

УДК 330.342.14

ФИНАНСОВАЯ РАЗВЕДКА И ПРЕДОТВРАЩЕНИЕ УГРОЗ: РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

М.В. Гагарина, Г.В. Носкова

Автономная некоммерческая организация высшего образования «Университет мировых цивилизаций имени В.В. Жириновского», Москва, email: mvgagarina@yandex.ru

Аннотация. В условиях стремительного роста цифровых финансовых потоков и усложнения преступных схем, основанных на использовании технологий, финансовая разведка становится ключевым элементом системы национальной безопасности. В статье рассматривается, как искусственный интеллект трансформирует подходы к выявлению, анализу и предупреждению финансовых угроз — от отмывания преступных доходов и финансирования терроризма до цифрового мошенничества. ИИ сегодня — это не просто вспомогательный инструмент, а полноценный аналитический механизм, способный в реальном времени просеивать гигантские массивы транзакционных данных, выявлять поведенческие аномалии и строить предиктивные модели, указывающие на риски ещё до их фактической реализации. Особое внимание уделено российскому контексту: росту теневого сектора экономики, технологическому обновлению Росфинмониторинга, активному внедрению ИИ в банковскую сферу и, одновременно, угрозе использования интеллектуальных алгоритмов преступными группами. Статья акцентирует необходимость комплексного подхода — синхронизации баз данных, подготовки кадров нового поколения и создания этически и юридически выверенной инфраструктуры контроля за ИИ. В результате анализ показывает, что именно симбиоз человека и алгоритма — с ясным распределением ответственности и функций — способен сформировать эффективную, предиктивную и справедливую систему финансовой разведки, соответствующую вызовам XXI века.

Ключевые слова: экономическая безопасность, финансовые кризисы, цифровая архитектура, макроэкономическая стабильность, предиктивная аналитика, структурные уязвимости, цифровой суверенитет, институциональная координация, киберустойчивость, искусственный интеллект, большие данные, стратегическое управление, экспортозависимость, технологическая изоляция.

FINANCIAL INTELLIGENCE AND THREAT PREVENTION: THE ROLE OF ARTIFICIAL INTELLIGENCE

M.V. Gagarina, G.V. Noskova

Autonomous Non-Commercial Organization of Higher Education «V.V. Zhirinovsky University of World Civilizations», Moscow, email: mvgagarina@yandex.ru

Abstract. With the rapid growth of digital financial flows and the increasing complexity of criminal schemes based on the use of technology, financial intelligence is becoming a key element of the national security system. The article examines how artificial intelligence is transforming approaches to identifying, analyzing, and preventing financial threats, from money laundering and terrorist financing to digital fraud. AI today is not just an auxiliary tool, but a full-fledged analytical mechanism capable of sifting through huge amounts of transactional data in real time, identifying behavioral anomalies and building predictive models indicating risks even before their actual implementation. Special attention is paid to the Russian context: the growth of the shadow economy, the technological renewal of Rosfinmonitoring, the active introduction of AI into the banking sector and, at the same time, the threat of the use of intelligent algorithms by criminal groups. The article highlights the need for an integrated approach — database synchronization, next-generation personnel training, and the creation of an ethically and legally sound AI monitoring infrastructure. As a result, the analysis shows that it is precisely the symbiosis of a person and an algorithm — with a clear distribution of responsibilities and functions — that is able to form an effective, predictive and fair financial intelligence system that meets the challenges of the 21st century.

Keywords: economic security, financial crises, digital architecture, macroeconomic stability, predictive analytics, structural vulnerabilities, digital sovereignty, institutional coordination, cyber resilience, artificial intelligence, big data, strategic management, export dependence, technological isolation.

