УДК 336.132.1:004.8
DOI: 10.34020/1993-4386-2025-3-58-65

МЕТОДИЧЕСКИЕ И ПРАКТИЧЕСКИЕ АСПЕКТЫ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТИ РОСФИНМОНИТОРИНГА*

А. М. Выжитович
Сибирский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации,
Новосибирский государственный университет экономики и управления,
Институт экономики и организации промышленного производства СО РАН,
Новосибирск, Россия

Я. О. Каменева, О. В. Панагушина
Сибирский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации,
Новосибирск, Россия

В статье рассматриваются технологии искусственного интеллекта и аналитики больших данных, используемые или планируемые к внедрению в деятельность Росфинмониторинга. Проанализированы современные тенденции и передовые методы автоматизации выявления незаконных сомнительных операций, алгоритмы обнаружения аномалий и потенциальных угроз экономической безопасности, применяемые Росфинмониторингом. Также освещаются вопросы внедрения автоматизированных решений в систему финансового мониторинга, их роль в формировании безопасной и прозрачной экономики. Результаты исследования демонстрируют перспективы повышения эффективности мероприятий по обеспечению экономической безопасности государства за счет использования инновационных технологий автоматизации.

Ключевые слова: финансовый мониторинг, экономическая безопасность, искусственный интеллект.

Современные системы финансового мониторинга нуждаются в адаптации к цифровой среде в целях противодействия применению злоумышленниками инноваций в преступных схемах. Именно поэтому Федеральная служба по финансовому мониторингу должна объединять различные источники информации, использовать передовые методы и технологии, включая искусственный интеллект (далее – ИИ) и машинное обучение. Использование ИИ помогает улучшить работу органов финансового мониторинга и увеличивает шансы обнаружения незаконных финансовых операций, позволяет выявлять аномалии, способные причинить ущерб экономической безопасности государства.

Обеспечение эффективной работы финансового мониторинга предполагает не только обновление технической базы, но и выработку нормативных правовых актов, а также инструкций для взаимодействия между государственными органами, банками и другими участниками финансовой сферы.

История цифровой трансформации Росфинмониторинга связана с развитием Единой информационной системы (ЕИС), которая начала создаваться с 2001 года.

На первом этапе работы с ЕИС, который начался в 2011 году и продолжался до 2014 года, Федеральная служба по финансовому мониторингу вела работу по сбору и систематизации данных, а также участвовала в совершенствовании нормативно-правовой базы и в разработке методических материалов.

Второй этап, длящийся с 2014 по 2018 годы, можно определить, как самый значимый, ведь именно в этот период ЕИС подверглась существенной трансформации:

– создана новая версия – ЕИС-3, в которой была добавлена возможность автоматизированного выявления, распознавания и структурирования сведений из всех поступающих информационных потоков в Росфинмониторинг;

– внедрение инновационных технологических решений, на основе которых происходило развитие центров обработки данных и информационно-технологической инфраструктуры в целом;

* Статья подготовлена в рамках приоритетного направления 5.6.1.5 (проект 5.6.1.5. (0260-2021-0002) Интеграция и взаимодействие мезоэкономических систем и рынков в России и её восточных регионах: методология, анализ, прогнозирование) плана НИР ИЭОПП СО РАН 2025 г.

– в целях реализации риск-ориентированного подхода был создан Центр оценки рисков, который стал ключевым элементом системы управления рисками экономической безопасности;

– разработана и внедрена система взаимодействия с участниками финансового мониторинга, работающая через удобный и безопасный функционал Личных кабинетов на сайте Росфинмониторинга,

В настоящее время продолжается новый этап, начавшийся в 2020 году, – цифровая трансформация ЕИС. В рамках этого этапа был разработан и утвержден «План информатизации Федеральной службы по финансовому мониторингу на 2020 год и плановый период 2021 и 2022 годов».

Основополагающим элементом данного этапа стала разработка Интеллектуальной цифровой технологической платформы (ИТЦП). Она позволила автоматизировать решение работниками Росфинмониторинга рутинных задач и высвободить время на решение более сложных аналитических задач, поскольку система самостоятельно способна обработать большое количество данных в режиме реального времени и вывести работнику полученные системой результаты. Таким образом, на данном этапе набирает оборот развитие технологий машинного обучения и искусственного интеллекта, которые позволят получать и применять новые знания для выявления рисков ПОД/ФТ, для выработки мер по их минимизации и оценки эффективности принятых мер [1].

