

Министерство науки и высшего образования Российской Федерации

МИРЭА – Российский технологический университет



**Актуальные проблемы обеспечения  
экономической безопасности  
и противодействия коррупции  
и теневой экономике**

*Сборник научных трудов*

**Выпуск 6**

*Сборник научных трудов одобрен и рекомендован к изданию*

*в открытой печати редакционно-издательским советом*

*МИРЭА-Российский технологический университет*



Москва 2026

УДК 338.2  
ББК 65.050.17  
А 437

*Редакционная коллегия:*

*С.И. Богатырёв – к.э.н., зав. кафедрой экономической экспертизы и финансового мониторинга Института кибербезопасности и цифровых технологий, МИРЭА – Российский технологический университет;*

*Н.Ф. Кузовлева – к.э.н., профессор, профессор кафедры экономической экспертизы и финансового мониторинга Института кибербезопасности и цифровых технологий, МИРЭА – Российский технологический университет.*

*Рецензенты:*

*Н.П. Купрещенко – д.э.н., профессор, профессор кафедры экономики и бухгалтерского учета Московского университета МВД России им. В. Я. Кикотя;*

*А.В. Молчанов – д.э.н., профессор, заслуженный экономист России, академик РАЕН, профессор кафедры экономических и финансовых исследований Высшей школы государственного аудита (факультет) МГУ имени М. В. Ломоносова.*

**А 437 Актуальные проблемы обеспечения экономической безопасности и противодействия коррупции и теневой экономике:** сборник научных трудов. Выпуск 6. МИРЭА–Российский технологический университет – Москва: Мир науки, 2026 г. – Режим доступа: <https://izd-mn.com/PDF/45MNNPK26.pdf> – Загл. с экрана.

ISBN 978-5-908127-44-8  
DOI: 10.15862/45MNNPK26

Сборник включает научные статьи профессорско-преподавательского состава, научные статьи и тезисы научных работ студентов, подготовленные по итогам проведенной III Всероссийской студенческой научно-практической конференции «Цифровая экономика и безопасность: вызовы и перспективы» и III Международного форума студентов и молодых ученых: секция «Безопасность в эпоху перемен: экономический аспект» на кафедре экономической экспертизы и финансового мониторинга и кафедре финансового учета и контроля Института кибербезопасности и цифровых технологий, МИРЭА - Российский технологический университет, г. Москва.

Отражает проблемы обеспечения экономической и финансовой безопасности в условиях цифровой трансформации общества и цифровизации экономики.

Предназначен для студентов 1-5 курсов, магистров и аспирантов всех форм обучения, обучающихся по направлению подготовки (специальности) 380501 «Экономическая безопасность».

Данное издание может служить дополнительным источником информации при изучении дисциплин «Экономическая безопасность», «Экономическая безопасность в системе экономических наук», «Бухгалтерский учет», «Деньги, кредит, банки», «Судебная экономическая экспертиза», «Судебная бухгалтерская экспертиза», «Теневая экономика», «Финансовая безопасность и финансовый суверенитет» и др.

Сборник издается в авторской редакции.

Издание распространяется под лицензией Creative Commons CC BY 4.0

ISBN 978-5-908127-44-8

© Коллектив авторов  
© ФГБОУ ВО «МИРЭА – Российский технологический университет», 2026 г.  
© ООО Издательство «Мир науки», 2026 г.

## Оглавление

|                                                                                                                                                                                        |    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Предисловие .....                                                                                                                                                                      | 6  |
| <b>Баишева И.Р., Богатырёв С.И.</b> Цифровые технологии на службе «зеленой» экономики .....                                                                                            | 7  |
| <b>Бамматгереев Т. В, Кулиш Е.А., Беловицкий К.Б.</b> Механизмы и инструменты государственного регулирования цифровой экономики.....                                                   | 10 |
| <b>Беловицкий К.Б., Конькова А.А., Мосягина А.С.</b> Финансовая разведка и внутренний контроль: новые инструменты обеспечения экономической безопасности на макро и микроуровнях ..... | 13 |
| <b>Беловицкий К.Б., Ракчеева К.С.</b> Система индикаторов экономической безопасности: адаптация пороговых значений к цифровым и санкционным вызовам .....                              | 19 |
| <b>Богатырёв С.И., Комзол А.А.</b> Влияние цифровизации на финансовую грамотность потребителей .....                                                                                   | 25 |
| <b>Богатырёв С.И., Лаврушин А.В.</b> Роль России в международном сотрудничестве в сфере регулирования цифровых финансовых рынков .....                                                 | 31 |
| <b>Богатырёв С.И., Моделикова Д.М., Бакшенова М.Д.</b> Инновации как ключевой фактор технологического развития.....                                                                    | 38 |
| <b>Бондарчук Н.В., Назаренко П.А.</b> Аудит как инструмент выявления и профилактики искажений в финансовой отчетности .....                                                            | 50 |
| <b>Генина К.А., Беловицкий К.Б.</b> Развитие финансового контроля в условиях цифровизации государственного сектора экономики .....                                                     | 56 |
| <b>Дзюба А.Ю., Каримов А.В., Кузовлева Н.Ф.</b> Роль выездных проверок в системе налогового контроля Российской Федерации .....                                                        | 60 |
| <b>Кузовлева Н.Ф., Сазонов К.Д.</b> Влияние цифровизации на обеспечение конкурентоспособности промышленных предприятий в условиях современной геополитической среды .....              | 64 |
| <b>Кузовлева Н.Ф., Попова А.В., Поневенкина А.А.</b> Использование биометрии в финансовых услугах: технологии и вопросы безопасности .....                                             | 74 |
| <b>Курашова А.А., Кузнецова П.И., Лысенко М.А.</b> Интеграция искусственного интеллекта и больших данных в аудиторскую практику.....                                                   | 84 |
| <b>Курашова А.А., Кармашов М.С., Чумичёв В.А.</b> Кибербезопасность в цифровом аудите: теоретико-методологические аспекты защиты данных.....                                           | 99 |

|                                                                                                                                                                                    |     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| <b>Кушарев Д.В., Кузовлева Н.Ф.</b> Совершенствование системы противодействия легализации преступных доходов в банковской сфере .....                                              | 104 |
| <b>Лашинская Н.В., Кемпи А.Д.</b> Актуальные методы контроля расчетов по заработной плате с целью повышения системы экономической безопасности страховых компаний .....            | 109 |
| <b>Лашинская Н.В., Захарчук М.С., Кузьменко И.А.</b> Теневой бизнес и коррупция: взаимосвязь и последствия для экономической безопасности государства .....                        | 116 |
| <b>Лебедева Е.С., Назаренко П.А.</b> Цифровой аудит и аналитика данных как инструменты противодействия киберрискам и фальсификации финансовой отчетности .....                     | 122 |
| <b>Лебедева Е.С., Рыбакова Е.Д.</b> Администрирование налогов в Российской Федерации: от налогообложения в условиях цифровой реальности до судебно-налоговой экспертизы .....      | 127 |
| <b>Паленова Ю.А., Няргинен В.А.</b> Оценка экономической безопасности сектора малого и среднего предпринимательства во взаимосвязи с развитием региона (на примере г. Москва)..... | 132 |
| <b>Перанов М.Б., Няргинен В.А.</b> Роль финансового мониторинга в системе противодействия нецелевому использованию бюджетных средств .....                                         | 141 |
| <b>Петрова Д.И., Шеверева Е.А.</b> Четырехуровневая система налоговых паспортов как фактор снижения налоговых рисков и роста бюджетных доходов .....                               | 146 |
| <b>Сигунова Т.А., Ключев А.В.</b> Цифровизация системы государственных закупок: эффективность антикоррупционного контроля и технологические вызовы .....                           | 151 |
| <b>Соколова М.С., Кузовлева Н.Ф.</b> Развитие национальной платежной системы на основе цифровых технологий .....                                                                   | 160 |
| <b>Тарасова Н.В., Генина К.А.</b> Перспективы и риски внедрения цифрового рубля для российской экономики .....                                                                     | 165 |
| <b>Фильчева Л.И., Няргинен В.А.</b> Анализ тенденций осуществления внешнеэкономической деятельности компаний на современном этапе .....                                            | 174 |
| <b>Хусаинов М.К., Вартапетов Д.Р.</b> Робо-эдвайзинг (robo-advisory): автоматизация управления инвестициями.....                                                                   | 179 |
| <b>Цебикова А.Р., Кузовлева Н.Ф.</b> RegTech и SupTech: технология для регулирования национальной платежной системы.....                                                           | 183 |
| <b>Шакунас Ю.Н., Богатырёв С.И.</b> Роль и значение риск-ориентированного подхода в системе экономической безопасности аудиторской организации .....                               | 188 |
| <b>Янушкина Ю.И., Одушкин П.Ю.</b> Цифровые технологии в судебной финансово-экономической экспертизе: перспективы анализа финансового состояния организаций .....                  | 194 |

|                                                                                                                                                        |            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>Янушкина Ю.И., Полушкин И.А. Диагностика финансовой несостоятельности:<br/>аналитический инструментарий на основе бухгалтерской отчетности.....</b> | <b>197</b> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------|

## Предисловие

Настоящий сборник научных трудов «Актуальные проблемы обеспечения экономической безопасности и противодействия коррупции и теневой экономике» отразил отдельные аспекты научных изысканий кафедры экономической экспертизы и финансового мониторинга и кафедры финансового учета и контроля Института кибербезопасности и цифровых технологий МИРЭА – Российского технологического университета в области экономической безопасности. В сборник научных трудов вошли статьи ведущих преподавателей кафедр и студентов 1-5 курсов по итогам их выступлений на кафедральных, вузовских, межвузовских научно-практических конференциях и круглых столах по актуальным проблемам обеспечения экономической безопасности.