Дата поступления статьи в редакцию: 22.05.2025

Дата принятия статьи в печать: 23.06.2025

Введение

В условиях стремительно усложняющейся финансовой реальности, где ежедневно совершаются миллионы операций и информационные потоки становятся все более плотными и непрозрачными, роль финансовой разведки приобретает первостепенное значение. Современные преступные схемы, будь то отмывание доходов, полученных преступным путём, финансирование экстремистской деятельности, нелегальная торговля или транснациональное кибермошенничество, всё чаще маскируются под легальную активность и проникают в легальный финансовый оборот [1]. Несмотря на свою теневую природу, такие процессы всё равно оставляют после себя цифровые следы, а задача специалистов — своевременно их обнаружить, грамотно интерпретировать и оперативно отреагировать. Однако по мере того, как преступные группы осваивают новые технологии, автоматизируют процессы и действуют на глобальном уровне, традиционные подходы к финансовому мониторингу начинают терять эффективность. Регуляторы, завязанные на нормативные рамки и рутинные процедуры, не всегда способны угнаться за динамикой цифрового криминала. Именно на этом фоне всё большую значимость приобретает искусственный интеллект — не как маркетинговый тренд, а как реальный функциональный ресурс, способный радикально трансформировать всю систему финансовой безопасности. Искусственный интеллект уже не просто вычисляет — он обучается, самообновляется, подстраивается под новые сценарии. Его способность выявлять тонкие аномалии и нестандартные поведенческие паттерны делает его незаменимым в тех ситуациях, где человеческий анализ пасует. ИИ способен в режиме реального времени просеивать массивы данных, сравнивать сложные взаимосвязи между субъектами, выявлять ранее незаметные закономерности, а главное — формировать предиктивные модели, способные указывать на потенциальную угрозу ещё до её фактического наступления. Это не просто шаг вперёд — это смена парадигмы, в которой борьба с финансовыми преступлениями перестаёт быть исключительно реакцией и становится проактивной системой с высоким уровнем технологической осведомлённости.

Финансовая разведка в современном понимании — это далеко не просто совокупность государственных ведомств, таких как Росфинмониторинг или международных коалиций, таких как Egmont Group. Это многослойная, гибкая и технологически насыщенная система, где ключевую роль играет взаимодействие разных уровней: государственных регуляторов, частных банков, финтех-компаний, аналитических центров и разработчиков цифровых решений. В условиях стремительной цифровизации, появления новых форм денег — от криптовалют до децентрализованных финансовых платформ и токенизированных активов — традиционная модель реагирования на финансовые угрозы больше не работает. Сегодня важен не столько анализ постфактум, сколько способность видеть угрозу до того, как она воплотилась. И именно здесь искусственный интеллект выходит на первый план — как технология, способная обеспечить упреждающее мышление и автоматизированный контроль на принципиально новом уровне [2].

ИИ в сфере финразведки — это уже не просто набор статистических моделей и инструментарий работы с большими данными. Это динамичные, самообучающиеся алгоритмы, способные распознавать текст, интерпретировать речь, классифицировать изображения, анализировать поведенческие паттерны и синтезировать выводы из фрагментарной информации. Такие системы легко работают с неструктурированными источниками — будь то телефонные звонки, сообщения в мессенджерах или PDF-документы. Они умеют отслеживать движение активов в нескольких юрисдикциях одновременно, выявлять несостыковки в цифровых профилях и соединять точки, которые человеческий аналитик, ограниченный временем и объемом восприятия, просто не заметит. Например, технологии NLP — обработки естественного языка — способны выявлять тонкие лингвистические маркеры мошенничества в переписке между клиентом и банком, а методы кластеризации и графового анализа раскрывают многослойные сети, где отмывание средств маскируется под череду легитимных операций через подставных лиц, оффшоры и фиктивные компании.

Однако по мере усиления этих технологий встает вопрос не только об их возможностях, но и об ответственности. Применение ИИ в такой критически чувствительной области, как финансовая разведка, требует предельной этической и правовой точности. Что делать, если алгоритм пометил конкретную транзакцию или компанию как подозрительную? Кто несёт ответственность за ошибку — система, программист или регулятор? Особенно тревожит феномен «чёрного ящика», характерный для многих современных моделей машинного обучения: когда даже их создатели не могут объяснить, почему именно был сделан тот или иной вывод. Это создаёт риски не только для эффективности, но и для прав человека — риск ложных обвинений, дискриминации, вторжения в частную жизнь. Значит, ключевым вызовом становится обеспечение прозрачности, интерпретируемости и подотчётности автоматизированных решений. Финансовая разведка, вооружённая ИИ, должна не просто быть эффективной — она обязана оставаться справедливой, контролируемой и поддающейся общественному и правовому надзору.

Нельзя оставлять без внимания растущую угрозу, связанную с тем, что искусственный интеллект всё активнее осваивается не только государственными структурами и финансовыми институтами, но и самими преступниками. Современные киберпреступные группировки уже создают собственные алгоритмы, нацеленные на обход существующих систем мониторинга и выявления подозрительной активности. Эти алгоритмы умеют подстраиваться под требования регуляторов, имитировать поведение реальных клиентов, генерировать фальшивые цифровые профили и формировать целые цепочки псевдотранзакций, которые визуально не отличаются от легальных финансовых потоков. И если ранее борьба с финансовыми преступлениями велась между людьми, то сегодня это сражение алгоритмов, где побеждает не тот, кто сильнее, а тот, кто быстрее обучается, точнее прогнозирует и быстрее адаптируется к новым условиям. В этой гонке на выживание нейросети могут быть как щитом, так и оружием [3].

