопределенности (Benkler, 2001; Dulsrud & Bygstad, 2022). Университеты, выступая держателями огромных массивов конфиденциальных данных (персональные данные студентов и сотрудников, результаты интеллектуальной деятельности, научные разработки), становятся лакомой мишенью для кибератак, что актуализирует работы по уголовно-правовой охране цифровой информации (Бегишев, Бикеев, 2020, 2021). Одновременно обостряются проблемы защиты интеллектуальной собственности в условиях открытой науки и коллабораций, риски несанкционированного использования данных алгоритмами ИИ (Rojas & Chiappe, 2024) и коррупционные угрозы при осуществлении масштабных ИТ-закупок (Бикеев, 2022). В российском контексте эти риски усугубляются спецификой правоприменения и наличием пробелов в отраслевых регламентах Минобрнауки, напрямую затрагивающих, например, порядок работы с персональными данными в научно-образовательном процессе или требования к безопасности информационных систем вузов.

С другой стороны, экономические и управленческие риски зачастую недооцениваются. К ним относятся риски неверной оценки эффективности инвестиций в цифровизацию, высокие издержки на интеграцию и поддержку сложных платформ, а также фундаментальные управленческие дефициты, ведущие к провалам трансформационных проектов (Назайкинская, Рамсбергер, 2025; Санников, Ширинкина, 2023b). Как справедливо отмечается в исследованиях Сколково, до 75 % неудач цифровой трансформации связаны с человеческим фактором, сопротивлением изменениям и неготовностью организационной культуры (Архитектура трансформации..., 2023). Внешние макрориски, такие как санкционное давление, разрыв международных научных связей и ограничение доступа к критическим технологиям (Кувалин, 2024; Золотарев, 2024), лишь усугубляют ситуацию.

Несмотря на растущий интерес к теме цифровых экосистем в образовании (Nguyen & Tuamsuk, 2022; Gomez et al., 2013), в научной литературе сохраняется существенный пробел. Большинство работ сфокусировано либо на технологических и педагогических аспектах (Rojas & Chiappe, 2024), либо на экономических моделях и управленческих подходах (Санников, 2024; Volz et al., 2025), либо на узких правовых вопросах, таких как защита интеллектуальной собственности или персональных данных (Oluoha et al., 2023). Вместе с тем практически отсутствует системный анализ национального правового поля (ФЗ-152 «О персональных данных», ФЗ-149 «Об информации»¹, ФЗ-273 «Об образовании»², отраслевые приказы Минобрнауки) как источника конкретных рисков (далее в том числе *compliance*) для цифровых экосистем университетов (Dulsrud & Bygstad, 2022). Комплексный системный анализ, рассматривающий цифровую экосистему университета

¹ О персональных данных. № 152-ФЗ от 27.07.2006 (последняя редакция). КонсультантПлюс. https://www.consultant.ru/document/cons_doc_LAW_61801/

² Об образовании в Российской Федерации. № 273-ФЗ от 29.12.2012 (последняя редакция). КонсультантПлюс. https://www.consultant.ru/document/cons_doc_LAW_140174/

как единый объект и выявляющий взаимосвязь и взаимовлияние правовых, экономических и криминологических рисков, до настоящего времени не проводился.

Таким образом, проблема исследования заключается в противоречии между объективной необходимостью формирования цифровых экосистем для развития университетов и отсутствием целостной системы управления комплексными рисками, возникающими в этом процессе. Это противоречие обусловлено фрагментарностью научных знаний и управленческих практик в данной области.

Целью настоящего исследования является проведение системного анализа правовых и экономических рисков цифровых экосистем университетов и разработка на его основе концептуальной модели управления данными рисками.

Для достижения цели поставлены следующие задачи:

1. На основе синтеза подходов системной экономической теории (Клейнер, 2024), теории цифровых экосистем (Briscoe, 2009; Leal et al., 2025) и анализа университетских кейсов (Санников, Ширинкина, 2023а; Reichert, 2019; Kozirog, 2022) уточнить понятийный аппарат и построить структурную модель цифровой экосистемы университета как объекта рискориентированного управления.

2. Выявить, систематизировать и классифицировать комплекс правовых (киберпреступность, информационные системы (далее – ИС), данные, коррупция), экономических (транзакционные издержки, эффективность инвестиций) и управленческих рисков на микро-, мезо- и макроуровнях.

3. Проанализировать российское законодательство в сфере цифровых экосистем (ФЗ-152³, ФЗ-273⁴, ФЗ-149⁵, отраслевые акты) и передовые зарубежные регуляторные модели (GDPR, DGA, AI Act – Pastor Sempere, 2025) с целью адаптации к деятельности университетов.

4. Исследовать управленческие практики и «болевые точки» реализации трансформационных проектов в вузах (Назайкинская, Рамсбергер, 2025; Архитектура трансформации..., 2023) как источник проектных и операционных рисков.

5. Разработать концептуальную модель управления рисками цифровой экосистемы университета, интегрирующую инструменты правового соответствия, экономические оценки, инструменты проектного управления и формирование «экосистемы надежности» (van den Hoven et al., 2021). Модель должна быть операционализирована через предложение конкретных инструментов и этапов внедрения для университетов с разным уровнем цифровой зрелости.

Научная гипотеза заключается в том, что эффективное управление рисками цифровой экосистемы университета возможно только на основе системного подхода, рассматривающего ее как сложный, многоуровневый объект и требующего интеграции правовых, экономических и управленческих механизмов в единый контур управления, нацеленный на минимизацию транзакционных издержек и построение цифрового доверия.

Теоретический обзор. Настоящее исследование базируется на междисциплинарном синтезе четырех ключевых исследовательских направлений: 1) теории цифровых экосистем и их экономики; 2) системном подходе в экономике и управлении; 3) правовых и криминологических аспектах цифровой среды; 4) специфике цифровой трансформации высшей школы. Анализ более 40 релевантных источников позволил выявить как устоявшиеся концепции, так и существующие лакуны, которые призвано заполнить настоящее исследование.

1. Эволюция концепции цифровых экосистем и их экономические основы.

Изначально метафора экосистемы, заимствованная из биологии, была применена к бизнес-среде Джеймсом Муром (Санников, Ширинкина, 2023b), определившим бизнес-экосистему как экономическое сообщество, поддерживаемое фундаментом взаимодействующих организаций и индивидов. Фундаментальный вклад в понимание архитектуры и свойств цифровых экосистем (далее – ЦЭ) внес Бриско (Briscoe, 2009; Satalkina & Steiner, 2020), определивший их как цифровые аналоги биологических экосистем, обладающие свойства-

³ О персональных данных. № 152-ФЗ от 27.07.2006 (последняя редакция). КонсультантПлюс. https://www.consultant.ru/document/cons_doc_LAW_61801/

⁴ Об образовании в Российской Федерации. № 273-ФЗ от 29.12.2012 (последняя редакция). КонсультантПлюс. https://www.consultant.ru/document/cons_doc_LAW_140174/

⁵ Об информации, информационных технологиях и о защите информации. № 149-ФЗ от 27.07.2006 (последняя редакция). КонсультантПлюс. https://www.consultant.ru/document/cons_doc_LAW_61798/

ми самоорганизации, масштабируемости и устойчивости. Его работа заложила основы *Ecosystem-Oriented Architecture*, выделив ключевые элементы: Агентов (сервисы), Популяции и Хабитаты (узлы сети).

В контексте экономики ЦЭ Кругста (Krogstie, 2012) подчеркивает их социотехническую природу, разделяя экосистемы на контент-ориентированные и программные, и указывая на вызовы моделирования для таких открытых, адаптивных систем. Барыкин с соавт. (Barykin et al., 2020) развивают это определение, характеризуя ЦЭ как самоорганизующуюся, устойчивую систему на базе цифровых платформ, формирующую единую информационную среду, где конкуренция замещается коллаборацией. Важный аспект, поднятый в работе, – экономический эффект снижения предельных издержек на создание новых приложений практически до нуля за счет рекомбинации существующих сервисов (Briscoe, 2009; Hniezdovskyi et al., 2025).