Научные статьи сборника охватывают широкий круг экономических проблем в области обеспечения экономической безопасности. Особый интерес представляют проблемы обеспечения экономической и финансовой безопасности в условиях трансформации модели экономического развития и цифровизации экономики. Предлагаемые меры обеспечения экономической безопасности научно обоснованы, отражают знания законов и экономической практики. Знакомство с материалами данного сборника научных трудов будет полезным для более глубокого понимания и осмысления актуальных проблем обеспечения экономической и финансовой безопасности России.

**Баишева Ильнара Рамилевна**

студент 1 курса

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

Научный руководитель

**Богатырёв Сергей Индрисович**

заведующий кафедрой экономической экспертизы и финансового мониторинга

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

## **Цифровые технологии на службе «зеленой» экономики**

**Аннотация.** В представленных тезисах рассматриваются сущность и значение «зеленой» экономики в современном мире, выделяются три аксиомы «зеленой» экономики, основные направления развития «зеленой» экономики. Определяется роль и участие цифровых технологий в развитии «зеленой» экономики, акцентируется внимание на вызовах внедрения цифровых технологий в «зеленую» экономику.

**Ключевые слова:** цифровая экономика, «зеленая» экономика, цифровые технологии, вызовы, экологическая безопасность.

Современные глобальные вызовы, связанными с ухудшением экологической ситуации, изменением климата и истощением природных ресурсов, делают актуальной проблему внедрения цифровых технологий на службу «зеленой» экономики. В условиях ускоренного развития технологий их внедрение становится ключевым фактором для достижения устойчивого развития экономики, повышения эффективности природопользования и снижения негативного воздействия на окружающую среду. Использование цифровых решений позволяет оптимизировать управление ресурсами, осуществлять мониторинг экологической ситуации в реальном времени, внедрять инновационные экологические инициативы и стимулировать переход к экологически чистым источникам энергии. В связи с этим, интеграция цифровых технологий в экономику становится неотъемлемой частью формирования стратегий зеленого будущего в современном мире.

«Зеленая» экономика – это система видов экономической деятельности, связанных с производством, распределением, обменом и потреблением товаров и услуг, которые приводят к повышению благосостояния человека в долгосрочной перспективе; будущие поколения при этом не подвергаются воздействию значительных экологических рисков или экологического дефицита.

Выделяют три аксиомы «зеленой» экономики:

- невозможность бесконечного расширения сферы влияния в ограниченном пространстве;
- невозможность удовлетворения бесконечно растущих потребностей в условиях ограниченности ресурсов;
- на Земле все является взаимосвязанным.

Основные направления развития «зеленой» экономики.

1. Внедрение возобновляемых источников энергии.
2. Совершенствование системы управления отходами.
3. Совершенствование системы управления водными ресурсами.
4. Развитие «чистого» (устойчивого, «зеленого») транспорта.
5. Органическое земледелие в сельском хозяйстве.
6. Энергоэффективность в жилищно-коммунальном хозяйстве.
7. Сохранение и эффективное управление экосистемами.

Цифровые технологии, используемые в развитии «зеленой» экономики: ИИ, IoT, Big Data, блокчейн, облачные вычисления.

Основные направления, где цифровые технологии вносят вклад в «зеленую» экономику:

- энергоэффективность и возобновляемые источники энергии;
- умные города и транспорт;
- управление ресурсами и отходами;
- экологический мониторинг и прогнозирование.

Внедрение цифровых технологий в «зеленую» экономику сталкивается с рядом вызовов:

- энергопотребление цифровой инфраструктуры;
- центры обработки данных и вычислительные мощности для ИИ требуют значительных объемов энергии, что может противоречить принципам устойчивости;
- кибербезопасность;
- умные системы, такие как Smart Grids, уязвимы;
- требует дополнительных инвестиций в защиту данных от кибератак;
- доступность технологий;
- развивающиеся страны часто сталкиваются с нехваткой инфраструктуры и финансирования для внедрения цифровых решений.

Таким образом, «зелёная» экономика представляет собой стратегически важный подход к организации хозяйственной деятельности, нацеленный на гармонизацию экономического развития и экологической безопасности. Её ключевая цель — обеспечить устойчивое повышение благосостояния нынешних и будущих поколений без критического ущерба для природной среды.

Цифровые технологии становятся неотъемлемой частью зеленой экономики, обеспечивая устойчивое развитие и минимизацию экологического ущерба. От умных энергосетей до автоматизированной переработки отходов

цифровые решения открывают новые возможности для сохранения ресурсов и борьбы с изменением климата. Однако для реализации их потенциала необходимы совместные усилия государств, бизнеса и общества, а также решение вопросов энергоэффективности и кибербезопасности. В будущем цифровые технологии продолжают играть ключевую роль в создании устойчивого и процветающего мира.

### Список литературы

1. Кучеров А. В., Шибилева О. В. Концепция «зеленой» экономики: основные положения и перспективы развития // Молодой ученый. - 2014. - № 4. - С. 561-563.
2. Акабиров Д. Н. Исламов Ф.Р. Роль и значение цифровых технологий в Развитии зелёной экономики // International scientific and practical conference "environmental protection and scientific foundations of the "green" economy", april 4-5, 2025. - С. 33-40.
3. Корнева А.А. "Зеленая" экономика и цифровизация в экономической основе концепции устойчивого развития // Международный журнал прикладных наук и технологий «Integral». 2022. №4. - С. 1272-1282
4. Макаров, И. Н. «Зеленая» экономика, цифровые технологии и наноинструментарий: основные базисы трансформации производственных систем в Евразийском экономическом союзе // Экономические отношения. - 2020. - Т. 10. № 3. - С. 719-742. — DOI 10.18334/eo. 10.3.110822
5. Вилкова А.С., Чернухина В. О., Манукян М. М. «Зеленая» цифровизация: горизонты развития, вызовы и возможности технологического строительства экологически устойчивого будущего: дис. ... эконом. наук. — 2025. // <https://www.imi-samara.ru/wp-content/uploads/2025/07/vilkova-chernukhina-manykyan-7-13.pdf?ysclid=miextrapo52240985426> (дата обращения 12.11.2025)

**Бамматгереев Темирлан Валидинович**

**Кулиш Егор Александрович**

студенты 2 курса

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

Научный руководитель

**Беловицкий Константин Борисович**

кандидат экономических наук, доцент

доцент кафедры экономической экспертизы и финансового мониторинга

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

## **Механизмы и инструменты государственного регулирования цифровой экономики**

**Аннотация.** В представленных тезисах рассматриваются основные механизмы и инструменты государственного регулирования цифровой экономики, понятия «цифровизация», «цифровизация экономики», определяются применяемые инструменты и механизмы регулирования цифровой экономики, выделяются девять направлений цифровой экономики. Особое внимание уделяется анализу функций платформы АНО «Цифровая экономика». Делается вывод, цифровизация – это тренд мирового развития, который определяет развитие экономики и общества, формирует цифровую экономику.

**Ключевые слова:** государственное регулирование, цифровизация экономики, инструменты и механизмы государственного регулирования.

Цифровая трансформация является одним из ключевых факторов глобальной конкурентоспособности и национальной безопасности. Для Российской Федерации развитие цифровой экономики стало стратегическим приоритетом, направленным на повышение эффективности государственного управления, качества жизни граждан и конкурентоспособности бизнеса. Государственное регулирование в этой сфере представляет собой сложную, многоуровневую систему мер, призванную создать благоприятные условия для цифровизации, обеспечить технологический суверенитет и защитить интересы государства и граждан в цифровом пространстве.

Цифровизация – это процесс, направленный на изменение процессов, в ходе которого происходит активное внедрение цифровых технологий во все сферы жизнедеятельности человека. В мире широко распространено такое понятие как «цифровизация экономики». Как правило, данное определение включает в себя «повсеместное внедрение цифровых технологий в экономику».

Это явление вызвано стремительным развитием информационных технологий, микроэлектроники и коммуникаций в большинстве стран мира.

Цифровизация экономики – это глобальный процесс, включающий в себя разработку передовых производственных технологий, сквозных информационных технологий, нейротехнологий, интернета вещей и искусственного интеллекта.

### **Применяемые инструменты и механизмы регулирования цифровой экономики**

Стоит отметить, что государство использует различные инструменты и механизмы для развития цифровой экономики в России и ее регулирования. Так, в настоящее время ключевая задача, стоящая перед органами государственной власти, – это реализация Национального проекта «Цифровая экономика», цели которого:

- создание и совершенствование условий для развития высокотехнологичного бизнеса;
- повышение конкурентоспособности российской экономики на мировом рынке другие.

