

Алиев Элдияр Сталбекович

Магистрант

Кыргызско-Российского Славянского университета им.

Б.Н.Ельцина

Кыргызстан, г. Бишкек

РИСКИ ВНЕДРЕНИЯ ЦИФРОВЫХ ПЛАТФОРМ В ЭЛЕКТРОННОМ БИЗНЕСЕ И ИНСТРУМЕНТЫ ИХ СНИЖЕНИЯ

Аннотация. В статье рассматриваются современные риски внедрения цифровых платформ в электронном бизнесе, а также комплекс инструментов и технологий, направленных на их снижение. Актуальность исследования обусловлена ускоренной цифровизацией экономики, ростом зависимости бизнеса от онлайн-платформ и усилением киберугроз в глобальной информационной среде. Цель работы заключается в комплексном анализе природы цифровых рисков, выявлении их причин и оценке современных методов управления ими. В исследовании показано, что цифровые платформы одновременно выступают источником конкурентных преимуществ и зоной повышенной уязвимости для бизнеса. Особое внимание уделяется технологическим сбоям, утечкам данных, кибератакам, правовым ограничениям и зависимости от внешних цифровых экосистем. Рассматриваются современные инструменты управления рисками, включая искусственный интеллект, блокчейн, облачные технологии, системы кибербезопасности и аналитические платформы обработки больших данных.

Ключевые слова: электронный бизнес, цифровые платформы, цифровая экономика, риск-менеджмент, кибербезопасность, информационные риски, искусственный интеллект, облачные технологии, блокчейн, цифровая трансформация.

Алиев Элдияр Сталбекович

магистрант

Б.Н. Ельцин атындагы Кыргыз-Россия Славян университети

Кыргыз Республикасы, Бишкек шаары

ЭЛЕКТРОНДУК БИЗНЕСТЕ САНАРИПТИК ПЛАТФОРМАЛАРДЫ КИРГИЗҮҮДӨГҮ ТОБОКЕЛДИКТЕР ЖАНА АЛАРДЫ АЗАЙТУУ ИНСТРУМЕНТТЕРИ

Аннотация. Бул макалада электрондук бизнес чөйрөсүндө санариптик платформаларды киргизүү учурунда пайда болгон тобокелдиктер жана аларды азайтуунун заманбап ыкмалары изилденет. Теманын актуалдуулугу санариптик экономиканын тездик менен өнүгүшү, уюмдардын платформалык чечимдерге болгон көз карандылыгынын өсүшү жана глобалдык санариптешүү шарттарында киберкоркунучтардын көбөйүшү менен шартталган. Санариптик платформалар заманбап бизнес-экосистеманын негизги бөлүгү болуп калганы менен, алардын колдонулушу технологиялык, маалыматтык, каржылык, уюштуруучулук, укуктук жана рыноктук тобокелдиктердин пайда болушу менен коштолот. Макалада өзгөчө көңүл киберкоопсуздук маселелерине, маалыматтардын агып кетишине, санариптик инфраструктуранын бузулушуна жана ири экосистемалык операторлорго болгон көз карандылыкка бурулат. Ошондой эле жасалма интеллект, булут технологиялары, блокчейн системалары жана чоң маалыматтарды талдоо платформалары сыяктуу заманбап тобокелдиктерди башкаруу инструменттери каралат.

Негизги сөздөр: электрондук бизнес, санариптик платформалар, тобокелдиктерди башкаруу, киберкоопсуздук, санариптик экономика, маалыматтык коопсуздук, жасалма интеллект, булут технологиялары, блокчейн, чоң маалыматтар.

Aliev Eldiyar Stalbekovich
Master's Student
Kyrgyz-Russian Slavic University named after B. N. Yeltsin
Kyrgyzstan, Bishkek

RISKS OF IMPLEMENTING DIGITAL PLATFORMS IN E-BUSINESS AND TOOLS FOR THEIR MITIGATION

Abstract. The article examines the risks associated with the implementation of digital platforms in e-business, as well as modern methods and tools for their mitigation. The relevance of the study is driven by the rapid development of the digital economy, increasing dependence of organizations on platform-based solutions, and the growing number of cyber threats in the context of global digital transformation. Digital platforms have become a core component of modern business ecosystems; however, their implementation is accompanied by complex technological, informational, financial, organizational, legal, and market risks. Special attention is given to cybersecurity challenges, data breaches, failures of digital infrastructure, and the dependence of businesses on major ecosystem providers. The study analyzes modern risk management tools, including artificial intelligence technologies, cloud computing, blockchain systems, and big data analytics platforms. The findings suggest that the efficiency of e-business largely depends on the maturity of digital risk management systems and the ability of organizations to adapt to rapidly changing technological environments.

