УДК 33**Анализ влияния искусственного интеллекта на идентификацию и управление операционными рисками в условиях цифровизации финансовых рынков****Левичев Максим Александрович**

Магистр,
Финансовый университет при Правительстве Российской Федерации,
125993, Российская Федерация, Москва, Ленинградский просп., 49;
e-mail: maxsonee@yandex.ru

Аннотация

В статье рассматривается воздействие систем искусственного интеллекта на выявление и контроль операционных рисков в условиях перехода финансовой сферы на цифровые технологии. Актуальность исследования обусловлена усложнением природы операционных рисков, вызванным участвовавшими случаями кибервзломов, ошибками персонала, техническими неполадками и несовершенством рабочих процедур. Устаревшие способы оценки рисков постепенно заменяются компьютерными алгоритмами, которые могут обрабатывать значительные объемы информации и предупреждать о возможных опасностях без задержек. Описаны способы внедрения интеллектуальных систем, включая использование алгоритмов классификации, многослойных самообучающихся структур, комбинированных подходов, объединяющих традиционные методики измерения рисков с возможностями компьютерного анализа. Особый упор сделан на важность достоверности исходных данных, проверки работоспособности алгоритмов и налаживания взаимодействия между программистами, специалистами по рискам и контролирующими органами. Практические итоги исследования показывают, что применение интеллектуальных систем позволяет точнее выявлять киберугрозы, уменьшать денежные убытки и совершенствовать процедуры наблюдения. Однако обнаружены существенные трудности: искажения в обучающих выборках, проблемы совместимости с устаревшим программным обеспечением, недостаточная понятность работы сложных алгоритмов и возникающие моральные вопросы. В качестве примеров приведены случаи сбоев в работе автоматизированных торговых систем, вызывающих резкие колебания на биржах. Подчеркивается важность сохранения разумного соотношения между автоматизацией и участием человека в процессах контроля. Рассмотрены юридические вопросы, включая требования к открытости алгоритмов и защите персональной информации. Отмечается, что эффективное использование интеллектуальных систем предполагает перестройку рабочих процессов, вложения в подготовку кадров и создание комбинированных структур, где компьютерные технологии служат поддержкой для специалистов по рискам. В статье обращается внимание на двойственную природу интеллектуальных систем: с одной стороны, они повышают стабильность финансовых учреждений, с другой - создают новые виды рисков, нуждающиеся в продуманном регулировании. Будущее развитие связано с совершенствованием понятных алгоритмов, выработкой единых норм контроля и налаживанием взаимодействия между различными отраслями.

Для цитирования в научных исследованиях

Левичев М.А. Анализ влияния искусственного интеллекта на идентификацию и управление операционными рисками в условиях цифровизации финансовых рынков // Экономика: вчера, сегодня, завтра. 2025. Том 15. № 3А. С. 695-710.

Ключевые слова

Искусственный интеллект, операционные риски, цифровизация финансовых рынков, машинное обучение, управление рисками.

Введение

Искусственный интеллект постепенно меняет правила игры в финансовой сфере, оказывая глубокое воздействие на способы оценки и управления рисками. С ростом объемов данных, возникающих в связи с цифровизацией финансовых услуг, специалисты в области рисков, IT-инфраструктур и аналитики всё чаще обращаются к алгоритмам машинного обучения и другим инструментам AI, способным обрабатывать информацию в больших масштабах. При этом важным направлением становится анализ операционных рисков, которые связаны не только с технологическими сбоями и ошибками, но и с кибератаками, человеческим фактором и неэффективностью бизнес-процессов. Все эти аспекты требуют переосмысления классических подходов к контролю и выявлению уязвимостей, поскольку масштаб и сложность современных финансовых операций растут быстрее, чем возможности традиционного человеческого анализа.

Современные рынки демонстрируют всё более тесную связь между технологическими инновациями и глобальным финансовым оборотом. Влияние искусственного интеллекта на этот процесс становится заметнее, так как алгоритмы машинного обучения берут на себя значительную долю задач, связанных с предиктивной аналитикой. Если раньше операционные риски в основном касались сбоев бухгалтерских систем или несоответствий при ведении документации, то сегодня они включают целые цепочки событий, возникающих из многокомпонентных цифровых платформ [Медик, 2024]. Подобные системы обеспечивают различные аспекты функционирования финансовых процессов: от верификации личности клиента до высокоскоростного исполнения сделок. В результате возможности AI как инструмента анализа и принятия решений начинают играть ключевую роль в повышении устойчивости бизнеса.

Материалы и методы исследования

При этом важно учитывать, что искусственный интеллект способен не только мониторить ключевые метрики в режиме реального времени, но и прогнозировать потенциальные области риска задолго до их материализации. Одно из самых ценных качеств AI заключается в умении выявлять скрытые паттерны, ускользающие от человеческого глаза. Особенно это важно в контексте борьбы с мошенничеством, где оперативность и точность имеют решающее значение. Современные системы, построенные на деревьях решений, нейронных сетях или градиентном бустинге, могут не только распознавать подозрительные транзакции, но и учитывать контекст, связывая данные из разных источников [Kumar, Kumar, Kumari, Kumari, Kumari, Behura, 2024]. Однако автоматизация подобного рода требует серьезной проверки корректности моделей, а

также постоянного контроля за тем, чтобы алгоритмы не принимали ошибочных решений на основе статистической аномалии.

При попытках интеграции искусственного интеллекта в систему управления операционными рисками перед организациями встаёт ряд вопросов, связанных с качеством исходных данных и методами их обработки. Чем сложнее инструменты анализа, тем выше вероятность, что ошибки в исходных данных могут привести к неверным выводам или рекомендациям [Коновалова, Михайлов, Кузьмина, 2018]. В условиях цифровизации финансовых процессов, когда каждое действие клиента фиксируется в огромных базах данных, важно обеспечивать как техническую надёжность хранения информации, так и корректность её последующего анализа. Отсюда возникает необходимость тесного сотрудничества между специалистами в области кибербезопасности, аналитиками, профильными менеджерами и разработчиками алгоритмов, чтобы минимизировать риски и правильно интерпретировать результаты.