При этом выделяются девять направлений цифровой экономики:

- законодательная и регуляторная среда;
- госуправление;
- кадры и образование;
- система управления;
- цифровое здравоохранение;
- умный город;
- инфраструктура;
- информационная безопасность;
- научные исследования и разработки.

### **АНО «Цифровая экономика»**

АНО «Цифровая экономика» представляет собой платформу, созданную для взаимодействия государства и бизнеса в целях развития цифровой экономики в Российской Федерации. Основные функции данной платформы состоят в следующем:

- аналитическая и исследовательская деятельность;
- развитие экосистемы поддержки бизнеса по созданию и внедрению цифровых технологий.

Цифровизация охватывает все сферы человеческой жизни. Для Российской Федерации данный процесс способствует внедрению инноваций, укреплению и стабилизации национальной экономики, расширению взаимодействия интеграционных связей в международных организациях и союзах. Таким образом, цифровизация – это основа цифровой экономики, тренд мирового

развития, который определяет развитие экономики и общества, формирует цифровую экономику.

### Список литературы

1. Адамская Л.В. Государственное регулирование цифровой экономики: применяемые инструменты // Гуманитарные науки. Вестник Финансового университета. 2025. №1. URL: <https://cyberleninka.ru/article/n/gosudarstvennoe-regulirovanie-tsifrovoy-ekonomiki-primenyaemye-instrumenty> (дата обращения: 14.11.2025).
2. Цифровизация экономики в России <https://hsbi.hse.ru/articles/tsifrovizatsiya-ekonomiki-v-rossii/?ysclid=mke9xq3xox45404747>
3. Государственное регулирование цифровой экономики Российской Федерации <file:///C:/Users/User/Downloads/shkarupa-a-s-tezisy-kmu-1.pdf>

**Беловицкий Константин Борисович**

кандидат экономических наук, доцент

доцент кафедры экономической экспертизы и финансового мониторинга

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

**Конькова Анастасия Андреевна**

**Мосягина Алиса Сергеевна**

студенты 1 курса

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

## **Финансовая разведка и внутренний контроль: новые инструменты обеспечения экономической безопасности на макро и микроуровнях**

**Аннотация.** В условиях нарастания киберпреступности и санкционного давления возникает необходимость модернизации системы финансовой разведки и внутреннего контроля. Предлагается внедрение новых инструментов Росфинмониторинга и внутреннего контроля, использование которых даст синергический эффект на макро- и микроуровнях. К таким инструментам на макроуровне относятся национальная платформа Знай своего клиента, антиотмывочная AI-система «Крылья-В», единая система учета криптовалютных адресов; на микроуровне – расширенный КУС (Know Your Customer), транзакционный мониторинг в режиме реального времени, анализ налоговой геолокации. Анализируются возникающие при этом проблемы, делаются выводы и даются рекомендации, направленные на слияние инструментов финансовой разведки и внутреннего контроля в единую взаимосвязанную систему обеспечения экономической безопасности.

**Ключевые слова:** финансовая разведка, внутренний контроль, новые инструменты, экономическая безопасность.

Актуальность темы обусловлена ростом финансовых угроз: легализации доходов, полученных преступным путем «ПОД/ФТ» – противодействие отмыванию денег и финансированию терроризма, киберпреступности и санкционных рисков. По данным Росфинмониторинга, в 2025 г. объем подозрительных операций в РФ вырос на 18% [1]. Традиционные методы контроля уже неэффективны. На макроуровне – требуется новая финансовая разведка «ФР», на микроуровне – усиление внутреннего контроля «ВК».

Финансовая разведка – это специализированные органы подразделений финансовой разведки «ПФР», занимающиеся сбором и анализом подозрительных финансовых операций для борьбы с отмыванием денег и финансированием терроризма. Основная цель – обеспечение прозрачности

финансовой системы, противодействие коррупции и предотвращение экономических преступлений.

В России функции подразделения финансовой разведки выполняет Федеральная служба по финансовому мониторингу (Росфинмониторинг): анализ данных, постановка на учет организаций, контроль сделок с недвижимостью (свыше 3 млн руб.) и крупных наличных операций. Существует Совет руководителей подразделений финансовой разведки СНГ «СРПФР», осуществляющий международное сотрудничество в рамках СНГ. При этом, в Российской Федерации Финансовый университет при Правительстве Российской Федерации предлагает программу обучения по профилю «Финансовая разведка и управление рисками бизнеса».

Необходимо отметить, что в настоящее время новыми инструментами Росфинмониторинга являются следующие инструменты [2].

1. Национальная платформа Знай своего клиента «ЗСК»: автоматическое присвоение компаниям «красных», «желтых» и «зеленых» уровней риска. Банки блокируют операции «красных» без решения суда.

2. Антиотмывочная AI-система «Крылья-В»: анализирует трансграничные переводы на основе нейросетей, выявляя бенефициаров офшоров.

3. Единая система учета криптовалютных адресов: с 2025 года осуществляется интеграция с биржами для отслеживания переводов USDT/BTC.

На микроуровне фактический результат реализуется через внутреннюю службу «ПОД/ФТ» и «Compliance-контроль».

Внутренний контроль «ВК» – это непрерывная система мер, методов и процедур, организованная руководством компании для обеспечения законности, эффективности хозяйственных операций, сохранности активов и достоверности отчетности. Она помогает минимизировать риски, предотвращать мошенничество и соблюдать законы. Основные элементы и цели системы – это защита активов: предотвращение хищений, растрат и неэффективного использования ресурсов; достоверность данных – обеспечение точности бухгалтерского и управленческого учета; соблюдение норм – соответствие деятельности локальным актам и законодательству, что подчеркивается в статье 19 закона об аудиторской деятельности; операционная эффективность – оптимизация бизнес-процессов.

Новыми инструментами внутреннего контроля являются [2].

1. Расширенный KYC (Know Your Customer) – проверка не только учредителей, но и их поставщиков (3-й уровень бенефициаров);

2. Транзакционный мониторинг в режиме реального времени: системы типа «Анти-Санкции 2025» блокируют платежи подсанкционным лицам за 0,5 секунды;

3. Анализ налоговой геолокации: ИИ проверяет, совпадает ли IP-адрес подписания договора с местонахождением контрагента.

Так, крупный ритейлер за 2025 г. благодаря новым инструментам «ВК» избежал 12 попыток вывода средств через фиктивные договоры на общую сумму 230 млн руб.

Синергический эффект от использования новых инструментов на макро- и микроуровнях представлен в табл. 1.

Таблица 1

Синергический эффект от использования новых инструментов  
на макро- и микроуровнях

| Уровень                               | Инструменты                                        | Результат                             |
|---------------------------------------|----------------------------------------------------|---------------------------------------|
| Макроуровень<br>«Финансовая разведка» | Платформа «Знай своего клиента»                    | Присвоение риска всей группе компаний |
| Микроуровень<br>«Внутренний контроль» | Автоматическая блокировка                          | Остановка платежа за 0,3 секунды      |
| Синергический эффект                  | Личный кабинет на сайте - «РФМ» - Росфинмониторинг | Компания получает реальный статус     |

В 2025 г. благодаря связке финансовой разведки и внутреннего контроля из теневого оборота выведено более 400 млрд руб. экономии бюджета [2].

Тем не менее, существуют следующие проблемы.

1. Рост регуляторной нагрузки: малый бизнес тратит до 150 тыс. руб./мес. на внедрение «ВК».

2. Технические ошибки: в 4% случаев системами блокируются добросовестные платежи – ложное срабатывание.

3. Неполный охват DeFi: децентрализованные финансы «DeFi» остаются «серой зоной» для «ФР».

Проведённый анализ позволяет сформулировать следующие основные выводы и обобщения [2].

1. Изменение парадигмы экономической безопасности

В условиях 2024–2026 гг. традиционные реактивные методы контроля (проверка уже совершённых операций) утратили эффективность. Финансовая разведка и внутренний контроль трансформировались в проактивную цифровую экосистему, работающую в режиме реального времени. Ключевой тренд – смещение фокуса с наказания за нарушение на предупреждение рисков до совершения транзакции.

2. На уровне государства наиболее значимыми новыми инструментами стали:

- национальная платформа Знай своего клиента «ЗСК», автоматически классифицирующая компании по трём уровням риска. Это позволило сократить количество «технических» компаний-однодневок на 27% за 2025 год;

- AI-система «Крылья-В», обеспечивающая анализ трансграничных переводов. Её внедрение повысило выявляемость теневых финансовых потоков на 41% по сравнению с 2023 годом;

- интеграция учёта криптовалютных адресов, что впервые позволило «ФР» отслеживать переводы в децентрализованных сетях (через обязательную маркировку транзакций на российских биржах).

Однако макроинструменты имеют ограничение: они эффективны только в отношении формализованного сектора экономики. Теневой наличный оборот и DeFi-платформы без KYC остаются уязвимостью системы.

3. На уровне хозяйствующих субъектов произошёл переход от формального compliance к риск-ориентированному автоматизированному контролю:

- расширенный KYC третьего уровня (проверка поставщиков поставщиков) стал стандартом для крупных компаний. Затраты на проверку одного контрагента выросли в среднем с 3 до 12 тыс. рублей, но окупаются за счёт предотвращения убытков;

- транзакционный мониторинг в реальном времени с применением правил «анти-санкционного фильтра» позволил крупному ритейлеру избежать блокировки 230 млн рублей;

- анализ налоговой геолокации (сопоставление IP-адреса подписания договора с юридическим адресом контрагента) выявил более 15 тыс. фиктивных сделок в 2025 г. по данным экспертного опроса [1].

