

УДК 336.6

А. Х. Ярлушкин

Финансовый университет при правительстве Российской Федерации, Москва,
e-mail: alex.yarlushkin@gmail.com

МЕТОДЫ УПРАВЛЕНИЯ РИСКАМИ ПРИ ВНЕДРЕНИИ ИНСТРУМЕНТА НА ОСНОВЕ БОЛЬШИХ ДАННЫХ В ИНВЕСТИЦИОННУЮ ДЕЯТЕЛЬНОСТЬ КОРПОРАЦИИ

Ключевые слова: инвестиции, финансы, инвестиционное управление, большие данные, Финтех, корпорации, риски, анализ рисков.

В данной статье рассматриваются теоретические и практические аспекты управления рисками при внедрении инструмента на основе Больших Данных (Big Data) в инвестиционную деятельность крупной корпорации. Цель исследования – провести анализ существующих подходов к риск-менеджменту (в том числе с использованием международных стандартов ISO 31000, ISO/IEC 27005, COBIT, COSO ERM, MEHARI и других), выделить основные факторы, влияющие на появление рисков в процессе внедрения инструмента больших данных в инвестиционную деятельность корпорации, а также описать методы их идентификации, оценки, контроля и снижения. Особое внимание уделено характерным угрозам, возникающим при использовании облачных технологий и платформ для аналитики больших массивов данных, а также необходимости обеспечения соответствия требованиям по информационной безопасности (например, PCI DSS). В статье представлены рекомендации для руководителей и специалистов инвестиционных подразделений, а также даны практические советы по адаптации процесса риск-менеджмента к реалиям цифровой среды. Научная новизна статьи состоит в обобщении разрозненных подходов к управлению рисками и их адаптации к случаям использования Big Data именно в инвестиционном процессе, где характерны повышенные требования к надёжности информации и высокой стоимости потенциальных ошибок в принятии решений.

A. Kh. Yarlushkin

Financial University under the Government of the Russian Federation, Moscow,
e-mail: alex.yarlushkin@gmail.com

TITLE OF THE ARTICLE: RISK MANAGEMENT METHODS FOR THE IMPLEMENTATION OF A BIG DATA-BASED TOOL IN THE INVESTMENT ACTIVITIES OF A CORPORATION

Keywords: Investments, finance, investment management, big data, fintech, corporations, risks, risk analysis.

This article discusses the theoretical and practical aspects of risk management when implementing a Big Data-based tool in the investment activities of a large corporation. The purpose of the study is to analyze existing approaches to risk management (including using international standards ISO 31000, ISO/IEC 27005, COBIT, COSO ERM, MEHARI and others), identify the main factors influencing the emergence of risks in the process of implementing a big data tool in the investment activities of a corporation, and describe the methods their identification, evaluation, control and reduction. Particular attention is paid to the specific threats that arise when using cloud technologies and platforms for analyzing large amounts of data, as well as the need to ensure compliance with information security requirements (for example, PCI DSS). The article provides recommendations for managers and specialists of investment departments, as well as practical advice on adapting the risk management process to the realities of the digital environment. The scientific novelty of the article is the generalization of disparate approaches to risk management and their adaptation to the use of Big Data in the investment process, which is characterized by increased requirements for the reliability of information and the high cost of potential errors in decision-making.

Введение

В современных условиях роста конкуренции на международных рынках, экономической турбулентности и санкционной нагрузки для Российской Федерации – применение инновационных технологий и ав-

томатизация процессов являются важными факторами достижения конкурентного преимущества для Российских корпораций. В этой связи эффективная работа с данными становится одним из ключевых направлений для бизнеса. Все большее коли-

чество корпораций внедряют технологию больших данных для целей повышения эффективности инвестиционно-проектного управления.

Технология больших данных, представляет из себя большие объемы структурированной и неструктурированной информации, эффективно обрабатываемые аналитическими инструментами в режиме реального времени. В современной практике принято считать, что применение передовых технологий для работы с большими данными становится важным конкурентным преимуществом, которое может оказать значительное влияние на общую финансовую устойчивость и доходность корпорации [1].