Результаты и обсуждение

Особое внимание сегодня уделяется киберрискам, ведь финансовые организации становятся всё более привлекательной целью для хакеров. Традиционные методы противодействия кибератакам требуют значительных усилий по обновлению систем безопасности, но они могут быстро устаревать, учитывая динамику появления новых угроз. Искусственный интеллект в данном контексте предлагает инструменты не только для распознавания уже известных моделей атак, но и для адаптивного обучения, позволяющего системам узнавать о нетипичных способах взлома [Натальсон, 2024]. Таким образом, повышается вероятность своевременного обнаружения нарушений, снижается риск значимых финансовых потерь и утечки конфиденциальных данных. Однако все эти преимущества тесно связаны с необходимостью оптимизации алгоритмов, а также обеспечением прозрачности и аудируемости их решений.

Управление операционными рисками требует сбалансированного подхода к автоматизации. Чрезмерная зависимость от AI-технологий может обернуться непредвиденными последствиями, особенно если организация недооценивает важность ручной проверки и контроля. В то же время, попытка сохранить полностью человеческий анализ становится малоэффективной в долгосрочной перспективе, учитывая рост объёмов данных и скорость изменений на финансовых рынках [Идиятуллин, Аухадеев, Киснеева, Антипанова, 2024]. Оптимальный сценарий заключается в развитии гибридных систем, где искусственный интеллект берёт на себя рутинную часть анализа, а специалисты в области рисков и бизнес-процессов выступают в роли контролёров качества и стратегических архитекторов. Такой подход может повысить и точность прогнозов, и гибкость в реагировании на нестандартные ситуации.

Важнейшей частью операционного риска, связанного с внедрением технологий искусственного интеллекта, остаётся риск принятия решений на основе необъективного или неполного анализа. Модели машинного обучения могут попадать в ловушку предвзятости, если тренировочные выборки содержали искажённые данные или отражали исторические диспропорции рынка. Это может привести к несправедливым условиям для клиентов, к неверным выводам о прибыльности вложений или к упущенным возможностям в инвестиционном управлении [Бойченко, Фадина, 2023]. Комплаенс и регуляторы финансового рынка уже изучают вопросы, связанные с этикой и прозрачностью AI-решений, чтобы снизить вероятность масштабных скандалов и финансовых потерь, обусловленных алгоритмическими

ошибками. Поэтому важно закладывать механизмы контроля уже на этапе проектирования систем.

Цифровая трансформация финансовых рынков движется за счёт повышения эффективности и снижения затрат, но такой прогресс сопровождается и комплексными операционными рисками. Внедрение электронных платформ для торговли ценными бумагами или криптоактивами даёт участникам рынка новый уровень удобства, однако малейший сбой в алгоритмах может повлечь лавинообразные последствия. Примером может служить ситуация, когда высокочастотный трейдинговый алгоритм начинает некорректно реагировать на рыночную волатильность, порождая цепочку транзакций, которые ещё больше раскачивают рынок [Качалов, Слепцова, 2023]. В таких условиях роль надзора и продуманной организации risk-management процессов увеличивается многократно, а искусственный интеллект становится необходимым элементом контрольно-надзорных процедур, позволяя оперативно отследить аномальные паттерны поведения.

Серьёзным вызовом остаётся сложность интеграции AI-решений в уже существующие инфраструктуры. Банк или другая финансовая организация часто обладает историческими системами, которые не были изначально рассчитаны на масштабный анализ больших данных. Требуется модернизация не только унаследованных баз данных, но и аппаратных мощностей, сетевых протоколов, а также средств киберзащиты [Гребешкова, Фирстова, 2023]. Эта интеграция должна осуществляться аккуратно, чтобы не создавать новых точек уязвимости и не нарушать работу критичных сервисов. Более того, специалисты должны понимать, что искусственный интеллект не решит все проблемы автоматически: тщательная настройка, регулярные обновления и тестирование моделей на реальных и синтетических данных остаются неотъемлемыми этапами.

В то же время внедрение технологий искусственного интеллекта открывает путь к более эффективному управлению операционными рисками, связанными с человеческим фактором. Ошибки операторов, неправильный ввод данных и сомнительные решения, принятые под давлением временных ограничений, всё ещё составляют большую часть инцидентов в финансовой сфере. Алгоритмы, отслеживающие действия сотрудников в реальном времени и выявляющие аномалии, помогают своевременно сигнализировать о возможных нарушениях процедур [Верич, 2023]. Это способствует формированию культуры осознанного отношения к рискам и стимулирует непрерывное обучение персонала, ведь сотрудники видят, что автоматизированные системы могут повышать эффективность их работы, а не только служат инструментом надзора.

Задача полноценного анализа влияния искусственного интеллекта на управление операционными рисками включает и правовые аспекты. Регуляторы разных стран с разной скоростью адаптируют свои нормативные акты, пытаясь учесть особенности цифровизации. При этом у финансовых компаний появляются новые обязательства по раскрытию деталей использования AI и защиты данных клиентов [Ларина, Харламенкова, 2023]. Отдельные юрисдикции стремятся ввести дополнительные правила, касающиеся «прозрачности алгоритмов», чтобы минимизировать риск дискриминации и необоснованных отказов в услугах. Это порождает дискуссии о том, насколько нужно и возможно раскрывать внутреннюю логику нейронных сетей и других моделей, особенно если они содержат коммерческую тайну. В результате формируется многоуровневая система регулирования, где операционные риски могут быть распределены между компанией-разработчиком, финансовой организацией-внедренцем и конечными пользователями.

Когда речь идёт об управлении такими рисками, важно не забывать и о коммуникациях с клиентами, которые всё активнее пользуются цифровыми каналами для доступа к финансовым услугам. Уровень доверия со стороны клиентов прямо влияет на успешность внедрения AI-технологий: люди должны понимать, что их данные обрабатываются корректно и безопасно, а решения по кредитованию или страхованию не принимаются «вслепую» неопознанным алгоритмом [Гоглев, Касаткина, Мигалин, Муштак, 2022]. Создание ясных и доступных для понимания пояснений относительно работы AI, а также обеспечение возможности оспорить решение, становятся частью хорошей практики. Для финансовых организаций это не только обязательство по сохранению репутации, но и способ минимизировать операционные риски, возникающие в связи с недоверием и потенциальными жалобами клиентов.