На этом фоне искусственный интеллект перестаёт быть просто вспомогательным элементом — он превращается в полноценный стратегический ресурс, определяющий развитие всей системы финансовой разведки. Его внедрение влияет не только на технические аспекты анализа данных, но и трансформирует подходы к управлению финансовыми рисками, перестраивает принципы комплаенса, меняет логику работы регуляторных органов и задаёт новую планку в международном сотрудничестве в сфере финансовой безопасности. Мы наблюдаем сдвиг от локальной аналитики к сквозной, предиктивной модели, где каждое действие алгоритма имеет значение в глобальном масштабе.

Постепенно складывается новая организационная модель — человеко-машинный симбиоз. В этой модели машина выполняет роль вычислительного ядра, способного быстро анализировать, сортировать и выявлять потенциальные угрозы в массиве данных, тогда как человек остаётся носителем критического мышления, этических норм и стратегического контекста. Такой альянс позволяет добиться баланса между скоростью и осмысленностью решений, автоматизацией и гуманной ответственностью. Именно при таком распределении ролей появляется шанс построить не просто эффективную, а по-настоящему устойчивую, справедливую и адаптивную систему финансовой разведки — способную не только выявлять уже совершённые правонарушения, но и предотвращать их заранее.

Материал и методы исследования

Для России, находящейся в условиях повышенной внешнеполитической напряжённости, санкционной нагрузки и растущей цифровизации экономики, такие системы — уже не предмет теоретических размышлений, а насущная необходимость. Финансовая система страны сталкивается с множеством угроз, среди которых — не просто масштабное отмывание денег или финансирование экстремистских структур, но и целенаправленные попытки дестабилизации экономики через цифровые каналы. Эти процессы происходят незаметно, внутри банковских операций, в криптовалютных кошельках, в транзакциях через оффшорные платформы, и их сложно обнаружить без интеллектуальной технологической поддержки. Именно поэтому искусственный интеллект становится для России не просто инновацией, а системообразующим фактором в деле финансовой безопасности. Он даёт возможность не только реагировать, но и предвидеть — а это и есть ключевое преимущество в эпоху, когда угрозы становятся всё менее материальными, но всё более разрушительными.

Результаты исследования и их обсуждение

По оценкам аналитиков, объём теневой экономики в России по-прежнему остаётся колоссальным: от 2 до 5% валового внутреннего продукта, что в абсолютных цифрах может достигать порядка 6 триллионов рублей ежегодно. Эта сумма сопоставима с расходами федерального бюджета на здравоохранение или образование, и её вывод из легального оборота создаёт не только фискальные, но и социально-политические риски. Согласно данным Росфинмониторинга, только за 2023 год российские финансовые учреждения направили более 13 миллионов сообщений о подозрительных операциях. Такая статистика демонстрирует не только масштаб работы в этой сфере, но и растущую сложность выявляемых схем: они становятся всё более цифровыми, распределёнными, алгоритмически замаскированными. За каждой транзакцией может стоять как обычная платёжная активность, так и многоуровневая отмывочная операция, встроена в цепочку оффшорных, криптовалютных и псевдоюридических структур.

Особенно настораживает диспропорция между объёмом поступающих сигналов и числом реальных уголовных дел: на одно возбужденное дело приходится десятки тысяч подозрительных транзакций, которые, по сути, выпадают из поля оперативной реакции. Это либо свидетельствует о перегруженности фильтрующих систем, либо указывает на высокую долю ложноположительных срабатываний, когда сигналы не подтверждаются дальнейшими расследованиями. Такая ситуация — тревожный симптом: она

означает, что существующие методы мониторинга утратили чувствительность к качественным признакам финансовых правонарушений и не успевают за эволюцией криминальных моделей.