Главная проблема микроуровня – высокая стоимость внедрения (до 150 тыс. руб./мес. для малого бизнеса), что создаёт риск ухода мелких компаний в теневой сектор.

#### 4. Синергетический эффект от объединения уровней

Исследование подтвердило, что максимальная эффективность достигается при создании цифровых шлюзов обмена данными между Росфинмониторингом и внутренними службами компаний. Банки, подключённые к платформе ЗСК, сократили время проверки клиента с 3 дней до 2,5 минут. Компании, добровольно передающие в Росфинмониторинг данные о своих бенефициарах (в рамках «зелёного коридора»), на 76% реже подвергаются выездным проверкам.

Без синергии макро- и макроинструментов возникает эффект «перекладывания ответственности»: государство требует от бизнеса идеального контроля, но не предоставляет качественной исходной информации.

#### 5. Проблемы, требующие дальнейшего решения

В ходе работы идентифицированы три системные проблемы:

1. Ложные срабатывания (false positive). В 4% случаев системы блокируют добросовестные платежи. Это создаёт репутационные риски и судебные иски. Перспективное решение – внедрение алгоритмов объяснимого ИИ (XAI), позволяющих компании понять причину блокировки.

2. Неполный охват новых финансовых инструментов. DeFi-протоколы и P2P-криптообменники остаются «серой зоной». Предлагается законодательно ввести обязательную валидацию транзакций через провайдеров виртуальных активов (VASP) с лицензией ЦБ РФ.

3. Разрыв квалификаций. Требуются специалисты нового профиля — «комплаенс-аналитик с компетенциями в области Data Science». Университетские программы, включая первый курс, должны интегрировать модули по финансовой разведке и транзакционному мониторингу.

#### 6. Практические рекомендации

На макроуровне:

- создать единый открытый реестр «зелёных» контрагентов с API-доступом для бизнеса;
- распространить платформу «Знай своего клиента» на самозанятых и ИП (в пилотном режиме с 2027 г.);
- установить переходный период в 9 месяцев для малого бизнеса по внедрению системы анализа IP-геолокации с компенсацией затрат через налоговый вычет.

На микроуровне:

- внедрить многоуровневую схему контроля: для контрагентов до 1 млн руб;
- базовый KYC, для сделок от 10 млн руб. — расширенный KYC 3-го уровня;
- проводить ежеквартальный стресс-тест систем транзакционного мониторинга на исторических данных (метод backtesting);
- обязательно назначить ответственного за «антисанкционный комплаенс» из числа действующих сотрудников финансового отдела с доплатой не менее 30% к окладу.

Для образовательной сферы:

- рекомендовано изучение открытых курсов «Цифровой финансовый мониторинг» на платформе Университета Росфинмониторинга;
- полезно отслеживать ежеквартальные обзоры «Типологии ПОД/ФТ», публикуемые Евразийской группой по противодействию легализации доходов «ЕАГ»;

#### 7. Прогноз на 2027–2028 гг. и перспективы исследования

Ожидается, что в ближайшие два года произойдёт слияние инструментов финансовой разведки и налогового контроля в единую национальную риск-ориентированную систему (аналог цифрового профиля риска). На микроуровне стандартом станет непрерывный аудит транзакций в режиме 24/7 с автоматической приостановкой подозрительных операций.

Перспективными направлениями дальнейших исследований являются:

- оценка экономической эффективности внедрения ИИ-инструментов финансовой разведки (соотношение затрат и предотвращённого ущерба);
- сравнительный анализ систем внутреннего контроля в организациях с государственным участием и частных компаниях;
- разработка методики адаптации малого и среднего бизнеса к новым требованиям без роста теневого сектора.

Таким образом, финансовая разведка и внутренний контроль в их современном виде представляют собой не отдельные инструменты, а взаимосвязанную систему обеспечения экономической безопасности. На макроуровне она реализуется через AI-платформы государственного мониторинга, на микроуровне – через автоматизированный комплаенс и риск-ориентированные процедуры. Успешность системы определяется двумя факторами: качеством цифрового взаимодействия между уровнями и уровнем подготовки специалистов. Для студента понимание этих процессов является фундаментом для дальнейшей профессиональной деятельности в сфере финансов, аудита или корпоративной безопасности.

### Список литературы

1. Отчет о деятельности Росфинмониторинга за 2025 год. – М., 2026. – 84 с. <https://www.fedsfm.ru/activity/annual-reports>
2. Басов А.В. Цифровая финансовая разведка России: итоги 2025 / А.В. Басов // Деньги и кредит. – 2026. – №2. – С. 34–41.

**Беловицкий Константин Борисович**

кандидат экономических наук, доцент

доцент кафедры экономической экспертизы и финансового мониторинга

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

**Ракчеева Ксения Сергеевна**

студент 1 курса

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

## **Система индикаторов экономической безопасности: адаптация пороговых значений к цифровым и санкционным вызовам**

**Аннотация.** В статье обосновывается необходимость, предлагаются направления и делаются выводы о возможной адаптации пороговых значений индикаторов экономической безопасности к цифровым и санкционным вызовам.

**Ключевые слова:** пороговые значения, цифровизация, санкции, устойчивое развитие, экономическая безопасность.

Экономическая безопасность представляет собой состояние экономики, при котором обеспечивается устойчивость к внутренним и внешним угрозам, защита национальных интересов и возможность устойчивого развития. Одним из ключевых инструментов ее оценки и мониторинга является система индикаторов с пороговыми (критическими) значениями. Превышение или недостижение этих порогов сигнализирует о возникновении угроз, требующих оперативного реагирования [2, 6].

В России основой такого мониторинга служит Стратегия экономической безопасности Российской Федерации на период до 2030 года [1]. Росстат предусматривает около 40 индикаторов экономической безопасности. Однако многие из них не имеют утвержденных пороговых значений или устарели в контексте постпандемийных шоков и санкционного давления с 2022 года. Цифровая трансформация и гибридные угрозы (санкции + киберриски) делают необходимой адаптацию системы: статичные пороги должны стать динамичными, а набор индикаторов – более чувствительным к новым вызовам.

Концепция пороговых значений восходит к работам отечественных ученых [6], где они определяются как предельные величины, нарушение которых приводит к дестабилизации воспроизводственных процессов и формированию кризисных тенденций. Пороги группируются по сферам: производственная, финансовая, социальная, внешнеэкономическая и инновационная (табл. 1).

Пороговые значения часто устанавливаются экспертным путем, на основе сравнения со странами G7, мировыми средними или историческими максимумами. Однако в условиях санкций традиционные сравнения теряют

релевантность, а цифровизация вводит новые измерения рисков, такие как уровень киберугроз или зависимость от иностранных цифровых инфраструктур [2, 6].

Таблица 1

Основные индикаторы экономической безопасности и их пороговые значения

| Индикатор                                                      | Классическое пороговое значение | Примечание                 |
|----------------------------------------------------------------|---------------------------------|----------------------------|
| Темпы роста ВВП                                                | 1,5–4 %<br>(в обычных условиях) | Ниже – стагнация           |
| Доля инвестиций в ВВП                                          | не менее 25 %                   | Инвестиционная активность  |
| Доля обрабатывающей промышленности в промышленном производстве | не менее 70 %                   | По отдельным методикам     |
| Уровень износа основных фондов                                 | критический порог 50–60 %       | Выше – угроза производству |
| Доля импорта в критически важных товарах                       | не более 25 %                   | Угроза зависимости         |

Санкции 2022-2025 годов привели к разрыву традиционных торгово-финансовых связей, ограничению доступа к технологиям и рынкам капитала. Экономика России продемонстрировала высокую адаптивность через параллельный импорт, переориентацию на дружественные рынки и развитие внутреннего производства. Тем не менее, все это потребовало пересмотра индикаторов [3].

Ключевые проблемы традиционных порогов заключаются в следующем.

1. Внешнеэкономическая зависимость. Пороги по доле импорта становятся менее жесткими для “недружественных” стран, но требуют новых индикаторов диверсификации (доля импорта из дружественных государств, уровень параллельного импорта).

2. Финансовая устойчивость. Ограничения на SWIFT и резервы вызвали необходимость в индикаторах, отражающих долю расчетов в национальных валютах, устойчивость к вторичным санкциям и использование альтернативных платежных систем.

3. Технологический суверенитет. Классический показатель расходов на НИОКР (2% ВВП) должен дополняться индикатором доли критически важных

технологий отечественной разработки (цель не менее 70–80% в приоритетных секторах).

Адаптация предполагает введение “санкционно-устойчивых” порогов, учитывающих сценарии давления разной интенсивности (табл. 2).