Ключевая особенность искусственного интеллекта в том, что он непрерывно «учится», обрабатывая новые массивы данных и совершенствуя методы анализа. В контексте цифровизации финансовых рынков это означает, что эффективность систем мониторинга повышается по мере накопления исторических данных, и алгоритмы всё лучше умеют определять аномальные ситуации [Болонин, Асрян, 2024]. Однако одновременно возникает и новая форма операционных рисков: модель может изменять собственные параметры и при неправильной интерпретации входных данных уходить всё дальше от ожидаемого поведения. В этом случае задача специалистов и регуляторов – обеспечить наличие механизма «обратной связи», чтобы при необходимости вернуть модель к предыдущему состоянию и оценить, какой именно фрагмент данных вызвал сбой.

В свете этого особое значение приобретает вопрос тестирования и валидации моделей. Финансовые организации используют песочницы и тестовые среды, где AI-алгоритмы могут работать с историческими и синтетическими данными, не затрагивая реальных клиентских транзакций [Buntić, Damić, Dužević, 2021]. Такой подход позволяет выявить потенциальные ошибки ещё до запуска системы в производство. Кроме того, обязательной становится практика стресс-тестирования, когда модели сознательно подвергают экстремальным условиям, чтобы проверить их устойчивость. Таким образом, формируется логика итеративного усовершенствования: каждая новая версия AI-модуля проходит цикл проверок, и только после получения удовлетворительных результатов допускается к работе на реальном рынке.

Наряду с этим всё более актуальным становится риск «чёрного ящика», когда сложно объяснить, на каком основании тот или иной алгоритм выдал определённое решение. Хотя объяснимый искусственный интеллект (Explainable AI) привлекает внимание исследователей и практиков, пока ещё не все инструменты машинного обучения легко интерпретируемы. Сложные нейросетевые структуры, такие как глубокие свёрточные или рекуррентные сети, обладают миллионами параметров, связь между которыми трудно отследить человеко-ориентированными методами [Ахматова, 2023]. В условиях финансового сектора, где прозрачность и отчётность имеют высокую ценность, данный аспект может вызывать сомнения со стороны контроля и аудита. Тем не менее растёт число исследований и разработок в области методов локальной интерпретации и визуализации, которые помогут снизить операционные риски, связанные с неправильным пониманием решений AI.

Успех применения искусственного интеллекта для управления операционными рисками во многом определяется качеством межфункционального взаимодействия внутри финансовых организаций. Ведь IT-отделы, риск-менеджеры и бизнес-подразделения преследуют разные цели и имеют разные точки зрения на процессы. Налаживание эффективной коммуникации и понимание взаимосвязей между технологиями и бизнес-задачами позволяют выработать

единый набор критериев оценки эффективности AI-инструментов. Тем самым создаётся среда, в которой инновации служат интересам устойчивости и безопасности, а не становятся дополнительным источником неопределённости. В итоге вся корпоративная культура должна эволюционировать так, чтобы сотрудники видели в новых технологиях помощников, а не угрозу своим рабочим местам или привычным методам работы.

Переход к цифровым экосистемам и активное внедрение искусственного интеллекта меняют и ландшафт конкуренции. Банки, финтех-стартапы, страховые и инвестиционные компании всё более активно внедряют алгоритмы машинного обучения для улучшения клиентского опыта, оптимизации внутренних процессов и снижения расходов. В такой среде способность быстрее и точнее идентифицировать операционные риски даёт конкурентное преимущество, позволяя оперативно реагировать на инциденты или, что ещё лучше, предотвращать их. Тем не менее это же порождает дополнительные вопросы, полезут ли конкуренты вглубь технологий друг друга, чтобы найти слабые места, и какими методами будут защищать свои наработки. Исходя из этой логики, усиление сотрудничества и обмен информацией между участниками рынка может снизить общий уровень угроз.

Одним из перспективных направлений в управлении операционными рисками становится использование гибридных методологий, сочетающих классические статистические модели и алгоритмы машинного обучения. Традиционные методы, такие как Value-at-Risk или сценарный анализ, обеспечивают достаточно хорошую прогностическую точность при нормальных условиях рынка. Но в случае резкой смены рыночной конъюнктуры или возникновения системных шоков они могут дать сбой. Тогда на помощь приходят AI-модели, обладающие способностью находить нелинейные связи в данных и адаптироваться к новым условиям. В интеграции этих подходов кроется возможность более точного определения «непредвиденных» ситуаций, которые не укладываются в стандартные предположения о распределении вероятностей.

Естественно, потенциал AI-решений при оценке и управлении операционными рисками неразрывно связан с вопросом о квалификации персонала, работающего с такими системами. Сотрудники должны обладать не только базовыми навыками анализа данных, но и глубоким пониманием механизмов функционирования алгоритмов. Чем выше сложность алгоритма, тем труднее расшифровать логику его выводов, и тем важнее предупреждать и исправлять ошибки в самом зародыше [Натальсон, 2024]. Регулярные программы обучения, переквалификации и обмена опытом становятся для финансовых организаций необходимостью, без которой любые инвестиции в технологическую инфраструктуру могут оказаться неэффективными. Более того, такой подход снижает операционные риски, связанные с «узким местом» в экспертизе отдельных сотрудников.

Не стоит забывать, что искусственный интеллект может быть использован не только для защиты, но и для атаки в сфере финансов. Злоумышленники могут применять генеративные модели для создания более правдоподобных схем мошенничества, рассылки фишинговых писем, подделки цифровых документов [Качалов, Слепцова, 2023]. Такая эволюция криминальной активности означает, что системы безопасности и инструменты управления рисками должны развиваться особенно динамично. Если AI даёт преимущество одной стороне, другая сторона стремится нивелировать его, что приводит к непрерывной гонке вооружений на техническом уровне. В результате команды, отвечающие за обеспечение безопасности, вынуждены постоянно обновлять свои методики, а значит – инвестировать в AI-решения и обучать специалистов, способных противостоять новейшим угрозам.