Применительно к управлению Вольц с соавт. (Volz et al., 2025) в своем систематическом обзоре выявляют 17 динамических способностей, необходимых компаниям для интеграции в ЦЭ, смещая фокус с внутренних способностей фирмы на многоуровневые, встроенные в структуры экосистемы способности к координации и совместному созданию ценности. Этот подход крайне релевантен для университетов, которым необходимо развивать подобные способности для оркестрации сложных сетей взаимодействия.

2. Системно-экономический подход как методологический фундамент.

Труды Г. Б. Клейнера предоставляют мощный методологический аппарат для нашего исследования. Его тетрадная модель социально-экономических систем, включающая объектную, средовую, процессную и проектные подсистемы (Клейнер, 2023, 2024а), является эвристичным инструментом для структурного анализа цифровой экосистемы университета. Данная модель позволяет преодолеть фрагментарность и рассматривать экосистему как целостность, где, например, ИТ-инфраструктура (объектная подсистема) неразрывно связана с цифровой культурой (средовая подсистема) и проектными командами (проектная подсистема).

Развивая эту идею, Качалов с соавт. (2024) в монографии «Управление деятельностью социально-экономических экосистем» прямо указывают, что экосистемы по своей сути являются индустриальными объектами, выходящими за границы классического понимания отрасли, и требуют перехода от циклического управления к проектному, ориентированному на преобразование. Они предлагают архитектуру системы управления уровнем риска, состоящую из четырех подсистем, что созвучно нашей задаче классификации рисков.

Концепция многополярного управления (Клейнер, 2024b), предполагающая распределение власти между инспиративным, интеллектуальным, культурным и духовным лидерством, предлагает рамки для анализа управленческих рисков, связанных с несбалансированностью развития разных «полюсов» университетской экосистемы.

3. Правовые и криминологические риски в цифровой среде: фокус на университеты.

Правовой аспект исследования опирается на два ключевых блока. Первый – это работы, раскрывающие системные угрозы, порождаемые самим развитием цифрового права (Goodfellow & Lea, 2013). Классическая статья Бенклера (Benkler, 2001) демонстрирует, как расширение эксклюзивных прав интеллектуальной собственности (Закон об авторском праве в цифровую эпоху – *DMCA*, *UCTTA*) искусственно подавляет *emerging*-модели пирингового производства, к которым можно отнести и открытую научную коллаборацию. Это создает фундаментальный правовой риск для академической среды.

Второй блок – это исследования, непосредственно посвященные киберпреступности. Монография Бегишева и Бикеева (2020) «Преступления в сфере обращения цифровой информации» предоставляет развернутую классификацию киберугроз и критический анализ отставания уголовного законодательства от технологических реалий. Выявленный авторами «феномен безопасной компьютерной атаки», обусловленный халатностью и низкой культурой информационной безопасности, напрямую указывает на управленческий и кадровый риск для университетов. Более поздние работы Бикеева с соавт. (Бикеев, Клемин и др., 2022; Бикеев, Латыпова и др., 2022) о применении цифровых технологий в противодействии коррупции и использовании цифровых профилей задают контекст для анализа коррупционных и операционных рисков в экосистеме.

Современный европейский регуляторный опыт, детально проанализированный в монографии под редакцией Пастор Семпере (Pastor Sempere, 2025), показывает вектор движения к созданию комплексных правовых рамок для цифровых активов, идентичностей и пространств данных (регламенты *MiCA*, *eIDAS*, *FiDA*, *AI Act*, *DSA*, *DMA*) (Лойко, 2022). Концепция «Умных правовых экосистем» (*Smart Legal Ecosystems*), где нормативные требования встроены в киберфизические системы, представляет особый интерес для проектирования безопасных университетских экосистем. Однако данный подход требует адаптации к условиям

национального правового поля, где регуляторные требования к цифровой среде университетов (например, в области защиты персональных данных по ФЗ-152⁶, использования средств криптографической защиты информации, импортозамещения программного обеспечения) зачастую имеют иную архитектуру и порождают специфические риски соответствия.

4. Цифровая трансформация университетов: от платформ к экосистемам.

Исследования, специфичные для высшей школы, эволюционируют от изучения виртуальных обучающих сред к концепции цифровой образовательной экосистемы (*Digital Learning Ecosystem*, далее – *DLE*) (Wu et al., 2024). Систематический обзор Нгуен и Туамсук (Nguyen & Tuamsuk, 2022) выявляет компоненты *DLE* (биотические – участники, абиотические – технологии, контент, инфраструктура) и, что крайне важно, прямо указывает на пробелы в исследованиях, касающихся вопросов авторского права, интеллектуальной собственности на учебные материалы и интеграции контента. Этот пробел наше исследование нацелено заполнить.

Работы Европейской ассоциации университетов (далее – *EUA*) (Reichert, 2019; Kozirog et al., 2022) подчеркивают новую центральную роль университетов как «честных брокеров» и оркестраторов региональных инновационных экосистем. При этом они отмечают риски смещения исследовательских приоритетов в сторону краткосрочных прикладных проектов и выявляют проблему недостаточного развития рамок для урегулирования конфликтов интересов (только 43 % опрошенных учреждений имеют такие рамки (фреймворки)).

Фундаментальный вклад в понимание управления трансформацией вносят практико-ориентированные исследования Московской школы управления Сколково (Архитектура трансформации..., 2023; Назайкинская, Рамсбергер, 2025). Санников и Ширинкина показывают, что провалы трансформационных проектов в университетах в 75 % случаев обусловлены не технологическими, а управленческими и культурными дефицитами: несогласованностью видения, сопротивлением изменениям, отсутствием *data-driven* культуры и «боязнью неопределенности» (Санников, Ширинкина, 2023b). Это напрямую соотносится с управленческими рисками, анализируемыми в нашем исследовании.

Диссертационное исследование Санникова (2024) и его статьи в соавторстве с Ширинкиной (2023a) представляют готовые модели и эмпирически проверенную методику оценки сформированности цифровой экосистемы университета. Ключевой тезис о том, что эффективность экосистемы определяется ее способностью минимизировать транзакционные издержки, становится центральной экономической метрикой в нашем анализе.

5. Выявленные лакуны и исследовательский задел.

Проведенный анализ позволяет зафиксировать существующие пробелы в литературе:

1. Фрагментарность: большинство работ фокусируется либо на экономике, либо на праве, либо на педагогике цифровых экосистем. Комплексные исследования, проводящие системный синтез и выявляющие взаимосвязь правовых, экономических и управленческих рисков в едином объекте, единичны. Настоящее исследование нацелено на преодоление этой фрагментарности.

2. Недооценка правовых рисков: в то время как работы по *DLE* (Nguyen & Tuamsuk, 2022) лишь констатируют пробел в области ИС, а *EUA* (Kozirog et al., 2022) отмечают слабость управления конфликтами интересов, отсутствует комплексный анализ всей цепи правовых рисков в привязке к национальному законодательству: от киберпреступности и защиты данных по ФЗ-152⁷ до правового регулирования платформ и коррупционных схем в ИТ-закупках.

3. Отсутствие интегративных моделей управления рисками, адаптированных к российским реалиям: предложенные модели управления (Качалов и др., 2024; Санников, 2024) не интегрируют в полной мере правовой комплаенс и криминологический анализ. Концепция «экосистемы доверия» (van den Hoven et al., 2021), разработанная для европейского контекста, не адаптирована к специфике российской высшей школы и ее правовым реалиям, включая особенности регуляторного давления и унаследованные управленческие практики, что и составляет предмет настоящего исследования.

4. Теоретико-аналитический характер большинства работ и отсутствие апробированных инструментов операционализации моделей для университетов с разным уровнем цифровой зрелости.

⁶ О персональных данных. № 152-ФЗ от 27.07.2006 (последняя редакция). КонсультантПлюс. https://www.consultant.ru/document/cons_doc_LAW_61801/

⁷ Там же.