Современная деловая среда всё активнее использует инструменты на основе Больших Данных (Big Data) для повышения эффективности, скорости и точности принятия инвестиционных решений. По данным исследовательской компании IDC, мировой рынок решений в области Big Data и аналитики в 2023 году превысил 200 млрд долларов США, демонстрируя стабильный рост ежегодно [2]. Среди основных драйверов роста можно назвать широкое распространение облачных технологий, быстрое увеличение объёмов структурированных и неструктурированных данных (от данных транзакций до поведения пользователей в Интернете), а также совершенствование инструментов машинного обучения и искусственно-го интеллекта.

Однако вместе с новыми возможностями Big Data-инструменты несут в себе дополнительную совокупность рисков, связанных с безопасностью данных, сложностью аппаратного и программного окружения, а также со стратегическими и операционными рисками, которые возникают при принятии решений на основе больших массивов данных. Внедрение подобных инструментов в инвестиционную деятельность требует комплексного управления рисками с учётом специфики аналитических систем, юридических аспектов, а также стандартов управления информационной безопасностью.

Цель исследования – провести анализ существующих подходов к риск-менеджменту (в том числе с использованием международных стандартов ISO 31000, ISO/IEC 27005, COBIT, COSO ERM, MENARI и других), выделить основные факторы,

влияющие на появление рисков в процессе внедрения инструмента больших данных в инвестиционную деятельность корпорации, а также описать методы их идентификации, оценки, контроля и снижения. Для достижения этой цели были сформулированы следующие задачи:

1. Проанализировать специфику инвестиционных процессов в контексте использования больших данных.

2. Рассмотреть теоретические и нормативные основы управления рисками (ISO 31000, ISO/IEC 27005, COBIT, COSO ERM, MENARI и др.) в условиях цифровой трансформации.

3. Выявить ключевые источники и виды рисков при внедрении Big Data в инвестиционную деятельность.

4. Предложить методы идентификации, оценки и снижения рисков, включая инструменты информационной безопасности и надлежащего корпоративного управления.

5. Сформулировать рекомендации для практиков по организации эффективной системы риск-менеджмента.

Научная новизна статьи состоит в обобщении разрозненных подходов к управлению рисками и их адаптации к случаям использования Big Data именно в инвестиционном процессе, где характерны повышенные требования к надёжности информации и высокой стоимости потенциальных ошибок в принятии решений.

Материал и методы исследования

Инвестиционная деятельность крупных корпораций включает анализ макроэкономических показателей, оценку рынка, отбор перспективных проектов, формирование портфеля инвестиций, мониторинг и выход (дивестиции). Принятие решений в таких компаниях основывается на:

- Точных финансовых показателей (например, финансовая отчётность потенциальных объектов инвестирования, котировки акций и т.д.).
- Статистических данных о поведении рынков, динамике стоимости активов, объёмах торгов.
- Сценарном моделировании, прогнозировании будущих доходов и рисков.
- Данных внешних агентств (рейтинговых, аудиторских, консалтинговых).
- Внутренних данных (собственные аналитики, модели, прогнозы).

Внедрение решений на основе Big Data расширяет спектр доступной информации: появляются поведенческие данные клиентов, создаются алгоритмы машинного обучения для прогнозирования движения рынка, анализируется активность социальных сетей, совокупные эффекты работы предприятий. Однако объём и сложность данных влекут за собой новые риски, особенно если решение принимается полностью на основе автоматических моделей без достаточного человеческого контроля.