Таблица 2

“Санкционно-устойчивые” пороги экономической безопасности [4,5].

| Сфера                               | Проблема традиционных порогов                         | Требуемый новый / модифицированный индикатор                            | Пример целевого диапазона           |
|-------------------------------------|-------------------------------------------------------|-------------------------------------------------------------------------|-------------------------------------|
| Внешиэкономическая                  | Жесткие пороги по доле импорта теряют смысл           | Доля импорта из дружественных стран, уровень параллельного импорта      | Не задан (динамичный)               |
| Финансовая                          | Ограничения SWIFT и резервов                          | Доля расчетов в национальных валютах, устойчивость к вторичным санкциям | >80% по нацвалютам (цель)           |
| Технологический суверенитет         | Классические расходы на НИОКР (2% ВВП) – недостаточно | Доля критически важных технологий отечественной разработки              | 70–80% в приоритетных секторах      |
| Цифровая безопасность               | Отсутствовал                                          | Доля защищенных критических инфраструктур, частота успешных атак        | 100% для особо важных объектов      |
| Цифровая суверенность               | Нет                                                   | Доля отечественного ПО и оборудования в госсекторе                      | ≥95% для критической инфраструктуры |
| Зависимость от иностранных платформ | Нет                                                   | Доля трафика через зарубежные сервисы                                   | снижение до <20%                    |
| Развитие цифровой инфраструктуры    | Нет                                                   | Охват 5G/6G, доля отечественных дата-центров                            | >50% по дата-центрам                |
| Риски криптоактивов                 | Нет                                                   | Объем транзакций в обход санкций (доля во внешнеторговом обороте)       | мониторинг, порог – экспертно       |

Цифровизация экономики создает как возможности (рост производительности, новые рынки), так и угрозы (кибератаки, утечки данных,

зависимость от иностранных платформ и алгоритмов). Цифровые активы (криптовалюта, CBDC) используются для обхода санкций, но одновременно повышают риски волатильности и отмывания.

Необходимы новые или модифицированные индикаторы, обусловленные развитием цифровизации. Пороговые значения здесь должны быть динамичными и учитывать технологический прогресс [4,5].

1. Уровень кибербезопасности (доля защищенных критически важных информационных объектов, частота успешных атак).

2. Цифровая суверенность (доля отечественного ПО и оборудования).

3. Зависимость от иностранных цифровых платформ (доля трафика через зарубежные сервисы).

4. Уровень развития национальной цифровой инфраструктуры (охват 5G/6G, доля отечественных дата-центров).

5. Риски криптоактивов (объем транзакций в обход санкций как доля внешнеторгового оборота).

Предложения по адаптации системы предполагают.

1. Переход к многоуровневой и сценарной системе порогов.

Вместо фиксированных значений — диапазоны: “благополучный”, “рисковый”, “критический”, с учетом базового, санкционного и цифрового сценариев (табл. 3).

Таблица 3  
Многоуровневая система порогов [4,5]

| Сценарий    | Характер порога                  | Пример значения (условно)                                      |
|-------------|----------------------------------|----------------------------------------------------------------|
| Базовый     | Фиксированный                    | импорт <25%                                                    |
| Санкционный | Динамический, с учетом замещения | импорт из недружественных стран <10%, из дружественных – любой |
| Цифровой    | Акцент на киберустойчивость      | время восстановления после атаки <4 часов                      |

2. Интеграция новых индикаторов.

К числу таких индикаторов можно отнести:

- индекс технологического суверенитета (доля отечественных компонентов в ключевых отраслях);
- коэффициент санкционной устойчивости (доля внешней торговли с дружественными странами и в национальных валютах);
- индикатор цифровой resilience (время восстановления после киберинцидента);
- уровень импортозамещения в критических товарах и технологиях (табл. 4).

Таблица 4

Уровень импортозамещения в критических товарах и технологиях [4,5]

| Этап             | Мера                                                               | Ответственные                  | Срок      |
|------------------|--------------------------------------------------------------------|--------------------------------|-----------|
| Методологический | Использование машинного обучения для прогноза порогов              | Росстат, ЦБ, Минэкономразвития | 2025–2026 |
| Нормативный      | Закрепление обновленной системы в актах                            | Правительство                  | 2026      |
| Технологический  | Создание межведомственной платформы мониторинга в реальном времени | Минцифры, Минфин               | 2026–2027 |
| Кадровый         | Подготовка кадров с акцентом на цифровые компетенции               | ВУЗы, ИПК                      | постоянно |

3. Методологические улучшения:

- использование машинного обучения для прогнозирования достижения пороговых значений;
- регулярный (ежегодный или ежеквартальный) пересмотр на основе данных Росстата, Банка России и отраслевых министерств;
- внедрение композитных индексов, агрегирующих группы показателей.

4. Институциональные меры включают:

- закрепление обновленной системы в нормативных актах;
- создание межведомственной платформы мониторинга в реальном времени;
- подготовка кадров в области экономической безопасности с акцентом на цифровые компетенции.

Адаптация системы индикаторов экономической безопасности к цифровым и санкционным вызовам — не техническая корректировка, а стратегическая необходимость для обеспечения суверенитета и устойчивого развития. Переход от статичных порогов к динамичной, многофакторной модели позволит своевременно выявлять угрозы и формировать адекватные ответные меры. Реализация предложенных подходов требует консолидации усилий государства, бизнеса и научного сообщества. В конечном итоге, эффективная система индикаторов станет инструментом не только защиты, но и активного позиционирования России в многополярном цифровом мире.

## Список литературы

1. Указ Президента РФ от 13 мая 2017 г. № 208 “О Стратегии экономической безопасности Российской Федерации на период до 2030 года”  
<https://www.garant.ru/products/ipo/prime/doc/71572608/?ysclid=mqal61lmmf39869086>
2. Беловицкий, К. Б. Экономическая безопасность: учебник / К. Б. Беловицкий, М. А. Булатенко, Н. Ф. Кузовлева. — Москва: Дашков и К, 2023. — 586 с. — ISBN 978-5-394-05135-7. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/316007> (дата обращения: 12.06.2026). — Режим доступа: для авториз. пользователей.
3. Криворотов В.В., Калина А.В., Белик И.С. ПОРОГОВЫЕ ЗНАЧЕНИЯ ИНДИКАТИВНЫХ ПОКАЗАТЕЛЕЙ ДЛЯ ДИАГНОСТИКИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ НА СОВРЕМЕННОМ ЭТАПЕ. Вестник УрФУ. Серия экономика и управление. 2019. Том 18. № 6. С. 892–910
4. Митяков, С. Н. Система индикаторов для оценки влияния сферы информационных технологий на экономическую безопасность России / С. Н. Митяков, Е. С. Митяков, П. А. Харитонов // Экономическая безопасность. – 2025. – Т. 8, № 1. – С. 195-212. – DOI 10.18334/ecsec.8.1.122539. – EDN JLVOLW.
5. Луцкан Сергей Петрович Модель оценки экономической безопасности в эпоху цифровой трансформации экономики // Инновационная экономика: информация, аналитика, прогнозы. 2024. №5. URL: <https://cyberleninka.ru/article/n/model-otsenki-ekonomicheskoy-bezopasnosti-v-epohu-tsifrovoy-transformatsii-ekonomiki> (дата обращения: 12.06.2026).
6. Экономическая безопасность России: общий курс: учебник / под ред. В.К. Сенчагова. 3-е изд. перераб. И доп. М.: БИНОМ. Лаборатория знаний, 2014. 815 с.

**Богатырёв Сергей Индрисович**

заведующий кафедрой экономической экспертизы и финансового мониторинга  
ФГБОУ ВО «МИРЭА – Российский технологический университет»  
Россия, г. Москва

**Комзол Анна Артёмовна**

студент 1 курса  
ФГБОУ ВО «МИРЭА – Российский технологический университет»  
Россия, г. Москва

## **Влияние цифровизации на финансовую грамотность потребителей**

**Аннотация.** В статье рассматривается влияние цифровизации на финансовую грамотность потребителей; анализируется динамика финансовой грамотности в условиях цифровизации; выявляются проблемные зоны сервисов рассрочки BNPL; исследуется распространение кибермошенничества; предлагаются системные меры борьбы: стратегии и образовательные инициативы, в т.ч. повышение инвестиционной грамотности и освоение новых компетенций.

**Ключевые слова:** цифровизация, финансовая грамотность, кибермошенничество, образовательные инициативы, экономическая безопасность.

Цифровизация финансов кардинально изменила поведение потребителей: доля безналичных платежей в России превысила 80%, а рынок BNPL-сервисов за год вырос до 940 млрд рублей. Однако развитие технологий опережает формирование у населения необходимых компетенций. Лишь 16,4% россиян обладают продвинутым уровнем цифровой финансовой культуры, тогда как 65,4% находятся лишь на базовом уровне [3].

Цифровая среда порождает новые риски: «эффект абстракции денег» стимулирует импульсивные траты и закредитованность, а кибермошенничество затрагивает каждого третьего гражданина. Запуск в 2026 году цифрового рубля добавляет ещё один вызов. При этом государственная стратегия повышения финансовой грамотности до 2030 года пока демонстрирует низкую вовлечённость взрослого населения (10%) [7,8].

Таким образом, изучение влияния цифровизации на финансовую грамотность – необходимое условие для выработки эффективных мер защиты прав потребителей и обеспечения их безопасного поведения в новой финансовой реальности.