Таким образом, теоретический обзор не только демонстрирует солидную научную базу, на которую опирается исследование, но и четко артикулирует его научную новизну и практическую направленность. Настоящая работа призвана преодолеть выявленную фрагментарность, проведя комплексный системный анализ рисков цифровой экосистемы университета с учетом национального правового контекста и разработав интегративную модель управления, синтезирующую подходы системной экономики, права и менеджмента и предлагающую пути ее практической операционализации.

Результаты исследования

Проведенный системный анализ позволил выявить, классифицировать и глубоко проанализировать комплекс взаимосвязанных правовых и экономических рисков цифровых экосистем университетов. Основным результатом исследования является многоуровневая система рисков, структурированная по принципу тетрадной модели (Клейнер, 2023) и проецирующаяся на микро-, мезо- и макроуровни функционирования университета. Кроме того, разработана интегративная модель управления данными рисками.

1. Многоуровневая система рисков цифровой экосистемы университета

1.1. *Риски микроуровня (внутриэкосистемные)* связаны с функционированием конкретных элементов и подсистем цифровой экосистемы.

1.1.1. Критически высокие риски кибербезопасности и работы с данными:

– риск утечки конфиденциальных данных: университеты аккумулируют массивы персональных данных (студентов, сотрудников), биометрические данные, медицинские справки, результаты интеллектуальной деятельности. Отсутствие «цифровой гигиены» и сложность управления правами доступа в распределенной системе создают угрозы, сопоставимые с рисками в здравоохранении (Бикеев, Латыпова и др., 2022). Работа Бегишева и Бикеева (2020) прямо указывает на рост (на 33,7 %) преступлений в сфере цифровой информации, где вузы являются лакомой мишенью. В российских условиях данный риск усугубляется комплексом требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»⁸, в частности, необходимостью локализации обработки данных и соблюдения отраслевых стандартов Роскомнадзора, что создает значительные операционные и соответствующие издержки, особенно для вузов, использующих иностранные облачные сервисы;

– риск несанкционированного доступа и кибератак: выявлен «феномен безопасной компьютерной атаки» (Бегишев, Бикеев, 2020), обусловленный не только халатностью, но и системными причинами: нежеланием нести финансовые расходы на безопасность, низкой культурой информационной безопасности и нехваткой квалифицированных кадров. Это подтверждается кейсом внедрения системы электронного документооборота (далее – СЭД), где организационно-управленческие, а не технические факторы стали ключевым риском срыва проекта (Санников, Ширинкина, 2023а);

– риски, связанные с использованием ИИ: систематический обзор Рохаса и Чиappe (Rojas & Chiappe, 2024) выявляет проблемы алгоритмической предвзятости (*bias*), «цифрового следа» студентов и отсутствия прозрачности (*XAI – explainable AI*) в алгоритмах, принимающих педагогические и управленческие решения. Это порождает риски дискриминации и нарушения академических прав. В отсутствие прямого национального аналога *AI Act* правовая оценка таких рисков в российских вузах опирается на общие нормы о защите прав субъектов данных и недопустимости дискриминации, что создает высокую степень неопределенности.

1.1.2. Риски интеллектуальной собственности (далее – ИС) и правового вакуума:

– конфликт моделей создания ИС: существует фундаментальное противоречие между традиционной, «закрытой» моделью защиты ИС (патенты, авторское право) и появляющимися моделями открытой науки и пирингового производства (Benkler, 2001). Чрезмерно протекционистская позиция университетов в вопросах ИС, отмеченная Reichert (2019), может сама по себе стать барьером для инноваций и коллабораций;

⁸ О персональных данных. № 152-ФЗ от 27.07.2006 (последняя редакция). КонсультантПлюс. https://www.consultant.ru/document/cons_doc_LAW_61801/

– риск неопределенности правового статуса результатов: создание цифровых образовательных ресурсов, данных, алгоритмов силами смешанных команд (преподаватели, студенты, ИТ-специалисты) порождает сложные вопросы об обладателе прав и порядке их использования, что напрямую указывается как пробел в исследованиях (Nguyen & Tuamsuk, 2022). Этот риск в российских университетах осложнен внутренними положениями об информационных системах, которые зачастую не учитывают специфику совместной цифровой деятельности и коллаборации с внешними партнерами.

1.1.3. Локальные коррупционные риски.

Анализ работы Бикеева (2022) позволяет экстраполировать риски коррупционных схем при осуществлении крупных ИТ-закупок (тендеры на поставку оборудования, разработку платформ). Цифровизация процессов, как показано на примере медицинских профилей (Бикеев, Клемин и др., Латыпова, 2022), может быть эффективным инструментом противодействия таким схемам за счет создания «цифрового следа». Тем не менее сам процесс цифровизации закупок в рамках Федерального закона № 44-ФЗ⁹ и № 223-ФЗ¹⁰ сопряжен с рисками недобросовестного формулирования технических требований, завышения смет и лоббирования конкретных вендоров.

1.2. Риски мезоуровня (экосистемные/управленческие) связаны с управлением экосистемой как целостным образованием и ее взаимодействием с ближайшим окружением.

1.2.1. Управленческие и проектные риски (наиболее значимые по эмпирическим данным):

– риск провала трансформационного проекта: исследование Сколково (Назайкинская, Рамсбергер, 2025) идентифицирует пять ключевых признаков провала, коренящихся в дефицитах управления: 1) несогласованность обязательств руководства и исполнителей; 2) несоответствие видения и результатов; 3) отсутствие глубинных культурных изменений («Если преобразования не затрагивают ценности и негласные нормы... изменения остаются поверхностными»); 4) сохранение старых управленческих механизмов (например, системы оценки эффективности); 5) краткосрочность изменений;

– риск «боязни неопределенности»: в государственных и окологосударственных учреждениях, к которым относятся вузы, краткосрочные выгоды от цифровизации часто перевешиваются долгосрочными, но гипотетическими рисками (Санников, Ширинкина, 2023а). Яркий пример – заморозка проекта по внедрению СЭД из-за неопределенности с долгосрочным архивным хранением электронных документов. Этот риск актуализируется в условиях быстро меняющегося регулирования, например, требований по импортозамещению программного обеспечения, вынуждающих пересматривать архитектуру экосистемы;

– риск несбалансированности развития подсистем: согласно концепции многополярного управления (Клейнер, 2024с), в процессе цифровой трансформации вузов наблюдается диспропорция между развитием подсистем. Гипертрофированное наращивание объектной подсистемы (закупки оборудования и ПО) не сопровождается адекватным развитием средовой (формирование цифровой культуры и доверия) и проектной (развитие компетенций в управлении изменениями) подсистем, что создает системный риск неэффективности инвестиций.

1.2.2. Экономические риски эффективности:

– риск недостижения экономического эффекта: ключевой тезис Санникова (2024) о минимизации транзакционных издержек как цели экосистемы может не реализоваться. Высокие первоначальные инвестиции (Barykin et al., 2020) и стоимость владения сложными платформами могут не окупиться, если не обеспечена реальная интеграция сервисов и перестройка процессов;

– риск некорректной оценки эффективности: работа Федотова (2024) критикует узкофинансовые показатели. Для экосистемы необходима многосубъектная оценка (студенты, преподаватели, администрация), учитывающая не только экономичность (*efficiency*), но и результативность (*effectiveness*) и влияние (*impact*), такие как рост удовлетворенности, улучшение образовательных результатов, усиление регионального влияния.

⁹ О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд. № 44-ФЗ от 05.04.2013 (последняя редакция). КонсультантПлюс. https://www.consultant.ru/document/cons_doc_LAW_144624/

¹⁰ О закупках товаров, работ, услуг отдельными видами юридических лиц. № 223-ФЗ от 18.07.2011 (последняя редакция). КонсультантПлюс. https://www.consultant.ru/document/cons_doc_LAW_116964/

1.2.3. Риски регуляторного соответствия и «экосистемы доверия»:

– европейский тренд на создание «цифровой экосистемы доверия» (van den Hoven et al., 2021) через *GDPR*, *DGA* и *AI Act* задает высокую планку требований к защите данных, прозрачности алгоритмов и «альтруизму данных». Российским университетам, работающим в глобальном пространстве, необходимо соответствовать этим стандартам, что создает дополнительные сложности и риски несоответствия. Одновременно необходимость соблюдения российского регулирования (ФЗ-152¹¹, ФЗ-149 «Об информации»¹², требования ФСТЭК¹³) формирует дублирующие или конфликтующие соответствующие процедуры, увеличивая транзакционные издержки.