Keywords: e-business, digital platforms, risk management, cyber threats, digital economy, information security, artificial intelligence, cloud technologies, blockchain, big data.

Современная мировая экономика вступила в этап, при котором цифровые платформы становятся не просто инструментом ведения бизнеса, а основной инфраструктурой взаимодействия между всеми участниками рынка. Электронная коммерция, маркетплейсы, финтех-сервисы, логистические платформы и цифровые экосистемы формируют новую архитектуру экономических отношений, где данные становятся ключевым ресурсом, а скорость обработки информации определяет конкурентоспособность компаний. Однако вместе с этим ростом цифровизации возникает и новая система рисков, которая отличается высокой сложностью, многослойностью и динамичностью. В отличие от традиционных бизнес-моделей, где риски часто имели ограниченный и локальный характер, цифровые платформы создают условия, при которых одно нарушение в системе может привести к цепной реакции и масштабным последствиям для всей экосистемы.

Особенность внедрения цифровых платформ заключается в том, что бизнес становится полностью зависимым от устойчивости информационной инфраструктуры, качества программного обеспечения и уровня защиты данных. Даже кратковременные сбои серверов или ошибки алгоритмов способны привести к значительным финансовым потерям, потере клиентов и ухудшению репутации компании. В условиях высокой конкуренции на рынке электронного бизнеса репутационные риски становятся не менее значимыми, чем финансовые, поскольку доверие пользователей является основой функционирования цифровых сервисов. Потеря доверия, вызванная утечкой данных или кибератакой, часто приводит к долгосрочному снижению рыночной позиции компании. Существенную роль в структуре цифровых рисков играют технологические сбои, возникающие при интеграции различных платформенных решений. Современные цифровые системы состоят из множества взаимосвязанных компонентов, включая облачные сервисы, API-интерфейсы, базы данных и сторонние программные модули.

Любая несовместимость или ошибка интеграции может вызвать системный сбой, который распространяется на весь бизнес-процесс.

Особенно уязвимыми являются компании, использующие быстро масштабируемые облачные решения без достаточного уровня резервирования и тестирования архитектуры. В таких условиях возрастает необходимость внедрения многоуровневых систем резервного копирования и распределённых вычислительных инфраструктур, позволяющих минимизировать последствия технических отказов. Не менее значимыми являются информационные и киберриски, которые в последние годы приобретают глобальный характер. Рост числа кибератак, направленных на коммерческие организации, связан с увеличением объёмов цифровых данных и их высокой ценностью. Злоумышленники используют методы фишинга, вредоносного программного обеспечения, атак типа «отказ в обслуживании» и сложные схемы социальной инженерии для получения доступа к конфиденциальной информации. В результате компании сталкиваются с утечками персональных данных пользователей, финансовыми потерями и юридической ответственностью. В условиях усиления международного регулирования в сфере защиты данных нарушение информационной безопасности может привести не только к экономическим убыткам, но и к правовым санкциям, включая штрафы и ограничения деятельности. Финансовые риски цифровых платформ также приобретают новую специфику. В отличие от традиционного бизнеса, где основные затраты связаны с производством и логистикой, в электронном бизнесе значительная часть расходов направлена на поддержку цифровой инфраструктуры, облачных сервисов, лицензий программного обеспечения и кибербезопасности. Ошибки в выборе бизнес-модели монетизации, неверная оценка стоимости привлечения пользователей или зависимость от рекламных моделей могут привести к нестабильности доходов.

Особенно уязвимыми являются стартапы, работающие в условиях высокой конкуренции и ограниченного финансирования, где даже

незначительное увеличение операционных затрат может привести к потере устойчивости проекта.

Организационные риски связаны с недостаточной готовностью компаний к цифровой трансформации. Внедрение цифровых платформ требует не только технологических изменений, но и перестройки управленческих процессов, формирования новых компетенций и изменения корпоративной культуры. Часто организации сталкиваются с дефицитом квалифицированных специалистов в области анализа данных, кибербезопасности и разработки программного обеспечения. Кроме того, сопротивление персонала изменениям и недостаточная цифровая грамотность сотрудников могут существенно замедлить процесс внедрения платформенных решений и снизить их эффективность. Правовые риски в сфере цифровых платформ становятся всё более значимыми на фоне развития международного регулирования цифровой экономики. Различия в законодательстве разных стран, требования к хранению и обработке персональных данных, ограничения на трансграничную передачу информации создают дополнительные сложности для компаний, работающих на глобальном рынке. Несоблюдение нормативных требований может привести к судебным разбирательствам и ограничению деятельности компании в отдельных юрисдикциях. Рыночные риски в цифровой экономике проявляются через высокую конкуренцию и зависимость от крупных платформенных экосистем. Многие компании вынуждены работать внутри инфраструктуры глобальных технологических гигантов, что создаёт эффект технологической зависимости.