По данным Европейского агентства по безопасности сетей и информации (ENISA), корпорации, переходящие к облачным и Big Data-решениям, часто недооценивают комплексность рисков, рассматривая главным образом вопросы технической защиты (шифрование, сетевые экраны) и пренебрегая организационными или правовыми аспектами [3]. Именно поэтому стандарты управления рисками, такие как ISO 31000, COSO ERM и ISO/IEC 27005, призваны обеспечить комплексный подход: от идентификации и анализа рисков до разработки стратегии и процедур по их мониторингу. Разберем существующие модели риск-менеджмента:

Стандарт ISO 31000:2009 «Risk management – Principles and guidelines» является одним из ключевых международных документов, описывающих общие принципы управления рисками. Он предлагает единый процесс, включающий несколько шагов [4]:

1. Установление контекста и постановка целей.
2. Идентификация рисков.
3. Анализ рисков (качественный или количественный).
4. Оценка (приоритизация) рисков.
5. Обработка (реагирование на) риски – принятие, уклонение, передача, смягчение.
6. Мониторинг и обзор.

Особенностью ISO 31000 является универсальность: он применим как к финансовым, так и к технологическим или репутационным рискам. Поэтому при работе с Big Data в инвестициях корпорация может использовать эту модель в качестве «каркаса», адаптируя конкретные детали под свою специфику.

ERM (Enterprise Risk Management) по версии COSO (Committee of Sponsoring Organizations of the Treadway Commission) – ещё один широко распространённый подход

к управлению рисками. Основное внимание в нём уделяется [5]:

- Установке «аппетита к риску» (Risk Appetite) в рамках стратегии компании.
- Интеграции риск-менеджмента во все уровни организации (от совета директоров до линейных подразделений).
- Оценке как «возможностей» (opportunities), так и «угроз» (threats), которые могут повлиять на достижение целей компании.

В условиях Big Data-кейсов этот фреймворк может применяться при оценке стратегических рисков – например, необходимости дорогостоящего развёртывания инфраструктуры для аналитики и сопоставления потенциальных выгод (улучшенные прогнозы, экономия на транзакциях) с риском недостижения желаемого результата.

Стандарт ISO/IEC 27005 ориентирован конкретно на управление рисками в области информационной безопасности. Он описывает процесс управления рисками, разбивая его на этапы [6]:

1. Установление контекста (определение границ системы, существующих механизмов безопасности и т.д.).
2. Идентификация активов, угроз и уязвимостей.
3. Оценка последствий (impact) и вероятности (likelihood) реализации угрозы.
4. Формирование плана обработки рисков: выбор мер контроля (технических, административных и физических).
5. Мониторинг, обновление и рецензирование.

Для Big Data-инструментов, особенно тех, которые используют облачные сервисы и обрабатывают большие объёмы конфиденциальных данных, ISO/IEC 27005 помогает выявлять и анализировать разнообразные киберриски: угрозы взлома, утечки данных, отказов инфраструктуры, сложность контроля за распределёнными вычислительными средами и т. д.

МЕHARI (Méthode Harmonisée d'Analyse de Risques) – это методика французского клуба по информационной безопасности (CLUSIF) [7] для анализа рисков. Она предоставляет набор анкет, сценариев угроз и советов по выбору мер снижения. Отличается детализированным подходом и готовыми шаблонами для идентификации рисков. МЕHARI может оказаться полезной, если требуется быстро провести оценку комплексных ИТ-ландшафтов, учитывая осо-

бенности облачных технологий и инвестиционных систем.

Все перечисленные методы (ISO 31000, COSO ERM, ISO/IEC 27005, MEHARI) имеют общую структуру управления рисками: нужно последовательно идентифицировать, анализировать, оценивать и обрабатывать риски, а затем мониторить результат. Разница кроется в сфере применения и степени детализации. Для инвестиционной деятельности, где ключевыми оказываются финансовые параметры и стратегические цели, часто выступает на первый план COSO ERM. Для киберрисков и конфиденциальности – ISO/IEC 27005, тогда как ISO 31000 задаёт общий «зонтик» для всех типов рисков, а MEHARI даёт конкретные практические инструменты.

Процесс внедрения Big Data-инструмента в корпорации обычно разбивается на несколько этапов:

1. Формирование целей и требований:

- Определить бизнес-цели (например, улучшение точности прогнозирования доходности, оптимизация портфеля, выявление инсайтов из неструктурированных данных).