1.3. Риски макроуровня (внешние) обусловлены воздействием внешней среды на экосистему университета:

– геополитические и технологические риски: анализ пленарных докладов симпозиума ЦЭМИ РАН (Кувалин, 2024; Золотарев, 2024) указывает на экзистенциальные риски, связанные с санкционным давлением: разрыв логистических и технологических цепочек, потеря доступа к международным R & D-центрам и патентам, угроза использования «принудительных лицензий». Это напрямую бьет по способности университетов поддерживать и развивать сложную ИТ-инфраструктуру и вести передовые исследования. Для российских вузов это выливается в конкретные задачи импортозамещения, перехода на отечественное программное обеспечение и перестройки научной кооперации, что сопряжено с высокими транзакционными издержками и рисками снижения качества цифровых сервисов;

– риск цифрового неравенства: исследования *EUA* (Kozirog et al., 2022) и обзоры по ИИ (Rojas & Chiappe, 2024) предупреждают, что цифровизация может усугубить неравенство как между университетами (ведущие vs периферийные), так и внутри них (студенты с разным уровнем доступа к технологиям и цифровым компетенций).

2. Интегративная модель управления рисками цифровой экосистемы университета

На основе систематизации рисков разработана трехконтурная модель управления (см. рисунок), ориентированная на создание «цифровой экосистемы доверия» (van den Hoven et al., 2021) и минимизацию транзакционных издержек (Санников, 2024). Модель предлагает не только концептуальные рамки, но и конкретные инструменты для каждого контура, адаптированные к уровням цифровой зрелости вуза.

Первый (превентивный) контур: правовой и регуляторный каркас. Цель: минимизация рисков несоответствия и создание правовой определенности. Инструменты для университета: 1) регулярный правовой аудит экосистемы на соответствие ФЗ-152, ФЗ-273, отраслевым приказам Минобрнауки, политикам импортозамещения; 2) разработка и актуализация внутренних регламентов: политика ИС для цифровых ресурсов, регламент обработки персональных данных, положение об этике использования ИИ; 3) создание или усиление комплаенс-функции, ответственной за мониторинг изменений в регулировании.

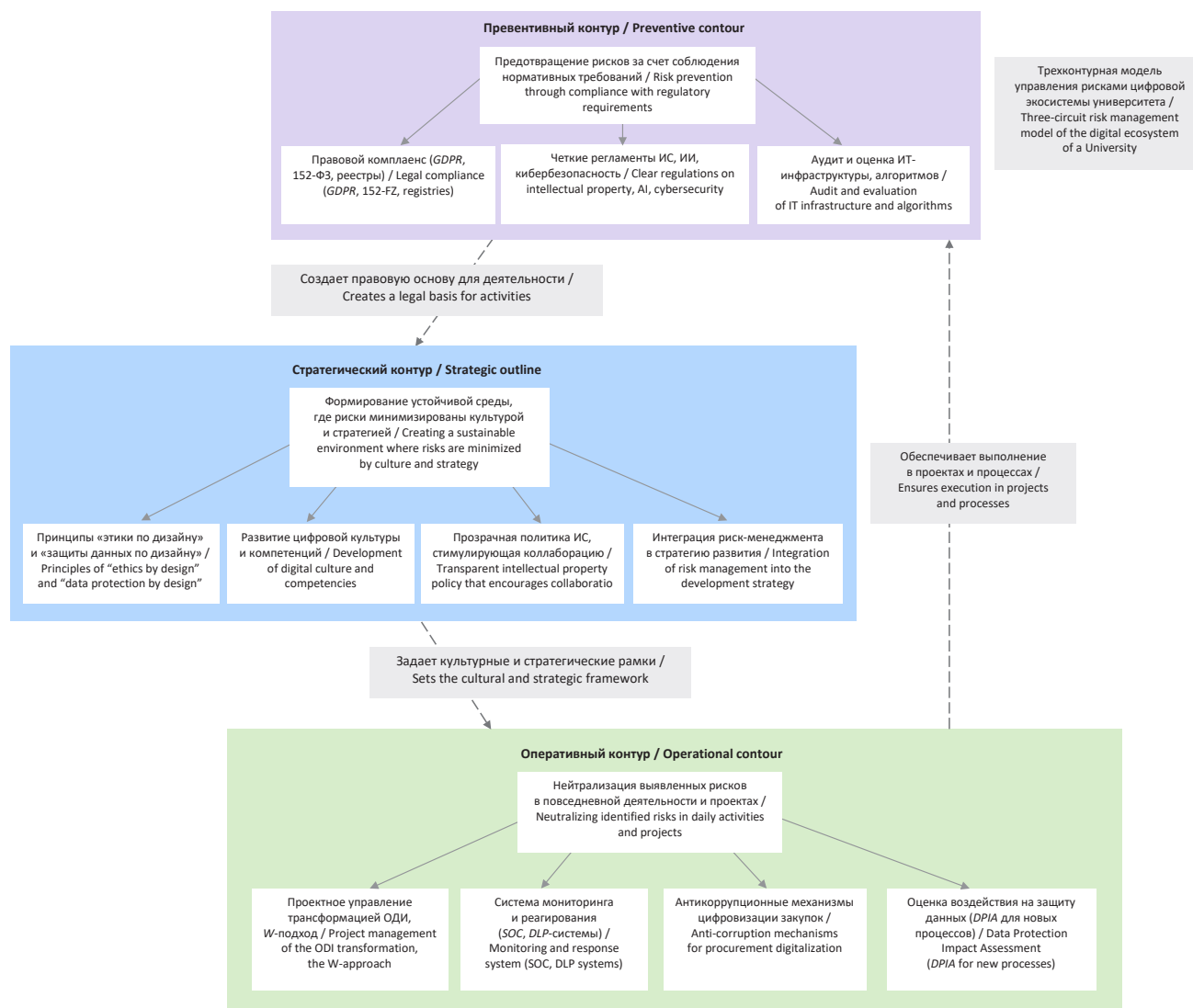
Второй (оперативный) контур: проектное управление и интеграция. Цель: управление реализацией и минимизация проектных рисков. Инструменты для университета: 1) применение гибких методологий (*Agile*, *Scrum*) для ИТ-проектов с обязательным включением в команды представителей бизнес-подразделений и юристов; 2) внедрение инструментов риск-менеджмента на уровне проектов (матрицы рисков, регулярные риск-ревью); 3) использование методологии Санникова (2024) для диагностики цифровой зрелости и определения приоритетных направлений трансформации.

Третий (стратегический) контур: культура доверия и стратегическое развитие. Цель: формирование среды, где соблюдение правил становится естественной нормой. Инструменты для университета: 1) программы развития цифровой грамотности и культуры безопасности для всех категорий сотрудников и студентов; 2) внедрение прозрачных механизмов обратной связи и соуправления развитием экосистемы (например, через цифровые платформы для сбора идей); 3) формирование «этического чартера» цифровой экосистемы, закрепляющего ценности открытости, безопасности и взаимного доверия.

¹¹ О персональных данных. № 152-ФЗ от 27.07.2006 (последняя редакция). КонсультантПлюс. https://www.consultant.ru/document/cons_doc_LAW_61801/

¹² Об информации, информационных технологиях и о защите информации. № 149-ФЗ от 27.07.2006 (последняя редакция). КонсультантПлюс. https://www.consultant.ru/document/cons_doc_LAW_61798/

¹³ Требования по безопасности информации к средствам обнаружения и реагирования на уровне узла (Выписка) (утв. Приказом ФСТЭК России № 58 от 26.02.2025). КонсультантПлюс. https://www.consultant.ru/document/cons_doc_LAW_509238/



Трехконтурная модель управления рисками цифровой экосистемы университета

Примечание: ОДИ (организационно-деятельностные игры) – методология, разработанная Г. П. Щедровицким.