В эпоху цифровой трансформации объемы данных растут экспоненциально, предоставляя беспрецедентные возможности для анализа и принятия обоснованных решений. Росфинмониторинг, осознавая этот потенциал, в рамках Международного центра оценки рисков (МЦОР), объединяющего подразделения финансовой разведки семи стран Содружества Независимых Государств (далее – Содружество или СНГ) – России, Армении, Беларуси, Казахстана, Кыргызстана, Таджикистана и Узбекистана, реализует инновационный проект [2, с. 9].

МЦОР – это не просто база данных, а высокотехнологичная платформа, призванная координировать усилия государств в борьбе с отмыванием денег и финансированием терроризма (ОД/ФТ). В условиях глобальной нестабильности и возрастающей сложности транснациональной преступности, совместные действия становятся критически важны. Объединение информационных ресурсов позволяет увидеть полную картину финансовых потоков на территории всего СНГ, выявляя скрытые паттерны и тенденции, которые не видны при анализе данных в изоляции.

МЦОР использует передовые аналитические методы и технологии обработки больших данных для выявления подозрительных операций и построения прогнозных моделей.

Объединение информации из различных источников позволяет:

– выявлять сложные схемы ОД/ФТ;

– проводить комплексный анализ финансовых операций;

– повышать эффективность расследований;

– укреплять международное сотрудничество.

Создание единого информационного пространства, объединяющего данные о финансовых потоках всех государств-участников Содружества, открывает беспрецедентные возможности для всестороннего анализа финансовых операций на территории всего СНГ. Это позволяет не только отслеживать текущую экономическую ситуацию в режиме реального времени, но и предсказывать потенциальные финансовые риски с гораздо большей точностью, чем это было возможно ранее. Такой комплексный подход к анализу данных дает возможность разработать и эффективно реализовать общие профилактические и превентивные меры, направленные на предотвращение финансовых кризисов, отмывания денег, финансирования терроризма и других угроз экономической стабильности всего региона. Благодаря своевременному выявлению аномалий и потенциально опасных тенденций, государства-участники СНГ получают возможность оперативно реагировать на угрозы, минимизируя их негативное воздействие.

С быстрыми темпами внедрения цифровых продуктов в жизнь общества растет и злоупотребление возможностями инноваций, особенно при совершении незаконных операций с криптоактивами. Проблема невозможности отслеживания движения криптоактивов актуальна и по сей день, однако Росфинмониторинг совместно с Центральным банком России запустили новый инструмент «Прозрачный блокчейн» в деятельность кредитных организаций. Для успешного функционирования проекта участники информируют Росфинмониторинг об операциях, связанных с оборотом криптовалюты, предоставляют данные адресов криптовалютных кошельков, наименование криптовалютной биржи, присвоенные криптовалютным транзакциям уровни рисков. Также для более четкого определения участников крипторынка Росфиномониторинг предложил две разновидности – криптоинвесторы и криптообменники.

С использованием информационной базы данных Платформы «Прозрачный блокчейн» выявлена схема экономического преступления в части придания правомерного вида преступному доходу в виде криптоактивов, полученных за распространение наркотических средств. Например, организованная преступная группа участвовала в незаконном обороте наркотиками через интернет-магазин и получала доход в виде виртуальных активов, которые попадали на криптовалютный кошелек, а затем активы были конвертированы в российские рубли с последующим зачислением на банковские счета родственников. В отношении членов преступной группы правоохранительными органами были возбуждены уголовные дела по признакам преступления, предусмотренного ч. 1 ст. 174.1 УК РФ (легализация преступных доходов) [3].

В контексте обеспечения финансовой безопасности Российской Федерации особое значение приобретает Национальный «Пояс финансовой безопасности». Эта масштабная инициатива представляет собой сложную и многогранную систему, которая объединяет передовые технологии анализа данных, инновационные методики финансового мониторинга и высококвалифицированных специалистов в области экономики, информационных технологий и кибербезопасности. Главным звеном этой системы является анализ больших данных (Big Data). Речь идет не просто о сборе информации, а о глубокой обработке огромных массивов данных, поступающих из самых разнообразных источников [2, с. 10].