### **1. Динамика финансовой грамотности в условиях цифровизации**

С одной стороны, цифровые сервисы облегчают доступ к финансовым продуктам, способствуют росту культуры сбережений и позволяют большему количеству людей контролировать свои финансы. Согласно данным

Финансового университета при Правительстве РФ, доля граждан с финансовой «подушкой безопасности» выросла с 15% до 40%.

Однако цифровизация создаёт и серьёзные риски. Уровень финансовой грамотности в России. По итогам 2025 года Индекс финансовой грамотности (способность человека к разумному управлению личными финансами) составил 12,61 балла из 21 возможного, что примерно соответствует уровню предыдущих лет [4]. Однако за этим внешним постоянством скрывается тревожная тенденция: финансовая грамотность россиян расслаивается — доля людей как с высоким, так и с низким уровнем растёт, тогда как число граждан со средними показателями сокращается. Увеличивается разрыв между теми, кто успешно адаптируется к цифровым условиям, и теми, кто остаётся уязвимым. Особенно тревожная ситуация среди молодёжи 18–34 лет: 51% молодых людей демонстрируют низкий уровень финансовой грамотности, и только 11% — высокий.

Цифровая финансовая культура. Первое совместное исследование Альфа-банка и агентства ОРО (2025) показало, что 65,4% россиян обладают лишь базовым уровнем цифровой финансовой культуры (ЦФК). Лишь 16,4% — продвинутый уровень, а 18,2% — низкий. При этом самооценка россиян по пятибалльной шкале составила 3,5 балла для финансовой культуры и 3,8 — для цифровой. Полностью уверены в цифровых знаниях 24,6% опрошенных, в финансовых — лишь 14,4%. Это тревожный разрыв между субъективной уверенностью и объективной компетентностью [3].

## **2. Проблемная зона: BNPL-сервисы и «эффект абстракции денег»**

Особую тревогу вызывает стремительное распространение сервисов рассрочки BNPL («покупай сейчас — плати потом»). Рынок BNPL в России за 2025 год достиг 940 млрд рублей, увеличившись примерно в 2,5 раза. При этом 82% россиян уже опробовали такие сервисы, из них 46% используют их как инструмент финансового планирования, а не спонтанных покупок.

Однако есть и обратная сторона. Виртуальные покупки усиливают феномен «финансовой абстракции» — деньги перестают восприниматься как ограниченный ресурс, что стимулирует импульсивное потребление. Цифровая среда активирует когнитивные искажения — виртуальные корзины создают иллюзию обладания ещё до оплаты. Доступность BNPL может усугублять этот эффект, особенно для групп с низкой финансовой грамотностью.

Осознавая риски, Банк России и правительство ввели регулирование BNPL-сервисов. С 1 апреля 2026 года вступил в силу Федеральный закон № 283-ФЗ «О деятельности по предоставлению сервиса рассрочки», который впервые выводит BNPL из серой зоны и встраивает его в общее правовое поле. Ключевые нововведения: операторы BNPL подлежат регистрации в реестре Банка России; обязательства по рассрочке свыше 50 тыс. рублей передаются в бюро кредитных историй; максимальный срок рассрочки ограничен шестью месяцами с

последующим сокращением до четырёх месяцев с 1 апреля 2028 года. Закон также запрещает скрытые комиссии и устанавливает ограничения на неустойку — не более 20% годовых от суммы просроченной задолженности. Однако закон пока не распространяется на схемы прямой рассрочки от продавца, что сохраняет определённые риски [9].

### 3. Цифровое мошенничество: масштабы и портрет жертвы

Одним из самых опасных проявлений роста цифровизации является распространение кибермошенничества.

По данным опроса Банка России, в 2024 году с разными видами кибермошенничества сталкивались 34% граждан, принявших участие в опросе. При этом 9% из тех, кто контактировал со злоумышленниками, лишились денег [5].

Хотя 84,4% респондентов не поддались на уловки, даже те, кто попадаетея, не являются безграмотными или невнимательными людьми. Вопреки стереотипам, жертвами мошенников чаще всего становятся работающие женщины со средним уровнем дохода и средним образованием, проживающие в городе и имеющие постоянную занятость, в возрасте от 25 до 44 лет.

Среди методов преобладает телефонное и СМС-мошенничество, а также мошенничество через мессенджеры. Впервые в топ-5 популярных методов вошло получение доступа к аккаунтам на Госуслугах. Примечательно, что более 70% пострадавших лишились собственных сбережений, а 15% отдали мошенникам кредитные деньги. Пострадавшие стали чаще заявлять о хищениях: 42,8% обращались в свой банк, 30% – в полицию [5].

Таблица 1  
Ущерб от кибермошенничества [5]

| Показатель                                        | Значение       | Период |
|---------------------------------------------------|----------------|--------|
| Общий ущерб от кибермашенников                    | 29.3 млрд.руб  | 2025г. |
| Рост ущерба по сравнению с 2024 годом             | +6.4%          | —      |
| Доля граждан, столкнувшихся с кибермошенничеством | 29%            | 2025г. |
| Средний ущерб на одну жертву                      | 16-22 тыс.руб. | 2025г. |

По действующему с июля 2024 года закону банк обязан возместить клиенту похищенные деньги, если не приостановил на два дня перевод на подозрительный счёт из базы данных Банка России.

### 4. Системные меры: стратегии и образовательные инициативы

С 2024 года в России реализуется «Стратегия повышения финансовой грамотности и формирования финансовой культуры до 2030 года». Её реализацию курируют Минфин России и Банк России, а в марте 2026 года была утверждена актуализированная редакция «дорожной карты» [8].

Основные результаты первого года работы: индекс финансовой грамотности населения вырос с 54 до 55 баллов, охват образовательных

программ в школах увеличился с 38% до 50% [4]. Однако показатель вовлечённости взрослого населения в программы повышения финансовой грамотности остаётся на крайне низком уровне – всего 10%. Бюджетные расходы в 2024 году составили 564 млн рублей, практически без привлечения внебюджетных средств.

**Образование и просвещение.** Важной инициативой стала разработка «Единой рамки компетенций в области финансовой грамотности и финансовой культуры» – систематизированного перечня знаний, умений и установок, которыми должны обладать граждане. Разработаны три учебно-методических комплекта для 5–6, 7 и 8–9 классов. 64% россиян считают, что финансовая и цифровая грамотность должны быть обязательными предметами в школе [7].

**Формирование здоровых финансовых привычек с детства** – залог устойчивости в будущем. В этом контексте примечательно, что уже 15,8 млн детей и подростков (6–17 лет) активно пользуются банковскими картами, а банки создают образовательные экосистемы, превращая приложения в интерактивные платформы с AI-персонажами и системами достижений [6].

## 5. Инвестиционная грамотность и новые компетенции

Отдельного внимания заслуживает инвестиционная грамотность. Доля россиян, высоко оценивающих свой уровень финансовой грамотности, в 2025 году достигла 63%. Растёт и число инвесторов: доля граждан, оценивающих своё благополучие как минимальное, сократилась вдвое — с 17% в 2024 году до 8% в 2025-м (табл.2).

Банк России внедряет новый инструмент оценки – индекс инвестиционной грамотности домохозяйств, который показывает, насколько разумно население инвестирует с учётом рисков и потенциальной доходности. Индекс будет рассчитываться каждые три года. В 2026 году Минфин и Банк России предлагают сосредоточить усилия на противодействии финансовому мошенничеству. Началось обсуждение программ повышения финансовой грамотности на рабочем месте.

Таблица 2  
Показатели инвестиционной грамотности

| Показатель                                                                                  | Значение           |
|---------------------------------------------------------------------------------------------|--------------------|
| Индекс инвестиционной грамотности                                                           | 14,79 из 25 баллов |
| Доля граждан, ошибочно полагающих, что инвестиции застрахованы государством                 | 42%                |
| Доля, неуверенных в этом                                                                    | 23%                |
| Распределение по уровню финансовой грамотности среди инвесторов: средний / высокий / низкий | 66% / 29% / 5%     |

## Заключение и рекомендации

За первым годом реализации Стратегии стоят значимые успехи, но цифровизация ставит новые, более сложные задачи. Можно сформулировать несколько ключевых выводов и рекомендаций.

1. Преодолеть разрыв между самооценкой и реальными знаниями.

Высокая самооценка цифровой грамотности (3,8 балла из 5 при объективном уровне знаний только у 16,4% с продвинутым уровнем) создаёт опасную иллюзию защищённости. Необходимы измеримые критерии оценки и адресные программы для групп с завышенной самооценкой.

2. Интегрировать защиту в дизайн сервисов. BNPL-сервисы должны по умолчанию включать механизмы, снижающие риски перекредитования: предупреждения о долговой нагрузке, периоды охлаждения, обязательное информирование о последствиях просрочек.

3. Сделать финансовое образование непрерывным. Низкая вовлечённость взрослого населения (10%) — системная проблема. Необходимы программы на рабочем месте, интеграция в городские сервисы и социальные сети с использованием геймификации.

4. Усилить кибергигиену как обязательный навык. Учитывая, что 34% граждан сталкивались с кибермошенничеством, а жертвами часто становятся экономически активные люди, программы кибергигиены должны стать обязательным элементом финансового просвещения.