Three-circuit risk management model of the digital ecosystem of a University

Note: ODI (Organizational-Activity Games – a methodology developed by G. P. Shchedrovitsky.

Синергетический эффект модели достигается за счет взаимодействия контуров. Например, превентивный контур задает правовые рамки (например, регламент по ИИ), оперативный – обеспечивает их выполнение в проектах по внедрению алгоритмических систем, а стратегический – формирует культуру, при которой этическое использование ИИ становится естественной нормой, снижая тем самым транзакционные издержки на контроль и принуждение. Для вузов с низкой цифровой зрелостью предлагается начинать с фокуса на превентивном и оперативном контурах, постепенно подключая стратегический. Для продвинутых вузов ключевой становится интеграция всех трех контуров в единую систему.

Таким образом, результаты исследования представляют собой не просто перечень рисков, а системную диагностику «болевых точек» цифровой трансформации университета и практико-ориентированный фреймворк для их устранения, интегрирующий управленческие, экономические и правовые инструменты и предлагающий конкретные шаги по внедрению.

Обсуждение. Проведенное исследование позволило не только систематизировать риски цифровых экосистем университетов, но и выявить фундаментальные противоречия, требующие пересмотра традиционных подходов к управлению высшей школой. Полученные результаты позволяют сформулировать следующие ключевые положения для научной дискуссии.

1. Синтез результатов и теоретическая значимость.

Предложенная многоуровневая система рисков демонстрирует, что цифровая трансформация университета – это не просто техническая модернизация, а глубокий социотехнический сдвиг (Mandych et al., 2023), затрагивающий все аспекты его деятельности. Выявленная взаимосвязь рисков подтверждает правомерность применения системной экономической теории (Клейнер, 2024b, 2024c) для анализа подобных сложных объектов. В частности, тетрадная модель оказалась высокоэффективным инструментом для диагностики слабых мест: так, отставание в развитии средовой подсистемы (цифровая культура, доверие) неизбежно нивелирует инвестиции в объектную подсистему (платформы, ИТ-инфраструктура), что находит эмпирическое подтверждение в исследованиях провалов трансформации (Назайкинская, Рамсбергер, 2025; Санников, Ширинкина, 2023b).

Разработанная трехконтурная модель управления является практическим ответом на выявленную в литературе фрагментарность подходов. Она интегрирует разрозненные аспекты: от превентивного правового режима (Pastor Sempere, 2025; van den Hoven et al., 2021) до стратегического формирования культуры доверия, адаптируя передовые концепции к российскому регуляторному контексту (ФЗ-152¹⁴, ФЗ-273¹⁵, политика импортозамещения). Модель согласуется с концепцией динамических способностей (Volz et al., 2025), но расширяет ее, добавляя правовую и криминологическую составляющие, что особенно актуально для университетов как публичных институтов с высокой социальной ответственностью. Новизна модели заключается именно в этом синтезе и ее операционализации через конкретные инструменты для каждого контура.

2. Вклад в существующие исследования.

Настоящее исследование вносит вклад в преодоление ключевых лакун, выявленных в теоретическом обзоре:

– Преодоление фрагментарности и уточнение новизны: работа предлагает целостный взгляд, увязывая, например, киберриски (Бегишев, Бикеев, 2020) с управленческими дефицитами (Архитектура трансформации..., 2023) и экономическими последствиями в виде роста транзакционных издержек (Санников, 2024). Показано, что кибератака – это не только технический инцидент, но и следствие недофинансирования информационно-безопасности, слабой культуры и неадекватной системы управления. Таким образом, вклад работы заключается не в открытии абсолютно новых категорий рисков, а в их системном синтезе в рамках единого объекта (цифровой экосистемы университета), построении целостной классификации, учитывающей национальную специфику, и в разработке интегративной модели управления, направленной на устранение выявленных системных противоречий.

– Углубление анализа правовых рисков: в отличие от работ, лишь констатирующих проблемы ИС (Nguyen & Tuamsuk, 2022), данное исследование раскрывает системный конфликт между «закрытой» и «открытой» моделями создания знаний (Benkler, 2001) и предлагает инструменты его разрешения через прозрачную политику ИС в стратегическом контуре управления. Более того, в анализ впервые включен комплексный обзор рисков, порождаемых именно российским правовым полем (от соответствия с ФЗ-152 до коррупционных схем в закупках по 44-ФЗ).

– Адаптация передовых концепций и предложение механизмов внедрения: концепция «экосистемы доверия» (van den Hoven et al., 2021) адаптирована к реалиям российской высшей школы с ее специфическим регуляторным давлением и унаследованными управленческими практиками. Основной практический вклад – предложение конкретных, дифференцированных по уровням зрелости вуза инструментов и шагов для реализации модели (см. раздел «Результаты»), что выводит работу за рамки чисто теоретического конструкта.

¹⁴ О персональных данных. № 152-ФЗ от 27.07.2006 (последняя редакция). КонсультантПлюс. https://www.consultant.ru/document/cons_doc_LAW_61801/

¹⁵ Об образовании в Российской Федерации. № 273-ФЗ от 29.12.2012 (последняя редакция). КонсультантПлюс. https://www.consultant.ru/document/cons_doc_LAW_140174/

3. Практическая имплементация и управленческие импликации.

Реализация предложенной модели требует от руководства университетов перехода от реактивного к проактивному управлению. Для апробации модели и снижения риска ее отрыва от практики предлагается следующий поэтапный план действий:

Для руководителей вузов: ключевая рекомендация – начать трансформацию не с закупки технологий, а с диагностики собственной цифровой зрелости (по методике Санникова (2024)) и «культурного аудита». Необходимо создание сквозной системы ответственности за риски, где ректорат отвечает за стратегический контур, проектные офисы – за оперативный, юридические и комплаенс-службы – за превентивный. В качестве первого шага предлагается инициировать пилотный проект по одному из критических рисков (например, составление реестра и карты обработки персональных данных в соответствии с ФЗ-152), реализуемый силами междисциплинарной рабочей группы.

– Для регуляторов и органов управления образованием: целесообразно инициировать разработку отраслевых стандартов и методических рекомендаций по управлению рисками цифровых экосистем, учитывающих предложенную классификацию. Особого внимания требует правовое регулирование использования ИИ в образовании и научных исследованиях. В качестве конкретной меры можно предложить создание типовых регламентов (политик) для вузов по работе с цифровыми ресурсами, защите данных и этике ИИ.

– Для ИТ-подразделений: результаты исследования обосновывают необходимость тесной интеграции с бизнес-подразделениями и юридическими службами. Внедрение любой новой платформы должно сопровождаться не только техническим, но и правовым аудитом, а также оценкой воздействия на культуру и процессы. На операционном уровне рекомендуется внедрить практику обязательного включения представителя соответствующей службы в состав проектных команд по внедрению ключевых цифровых сервисов.

4. Ограничения и перспективы дальнейших исследований.

Основное ограничение работы, как и было указано в методах, – ее теоретико-аналитический характер. Верификация и тонкая настройка предложенной модели, а также оценка эффективности конкретных инструментов требуют масштабной эмпирической апробации, что задает программу для дальнейшей работы.

Перспективные направления для будущих исследований включают:

1. Эмпирическую валидацию модели: проведение кейс-стади и практических исследований в университетах с разным уровнем цифровой зрелости для проверки эффективности трехконтурного подхода и предложенных инструментов. Первым шагом может стать разработка детальной дорожной карты внедрения модели для типового вуза.

2. Разработку метрик доверия: создание и апробация количественных и качественных показателей для оценки уровня «доверия» в цифровой экосистеме (например, индексы прозрачности, вовлеченности, удовлетворенности и безопасности).

3. Глубинное исследование этики ИИ: анализ конкретных кейсов использования алгоритмов для приема, обучения и оценки студентов с точки зрения дискриминации, прозрачности и подотчетности, а также разработка отраслевых этических руководств для российских вузов.