Система обрабатывает информацию из банковского сектора, охватывая все аспекты банковской деятельности – от операций с наличными средствами до международных переводов. Аналогичным образом, в анализ включаются данные из налоговой системы, позволяющие отслеживать налоговые поступления, выявлять схемы уклонения от налогообложения и бороться с теневой экономикой.

«Пояс финансовой безопасности» основан на анализе внешнеэкономической деятельности, включая экспортно-импортные операции, инвестиционные потоки и международные платежные системы. Он служит инструментом выявления подозрительных сделок и предотвращения нелегальной деятельности, связанной с таможенными нарушениями и контрабандой. Эта система выполняет функции информационного сбора и аналитики, формируя объективную оценку экономической ситуации для принятия управленческих решений, способствующих обеспечению стабильности и безопасности. Важной составляющей является комплексный подход к использованию современных технологий, что позволяет анализировать данные, выявлять закономерности и оценивать риски. Основные сложности связаны с реализацией ИИ-технологий, обеспечивающих конфиденциальность и минимизацию ложных срабатываний.

По мнению авторов настоящей работы, необходимо сформировать подходящие правовые и регуляторные рамки, которые обеспечивали бы надежную защиту данных и укрепляли доверие к искусственно-интеллектным системам.

Росфинмониторинг ежегодно представляет статистическую отчетность своей работы по противодействию экономическим преступлениям, характеризующую состояние национальной антиотмывочной системы. Так, в 2024 году совместно с правоохранительными органами выявлена и пресечена деятельность шести теневых финансовых площадок с общим оборотом более 11 млрд рублей. Заказчиками теневых услуг часто выступают реально действующие организации, среди которых есть и бюджетополучатели. Наиболее вовлеченными в теневые схемы остаются отрасли строительства, торговли и сфера услуг[1].

При этом основными инструментами для вывода бюджетных средств в теневой оборот и последующей легализации остаются технические компании в цепочках расчетов посредников, аффилированных с бенефициарами преступных схем, обналичивание денежных средств, в том числе с участием «дропов» (подставных лиц).

Авторы настоящей статьи описывают в ней свою разработку «Интерактивная Коллаборативная Система Обнаружения Аномалий» (ИКСОА), которую предлагается внедрить в работу Росфинмониторинга (ФСФМ). По их мнению, так как на фоне многопланового развития и поступательного экономического роста стран Евразийской группы (ЕАГ) внедрение высоких технологий помогает автоматизировать многие процессы, что снижает издержки, то внедрение ИКСОА будет способствовать сокращению времени на выявление аномалий и преступлений в сфере финансового мониторинга и улучшению качества работы подразделений.

Целями по внедрению ИКСОА выступают:

– ускорение процесса обнаружения аномальных и подозрительных операций;

– повышение качества аналитической работы работников структур финансового мониторинга за счет визуализаций и рекомендаций искусственного интеллекта;

– обучение специалистов работе с автоматизированным аналитическим комплексом;

– создание дополнительного источника для доказательной базы при проведении Росфинмониторингом финансовых расследований;

– интеграция с уже функционирующими платформами, унификация интерфейсов для работы с данными разного вида.

Система ИКСОА характеризуется масштабным функционалом, направленным на автоматизацию процессов выявления нарушений, что занимает достаточно долгий период разработки и внедрения. В нижеприведенной таблице представлены группы компонентов рассматриваемой Системы, включающих в себя большое количество функций.

Разработка и внедрение первой версии предлагаемого решения (MPV) займет от четырех до шести месяцев, а расширение до полной функциональности потребует еще дополнительных двенадцать месяцев, что представлено на рисунке 1. Особенность предлагаемой системы для Росфинмониторинга заключается в использовании глубокого анализа данных для автоматического обнаружения аномалий, превосходя традиционные методы на основе пороговых правил. Авторский вклад проявляется в разработке уникальной нейросетевой архитектуры, способной адаптироваться к изменяющимся условиям рынка, а также в интеграции с ИИ, обеспечивающего прозрачность и интерпретируемость решений. Такой подход позволяет повысить точность идентификации подозрительных операций и укрепить доверие к автоматизированному анализу в рамках нормативных требований.