Именно в этом контексте искусственный интеллект перестаёт быть просто вспомогательным инструментом для ускорения рутинных операций — он превращается в интеллектуальное ядро финансовой разведки. Это своего рода «новый мозг» системы, который не просто обрабатывает данные, а учится различать закономерности, выстраивает связи между событиями и предугадывает потенциальные риски на ранних этапах. По информации Минцифры, в 2023 году рынок ИИ в России вырос на 37% и приблизился к отметке 900 миллиардов рублей. Основной прирост пришёлся на банковский и финансово-аналитический секторы, где алгоритмы машинного обучения всё чаще применяются для оценки кредитных рисков, анализа аномалий в транзакционной активности, построения поведенческих профилей клиентов и даже прогнозирования вероятности вовлечённости в сомнительные схемы.

Такой переход от постфактум-анализа к прогнозной аналитике кардинально меняет логику всей системы: финансовая разведка получает возможность работать не по принципу «случилось — отреагировать», а по модели «возникает риск — нейтрализуй заранее». В условиях растущей сложности финансовых потоков и высокой скорости операций, это становится не просто конкурентным преимуществом, а вопросом системной устойчивости и экономической безопасности страны [4].

В контексте стремительной цифровизации и растущей сложности финансовых преступлений внедрение искусственного интеллекта в работу Росфинмониторинга можно без преувеличения назвать одним из наиболее показательных примеров глубокой государственной технологической трансформации. Так, в рамках усилий по модернизации инструментов анализа и повышения эффективности противодействия отмыванию денежных средств была запущена специализированная платформа — Международный центр оценки рисков, или МЦОР. Эта система, построенная на основе технологий машинного обучения, предназначена для интеллектуального анализа трансграничных финансовых потоков и оценки уровня риска операций в реальном времени. По оценке самих представителей службы, интеграция ИИ в аналитическую инфраструктуру позволила добиться впечатляющих результатов: время, затрачиваемое на обработку и интерпретацию подозрительных транзакций, сократилось на 60–70%, а точность выявления аффилированных субъектов, замешанных в сложных схемах легализации преступных доходов, значительно возросла.

Параллельно с этим следует отметить, что технологии искусственного интеллекта с не меньшим успехом находят применение и в частном секторе — прежде всего в банковской сфере. Один из крупнейших банков России, интегрировав в свою систему нейросетевой модуль анализа транзакций, зафиксировал снижение числа ложных срабатываний на подозрительные переводы почти на 45%. Это, в свою очередь, позволило не только разгрузить внутренние службы комплаенса, но и практически удвоить их эффективность в части выявления реальных угроз. Таким образом, ИИ начал выполнять не просто вспомогательную функцию, а превратился в ключевой элемент операционной модели современных финансовых институтов, где скорость и точность — параметры, от которых напрямую зависит не только деловая репутация, но и соблюдение регуляторных требований.

В то же время, как бы парадоксально это ни звучало, технологический прогресс обостряет и другую сторону реальности — рост цифровых преступлений. Важно понимать, что цифровизация финансовой среды — это возможности, которые она открывает перед государством и легальным бизнесом, с не меньшей скоростью осваиваются и криминальными структурами. По данным Министерства внутренних дел и Центра по борьбе с киберпреступностью, только в 2023 году количество выявленных схем, в которых использовались поддельные цифровые идентичности, созданные при помощи технологий deepfake и генеративных нейросетей (GAN), выросло на 32%. Особенно тревожно выглядит тенденция к массовому созданию так называемых «денежных мулов» — фальшивых аккаунтов в социальных сетях и мессенджерах, генерируемых автоматически с применением ИИ. Эти аккаунты используются для распределения, фрагментации и маскировки денежных потоков, связанных с преступной деятельностью.

Складывается крайне неоднозначная картина: с одной стороны, государство и бизнес укрепляют свою технологическую инфраструктуру за счёт внедрения ИИ, а с другой — сталкиваются с всё более изощрённым, интеллектуально подкованным противником. В этом противостоянии уже недостаточно полагаться на традиционные методы и ручной анализ: борьба выходит на уровень алгоритмов, где выигрывает не тот, у кого больше ресурсов, а тот, кто быстрее обучается и эффективнее адаптируется к меняющимся условиям. И именно по этой причине искусственный интеллект становится не просто инструментом модернизации, а краеугольным элементом новой архитектуры финансовой безопасности [5].

Несомненно, когда речь заходит о технологиях, особенно в таком сложном и чувствительном сегменте, как финансовая разведка, важно понимать: за цифровыми платформами и алгоритмами всегда стоят не только «железо» и программный код, но и, прежде всего, люди, компетенции и организационные ресурсы. И как бы стремительно ни развивались технологические решения, без достаточного количества квалифицированных специалистов, способных разрабатывать, внедрять и обслуживать эти решения, любое техническое преимущество рискует остаться нереализованным потенциалом. На сегодняшний день в России, по самым осторожным оценкам, насчитывается не более 50 тысяч специалистов, владеющих методами работы с искусственным интеллектом и большими данными. Причём, что особенно показательно, только незначительная часть из них работает в сферах, связанных с комплаенсом, безопасностью и противодействием финансовым преступлениям [6].