- Понять требования к объёму, скорости и формату данных, учесть регулятивную базу (GDPR, местные законы о конфиденциальности).

2. Пилотный проект:

- Часто компании начинают с «Proof of Concept» (PoC) или «Minimal Viable Product» (MVP), где на ограниченном наборе данных тестируется полезность Big Data-решения.

- На этом этапе уже целесообразно провести предварительный риск-анализ, так как ошибки в архитектуре могут вылиться в дорогостоящие проблемы позже.

3. Масштабирование и интеграция:

- Включение Big Data-инструмента в общую ИТ-инфраструктуру (ERP, CRM, системы электронного документооборота, кастомные инвестиционные платформы).

- Настройка каналов получения данных (API к биржам, партнёрам, провайдерам рыночной аналитики).

- Подключение облачных сервисов (PaaS, IaaS, SaaS) при необходимости.

4. Эксплуатация и постоянное совершенствование:

- Регулярное обучение аналитиков и экспертов в инвестиционном подразделении.

- Отслеживание изменений в законодательстве и технологиях, обновление моделей риск-менеджмента.

На каждом из этапов целесообразно проводить контрольные мероприятия:

- Архитектурный аудит: Проверка совместимости Big Data-инструмента с существующими системами, соответствие требованиям производительности и безопасности.

- Аудит информационной безопасности: Оценка механизма шифрования данных, разграничения прав доступа, защиты от сетевых атак, а также проверка соответствия таким стандартам, как ISO/IEC 27001.

- Мониторинг SLA при облачном размещении: Проверка показателей доступности, времени отклика, скорости масштабирования, а также исполнения провайдером своих обязательств.

- Регулярный пересмотр риск-профиля: Учитывая динамику рынка и быструю эволюцию технологий, риск-профиль и приоритеты могут меняться, поэтому важно проводить повторные оценки с определённой периодичностью (например, ежеквартально или ежегодно).

Результаты исследования и их обсуждение

Разберем основные риски и способы их снижения:

1. Технологические риски

Сбой в инфраструктуре.

- *Способы снижения:* дублирование критически важных компонентов (кластеризация, резервные каналы связи), использование мультиоблачных стратегий (multi-cloud), резервное копирование данных, тестирование планов восстановления.

Недостаточная производительность.

- *Способы снижения:* стресс-тесты на различных нагрузках, оптимизация рабочих нагрузок, применение адаптивных механизмов распределения вычислительных ресурсов.

2. Риски информационной безопасности
Неавторизованный доступ и утечки.

- *Способы снижения:* строгая политика разграничения прав (RBAC), регулярный аудит учетных записей, шифрование данных «на лету» (in transit) и «на хранении» (at rest), двухфакторная аутентификация, SIEM-системы для мониторинга инцидентов.

Атаки на облачного провайдера.

- *Способы снижения:* выбор проверенного провайдера, имеющего сертификаты безопасности (ISO/IEC 27001, SOC2), проведение собственного анализа SLA и условий договора, использование инструмен-

тов мониторинга Cloud Security Posture Management (CSPM).

3. Стратегические и финансовые риски
Неправильная трактовка результатов:

- *Способы снижения*: внедрение системы валидации аналитических моделей (валидность данных, кросс-проверки с историческими и внешними источниками), участие экспертов-аналитиков, которые имеют опыт в конкретной отрасли.

Недостаточная окупаемость:

- *Способы снижения*: чёткое определение ключевых показателей эффективности (KPI) и критериев успешности проекта, регулярный контроль бюджета, внедрение итеративных методологий (например, Agile/Scrum) для гибкого управления ресурсами.

4. Организационные риски

Сопrotивление изменениям:

- *Способы снижения*: обучение сотрудников, мотивационные программы, включение ключевых сотрудников инвестблока в процесс разработки.

Недостаток компетенций:

- *Способы снижения*: наём или пере-квалификация специалистов (Data Scientist, Data Engineer), партнёрство с консалтинговыми компаниями, постоянный профессиональный рост сотрудников через курсы, вебинары. Инвестиции в технологии анализа персонала позволят ускорить внедрение новой технологии [8].