[1] Федеральная служба по финансовому мониторингу: официальный сайт. URL: https://www.fedsfm.ru/special/mediaaboutus/8680 (дата обращения: 30.09.2025).

Таблица

Основные компоненты системы ИКСОА

Компоненты	Описание
Интерфейс гибридной работы «Человек+ИИ»	Интерактивная платформа, которая сочетает автоматическую фильтрацию и рекомендации ИИ с возможностью человеческого вмешательства и уточнения
	Встроенные «маркеры доверия» – уровни автоматической оценки важности данных, позволяющие работнику (аналитику) сфокусироваться на наиболее релевантных событиях
Механизм сценариев событий	ИИ предлагает сценарии развития событий и спрашивает у аналитика о возможных действиях или сценариях предложения, обучаясь на решениях человека
	В перспективе планируется автоматическая донастройка моделей на конкретные бизнес-кейсы
Обучение с экспертами	Работники создают метки и комментарии к обнаруженным событиям, что ускоряет обучение модели и повышает качество фильтрации
	В результате реализуется систематический сбор экспертных знаний и их применение для улучшения алгоритмов

Источник: разработано авторами.

Источник: разработано авторами

Рис. 1. Этапы плана внедрения ИКСОА

Потребность в алгоритмах сортировки и отбора информации обусловлена необходимостью быстрого и точного доступа к нужным данным при обработке больших объемов информации. Авторами разработан алгоритм, обеспечивающий систематизацию и структурирование данных, позволяя специалистам эффективно принимать решения. Внутренний механизм сортировки и фильтрации является ключевым для повышения эффективности работы предлагаемой системы, что особенно важно при динамично меняющихся критериях поиска. Таким образом, внедрение таких алгоритмов повышает производительность и точность анализа данных, что критически важно для современных информационных систем.

Алгоритм сортировки данных и отбора нужной информации специалистом-пользователем включает следующие блоки.

1. Раннее автоматизированная приоритезация: использование алгоритма активного обучения, который выбирает наиболее вероятные "качественные" или "означающие" события для дальнейшего анализа человеком; обучение модели на основе предыдущих решений аналитика.

2. Многоуровневая фильтрация через «динамическую сеть»: построение сети связей по входящим данным, выявление центров активности и аномалий; использование этой сети для быстрого визуального представления релевантных и подозрительных событий.

3. Интерактивная настройка фильтрации: человек может корректировать параметры фильтрации, например, повышать чувствительность по определенным признакам или исключать вредные источники, а также формировать встроенные рекомендации по конфигурации фильтров на основании исторических решений.

4. Параметры «Обратной связи» и «Обучения» включают постоянную оценку точности фильтрации, а также автоматическую корректировку веса критериев.

В результате Система сама становится более точной и адаптивной (под специфику работы специалиста).

Практика показывает, что обеспечение экономической безопасности во многом зависит от того, как контролирующие органы адаптируются в современных условиях к цифровым технологиям. Предложенная в данной статье система значительно усилит возможности Федеральной службы по финансовому мониторингу, ее территориальных органов и подконтрольных им финансовых организаций по защите экономики и финансовой системы страны от угроз посредством:

– быстрого и точного выявления финансовых преступлений – в режиме реального времени автоматизированная функциональность ИИ позволяет выявлять подозрительные транзакции клиента, сложные схемы мошенничества и выводить информацию специалисту уполномоченного органа или организации для традиционного анализа факторов риска [4, с. 120-121];

– повышения эффективности мониторинга и оперативности реагирования на выявленные сомнительные события, что способствует своевременному принятию мер по нейтрализации угроз и минимизации ущерба;

– усиления превентивных мер – рекомендации и прогноз автоматизированной системы во многом способствуют своевременному выявлению потенциально противозаконных денежных и имущественных операций, а также нетипичных моделей поведения;