Становится очевидным, что для построения по-настоящему интеллектуальной и устойчивой системы финансовой разведки требуются не просто технические решения, а масштабные инвестиции в человеческий капитал. Причём речь идёт не только о подготовке профильных специалистов в университетах, но и о создании прикладных образовательных программ, рассчитанных на сотрудников государственных ведомств, банковских структур и аналитических центров. Именно они в будущем будут работать на стыке права, технологий и финансовой безопасности, а значит, должны говорить с ИИ «на одном языке» — как в буквальном, так и в профессиональном смысле.

Наряду с кадрами, ключевым условием эффективности искусственного интеллекта остаётся наличие полноценных, качественно очищенных и взаимосвязанных данных. Без них — и это важно подчеркнуть — даже самый совершенный алгоритм остаётся, по сути, высокотехнологичной интуицией, а не инструментом точного анализа. Сегодня в России наблюдается фрагментарность в структуре баз данных: налоговые, судебные, миграционные, банковские массивы информации зачастую существуют в разрозненном виде, ограничены в доступе и плохо стыкуются между собой. Это серьёзно сдерживает возможности сквозного анализа и построения связей между субъектами и операциями. Искусственный интеллект, как и любой живой организм, требует «питания» — регулярного, достоверного и целостного информационного ресурса, без которого его эффективность сводится к догадкам.

Тем не менее, если смотреть в будущее, становится всё более очевидным: именно ИИ способен дать толчок к переходу от реактивной модели — где анализируются уже совершённые правонарушения — к проактивной стратегии, при которой система заранее распознаёт потенциальные риски и предотвращает реализацию преступной схемы. Алгоритмы уже сегодня демонстрируют способность строить поведенческие профили, анализировать нестандартную деловую активность, выявлять «слабые звенья» в компаниях — например, сотрудников, демонстрирующих повышенный уровень риска вовлечённости в коррупционные или мошеннические действия. Это не просто новый инструмент, а принципиально иной взгляд на задачи безопасности [7].

Российское государство, в целом, осознаёт стратегическое значение этих процессов. В рамках нацпроекта «Цифровая экономика» особое внимание уделяется направлению искусственного интеллекта: только до 2030 года планируется инвестировать более 140 миллиардов рублей в развитие технологий, часть которых направлена как раз на создание интеллектуальных систем, способных обеспечивать финансовую и экономическую устойчивость. Такой подход свидетельствует о формировании понимания, что ИИ — это уже не абстракция, а реальный рычаг контроля и развития.

И действительно, цифры говорят сами за себя: Россия стоит на пороге глубинной трансформации финансовой разведки. Угрозы стали цифровыми, распределёнными, кросс-границными — и следовательно, ответ на них также должен быть технологичным. Искусственный интеллект — пожалуй, единственный сегодня инструмент, способный превратить громоздкую, подверженную перегрузкам систему финансового мониторинга в гибкую и интеллектуально насыщенную сеть, которая способна не только фиксировать нарушения, но и видеть их зарождение, распознавать их форму, контекст и возможные последствия [8].

Однако для этого необходимо последовательно решить три ключевые задачи: во-первых, выстроить единую систему интеграции и обмена данными; во-вторых, вложиться в подготовку специалистов нового поколения, сочетающих технические, аналитические и правовые навыки; и, наконец, в-третьих, научиться не только использовать ИИ, но и контролировать его — как любую мощную технологию, он требует рамок, регуляции и этической подотчётности. Россия только начинает этот путь, но уже сегодня очевидно: в эпоху цифровых преступлений победить можно только цифровыми средствами. И победа в этой борьбе будет зависеть не от количества серверов или скорости обработки, а от того, насколько человечество сумеет сохранить баланс между машинной эффективностью и человеческой ответственностью [9].