Сложно переоценить важность нормативно-правового регулирования в данном контексте. Успех применения AI в финансовом секторе и спокойствие инвесторов значительной мерой зависят от того, насколько чётко определены и контролируются правила работы алгоритмов. Международные организации, такие как Базельский комитет по банковскому надзору, уже разрабатывают рекомендации по применению технологий машинного обучения и анализа больших данных. Вместе с тем на локальном уровне регуляторы могут вводить собственные стандарты, учитывающие национальную специфику и особенности правовой системы. В итоге операционные риски могут перерасти в юридические и репутационные, если компания не успеет адаптироваться к меняющимся требованиям или неправильно интерпретирует действующие законы.

В сфере идентификации операционных рисков AI помогает обрабатывать поток данных от внутренних систем и внешних источников: транзакционные логи, новости, комментарии в социальных сетях, экономические показатели и отчёты контрагентов. Совокупный анализ этих данных позволяет выявлять корреляции и паттерны, предвещающие возможное наступление неблагоприятных событий. К примеру, если алгоритм обнаруживает необычный всплеск сообщений о проблемах в сфере кибербезопасности, совпадающий по времени с нестандартными изменениями в транзакционной активности, система управления рисками может заранее перейти в режим повышенной готовности [Kumar, Kumar, Kumari, Kumari, Kumari, Behura, 2024]. Такая проактивность резко повышает шансы на своевременное предотвращение инцидентов или хотя бы минимизацию их последствий. При этом важно, чтобы результирующие сигналы AI переводились на понятный Risk-менеджерам язык, чтобы они могли вовремя принять соответствующие меры.

В борьбе за существенное сокращение операционных рисков не стоит забывать и о необходимости развития корпоративной культуры безопасности. Любая технология может оказаться уязвимой, если люди, с ней работающие, не обладают нужным уровнем ответственности и знаний. Комбинация AI-инструментов с жёсткими регламентами без понимания сути рисков со стороны персонала может создать ложное чувство безопасности [Идиятуллин, Аухадеев, Киснеева, Антипанова, 2024]. На практике же внедрение больших данных и машинного обучения не отменяет роль человека в принятии окончательных решений: экспертная оценка является необходимым элементом. Поэтому организациям важно не только интегрировать новые алгоритмы, но и формировать у сотрудников компетенции кибергигиены, понимание принципов machine learning и общее осознание потенциала и ограничений AI.

В некоторых случаях финансовые компании вынуждены исправлять ошибки своих AI-систем задним числом. Например, если автоматический скоринговый алгоритм из-за сбоя или неверной калибровки начинает неправомерно отклонять кредитные заявки, это может привести к накоплению претензий от клиентов и интереса со стороны надзорных органов. Анализ реальных кейсов показывает, что отлаженный процесс валидации и регулярных проверок алгоритмов снижает вероятность массовых инцидентов [Коновалова, Михайлов, Кузьмина, 2018]. В условиях быстрого развития технологий крайне важно, чтобы подобные проверки проводились не формально, а глубоко и всесторонне, с учетом и технических показателей, и правовых аспектов, и мнения конечных пользователей. Ведь репутационные убытки часто превышают прямой финансовый ущерб, когда выясняется, что компания использует непроверенные или неэтичные AI-решения.

В отношении операционных рисков, связанных с ошибками программного обеспечения или техническими сбоями, AI также предлагает инструменты для прогнозирования и профилактики.

Алгоритмы могут направлять сигналы о потенциальных неисправностях и узких местах системы с учётом её текущей нагрузки, истории отказов и состояния отдельных модулей. Это способствует переходу от реактивного обслуживания к проактивному: проблемы решаются ещё до того, как они начнут влиять на работу ключевых систем. При этом, однако, возникает необходимость дополнительной защиты самих AI-компонентов, ведь сбой в модуле прогнозной аналитики может привести к ложным сигналам и нерациональному перераспределению ресурсов. Таким образом, компании должны закладывать в архитектуру систем принципы «резервирования» и дублирования критически важных функций, чтобы принцип «одной точки отказа» не проявился в AI-модуле.

Заметным трендом последних лет стало расширение использования роботизированной автоматизации процессов (RPA) в сочетании с алгоритмами машинного обучения. Умные «виртуальные сотрудники» выполняют задачи, которые ранее лежали на людях: от проверки форм на соответствие правилам до составления отчётов и выгрузки данных. Это даёт ощутимую экономию времени и средств, а также снижает риск человеческой ошибки. Тем не менее любые изменения в процессах влекут новые риски, среди которых – неправильная настройка робота, уязвимости в сценариях автоматизации и недостаточная проверка качеств программных ботов [Гоглев, Касаткина, Мигалин, Муштак, 2022]. Если такие системы находятся в прямой связке с клиентскими сервисами, даже небольшая ошибка может обернуться масштабными последствиями. И здесь потолок эффективности AI определяется тем, насколько грамотно выстроена структура операционного контроля и непрерывного аудита.

Искусственный интеллект меняет и подходы к управлению персоналом в финансовых организациях. Интернет-ресурсы, внутренние порталы и базы знаний могут быть интегрированы с AI-модулем, который будет подсказывать сотрудникам варианты решения проблем, основываясь на прошлом опыте компании и индустриальной практике. Это создаёт условия для «самообучающейся» организации, где операционные риски могут снижаться за счёт быстрого обмена экспертизой [Болонин, Асрян, 2024]. На практике компании решают это путём чёткого распределения ролей и полномочий, а также фиксации всех действий в логах, чтобы можно было воспроизвести цепочку событий.

Цифровизация финансовых рынков не обходится без масштабного использования облачных технологий. Банки и другие участники рынка часто переходят на облачные платформы, чтобы гибко масштабировать свою инфраструктуру и ускорять инновации. При этом передача критически важных функций внешним провайдерам усложняет архитектуру операционных рисков. Если *falla* произойдет в облачной части системы, последствия могут затронуть сразу множество клиентов и партнёров. Искусственный интеллект, встроенный в такие облачные решения, предоставляет удобство и широкие возможности аналитики, но одновременно требует продуманного управления доступами, шифрованием и договорными отношениями. Когда критические данные обрабатываются «на расстоянии», риск утечки информации или несанкционированного доступа возрастает, а следовательно, компании должны уделять особое внимание вопросам регламентации и аудита облачных сервисов.