– масштабируемости и адаптации системы к новым угрозам – непрерывное обучение системы посредством обратной связи и новых данных позволяет ей адаптироваться к новым схемам злоумышленников;

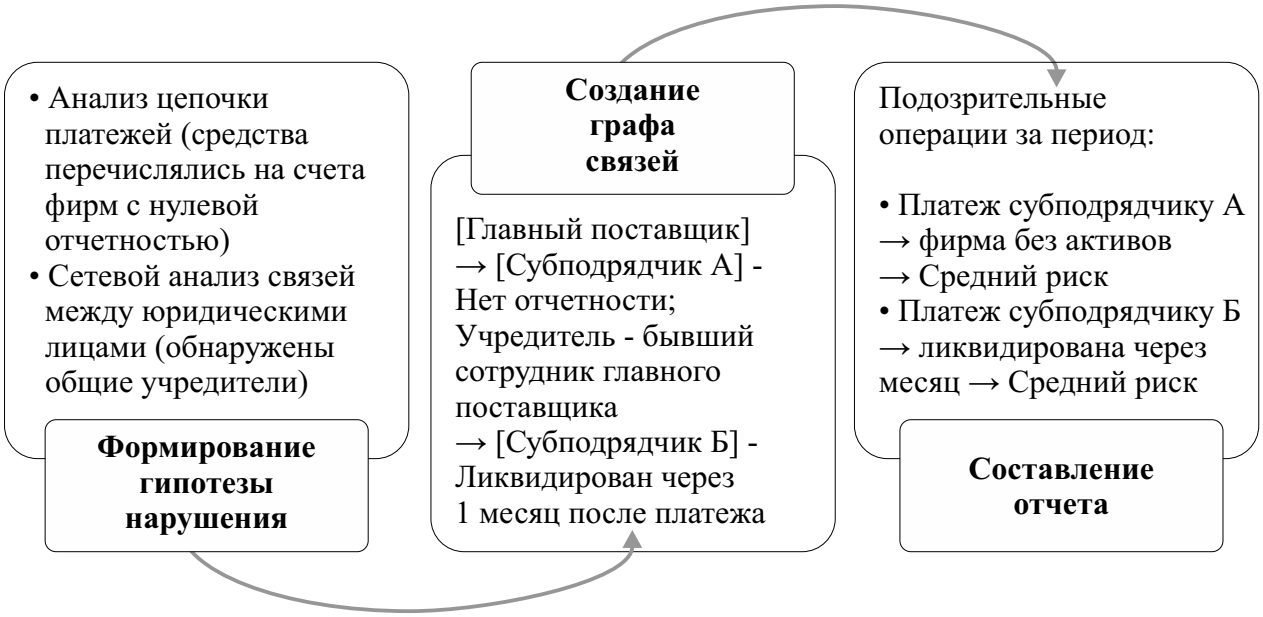
– повышения уровня международного сотрудничества – наличие современных технологических инструментов мониторинга укрепляет репутацию государства как надежного партнера на международной арене по борьбе с финансовыми преступлениями в сфере отмывания преступных доходов, финансирования терроризма, экстремизма и распространения оружия массового уничтожения [5].

Рассмотрим прикладное применение ИКСОА для мониторинга бюджетных средств на условном примере организации, получившей государственную субсидию или выполняющей в рамках проекта поставки для государственных нужд.

Система сможет помочь с выявлением аномалий с позиции формирования гипотез нарушений условий использования бюджетных средств для детального финансового мониторинга путем анализа данных в реальном времени, используя такие источники данных, как контракты, платежные поручения, операции по счетам, отчетность, применяемые рыночные цены и реестр госзакупок. Используемые методы включают в себя алгоритмы, разработанные в области машинного обучения, сетевой анализ, сравнение с эталонными показателями.

Допустим, Система выявила аномалию по привлечению фиктивных субподрядчиков и сформировала гипотезу – Поставщик привлекает в качестве субподрядчиков фирм-однодневок для вывода денежных средств. Были выявлены подозрительные операции по совершению платежа фирме без активов в лице Субподрядчика А, а также выявлена взаимосвязь с Субподрядчиком Б через учредителя, что говорит о сделках с фиктивными подрядчиками. Система составляет Отчет с нарушениями в соответствии с классификатором рисков и прилагает Граф связей между контрагнетами. Для организации финасового расследования подготовлена доказательная база, представленная в виде подготовленного отчета с источниками информации, фактами нарушений, рекомендациями по привлечению к ответственности и блокировке счетов или платежей до выяснения, а также задокументированная диаграмма выявленных связей. Весь описанный процесс выявления аномалий кратко представлен на рисунке 2.