5. Юридические и комплаенс-риски

Несоблюдение нормативов:

- *Способы снижения*: регулярные аудиты, поддержание системы менеджмента безопасности информации (ISMS), консультации с юридическим отделом, отслеживание изменений в законодательстве (например, новых требований GDPR или локальных законов).

Возможные штрафы и судебные иски:

- *Способы снижения*: внедрение процедур реагирования на инциденты (Incident Response Plan), хранение логов действий в безопасном месте, прозрачная политика конфиденциальности, договоры NDA со всеми участниками процесса.

Выводы

В статье проанализированы принципы и практические аспекты управления рисками при внедрении Big Data-инструмента

в инвестиционную деятельность крупной корпорации. Ключевой вывод заключается в том, что риск-менеджмент в сфере больших данных не может быть сведён к узкотехническим решениям: требуются комплексные меры, включающие организационные, правовые, стратегические и финансовые аспекты. Инвестиционные компании должны уделять особое внимание:

1. *Стратегической интеграции*: Big Data-инструмент следует увязывать с общей бизнес-стратегией и определённым «аппетитом к риску».

2. *Соответствию стандартам*: Использование ISO 31000 и COSO ERM для общего управления рисками, а также ISO/IEC 27005 для киберрисков, что даёт целостную систему контроля.

3. *Постоянному мониторингу рисков*: Рынки и технологии развиваются быстро, поэтому пересмотр риск-профиля необходим минимум ежегодно или даже ежеквартально.

4. *Развитию компетенций*: Проблема кадровой подготовки и организационной культуры часто оказывается ключевой при внедрении новых инструментов, особенно таких сложных, как Big Data.

5. *Координации с облачными провайдерами*: Надлежащее заключение договоров, ясное определение SLA и контроль их исполнения.

Таким образом, при должной адаптации описанных методов и стандартов к конкретной ситуации корпорация сможет минимизировать вероятность и последствия негативных сценариев, при этом максимально эффективно использовать преимущества анализа больших данных для принятия инвестиционных решений.

Возможное направление дальнейших исследований – детальный количественный анализ эффективности тех или иных мер риска (например, внедрение SIEM-систем, дублирование облачных сервисов), а также разработка интегрированных инструментов для автоматизации риск-менеджмента в Big Data-среде. Дополнительный интерес представляет изучение эволюции законодательных и этических требований, в том числе вопросов «прозрачного» использования пользовательских данных в аналитических алгоритмах и моделей.

Библиографический список

1. Chen H., Chiang R.H.L., Storey V.C. Business Intelligence and Big Data Analytics: From Big Data to Big Impact // MIS Quarterly. 2022. Vol. 36. P. 1165-1188.
2. Huo R., Vesset D. Worldwide Big Data and Analytics Software Forecast, 2023–2027 // IDC. 2023. [Электронный ресурс]. URL: <https://www.idc.com/getdoc.jsp?containerId=US50117823> (дата обращения: 10.11.2024).
3. European Union Agency for Cybersecurity, Cybersecurity of Critical Sectors // ENISA. 2024. [Электронный ресурс]. URL: <https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors> (дата обращения: 10.11.2024).
4. ISO 31000:2009: Risk management – Principles and guidelines. Geneva: International Organization for Standardization, 2009.
5. COSO. Enterprise Risk Management Integrating with Strategy and Performance. New York: Committee of Sponsoring Organizations of the Treadway Commission, 2017.
6. ISO/IEC 27005:2011: Information technology – Information security risk management. Geneva: International Organization for Standardization, 2011.
7. CLUSIF. Méthode harmonisée d'analyse des risques (MEHARI). Paris: Club de la Sécurité de l'Information Français, 2010.
8. Pasto T. Innovation Insight for People Analytics Technology // Gartner Research. 2024 [Электронный ресурс]. URL: <https://www.gartner.com/en/documents/5849247> (дата обращения: 10.11.2024).