В некоторых случаях компании сталкиваются с проблемами масштабирования AI-решений, когда модели, показавшие хорошие результаты в пилотных запусках, дают сбой при внедрении в промышленную среду. Это может быть связано с особенностями реальных данных, которые отличаются от тестовых, или с непредвиденным ростом нагрузки, когда количество транзакций в десятки раз превышает запланированные значения. Подобные инциденты свидетельствуют о том, что управление операционными рисками должно включать этап автоматизированного

мониторинга производительности AI-модулей и быстрого отклика на потенциальные отклонения. Технологические подразделения в тесной связке с риск-менеджерами должны анализировать логи и метрики в режиме реального времени, чтобы в случае необходимости перезапускать модели или включать резервные алгоритмы с более консервативными настройками.

С точки зрения стратегического планирования, искусственный интеллект способен предоставить огромные преимущества в прогнозировании и моделировании сценариев развития рынка. Однако при наличии погрешностей в данных или из-за недоработанной логики алгоритмов управленческие решения могут оказаться неверными в масштабах всего бизнеса [Верич, 2023]. Операционный риск здесь заключается в том, что топ-менеджмент полагается на неправильные предпосылки и расчёты, что впоследствии может привести к ошибкам в бюджете, инвестициях и управлении персоналом. Следовательно, в системах корпоративного управления должны существовать механизмы критического анализа AI-прогнозов и кросс-проверки результатов другими методами.

Анализируя опыт крупных финансовых организаций, можно заметить, что успешнее всего AI-технологии работают там, где их применение сопровождается комплексным пересмотром бизнес-процессов. Просто наложить «умный» алгоритм на существующие схемы – недостаточно, поскольку цифровая трансформация требует системных изменений, включая автоматизацию сбора и верификации данных, перестройку структуры принятия решений и формирование новых навыков персонала. Без этого операционные риски могут лишь вырасти, так как сотрудники будут взаимодействовать с AI-инструментами по старым правилам. Кроме того, важно корректно оценивать сроки и бюджеты на такие проекты: недооценка сложности может привести к затягиванию сроков и удорожанию внедрения, а также к появлению дополнительных уязвимостей на стыке традиционной и новой технологий.

Многие компании, стремясь повысить скорость внедрения AI, пользовались услугами сторонних провайдеров, специализирующихся на машинах обучения и аналитике больших данных. С одной стороны, это может резко ускорить получение результата, с другой – возникает риск непрозрачности алгоритмов и размывание ответственности. Если провайдер не предоставляет детальную информацию о характеристиках моделей или применяет проприетарные методики, финансовая организация оказывается в уязвимом положении. Любой сбой может привести к серьёзным репутационным потерям, в то время как внутренние специалисты компании могут оказаться не в состоянии оперативно разобраться в логике принятия решения внешним AI. Всё это затрагивает базовые принципы идентификации операционных рисков, когда нужно досконально понимать, из каких компонентов складывается та или иная технология.

При правильном подходе AI способствует не только выявлению и снижению операционных рисков, но и общему росту эффективности финансовых услуг. Более быстрое и точное принятие решений, лучшее персонализированное обслуживание клиентов, сокращение рутины и формирование новых цифровых продуктов – всё это помогает банкам и прочим финучреждениям занимать лидирующие позиции на рынке. Автоматизация и интеллектуальный анализ данных повышают прозрачность процессов, что в долгосрочной перспективе укрепляет доверие клиентов и регуляторов. Но нужно понимать, что переход к этому уровню технологической зрелости требует не только финансовых инвестиций, но и культурных, организационных изменений, а также новых компетенций.

Одной из сложнейших задач остаётся обеспечение непрерывности бизнеса в условиях

кризисов или серьёзных технологических катастроф. Искусственный интеллект может быть частью плана восстановления, автоматически перенастраивая бизнес-процессы и распределяя ресурсы в обход пострадавших узлов инфраструктуры. Однако если AI-модуль сам становится жертвой сбоя или кибератаки, это способно усугубить ситуацию. Именно поэтому план управления непрерывностью, ранее ориентированный только на физические и вычислительные ресурсы, теперь должен включать и резервирование AI-моделей, а также чёткие инструкции по переходу на ручной режим или упрощённые алгоритмы. Крайне важно заранее смоделировать подобные сценарии и проверить их работоспособность на практике.

Вопросу защиты клиентских данных в эпоху AI следует уделять особое внимание, поскольку любая утечка может привести к многомиллионным штрафам и подорвать репутацию организации. Здесь операционные риски тесно переплетены с правовыми и репутационными, а использование алгоритмов машинного обучения лишь усложняет задачу. Во-первых, модели могут самостоятельно производить производные данные, позволяющие косвенно идентифицировать человека даже после анонимизации. Во-вторых, расширяется круг сотрудников и систем, которые имеют доступ к чувствительной информации [Kumar, Kumar, Kumari, Kumari, Kumari, Behura, 2024]. В-третьих, возрастает вероятность атак по поиску уязвимостей именно в AI-инфраструктуре. Следовательно, компании должны внедрять принцип минимизации прав доступа, регулярно пересматривать политики безопасности и обеспечивать непрерывный мониторинг на предмет несанкционированных действий.

Стоит отметить, что развитие AI влияет и на макроэкономические аспекты финансовых рынков. Алгоритмические трейдинговые системы, автоматизированные кредитные скоринги и другие решения могут ускорять реакции рынка, иногда способствуя возникновению спекулятивных пузырей или резких ценовых скачков. С точки зрения операционных рисков, финансовые компании обязаны учитывать системную взаимосвязь своих AI-модулей с внешней средой, чтобы не оказаться в центре кризиса из-за неверной интерпретации рыночных сигналов. Подобный системный подход требует сотрудничества с регуляторами, профильными ассоциациями и даже конкурентами, поскольку глобальные кризисы наносят ущерб всем участникам рынка, независимо от их технологического уровня.

Актуальное направление исследований – это разработка мер, позволяющих коллективно отслеживать и контролировать поведение AI-систем на рынке. Идея заключается в создании единого наблюдательного пространства, в котором ключевые игроки и надзорные органы могут отслеживать аномальное поведение алгоритмов, способное привести к лавинообразному росту рисков [Бойченко, Фаина, 2023]. Такие механизмы включают обмен агрегированными данными о транзакционной активности, общие стандарты логирования и интерфейсы для оперативного взаимодействия в критических ситуациях. При этом соблюдаются принципы конфиденциальности и конкурентной тайны. Однако реализация подобных инициатив сталкивается с организационными и технологическими барьерами, а также с недоверием между конкурентами, что усложняет создание единой системы раннего предупреждения.