5. Готовить население к цифровому рублю. Запуск цифрового рубля потребует масштабной разъяснительной работы. Необходимо, чтобы граждане понимали не только преимущества, но и риски, связанные с новой формой денег.

Цифровизация финансов — объективная реальность. Её плюсы — доступность, скорость, контроль — огромны. Но для того чтобы они не обернулись финансовыми потерями для миллионов людей, государству, регулятору, бизнесу и образовательному сообществу необходимо действовать сообща, опережая риски и формируя у граждан навыки безопасного поведения в цифровой финансовой среде.

### Список литературы

1. Беловицкий К.Б. Экономическая безопасность организации: монография. - М.: Дашков и К°, 2023. - 182 с.

2. Правонарушения в финансовой сфере» (2021 год): Кузовлева Н. Ф. Правонарушения в финансовой сфере: учебное пособие / Н. Ф. Кузовлева. — Москва: РТУ МИРЭА, 2021. — 117 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: (дата обращения: 08.05.2026). — Режим доступа: для авториз. пользователей.

3. Альфа-банк, агентство ОРО. Исследование цифровой финансовой культуры россиян. — Москва: Альфа-банк, 2025. — 128 с. — Текст: непосредственный.

4. Аналитический центр НАФИ, «Росгосстрах Жизнь». Индекс финансовой грамотности. — Москва: НАФИ, 2025. — 96 с. — Текст: непосредственный.

5. Банк России. Кибермошенничество: портрет пострадавшего. — Москва: Банк России, 2024. — 72 с. — Текст: непосредственный.

6. Банк России. Основные направления развития финансовых технологий на период 2025–2027 годов. — Москва: Банк России, 2025. — 88 с. — Текст: непосредственный.

7. Минфин России. Доклад о реализации Стратегии повышения финансовой грамотности и формирования финансовой культуры до 2030 года за 2024 год. — Москва: Минфин России, 2024. — 112 с. — Текст: непосредственный.

8. Минфин России, Банк России. План мероприятий по реализации Стратегии повышения финансовой грамотности и формирования финансовой культуры до 2030 года: актуализированная редакция от 26.03.2026. — Москва: Минфин России, 2026. — 64 с. — Текст: непосредственный.

9. Российская Федерация. Законы. О деятельности по предоставлению сервиса рассрочки: Федер. закон № 283-ФЗ от 01.04.2026 // Собрание законодательства РФ. — 2026. — № 14. — С. 567–578. — Текст: непосредственный.

**Богатырёв Сергей Индрисович**

заведующий кафедрой экономической экспертизы и финансового мониторинга  
ФГБОУ ВО «МИРЭА – Российский технологический университет»  
Россия, г. Москва

**Лаврушин Арсений Владимирович**

студент 1 курса  
ФГБОУ ВО «МИРЭА – Российский технологический университет»  
Россия, г. Москва

## **Роль России в международном сотрудничестве в сфере регулирования цифровых финансовых рынков**

**Аннотация.** В статье рассматривается роль России в международном сотрудничестве в сфере регулирования цифровых финансовых рынков, определяются основные направления, проблемы и перспективы её участия в этом процессе. Для этого раскрывается содержание ключевых понятий: цифровые финансовые рынки, цифровые финансовые технологии и цифровые финансовые активы. Отмечается роль России в противодействии отмыванию доходов и финансированию терроризма, обеспечении кибербезопасности финансовой системы, контроле криптовалютных операций и стейблкоинов и защите глобальной финансовой стабильности.

**Ключевые слова:** цифровые финансовые рынки, цифровые финансовые активы, цифровые финансовые технологии, криптовалюты, цифровой рубль, международное регулирование, БРИКС, ФАТФ.

Актуальность темы обусловлена стремительным развитием цифровых финансовых технологий и их растущим влиянием на мировую экономику. Появление криптовалют, цифровых валют центральных банков и международных цифровых платёжных систем сделало невозможным регулирование этих рынков силами одного государства — необходимо международное взаимодействие. Для России тема особенно значима: в условиях санкционного давления и активной цифровизации экономики наша страна формирует собственную независимую финансовую инфраструктуру.

Цель исследования – выявить роль России в международном сотрудничестве в сфере регулирования цифровых финансовых рынков, определить основные направления, проблемы и перспективы её участия в этом процессе.

Для достижения цели были поставлены три задачи. Первая – раскрыть содержание ключевых понятий: цифровые финансовые рынки, цифровые финансовые технологии и цифровые финансовые активы. Вторая – рассмотреть

международное сотрудничество в этой сфере. Третья – проанализировать роль России, выявить проблемы и перспективы её участия.

Цифровые финансовые рынки – это система финансовых отношений и инфраструктуры, в которой обращение финансовых инструментов и активов осуществляется на базе цифровых технологий. Рынки – это самая широкая категория, своего рода «площадка», на которой всё происходит.

Цифровые финансовые технологии, или ФинТех – это совокупность технологических решений, которые обеспечивают работу цифровых финансовых рынков: блокчейн, смарт-контракты, искусственный интеллект, API-банкинг и так далее. Технологии – это «как» работает рынок.

Цифровые финансовые активы, сокращённо ЦФА – это объекты обращения на цифровом финансовом рынке: цифровые права, выпускаемые в информационной системе на основе распределённого реестра. Активы — это то, «что» обращается на рынке.

Таким образом, цифровые финансовые рынки – это среда, технологии – это инструмент, а активы – это объект. Каждая из этих категорий требует своего подхода к регулированию.

Рассмотрим первое понятие более подробно. Цифровые финансовые рынки имеют ряд особенностей, которые отличают их от традиционных. Это высокая скорость и круглосуточный режим операций, глобальный трансграничный характер расчётов, использование блокчейна и смарт-контрактов, снижение роли традиционных посредников и, как следствие, необходимость усиленного международного регулирования.

Структурно цифровые финансовые рынки включают четыре основных сегмента: рынок цифровых финансовых активов и криптоактивов, рынок цифровых валют центральных банков и стейблкоинов, цифровые платёжные системы и финтех-сервисы. Все они взаимосвязаны и образуют единое цифровое финансовое пространство.

Цифровые финансовые технологии – это совокупность технологических и программных решений, обеспечивающих создание, обращение и учёт цифровых финансовых активов, а также предоставление финансовых услуг в цифровой среде.

В состав цифровых финансовых технологий входит восемь ключевых категорий: блокчейн и распределённые реестры, смарт-контракты, технологии Big Data и искусственного интеллекта, открытые API и Open Banking, криптография, мобильные платежи, биометрия и кибербезопасность, а также относительно новые направления – RegTech и SupTech, то есть автоматизация комплаенса и надзора.

Важно понимать, что технологии сами по себе не являются предметом финансового регулирования – они регулируются опосредованно, через те операции и активы, которые с их помощью создаются.

Третье понятие – цифровые финансовые активы. В России оно закреплено законодательно. Согласно Федеральному закону от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [1], ЦФА – это цифровые права, которые включают денежные требования, права участия в капитале непубличного акционерного общества, права по эмиссионным ценным бумагам и права требовать передачи эмиссионных ценных бумаг.

Все цифровые активы делятся на две большие группы. Централизованные – те, у которых есть эмитент. К ним относятся цифровые валюты центральных банков, например, цифровой рубль; собственно, ЦФА согласно закону № 259-ФЗ; а также стейблкоины. Децентрализованные – без эмитента. Это классические криптовалюты вроде Bitcoin и Ethereum, токены децентрализованных финансов и невзаимозаменяемые токены – NFT.

Ключевое отличие ЦФА от криптовалют состоит в том, что ЦФА выпускаются в информационной системе, оператор которой включён в реестр Банка России. У каждого актива есть эмитент и юридически закреплённое лицо, отвечающее за обязательства. Криптовалюты, напротив, выпускаются децентрализованно, без эмитента – именно это создаёт основную сложность для регулятора.

В силу трансграничного характера цифровых финансовых рынков их эффективное регулирование возможно только при координации действий национальных регуляторов и международных организаций.

Основных целей такого сотрудничества четыре: противодействие отмыванию доходов и финансированию терроризма; обеспечение кибербезопасности финансовой системы; контроль криптовалютных операций и стейблкоинов; и защита глобальной финансовой стабильности.

В регулировании участвуют четыре ключевые международные организации. Международный валютный фонд [9] разрабатывает стандарты цифровых платежей и методологию по цифровым валютам центральных банков. ФАТФ [8] – межправительственный орган, отвечающий за борьбу с отмыванием доходов. Банк международных расчётов [6] через свой Innovation Hub ведёт исследования по цифровым валютам и токенизации. И «Большая двадцатка», G20, формирует глобальную повестку регулирования криптоактивов. Совместно эти организации разрабатывают единые стандарты регулирования цифровых активов и трансграничных цифровых платежей.

Чтобы наглядно показать масштаб проблемы регулирования, обратимся к динамике мирового рынка криптоактивов (рисунок 1). За восемь лет, с 2018 по 2026 год, общая капитализация выросла с менее чем 0,2 трлн долл. до пика 3,5 трлн долл. в 2025 году. По состоянию на 2026 год она составляет около 2,6 трлн долл.