При этом скорость появления новых конкурентов в цифровой среде значительно выше, чем в традиционной экономике, что усиливает нестабильность рыночных позиций компаний. В современных условиях особое значение приобретают инструменты снижения цифровых рисков. Одним из ключевых направлений является развитие систем кибербезопасности, включающих многоуровневую защиту данных,

шифрование информации, мониторинг сетевой активности и применение концепции нулевого доверия.

Существенную роль играет использование искусственного интеллекта, который позволяет анализировать большие массивы данных, выявлять аномалии в поведении пользователей и прогнозировать потенциальные угрозы в режиме реального времени. Это позволяет переходить от реактивной модели управления рисками к проактивной, основанной на предсказании и предотвращении угроз.

Облачные технологии также играют важную роль в снижении рисков, обеспечивая масштабируемость, резервирование данных и устойчивость к отказам оборудования. Использование распределённых дата-центров позволяет минимизировать влияние локальных сбоев и обеспечить непрерывность бизнес-процессов. Блокчейн-технологии в свою очередь обеспечивают прозрачность и неизменность данных, что особенно важно для финансовых операций и управления цифровыми контрактами. Аналитические платформы обработки больших данных позволяют компаниям формировать комплексное представление о рисках, выявлять скрытые закономерности и принимать более обоснованные управленческие решения. Несмотря на значительное развитие технологий управления рисками, существует ряд ограничений, связанных с высокой стоимостью внедрения цифровых решений, необходимостью подготовки квалифицированного персонала и сложностью интеграции различных систем безопасности.

Таким образом, проведённый анализ показывает, что внедрение цифровых платформ в электронном бизнесе является одновременно источником роста эффективности и фактором увеличения уровня комплексных рисков. Устойчивость организаций в цифровой экономике определяется способностью своевременно выявлять, оценивать и минимизировать эти риски с использованием современных технологических решений. Наиболее успешными становятся те компании, которые

рассматривают риск-менеджмент не как вспомогательную функцию, а как стратегический элемент цифровой трансформации, интегрированный во все уровни управления бизнесом.

Список использованных источников

1. Kerzner H. Project Management: A Systems Approach to Planning, Scheduling, and Controlling / H. Kerzner. Hoboken: Wiley, 2022.
2. PMI. A Guide to the Project Management Body of Knowledge (PMBOK Guide). 7th ed. Pennsylvania: Project Management Institute, 2021.
3. Hillson D. Practical Project Risk Management: The ATOM Methodology / D. Hillson, P. Simon. Vienna: Management Concepts, 2020.
4. Chapman C. Project Risk Management: Processes, Techniques and Insights / C. Chapman, S. Ward. New York: Wiley, 2021.
5. Meredith J. Project Management: A Managerial Approach / J. Meredith, S. Mantel. Hoboken: Wiley, 2022.
6. Лапыгин Ю.Н. Проектный менеджмент: управление проектами и рисками / Ю.Н. Лапыгин. М.: Инфра-М, 2021.
7. Балдин К.В. Риск-менеджмент / К.В. Балдин. М.: Дашков и К°, 2021.
8. Deloitte Insights. Digital Risk Management in Modern Organizations. URL: <https://www2.deloitte.com/> (дата обращения: 16.05.2026).
9. Gartner Research. AI Technologies in Risk Analytics. URL: <https://www.gartner.com/> (дата обращения: 16.05.2026).
10. Национальный статистический комитет Кыргызской Республики. Показатели цифровой экономики. URL: <https://stat.kg/> (дата обращения: 15.06.2026).
11. Министерство цифрового развития Кыргызской Республики. Официальный сайт. URL: <https://digital.gov.kg/> (дата обращения: 15.06.2026).

12. НИУ ВШЭ. Центр цифровой экономики. Аналитические материалы по цифровизации бизнеса. URL: <https://www.hse.ru/> (дата обращения: 15.06.2026).