Авторам настоящей статьи в силу конфиденциальности неизвестен алгоритм работы программного обеспечения ФСФМ, результаты анализа публикаций также показывают отсутствие его детализации в этой части. Исходя из понимания, что ФСФМ проверяет всех участников цепочки движения бюджетных средств по приинципу «вертикального контроля», контролируя каждого участника финансовой цепочки по отдельности на предмет соответствия заданным пороговым значениям и известным схемам, критериям риска вовлеченности в подозрительные операции, есть предположение, что предлагаемая ИКСОА действует на принципиально ином уровне.



Источник: разработано авторами

Рис. 2. Иллюстрация процесса выявления аномалий с помощтю ИКСОА

Применительно к ситуации с фиктивными субподрядчиками, текущий алгоритм Росфинмониторинга, вероятно, смог бы выявить нарушение только если Субподрядчик А или Субподрядчик Б уже находятся в «черном списке» или реестре недобросовестнвх поставщиков, было явное формальное несоотвествие в документах, проверка по конкретному платежу выявила, что у субподрядчика отозвана лицензия. Однако гипотезу о целенаправленной схеме по выводу денежных средств с привлечением взаимосвязанных фирм-однодневок текущей системе было бы сложно сгенерировать автоматически, оставляя эту задачу для аналитика, который вручную сопоставлял бы разрозненные данные.

В то время как ИКСОА могла бы автоматически выявить Субподрядчика А как фирму-однодневку на основе анализа его активов, налоговой нагрузки, историй операций, с помощью сетевого анализа мгновенно определить скрытую связь между главным Поставщиком и Субподрядчиком Б через общего учредителя, которую при ручной проверке можно было не заметить. ИКСОА самостоятельно формирует гипотезу о схеме и предоставляет аналитику готовый отчет с доказательной базой и рекомендациями.

Есть предположение, что внедрение Интерактивной Коллаборативной Системы Обнаружения Аномалий не заменяет существующий алгоритм Росфинмониторинга, а становится его мощным интеллектуальным дополнением, переводя существующую технологическую инфраструктуру финансого мониторинга из режима реактивного контроля по формальным признакам в режим проактивного, сетевого и поведенческого анализа. Таким образом, предлагаемая система позволит ускорить процесс выявления нарушений, который занимает несколько дней работы, до часов или минут, упростить работу аналитиков, предоставляя им не разрозненные данные, а готовые гипотезы с доказательной базой, углубить анализ, выявляя неочевидные и слабые связи, которые практически невозможно обнаружить без сетевого анализа и машинного обучения, догрузить существующее программое обеспечение ФСФМ более мощным аналитическим модулем, значительно повышающим его эффективность в борьбе с ухищренными схемами, например, нецелевого использования бюджетных средств.

Подводя итог, хотелось бы отметить, что внедрение предложенной ИКСОА создаст благоприятные условия на долгосрочную перспективу для защиты национальной экономики от противоправных финансовых операций. Технологии искусственного интеллекта позволят в режиме реального времени обнаруживать факты мошенничества за счет способности анализировать большие объемы данных, выявлять нетипичные транзакции и отслеживать аномалии, которые не поддаются традиционному наблюдению[2]. Результаты использования ИКСОА послужат дополнительным основанием для предоставления доказательств при проведении финансовых расследований Росфинмониторингом. Кроме того, алгоритмы ИКСОА предполагают автоматизировать рутинные задачи специалистов, что снижает их нагрузку и дает возможность сделать акцент на более сложных задачах. Все это не только повышает эффективность финансового мониторинга, но и снижает вероятность человеческой ошибки.