4. Сравнительный анализ регуляторных режимов: детальное сопоставление правовых рисков и возможностей для университетов в рамках российского, европейского и азиатского законодательства с целью разработки рекомендаций по гармонизации соответствующих процессов в международных коллаборациях.

Заключение

1. Цифровая экосистема университета представляет собой сложный социотехнический объект, функционирование которого сопряжено с комплексом взаимосвязанных правовых, экономических и управленческих рисков, структурируемых на микро-, мезо- и макроуровнях. Наиболее критичными являются риски, возникающие на стыке технологий и человеческого фактора: кибербезопасности, управления данными и организационной культуры. Особую остроту в российских условиях приобретают риски, порожденные дублирующими регуляторными требованиями, необходимостью импортозамещения и недостаточной проработанностью отраслевых регламентов.

2. Ключевым системным противоречием является конфликт между ускоренным технологическим развитием, требующим гибкости и открытости, и консервативной нормативно-правовой средой, а также унаследованными управленческими моделями, не адаптированными к экосистемной парадигме.

3. Эффективное управление рисками невозможно в рамках отраслевого или узкопрофессионального сотрудничества. Оно требует интегративной стратегии, синтезирующей блокировки соответствия, проектного управления трансформацией и целенаправленного управления цифровой культурой доверия, что и реализовано в предложенной трехконтурной модели.

4. Предложенная трехконтурная модель управления рисками с конкретным инструментарием представляет собой практический инструмент для руководства университетов, позволяющий перейти от фрагментарного реагирования на инциденты к созданию устойчивой, безопасной и развивающейся цифровой среды. Ее внедрение, адаптированное к уровню зрелости вуза, способно минимизировать транзакционные издержки и реализовать стратегический потенциал цифровизации.

Таким образом, построение безопасной и эффективной цифровой экосистемы является не технологическим вызовом, а в первую очередь управленческой и стратегической задачей, требующей системного мышления, междисциплинарного подхода и долгосрочных инвестиций в человеческий и институциональный капитал. Данное исследование предоставляет как теоретический базис для понимания этой задачи, так и практический фреймворк для ее решения.

Список литературы

Архитектура трансформации университета: экспертный доклад Центра трансформации образования Сколково. (2023). М.: Московская школа управления Сколково.

Бегишев, И. Р., Бикеев, И. И. (2020). *Преступления в сфере обращения цифровой информации*. Казань: Изд-во «Познание» Казанского инновационного университета.

Бегишев, И. Р., Бикеев, И. И., Галимов, А. Г. (2021). Признаки преступления в сфере обращения цифровой информации. *Материалы Международного форума "Kazan Digital Week – 2021"* (с. 261–268). EDN: SXBGKF

Бикеев, И. И. (2022). Некоторые вопросы применения цифровых технологий в противодействии коррупции. *Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции*. В 6 т. (с. 33–36). Казань: Изд-во «Познание» Казанского инновационного университета. EDN: LUBCJT

Бикеев, И. И., Клемин, А. В., Латыпова, Э. Ю. (2022). Индивидуальный цифровой медицинский профиль как эффективное средство противодействия коррупции. *Пробелы в российском законодательстве*, 15(7), 153–159. EDN: KTJNUV

Бикеев, И. И., Латыпова, Э. Ю., Гильманов, Р. Э. (2022). Содержание индивидуального медицинского профиля как инструмент повышения уголовно-правовой безопасности медицинской помощи. *Проблемы экономики и юридической практики*, 18(6), 143–149. EDN: HAGIMX

Григорьев, С. Г., Сабитов, Р. А., Смирнова, Г. С., Сабитов, Ш. Р. (2020). Концепция формирования и развития цифровой интеллектуальной экосистемы смешанного университетского обучения. *Информатика и образование*, 5(314), 15–23. EDN: LMWOIT. DOI: 10.32517/0234-0453-2020-35-5-15-23

Дорошенко, С. В., Шеломенцев, А. Г. (2017). Предпринимательская экосистема в современных социоэкономических исследованиях. *Институциональная экономика*, 4, 212–218. EDN: ZVMLAZ

Золотарев, П. С. (2024). Стратегическое планирование промышленного предприятия в кризисной ситуации: взаимодействие с корпоративными органами управления. В сб. *Стратегическое планирование и развитие предприятий: сборник пленарных докладов и материалов круглого стола XXIV Всероссийского симпозиума* (с. 74–83). Москва: ЦЭМИ РАН. EDN: MOJWUK. DOI: 10.34706/978-5-8211-0821-0-74-83

Качалов, Р. М., Кобылко, А. А., Слепцова, Ю. А. (2024). *Управление деятельностью социально-экономических экосистем*. Москва: ЦЭМИ РАН. EDN: EUSPAB.

Клейнер, Г. Б. (2024a). Многополярное управление организацией. *Российский журнал менеджмента*, 22(2), 163–178. EDN: CSLMLC. DOI: 10.21638/spbu18.2024.201

Клейнер, Г. Б. (2024b). Системный менеджмент: информационная реконструкция для новой экономики. В сб. *Стратегическое планирование и развитие предприятий: сборник пленарных докладов и материалов круглого стола XXIV Всероссийского симпозиума* (с. 8–18). Москва: ЦЭМИ РАН. EDN: CXPFXE. DOI: 10.34706/978-5-8211-0821-0-8-18

Клейнер, Г. Б. (2024c). Стратегическое планирование и экономические циклы: системный подход. *Научные труды ВЭО России*, 248(4), 452–460. EDN: GKWJKN. DOI: 10.38197/2072-2060-2024-248-4-452-460

Кувалин, Д. Б. (2024). Адаптация российских предприятий к санкционному кризису: проблемы и решения. В сб. *Стратегическое планирование и развитие предприятий: сборник пленарных докладов и материалов круглого стола XXIV Всероссийского симпозиума* (с. 19–31). Москва: ЦЭМИ РАН. EDN: ESJNEM. DOI: 10.34706/978-5-8211-0821-0-19-31

Лойко, А. И. (2022). Технологии цифровых экосистем. *Вестник Самарского государственного технического университета. Серия: Философия*, 4(1), 49–56. <https://doi.org/10.17673/vsgtu-phil.2022.1.7>

Назайкинская, О., Рамсбергер, В. (2025). *О чем молчат лидеры трансформации: Как дефициты управления ведут к провалам университетских проектов*. Москва: Московская школа управления Сколково, Центр трансформации образования.