На пути к более зрелой системе управления операционными рисками предприятия должны формировать у себя компетенции в области аналитики данных, кибербезопасности и разработки AI. Зачастую крупные организации идут по пути открытия собственных AI-лабораторий или центров экспертизы, которые работают в тесной связке с бизнес-подразделениями. В таких центрах проводятся эксперименты с новыми методами анализа данных, модельными подходами и сценарными симуляциями, а полученные результаты затем внедряются в основной контур управления рисками [Гребешкова, Фирстова, 2023]. Такая модель способствует постоянному

обновлению знаний и методик, необходима для своевременного реагирования на новые источники рисков и повышения конкурентоспособности. Конечно, создавать и поддерживать собственные исследовательские подразделения требуют немалых инвестиций, но выгода от снижения операционных потерь и укрепления позиций на рынке может быть существенной.

Значительную роль играет и структура внутрикорпоративного управления. Если процессы принятия решений в сфере рисков децентрализованы, различные подразделения могут внедрять AI-решения без согласования друг с другом. Это чревато дублированием ресурсов, отсутствием единой методологии и возникновением противоречий в анализе данных [Buntić, Damić, Dužević, 2021]. С другой стороны, слишком жёсткая централизация может замедлить инновации и привести к тому, что отдельные подразделения не будут чувствовать своей ответственности за результаты AI-проектов. На практике эффективная модель управления хочет сбалансировать централизованные рамочные требования к использованию AI с гибкостью на местах, позволяя бизнес-единицам адаптировать технологию к своим нуждам.

Особое внимание следует уделять тому, как искусственный интеллект может улучшить управление персоналом, ведь многие операционные риски связаны с человеческим фактором. AI-инструменты могут использоваться для анализа психологического состояния сотрудников, выявления признаков «выгорания» или потенциального конфликта интересов. В теории это даёт возможность компании вовремя реагировать и предотвращать ситуации, когда демотивированный или недобросовестный сотрудник провоцирует кризис [Гоглев, Касаткина, Мигалин, Муштак, 2022]. При этом важно соблюдать этические нормы и законодательство о защите личных данных сотрудников. Вместо тотального контроля целесообразно выстраивать систему поддержки, в которой AI вовремя подаёт сигналы HR-подразделению и руководству, а те уже принимают решение о дальнейших действиях.

Необходимость непрерывного совершенствования систем управления операционными рисками с участием AI порождает спрос на внешние сертификации и стандарты качества. Отраслевые ассоциации и консалтинговые фирмы разрабатывают методологии аудита AI, проверяя корректность работы алгоритмов, полноту набора данных для обучения, соответствие принципам этики и правовым нормам [Болонин, Асрян, 2024]. Компании, которые успешно проходят такие аудиты, получают дополнительные преимущества в глазах клиентов и партнёров, а также снижают вероятность штрафов и предписаний от регуляторов. Формирование комплексных отраслевых стандартов помогает унифицировать подходы к управлению рисками, что в конечном итоге укрепляет устойчивость всей финансовой экосистемы.

В перспективе дальнейшей цифровизации финансовых рынков искусственный интеллект станет неотъемлемой частью практически всех процессов: от первичной клиентской коммуникации до сложных инвестиционных стратегий. При этом управления операционными рисками не должно отставать – оно обязано встраиваться в каждую стадию жизненного цикла AI-моделей, начиная с определения бизнес-требований, выбора набора данных и заканчивая мониторингом и обновлением алгоритмов после развертывания в продакшене. Только так можно обеспечить надежность и безопасность новых решений, а также соответствие растущим требованиям регуляторов и ожиданиям клиентов. Финансовые организации, которые это осознают, уже сейчас формируют команды, способные сопровождать весь AI-конвейер, и внедряют методологии DevOps и MLOps, адаптированные к специфике работы с рисками.

Одной из актуальнейших тенденций является расширение применения нейросетевых языковых моделей, используемых для анализа и генерации документов, чатботов в службах поддержки или автоматического составления отчётности. Такие модели могут значительно

дополнить классические методы идентификации аномалий в текстовых данных, применяемые в регуляторных и внутреннебанковских отчётах. Однако всё это не отменяет необходимости тщательно проверять точность и уместность сгенерированных ответов, поскольку языковые модели могут «выдумывать» факты, делая ошибки или выдавая недостоверную информацию. Это, в свою очередь, может приводить к рискам искажения данных или неправильного информирования клиентов. Следовательно, необходимо встроить механизм валидации результатов языковых моделей, чтобы избежать потенциальной волны репутационных и финансовых потерь.

В эру гиперсоединения, когда мобильные и веб-приложения взаимодействуют с десятками различных сервисов и API, возникает опасность каскадных ошибок. Если один из сервисов, на который опирается AI-модель, передаст некорректные данные, итоговые расчёты тоже будут неверными. Приходится прорабатывать систему границ, фильтров и проверок, чтобы снизить вероятность проникновения некорректной информации. Более того, AI-системы могут сами генерировать собой данные для других компонентов системы, создавая замкнутую петлю аналитики. Любое искажение на входе может усилиться на выходе, провоцируя целый ряд системных ошибок. Поэтому ключевым становится принцип «доверяй, но проверяй», который требует регулярных аудитов цифрового контента и кросс-верификации результатов разных алгоритмов.

Управление операционными рисками в контексте цифровизации требует не только технического, но и организационного переосмысления. Процессы должны быть выстроены так, чтобы AI был органичной частью всей цепочки создания ценности, а не просто модным дополнением к существующим системам. Для этого необходимо привлекать высшее руководство к вопросам AI и формировать чёткое видение того, как именно интеллектуальные алгоритмы будут интегрированы с бизнес-моделью [Buntić, Damić, Dužević, 2021]. Когда руководство понимает сущность и ценность AI, оно может выделять достаточные ресурсы, принимать грамотные управленческие решения и выстраивать нужные приоритеты. В противном случае инновации в области анализа рисков могут «застрять» на уровне пилотных проектов, не принося реальных изменений и подвергая компанию дополнительной неопределённости.