[2] Доклад для общественных консультаций «Применение искусственного интеллекта на финансовом рынке». Банк России, 2023. URL: https://cbr.ru/Content/Document/File/156061/Consultation_Paper_03112023.pdf (дата обращения: 30.09.2025)

Литература

1. *Склонюк Т. В.* Цифровая трансформация дистанционного мониторинга в сфере ПОД / ФТ / ФРОМУ // Вестник евразийской науки. 2023. Т. 15, № s5. URL: https://esj.today/PDF/ 20FAVN523.pdf.

2. *Лисицын А. С.* Борьба с легализацией преступных доходов и финансированием терроризма в мире цифровых технологий: вызов времени // Финансовая безопасность. 2024. № 41. С. 8–10. URL: https://www.fedsfm.ru/content/журнал %20фб/журнал %20финансовая %20безопасность %20№ 41.pdf.

3. *Скотин А. И., Щербакова М. Н.* Криптокомплаенс – первый опыт и перспективы // Финансовая безопасность. 2024. № 43. С. 60–63. URL: https://www.fedsfm.ru/content/журнал %20фб/новые/финансовая %20безопасность_43.pdf.

4. *Рожков В. А.* Использование искусственного интеллекта и машинного обучения для выявления и борьбы с финансовыми преступлениями // Теория и практика современной науки. 2024. № 6 (108). С. 118–122.

5. *Кучумов А. В., Печерица Е. В.* Цифровые инновации, соответствующие требованиям ПОД/ФТ и риск-ориентированный подход // Экономический вектор. 2022. № 4 (31). С. 56–63. DOI 10.36807/2411-7269-2022-4-31-56-63

6. *Антропцева И. А.* Противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма в условиях цифровизации и деглобализации: публично- правовой аспект // Современное право. 2024. № 3. С. 56–59.

7. *Сабирова Э. Р.* Цифровизация в органах государственной власти, осуществляющих контроль в сфере экономических преступлений (практическое применение) / В сборнике: Актуальные проблемы российского права и законодательства // Сборник материалов XVI Всероссийской научно-практической конференции (Красноярск, 25–26 апреля 2023 г.). Составитель Е. В. Василенко. – Красноярск: Сибирский институт бизнеса, управления и психологии, 2023. С. 203–205.

8. *Басенко И. К., Герасимова Е. Б.* Анализ перспектив использования искусственного интеллекта для обнаружения и предотвращения экономических преступлений // Экономические науки. 2024. № 5 (234). С. 158–165. DOI: 10.14451/1.234.158

9. *Шараев П. С.* Противодействие отмыванию (легализации) денежных средств в условиях цифровой трансформации (финансово-правовой аспект) // Юридический вестник Самарского университета. 2022. Т. 8, № 3. С. 94–100. DOI 10.18287/2542-047X-2022-8-3-94-100

Сведения об авторах

Выжитович Александр Михайлович – кандидат экономических наук, доцент, Сибирский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации; Новосибирский государственный университет экономики и управления; Институт экономики и организации промышленного производства СО РАН, Новосибирск, Россия.
ORCID: 0000-0003-0139-1317
E-mail: vam_70@mail.ru

Каменева Яна Олеговна – студент, Сибирский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, Новосибирск, Россия.
E-mail: kameneva_yana@inbox.ru

Панагушина Ольга Владимировна – студент, Сибирский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, Новосибирск, Россия.
E-mail: olga11nsk@mail.ru

METHODOLOGICAL AND PRACTICAL ASPECTS OF USING ARTIFICIAL INTELLIGENCE IN THE ACTIVITIES OF RUSSIA FINANCE MONITORING AGENCY

A. M. Vyzhitovich
Siberian Institute of Management – branch of the Russian Academy of National Economy and Public Administration under the President of the Russian Federation, Novosibirsk State University of Economics and Management, Institute of Economics and Organization of Industrial Production of the Siberian Branch of the Russian Academy of Sciences, Novosibirsk, Russia

Ya. O. Kameneva, O. V. Panagushina
Siberian Institute of Management – branch of the Russian Presidential Academy of National Economy and Public Administration, Novosibirsk, Russia

The article discusses the technologies of artificial intelligence and big data analytics used or planned to be implemented in the activities of Rosfinmonitoring. It analyzes current trends and advanced methods of automating the detection of illegal and suspicious transactions, as well as algorithms for detecting anomalies and potential

threats to economic security, which are used by Rosfinmonitoring. The article also covers the implementation of automated solutions in the financial monitoring system and their role in creating a secure and transparent economy. The research findings demonstrate the potential for improving the effectiveness of economic security measures through the use of innovative automation technologies.