- Санников, Д. В. (2024). *Проектный менеджмент при формировании цифровой экосистемы университета: дис. ... канд. экон. наук*. Сургут: Сургутский государственный университет. EDN: KEJMGС
- Санников, Д. В., Ширинкина, Е. В. (2023a). Система электронного документооборота как «кровеносная система» цифровой экосистемы университета, или Как боязнь неопределенности препятствует развитию. *Лидерство и менеджмент*, 10(1), 219–240. EDN: FOOEUY. DOI: 10.18334/lim.10.1.117063
- Санников, Д. В., Ширинкина, Е. В. (2023b). Организационно-деятельностная игра как инструмент проектного управления при реализации стратегии цифровой трансформации университета. *Лидерство и менеджмент*, 10(2), 597–612. EDN: BOMPHU. DOI: 10.18334/lim.10.2.117212
- Федотов, Ю. В. (2024). Эффективность деятельности организации: вопросы измерения в условиях усиления требований ESG. В сб. *Стратегическое планирование и развитие предприятий: сборник пленарных докладов и материалов круглого стола XXIV Всероссийского симпозиума* (с. 53–65). Москва: ЦЭМИ РАН. EDN: ICWUIF. DOI: 10.34706/978-5-8211-0821-0-53-65
- Anvari, R., Moradi, F., & Shirvani, A. (2024). Digital learning ecosystem at educational institutions: A 4-university perspective. *Professional Studies: Theory and Practice*, 28(1). <https://doi.org/10.56131/pstp.2024.28.1.275>
- Barykin, S. Y., Kapustina, I. V., Kirillova, T. V., Yadykin, V. K., & Konnikov, Y. A. (2020). Economics of digital ecosystems. *Journal of Open Innovation: Technology, Market, and Complexity*, 6(4), 124. EDN: QRLVUV. DOI: 10.3390/joitmc6040124
- Benkler, Y. (2001). The battle over the institutional ecosystem in the digital environment. *Communications of the ACM*, 44(2), 84–90. EDN: DTBJCD. DOI: 10.1145/359205.359235
- Briscoe, G. (2009). *Digital Ecosystems: Doctoral dissertation*. Imperial College London.
- Dulrud, A., & Bygstad, B. (2022). Digital ecosystems as social institutions: exploring the role of consumption through four research streams of digital ecosystems. *Consumption and Society*, 1(1), 99–119. EDN: RCGULA. DOI: 10.1332/quph6141
- Gomez, S., Andersson, H., Park, J., Maw, S., Crook, A., & Orsmond, P. (2013). A digital ecosystems model of assessment feedback on student learning. *Higher Education Studies*, 3(2), 41–53. <https://doi.org/10.5539/hes.v3n2p41>
- Goodfellow, R., & Lea, M. R. (Eds.). (2013). *Literacy in the digital university: Critical perspectives on learning, scholarship, and technology*. Routledge. <https://doi.org/10.4324/9780203074510>
- Hniezdovskyi, O., Domashenko, D., Domashenko, S., Morozov, D., & Shylo, S. (2025). Digital solutions for risk management in sustainable development conditions of business ecosystems. *Applied Computer Science*, 21(2). EDN: YPZSVH. DOI: 10.35784/acs_6935
- Kozirog, K., Lucaci, S., & Berghmans, S. (2022). *Universities as key drivers of sustainable innovation ecosystems: Results of the EUA survey on universities and innovation*. Brussel: European University Association.
- Krogstie, J. (2012). Modeling of Digital Ecosystems: Challenges and Opportunities. In L. M. Camarinha-Matos, L. Xu, & H. Afsarmanesh (Eds.), *Collaborative Networks in the Internet of Services. PRO-VE 2012. IFIP Advances in Information and Communication Technology* (Vol. 380, pp. 137–145). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-32775-9_14
- Leal, M., Leal, C., & Silva, R. (2025). Entrepreneurial Ecosystems and Knowledge Management: Systematic Literature Review and Bibliometric Analysis. *Journal of the Knowledge Economy*. EDN: SWUCTC. DOI: 10.1007/s13132-025-02730-9
- Mandych, O., Zaika, S., Zaika, O., Zhyliakova, O., & Blyzniuk, O. (2023). Risk management of innovation activities in the digital ecosystem. *Innovations in the Scientific, Technical and Social Ecosystems*, 1(6), 24–45. <https://doi.org/10.56378/mozs20231805>
- Nguyen, L. T., & Tuamsuk, K. (2022). Digital learning ecosystem at educational institutions: A content analysis of scholarly discourse. *Cogent Education*, 9(1), 2111033. EDN: PZPPQD. DOI: 10.1080/2331186x.2022.2111033
- Oluoha, O. M., Odeskina, A., Reis, O., Okpeke, F., Attipoe, V., & Orieno, O. H. (2023). A privacy-first framework for data protection and compliance assurance in digital ecosystems. *IRE Journals*, 7(4), 620–646.
- Pastor Sempere, C. (2025). The Legal Framework for New Digital Assets, Identities, and Data Spaces. Introduction. In C. Pastor Sempere (Eds.), *Governance and Control of Data and Digital Economy in the European Single Market. Law, Governance and Technology Series* (Vol. 71). Springer, Cham. https://doi.org/10.1007/978-3-031-74889-9_1
- Reichert, S. (2019). *The role of universities in regional innovation ecosystems*. European University Association.
- Rojas, M. P., & Chiappe, A. (2024). Artificial Intelligence and Digital Ecosystems in Education: A Review. *Technology, Knowledge and Learning*, 29, 2153–2170. EDN: HSORBI. DOI: 10.1007/s10758-024-09732-7
- Satalkina, L., & Steiner, G. (2020). Digital Entrepreneurship and its Role in Innovation Systems: A Systematic Literature Review as a Basis for Future Research Avenues for Sustainable Transitions. *Sustainability*, 12(7), 2764. EDN: AGBKRE. DOI: 10.3390/su12072764
- van den Hoven, J., Comandé, G., Ruggieri, S., Domingo-Ferrer, J., Musiani, F., Giannotti, F., Pratesi, F., Stauch, M., & Lishchuk, I. (2021). Towards a Digital Ecosystem of Trust: Ethical, Legal and Societal Implications. *Opinio Juris in Comparatione*, 1(1), 131–156.
- Volz, F., Münch, C., Küffner, C., & Hartmann, E. (2025). Digital ecosystems and their impact on organizations – A dynamic capabilities approach. *International Journal of Management Reviews*, 27, 398–419. EDN: NDAXBE. DOI: 10.1111/ijmr.12396
- Wu, J., Chen, L., & Wen, B. (2024). Educational Ecosystems in Digital Media: Insights from Leading Universities in the United States. *Journal of Interdisciplinary Insights*, 2(1), 67–75. <https://doi.org/10.5281/zenodo.10903342>

References

- Anvari, R., Moradi, F., & Shirvani, A. (2024). Digital learning ecosystem at educational institutions: A 4-university perspective. *Professional Studies: Theory and Practice*, 28(1). <https://doi.org/10.56131/pstp.2024.28.1.275>