Говоря о долгосрочной перспективе, многие аналитики сходятся во мнении, что технологические изменения приведут к постепенному формированию киберфизических экосистем, где AI будет взаимодействовать с IoT-устройствами, биометрическими системами и блокчейн-платформами. Все эти технологии уже применяются в финансовом секторе, и их синергия может как повысить устойчивость рынков, так и создать новые непредвиденные риски. Например, валидация транзакций через блокчейн с использованием биометрических данных клиента может существенно снизить мошенничество, но если AI ошибочно идентифицирует человека, это создаст совершенно иные правовые и операционные проблемы. Таким образом, мы движемся к ситуации, когда комплексный подход к управлению рисками – не роскошь, а необходимость для сохранения конкурентоспособности.

На мировом уровне продолжается дискуссия о соотношении инноваций и регулятивных ограничений. Одни эксперты утверждают, что чрезмерный контроль может задушить инициативы в сфере AI, и тогда общество потеряет выгоды от масштабной цифровой трансформации финансов. Другие же настаивают на усилении надзорной роли государства, указывая на рост киберпреступности и риски массивной алгоритмической манипуляции рынками. В итоге формируется хрупкий баланс, где регуляционные меры должны быть достаточно гибкими, чтобы не сдерживать технологический прогресс, но и достаточно

жесткими, чтобы гарантировать защиту прав участников рынка и стабильность финансовых систем. Очевидно, что этот баланс будет меняться по мере эволюции технологий, и роль государства, профессиональных сообществ и общественного мнения в его корректировке будет возрастать.

Искусственный интеллект постепенно развивается не только как технология, но и как феномен, меняющий бизнес-процессы, рыночные структуры и даже потребительское поведение. В финансовом секторе эта революция особенно ярко заметна, так как здесь сталкиваются интересы большего числа стейкхолдеров: клиентов, акционеров, регуляторов, конкурентов. Управление операционными рисками приобретает всё более многоуровневый характер, где традиционные подходы к аудиту и контролю дополняются алгоритмическими решениями, способными обрабатывать большие массивы данных в реальном времени. Чем глубже интегрируется AI в повседневную деятельность компаний, тем тщательнее нужно выстраивать механизмы верификации и привлекать людей, обладающих не только техническими, но и стратегическими навыками. Именно так формируется основа для дальнейшего роста и успешной адаптации финансовых организаций к вызовам цифровой трансформации.

Заключение

Постепенно мы наблюдаем и зарождение новых специализаций: аналитики данных, эксперты в области этики AI, инженеры по проверке качества данных, «тренеры» для алгоритмов машинного обучения. Все они становятся важными элементами экосистемы управления операционными рисками. Такой тренд говорит о том, что AI выходит за рамки одного технологического направления и развивается как целостный подход к автоматизации и оптимизации, меняя при этом сущность банковских и страховых услуг. Если раньше риск-менеджеры вели учет инцидентов вручную или в таблицах, то теперь у них есть возможность опираться на панельные решения, где динамика риска отслеживается в реальном времени, а машинное обучение даёт прогнозы по вероятности тех или иных событий. Разумеется, это требует серьёзных инвестиций, но в быстро эволюционирующих условиях рынка становится критическим фактором конкурентоспособности.

Интегрально AI оказывает двоякое влияние. С одной стороны, он помогает более тонко диагностировать и предотвращать операционные риски, тем самым снижая убытки и повышая стабильность финансовых организаций. С другой стороны, сами AI-технологии добавляют сложности и неопределённости, порождая новые типы рисков, связанные с некорректной работой алгоритмов, этическими дилеммами и киберугрозами. Поэтому ключ к успеху – в умении балансировать, грамотно сочетая инновации с продуманным управлением, корпоративной культурой и нормативной базой. Те компании, которые научатся такому балансу, будут в выигрыше, сумев реализовать полный потенциал искусственного интеллекта в эпоху цифровизации финансового рынка.

Библиография

1. Натальсон А.В. Применение искусственного интеллекта для анализа рисков на рынке ценных бумаг // Экономика и управление: проблемы, решения. 2024. Т. 6. № 3 (144). С. 145-150.
2. Качалов Р.М. Слепцова Ю.А. Феномен риска в условиях применения алгоритмов искусственного интеллекта // Вестник Волгоградского государственного университета. Экономика. 2023. Т. 25. № 4. С. 5-16.
3. Kumar A. Kumar A. Kumari S. Kumari S. Kumari N. Behura A.K. Artificial intelligence: the strategy of financial risk

- management // Finance: Theory and Practice. 2024. Т. 28. № 3. С. 174-182.
4. Гоглев Н.Н. Касаткина Е.В. Мигалин С.А. Муштак О.И. Управление рисками с применением современных технологий искусственного интеллекта и анализа больших данных // Цифровая экономика. 2022. № 2 (18). С. 38-45.
 5. Верич Ю.Л. Проблемы и перспективы применения искусственного интеллекта на финансовых рынках // Актуальные вопросы учета и управления в условиях информационной экономики. 2023. № 5. С. 463-470.
 6. Buntić L. Damić M. Dužević I. Artificial intelligence in business models as a tool for managing digital risks in international markets // SHS Web of Conferences. 2021. Т. 92. С. 03005.
 7. Медик И.Н. Экономическая безопасность и управление корпоративными рисками при внедрении ИИ-технологий // Экономика: вчера, сегодня, завтра. 2024. Т. 14. № 3-1. С. 267-276.
 8. Болонин А.И. Асрян А.С. Риски внедрения искусственного интеллекта в банковский сектор // Инновации и инвестиции. 2024. № 2. С. 288-291.
 9. Идиятуллин Р.Г. Аухадеев А.Э. Киснеева Л.Н. Антипанова И.С. Искусственный интеллект для поддержки принятия инвестиционных решений в условиях неопределенности // Экономика и управление: проблемы, решения. 2024. Т. 4. № 6 (147). С. 198-204.
 10. Гребешкова И.А. Фирстова И.А. Применение искусственного интеллекта в области финансовых технологий // Актуальные вопросы учета и управления в условиях информационной экономики. 2023. № 5. С. 493-497.
 11. Ларина О.И. Харламенкова Д.А. Влияние искусственного интеллекта на качество цифровых финансовых продуктов // Стандарты и качество. 2023. № 12. С. 108-110.
 12. Коновалова М.Е. Михайлов А.М. Кузьмина О.Ю. Прогнозирование развития фондовых рынков в условиях становления цифровой экономики // Вестник Самарского государственного экономического университета. 2018. № 11 (169). С. 13-19.
 13. Ахматова Д.Р. Влияние ИИ-решений на финансовый сектор: прогнозирование будущих изменений // Вестник экономических и социологических исследований. 2023. № 2. С. 4-10.
 14. Андрущук В.В. Роль искусственного интеллекта в оптимизации финансовых операций на мировом рынке // Экономика: вчера, сегодня, завтра. 2024. Т. 14. № 3-1. С. 299-307.
 15. Бойченко О.В. Фаина Ю.Ю. Искусственный интеллект в управлении рисками организации // Экономика строительства и природопользования. 2023. № 4 (89). С. 67-74.