Keywords: financial monitoring, economic security, and artificial intelligence.

References

1. Sklonjuk T. V. Digital Transformation of Remote Monitoring in the Field of AML/CFT/FPWMD, *Vestnik evrazijskoj nauki*, 2023, Vol. 15, No. s5. (In Russ.). Available at: https://esj.today/PDF/ 20FAVN523.pdf.

2. Lisicyn A. S. Combating the Legalization of Criminal Proceeds and the Financing of Terrorism in the World of Digital Technologies: A Challenge of the Time, *Finansovaja bezopasnost'*, 2024. No. 41, pp. 8–10. (In Russ.). Available at: https://www.fedsfm.ru/content/журнал %20фб/журнал %20финансовая %20 безопасность %20№ 41.pdf.

3. Skotin A. I., Shherbakova M. N. Cryptocompliance: First Experience and Prospects, *Finansovaja bezopasnost'*, 2024, No. 43, pp. 60–63. (In Russ.). Available at: https://www.fedsfm.ru/content/журнал %20фб/новые/финансовая %20безопасность_43.pdf.

4. Rozhkov V. A. Using Artificial Intelligence and Machine Learning to Detect and Combat Financial Crimes, *Teorija i praktika sovremennoj nauki*, 2024, No. 6 (108), pp. 118–122. (In Russ.).

5. Kuchumov A. V., Pecherica E. V. Digital Innovations Compliant with AML/CFT Requirements and a Risk-Based Approach, *Jekonomicheskij vector*, 2022, No. 4 (31), pp. 56–63. (In Russ.). DOI 10.36807/2411-7269-2022-4-31-56-63

6. Antropceva I. A. Countering the Legalization (Money Laundering) of Criminal Proceeds and the Financing of Terrorism in the Context of Digitalization and Deglobalization: A Public Law Aspect, *Sovremennoe pravo*, 2024, No. 3, pp. 56–59. (In Russ.).

7. Sabirova Je. R. Digitalization in government agencies responsible for monitoring economic crimes (practical application), *Aktual'nye problemy rossijskogo prava i zakonodatel'stva* [Current problems of Russian law and legislation], Collection of materials of the XVI All-Russian Scientific and Practical Conference (Krasnoyarsk, April 25–26, 2023), Krasnoyarsk: Sibirskij institut biznesa, upravlenija i psihologii, 2023, pp. 203–205. (In Russ.).

8. Basenko I. K., Gerasimova E. B. Analysis of the Prospects for Using Artificial Intelligence to Detect and Prevent Economic Crimes, *Jekonomicheskie nauki*, 2024, No. 5 (234), pp. 158–165. (In Russ.). DOI: 10.14451/1.234.158

9. Sharaev P. S. Countering money laundering (legalization) in the context of digital transformation (financial and legal aspect), *Juridicheskij vestnik Samarskogo universiteta*, 2022, Vol. 8, No. 3, pp. 94–100. (In Russ.). DOI 10.18287/2542-047X-2022-8-3-94-100

About the authors

Aleksandr M. Vyzhitovich – Candidate of Economic Sciences, Associate Professor, Siberian Institute of Management – branch of the Russian Academy of National Economy and Public Administration under the President of the Russian Federation; Novosibirsk State University of Economics and Management; Institute of Economics and Industrial Production Organization SB RAS, Novosibirsk, Russia.
ORCID: 0000-0003-0139-1317
E-mail: vam_70@mail.ru

Yana O. Kameneva – student, Siberian Institute of Management – branch of the Russian Presidential Academy of National Economy and Public Administration, Novosibirsk, Russia.
E-mail: kameneva_yana@inbox.ru

Olga V. Panagushina – student, Siberian Institute of Management – branch of the Russian Presidential Academy of National Economy and Public Administration, Novosibirsk, Russia.
E-mail: olga11nsk@mail.ru