- Barykin, S. Y., Kapustina, I. V., Kirillova, T. V., Yadykin, V. K., & Konnikov, Y. A. (2020). Economics of digital ecosystems. *Journal of Open Innovation: Technology, Market, and Complexity*, 6(4), 124. <https://doi.org/10.3390/joitmc6040124>
- Begishev, I. R., & Bikeev, I. I. (2020). *Crime if the sphere of digital information circulation*. Kazan: Poznanie Publishing House. (In Russ.).
- Begishev, I. R., Bikeev, I. I., & Galimov, A. G. (2021). Signs of a crime in the field of digital information circulation. In *Proceedings of the International Forum "Kazan Digital Week – 2021"* (pp. 261–268). (In Russ.).
- Benkler, Y. (2001). The battle over the institutional ecosystem in the digital environment. *Communications of the ACM*, 44(2), 84–90. <https://doi.org/10.1145/359205.359235>
- Bikeev, I. I. (2022). Some issues of the use of digital technologies in anti-corruption. In *Digital Technologies and Law. Collection of scientific papers of the I International Scientific and Practical Conference. In 6 volumes* (pp. 33–36). Kazan: Poznanie Publishing House. (In Russ.).
- Bikeev, I. I., Klemin, A. V., & Latypova, E. Yu. (2022). Individual digital medical profile as an effective means of countering corruption. *Gaps in Russian Legislation*, 15(7), 153–159. (In Russ.).
- Bikeev, I. I., Latypova, E. Yu., & Gilmanov, R. E. (2022). The content of an individual medical profile as a tool for improving the criminal law safety of medical care. *Economic Problems and Legal Practice*, 18(6), 143–149. (In Russ.).
- Briscoe, G. (2009). *Digital Ecosystems: Doctoral dissertation*. Imperial College London.
- Doroshenko, S. V., & Shelomentsev, A. G. (2017). The entrepreneurial ecosystem in the contemporary socio-economic studies. *Russian Journal of Economic Theory*, 4, 212–218. (In Russ.).
- Dulrud, A., & Bygstad, B. (2022). Digital ecosystems as social institutions: exploring the role of consumption through four research streams of digital ecosystems. *Consumption and Society*, 1(1), 99–119. <https://doi.org/10.1332/QUPH6141>
- Fedotov, Yu. V. (2024). Efficiency in the performance of an organization: measurement under increased ESG requirements. *Strategic planning and development of an enterprise: collection of plenary reports and round table materials of the 24th All-Russia symposium* (pp. 53–65). Moscow: CEMI RAS. (In Russ.). <https://doi.org/10.34706/978-5-8211-0821-0-53-65>
- Gomez, S., Andersson, H., Park, J., Maw, S., Crook, A., & Orsmond, P. (2013). A digital ecosystems model of assessment feedback on student learning. *Higher Education Studies*, 3(2), 41–53. <https://doi.org/10.5539/hes.v3n2p41>
- Goodfellow, R., & Lea, M. R. (Eds.). (2013). *Literacy in the digital university: Critical perspectives on learning, scholarship, and technology*. Routledge. <https://doi.org/10.4324/9780203074510>
- Grigoriev, S. G., Sabitov, R. A., Smirnova, G. S., & Sabitov, Sh. R. (2020). The concept of the formation and development of a digital intellectual ecosystem of blended university learning. *Informatics and Education*, 5(314), 15–23. <https://doi.org/10.32517/0234-0453-2020-35-5-15-23>
- Hniezdovskyi, O., Domashenko, D., Domashenko, S., Morozov, D., & Shylo, S. (2025). Digital solutions for risk management in sustainable development conditions of business ecosystems. *Applied Computer Science*, 21(2). https://doi.org/10.35784/acs_6935
- Kachalov, R. M., Kobylko, A. A., & Sleptsova, Yu. A. (2024). *Managing the activities of socio-economic ecosystems*. Moscow: CEMI RAS. (In Russ.).
- Kleiner, G. B. (2024a). Multipolar management of organization. *Russian Management Journal*, 22(2), 163–178. (In Russ.). <https://doi.org/10.21638/spbu18.2024.201>
- Kleiner, G. B. (2024b). System management: informational reconstruction for a new economy. *Strategic planning and development of an enterprise: collection of plenary reports and round table materials of the 24th All-Russia symposium* (pp. 8–18). Moscow: CEMI RAS. (In Russ.). <https://doi.org/10.34706/978-5-8211-0821-0-8-18>
- Kleiner, G. B. (2024c). Strategic planning and economic cycles: systems approach. *Scientific Works of the Free Economic Society of Russia*, 248(4), 452–460. (In Russ.). <https://doi.org/10.38197/2072-2060-2024-248-4-452-460>
- Kozirog, K., Lucaci, S., & Berghmans, S. (2022). *Universities as key drivers of sustainable innovation ecosystems: Results of the EUA survey on universities and innovation*. Brussel: European University Association.
- Krogstie, J. (2012). Modeling of Digital Ecosystems: Challenges and Opportunities. In L. M. Camarinha-Matos, L. Xu, & H. Afsarmanesh (Eds.), *Collaborative Networks in the Internet of Services. PRO-VE 2012. IFIP Advances in Information and Communication Technology* (Vol. 380, pp. 137–145). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-32775-9_14
- Kuvalin, D. B. (2024). Adaptation of Russian enterprises to the sanction crisis: problems and solutions. *Strategic planning and development of an enterprise: collection of plenary reports and round table materials of the 24th All-Russia symposium* (pp. 19–31). Moscow: CEMI RAS. (In Russ.).
- Leal, M., Leal, C., & Silva, R. (2025). Entrepreneurial Ecosystems and Knowledge Management: Systematic Literature Review and Bibliometric Analysis. *Journal of the Knowledge Economy*. <https://doi.org/10.1007/s13132-025-02730-9>
- Loiko, A. I. (2022). Technologies of digital ecosystems. *Vestnik of Samara State Technical University. Series Philosophy*, 4(1), 49–56. (In Russ.). <https://doi.org/10.17673/vsgtu-phil.2022.1.7>
- Mandych, O., Zaika, S., Zaika, O., Zhyliakova, O., & Blyzniuk, O. (2023). Risk management of innovation activities in the digital ecosystem. *Innovations in the Scientific, Technical and Social Ecosystems*, 1(6), 24–45. <https://doi.org/10.56378/mozs20231805>
- Nazaykinskaya, O., & Ramsberger, V. (2025). *О чем молчат лидеры трансформации: Как дефициты управления ведут к провалам университетских проектов*. Moscow: Moscow School of Management Skolkovo, Center for Education Transformation. (In Russ.).
- Nguyen, L. T., & Tuamsuk, K. (2022). Digital learning ecosystem at educational institutions: A content analysis of scholarly discourse. *Cogent Education*, 9(1), 2111033. <https://doi.org/10.1080/2331186x.2022.2111033>

- Oluoha, O. M., Odeskina, A., Reis, O., Okpeke, F., Attipoe, V., & Orieno, O. H. (2023). A privacy-first framework for data protection and compliance assurance in digital ecosystems. *IRE Journals*, 7(4), 620–646.
- Pastor Sempere, C. (2025). The Legal Framework for New Digital Assets, Identities, and Data Spaces. Introduction. In C. Pastor Sempere (Eds.), *Governance and Control of Data and Digital Economy in the European Single Market. Law, Governance and Technology Series* (Vol. 71). Springer, Cham. https://doi.org/10.1007/978-3-031-74889-9_1
- Reichert, S. (2019). *The role of universities in regional innovation ecosystems*. European University Association.
- Rojas, M. P., & Chiappe, A. (2024). Artificial Intelligence and Digital Ecosystems in Education: A Review. *Technology, Knowledge and Learning*, 29, 2153–2170. <https://doi.org/10.1007/s10758-024-09732-7>
- Sannikov, D. V. (2024). *Project management in the formation of a university digital ecosystem: Cand. Sci. (Economics) thesis*. Surgut: Surgut State University. (In Russ.).
- Sannikov, D. V., & Shirinkina, E. V. (2023a). The electronic document management system as the distributor of the university's digital ecosystem, or how a fear of uncertainty hinders development. *Leadership and Management*, 10(1), 219–240. (In Russ.). <https://doi.org/10.18334/ilm.10.1.117063>
- Sannikov, D. V., & Shirinkina, E. V. (2023b). An organizational and activity game as a project management tool for implementing a university's digital transformation strategy. *Leadership and Management*, 10(2), 597–612. (In Russ.). <https://doi.org/10.18334/ilm.10.2.117212>
- Satalkina, L., & Steiner, G. (2020). Digital Entrepreneurship and its Role in Innovation Systems: A Systematic Literature Review as a Basis for Future Research Avenues for Sustainable Transitions. *Sustainability*, 12(7), 2764. <https://doi.org/10.3390/su12072764>
- van den Hoven, J., Comandé, G., Ruggieri, S., Domingo-Ferrer, J., Musiani, F., Giannotti, F., Pratesi, F., Stauch, M., & Lishchuk, I. (2021). Towards a Digital Ecosystem of Trust: Ethical, Legal and Societal Implications. *Opinio Juris in Comparatione*, 1(1), 131–156.
- Volz, F., Münch, C., Küffner, C., & Hartmann, E. (2025). Digital ecosystems and their impact on organizations – A dynamic capabilities approach. *International Journal of Management Reviews*, 27, 398–419. <https://doi.org/10.1111/ijmr.12396>
- Wu, J., Chen, L., & Wen, B. (2024). Educational Ecosystems in Digital Media: Insights from Leading Universities in the United States. *Journal of Interdisciplinary Insights*, 2(1), 67–75. <https://doi.org/10.5281/zenodo.10903342>
- Zolotarev, P. S. (2024). Strategic planning of an industrial enterprise under crisis: interaction with corporate management bodies.. *Strategic planning and development of an enterprise: collection of plenary reports and round table materials of the 24th All-Russia symposium* (pp. 74–83). Moscow: CEMI RAS. (In Russ.). <https://doi.org/10.34706/978-5-8211-0821-0-74-83>
- Architecture of a university transformation: an expert report by the Skolkovo Center for Education Transformation*. (2023). Moscow: Moscow School of Management Skolkovo. (In Russ.).

Вклад автора

Автор подтверждает, что полностью отвечает за все аспекты представленной работы.

Author's contribution

The author confirms sole responsibility for all aspects of the work.

Информация об использовании искусственного интеллекта

ИИ не использовался.

Information about the use of artificial intelligence

AI was not used.

Конфликт интересов / Conflict of Interest

Автором не заявлен / No conflict of interest is declared by the author

История статьи / Article history

Дата поступления / Received 04.11.2025

Дата одобрения после рецензирования / Date of approval after reviewing 05.02.2026

Дата принятия в печать / Accepted 25.02.2026