Analysis of Artificial Intelligence Impact on Identification and Management of Operational Risks in Digitalized Financial Markets

Maksim A. Levichev

Master's Degree,
Financial University under the Government of the Russian Federation,
125993, 49, Leningradsky ave., Moscow, Russian Federation;
e-mail: maxsonee@yandex.ru

Abstract

The article examines the impact of artificial intelligence (AI) systems on identifying and controlling operational risks during financial sector digitalization. The research relevance stems from increasing operational risk complexity due to frequent cyberattacks, human errors, technical failures, and imperfect procedures. Outdated risk assessment methods are being replaced by computer algorithms capable of processing vast data volumes and providing real-time risk warnings. The study describes AI implementation approaches including classification algorithms, multilayer self-learning structures, and hybrid methods combining traditional risk measurement techniques with computational analysis. Particular emphasis is placed on data quality verification, algorithm validation, and establishing effective collaboration between programmers, risk specialists, and regulators. Practical findings demonstrate that intelligent systems improve cyberthreat detection

accuracy, reduce financial losses, and enhance monitoring procedures. However, significant challenges were identified: biased training datasets, legacy system incompatibility, algorithmic opacity ("black box" problem), and emerging ethical dilemmas. Case studies of automated trading system failures causing market volatility are presented. The research highlights the need for balanced human-AI interaction in control processes and examines legal aspects including algorithm transparency requirements and personal data protection. Effective AI implementation requires workflow restructuring, personnel training investments, and creating hybrid structures where technology supports risk professionals. The article notes AI's dual nature: while increasing financial institutions' stability, it simultaneously creates new risk categories requiring thoughtful regulation. Future development directions include explainable AI algorithms, unified control standards, and cross-industry collaboration.

For citation

Levichev M.A. (2025) Analiz vliyaniya iskusstvennogo intellekta na identifikatsiyu i upravlenie operatsionnymi riskami v usloviyakh tsifrovizatsii finansovykh rynkov [Analysis of Artificial Intelligence Impact on Identification and Management of Operational Risks in Digitalized Financial Markets]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 15 (3A), pp. 695-710.

Keywords

Artificial intelligence, operational risks, financial market digitalization, machine learning, risk management

References

1. Natalson A.V. Application of artificial intelligence for risk analysis in the securities market // *Economics and management: problems, solutions*. 2024. Vol. 6. No. 3 (144). pp. 145-150.
2. Kachalov R.M. Sleptsova Yu.A. The phenomenon of risk in the application of artificial intelligence algorithms // *Bulletin of the Volgograd State University. Economy*. 2023. Vol. 25. No. 4. pp. 5-16.
3. Kumar A. Kumar A. Kumari S. Kumari S. Kumari N. Behura A.K. Artificial intelligence: the strategy of financial risk management // *Finance: Theory and Practice*. 2024. Vol. 28. No. 3. pp. 174-182.
4. Goglev N.N. Kasatkina E.V. Migalin S.A. Mushtak O.I. Risk management using modern artificial intelligence technologies and big data analysis // *Digital Economy*. 2022. No. 2 (18). pp. 38-45.
5. Verich Yu.L. Problems and prospects of using artificial intelligence in financial markets // *Actual issues of accounting and management in the information economy*. 2023. No. 5. pp. 463-470.
6. Buntić L. Damić M. Dužević I. Artificial intelligence in business models as a tool for managing digital risks in international markets // *SHS Web of Conferences*. 2021. Vol. 92. p. 03005.
7. Medik I.N. Economic security and corporate risk management in the implementation of AI technologies // *Economics: yesterday, today, tomorrow*. 2024. Vol. 14. No. 3-1. pp. 267-276.
8. Bolonin A.I. Asryan A.S. Risks of introducing artificial intelligence into the banking sector // *Innovations and investments*. 2024. No. 2. pp. 288-291.
9. Idiyatullin R.G. Aukhadeev A.E. Kisneeva L.N. Antipanova I.S. Artificial intelligence to support investment decision-making in conditions of uncertainty // *Economics and management: problems, solutions*. 2024. Vol. 4. No. 6 (147). pp. 198-204.
10. Grebeshkova I.A. Firstova I.A. Application of artificial intelligence in the field of financial technologies // *Actual issues of accounting and management in the information economy*. 2023. No. 5. pp. 493-497.
11. Larina O.I. Kharlamenkova D.A. The influence of artificial intelligence on the quality of digital financial products // *Standards and quality*. 2023. No. 12. pp. 108-110.
12. Konovalova M.E. Mikhailov A.M. Kuzmina O.Y. Forecasting the development of stock markets in the context of the digital economy // *Bulletin of Samara State University of Economics*. 2018. No. 11 (169). pp. 13-19.
13. Akhmatova D.R. The impact of AI solutions on the financial sector: forecasting future changes // *Bulletin of Economic and Sociological Research*. 2023. No. 2. pp. 4-10.

14. Andrushchuk V.V. The role of artificial intelligence in optimizing financial transactions in the global market // Economics: yesterday, today, tomorrow. 2024. Vol. 14. № 3-1. pp. 299-307.
15. Boychenko O.V. Fadina Yu. Artificial intelligence in risk management of an organization // Economics of construction and environmental management. 2023. No. 4 (89). pp. 67-74.