Выводы

В конечном итоге, становится всё более очевидным: финансовая разведка в XXI веке находится не просто в стадии технологического обновления, а переживает структурный сдвиг, затрагивающий как её цели, так и инструменты. Рост масштабов, многообразия и скрытности финансовых преступлений, происходящий на фоне тотальной цифровизации экономики, требует от аналитических и надзорных систем не только быстрой реакции, но и способности к предвосхищению угроз. В этом контексте искусственный интеллект выступает уже не как вспомогательная технология, а как новая когнитивная среда — автономная, обучающаяся, способная к адаптации в условиях нестабильной, фрагментированной и глобально распределённой финансовой реальности. Его внедрение позволяет перейти от традиционного линейного мониторинга к сложным, нелинейным архитектурам анализа, которые способны не только интерпретировать происходящее, но и выявлять уязвимости ещё до того, как они превратятся в точки атаки. Тем не менее, параллельно с этим технологическим рывком обостряются и инфраструктурные, и институциональные вызовы. Без надёжной синхронизации информационных систем, без доступа к полным и чистым наборам данных, без интеграции правовых норм и этических стандартов в алгоритмическое ядро даже самый совершенный ИИ-алгоритм рискует быть бесполезным — или, что хуже, опасным. Как показывает текущая российская практика, наличие передовых технических решений ещё не означает готовности всей системы к их адекватному использованию. Здесь требуется не просто модернизация, а целенаправленное формирование экосистемы: от создания нормативной среды, регулирующей применение ИИ в чувствительных сферах, до выстраивания профессиональной подготовки нового типа — для специалистов, способных мыслить одновременно как технари, юристы и аналитики. Именно поэтому у России в текущих условиях есть не столько обязанность догонять технологических лидеров, сколько уникальный исторический шанс — разработать и внедрить собственную модель интеллектуальной финансовой безопасности, учитывающую как геополитическую специфику, так и внутреннюю институциональную логику. Эта модель, по сути, должна быть построена на принципиальном балансе: между скоростью обработки и глубиной интерпретации, между автономностью машинного анализа и человеческой ответственностью, между эффективностью принятия решений и их социальной легитимностью. Лишь в этом случае искусственный интеллект сможет занять своё место не как формальный атрибут цифровой эпохи, а как жизненно важный стратегический элемент — основа для устойчивого, справедливого и технологически суверенного будущего финансовой разведки.

Литература

1. Шугаева О.В., Зайченко А.А., Золкин А.Л., Новосельский С.О., Петрушина О.В. Цифровая трансформация администрирования платежно-расчетных отношений в деятельности таможенных органов // Евразийский Союз: вопросы международных отношений. 2024. Т. 13. № 4 (57). С. 815-826.
2. Новосельский С.О., Антропова Т.Г., Грунина О.А. Оценка цифровой трансформации социально-экономической системы России в условиях геополитической турбулентности // Евразийский Союз: вопросы международных отношений. 2023. Т. 12. № 3 (49). С. 176-188.
3. Пузырев С.А. Роль подразделений финансовых разведок в борьбе с легализацией преступных доходов // Обеспечение финансовой безопасности России. М.: Научно-исследовательский центр финансовой безопасности, 2013. С. 74-77.
4. Козлова А.М., Гагарина М.В. Фальсификация финансовой отчетности как вид корпоративного мошенничества // Бухгалтерский учет: достижения и научные перспективы XXI века: Материалы Международной научно-практической конференции, Москва, 24 ноября 2022 года. Ярославль-Москва: Канцлер, 2023. С. 52-56.
5. Жиликов Д.И., Новосельский С.О., Плахутина Ю.В., Петрушина О.В., Почечун П.И. Ретроспективный анализ налоговых доходов федерального бюджета // Экономические науки. 2023. № 219. С. 173-181.
6. Земсков В.В., Прасолов В.И. Основы организации финансовой разведки и финансовых расследований. М.: ООО «Издательство Прометей», 2023. 288 с.
7. Фешина С.С., Хрусталева Е.Ю., Королева Л.П., Филичева А.А. Финансовая разведка как инструмент информационно-аналитической поддержки принятия решений в условиях возрастающих внешних ограничений // Контрোলлинг. 2023. № 2 (88). С. 62-71.
8. Новосельский С.О., Кирсанов К.А., Яковлев В.М. Ретроспективный анализ функционирования социально-экономической системы Российской Федерации в условиях геополитической турбулентности. М., 2022. 192 с.
9. Венчиков А.А. Зарубежный опыт формирования отчетности финансовых институтов в подразделениях финансовой разведки по операциям с наличными денежными средствами // Вызовы цифровой экономики: кадры для региона: Сборник статей VII Всероссийской научно-практической конференции, Брянск, 12 декабря 2023 года. Брянск: Брянский государственный инженерно-технологический университет, 2023. С. 40-43.