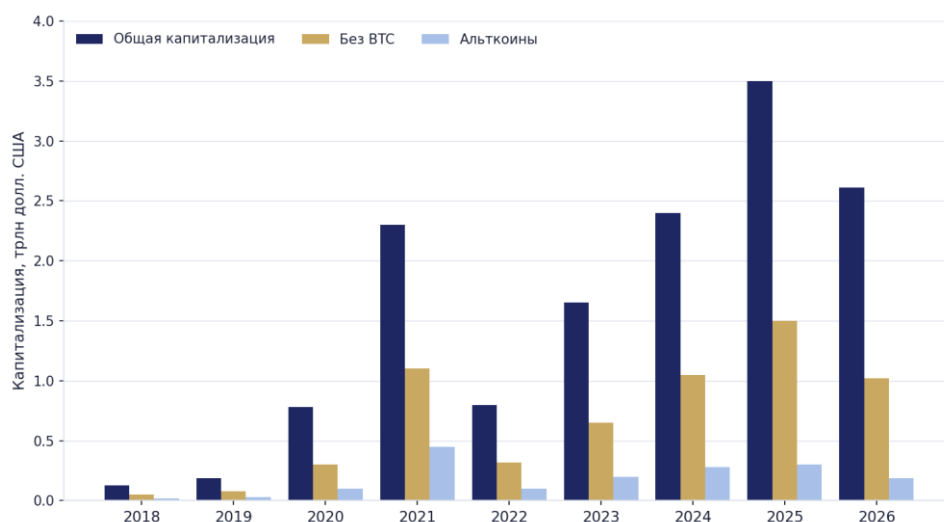


Рисунок 1. Динамика капитализации мирового рынка криптоактивов, 2018–2026 гг. (трлн долл. США)

Источник: составлено автором по данным CoinMarketCap [11]

Анализ динамики позволяет сделать два ключевых вывода. Во-первых, рынок криптоактивов вышел за рамки маргинального явления: его пиковая капитализация (3,5 трлн долл. в 2025 г.) сопоставима с ВВП крупных экономик. Во-вторых, рынок чрезвычайно волатилен: резкие подъёмы 2021 и 2025 годов сменяются столь же резкими спадами (2022, 2026 годы). Доля капитализации без учёта биткоина устойчиво превышает 1 трлн долл. начиная с 2021 года, что говорит о развитии экосистемы альткоинов и стейблкоинов, имеющих самостоятельное регуляторное значение.

Именно такая динамика и делает невозможным регулирование исключительно на национальном уровне. Необходимы согласованные международные стандарты.

Российская Федерация одновременно выстраивает национальную модель регулирования цифровых финансовых рынков и развивает партнёрство в рамках международных интеграционных объединений.

На национальном уровне можно выделить пять основных направлений. Первое – развитие законодательства о ЦФА: базовый Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [1] и поправки 2022–2024 годов. Второе – регулирование криптовалют и легализация майнинга, осуществлённая Федеральным законом от 08.08.2024 № 221-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» в части регулирования майнинга цифровой валюты [2]. Третье – запуск цифрового рубля: пилот Банка России с 2023 года и массовое внедрение с 2025 года [3]. Четвёртое – противодействие отмыванию доходов в цифровой среде: интеграция Росфинмониторинга с реестром операторов ЦФА. Пятое —

развитие трансграничных цифровых платежей: СПФС, СБП-trans и другие альтернативы SWIFT.

На международном уровне Россия активно работает в пяти направлениях: в рамках БРИКС обсуждаются проект единой цифровой платёжной платформы, BRICS Pay и BRICS Bridge [7]; в Евразийском экономическом союзе ведётся гармонизация регулирования ЦФА; в ФАТФ Россия участвует в разработке стандартов для поставщиков услуг виртуальных активов [8]; в ШОС и АСЕАН развиваются расчёты в национальных валютах с использованием цифровых валют центральных банков; кроме того, действуют двусторонние соглашения – в первую очередь пилоты по интероперабельности цифрового рубля с Китаем и Беларусью.

В качестве эмпирического подтверждения активности России в цифровой финансовой сфере приведу данные по российскому финтех-рынку за 2025 год. Рынок развивается мультисегментно: ядро составляют платёжные сервисы – это 23 процента, разработчики и платформы – 18 процентов, а также финансовые маркетплейсы и B2B-сервисы. По данным аналитического агентства Smart Ranking [12], сегмент платёжных сервисов в первых трёх кварталах 2025 года вырос на 29 процентов. Это формирует основу для дальнейшего развития цифровых финансовых рынков в России и усиливает её переговорную позицию на международной арене.

Регулирование цифровых финансовых рынков может осуществляться различными методами и в различных формах.

По характеру воздействия методы делятся на прямые (административные) и косвенные (экономические). Прямые методы предполагают непосредственное установление правил поведения участников рынка: лицензирование операторов информационных систем ЦФА, регистрация в реестре Банка России, обязательная идентификация клиентов (KYC/AML), запреты и ограничения на отдельные операции с криптовалютами, требования к раскрытию информации. Косвенные методы воздействуют на поведение участников через экономические стимулы: налогообложение операций с цифровыми активами, дифференцированные требования к капиталу и резервированию, тарифная политика операторов, льготы и преференции для эмитентов ЦФА.

По юридической природе различают законодательные (правовые) и экономические формы регулирования. Законодательные формы – это нормативные правовые акты, устанавливающие правила обращения цифровых активов: федеральные законы, постановления Правительства, нормативные акты Банка России и Росфинмониторинга. Экономические формы – это инструменты денежно-кредитной, бюджетной и налоговой политики, применяемые к цифровой финансовой сфере: ставка по цифровому рублю, налоговый режим для операций с ЦФА, поддержка экспорта финтех-решений.

Применительно к России наиболее перспективным представляется комбинированный подход, сочетающий все четыре указанные группы методов: прямое регулирование обеспечивает правовую определённость, а косвенные и экономические инструменты – гибкость и инвестиционную привлекательность цифрового финансового рынка.

По результатам анализа можно выделить как ключевые перспективы, так и серьёзные проблемы.

Среди перспектив: массовое внедрение цифрового рубля, что повысит прозрачность и скорость расчётов; создание альтернативных международных платёжных систем, снижающих зависимость от долларовой инфраструктуры; усиление сотрудничества со странами Азии и БРИКС, формирующее многополярную финансовую архитектуру; рост рынка ЦФА как нового инструмента привлечения капитала; и развитие RegTech и SupTech – автоматизированных систем надзора и комплаенса.

Среди ключевых проблем: санкционные ограничения, затрудняющие интеграцию в глобальные финансовые системы; существенные различия в национальном законодательстве разных стран, мешающие гармонизации регуляторных подходов; растущие риски кибербезопасности; слабый международный контроль над децентрализованными криптовалютами; и пока недостаточная интеграция российских платформ в международные стандарты.

Россия играет активную и многоплановую роль в международном сотрудничестве по регулированию цифровых финансовых рынков. Несмотря на санкционные ограничения, наша страна не только развивает собственную нормативную базу и инфраструктуру цифровых финансов, но и формирует альтернативные международные форматы сотрудничества, прежде всего, в рамках БРИКС, ЕАЭС, ШОС. Именно такая двухуровневая стратегия – национальная и международная – представляется наиболее перспективной в условиях современной фрагментации мировой финансовой системы.

### Список литературы

1. Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (с изм. и доп.). — URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_358753/](http://www.consultant.ru/document/cons_doc_LAW_358753/) (дата обращения: 29.05.2026).

2. Федеральный закон от 08.08.2024 № 221-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» (в части регулирования майнинга цифровой валюты). — URL: <http://publication.pravo.gov.ru/document/0001202408080043> (дата обращения: 29.05.2026).

3. Положение Банка России от 03.08.2023 № 820-П «О платформе цифрового рубля». — URL: <https://www.cbr.ru/StaticHtml/File/41186/820-P.pdf> (дата обращения: 29.05.2026).

4. Банк России. Развитие финансовых технологий: официальный сайт Центрального банка Российской Федерации. — URL: <https://www.cbr.ru/fintech/dr/> (дата обращения: 29.05.2026).

5. Банк России. Электронная библиотека: каталог изданий. — URL: <https://library.cbr.ru/catalog/lib/books/963535/> (дата обращения: 29.05.2026).

6. Bank for International Settlements. BIS Innovation Hub: research projects on CBDC and tokenisation. — URL: <https://www.bis.org/about/bisih/> (дата обращения: 29.05.2026).

7. BRICS Information Portal. — URL: <https://infobrics.org> (дата обращения: 29.05.2026).

8. Financial Action Task Force (FATF). Consolidated FATF Standards on Information Sharing. — URL: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Consolidated-fatf-standard-information-sharing.html> (дата обращения: 29.05.2026).

9. International Monetary Fund. Digital Payments and Finance. — URL: <https://www.imf.org/en/topics/digital-payments-and-finance> (дата обращения: 29.05.2026).

10. World Economic Forum. Centre for the Fourth Industrial Revolution. — URL: <https://www.weforum.org/> (дата обращения: 29.05.2026).

11. CoinMarketCap. Global Cryptocurrency Charts: Total Cryptocurrency Market Cap. — URL: <https://coinmarketcap.com/charts/> (дата обращения: 29.05.2026).

12. Smart Ranking. Аналитика российского финтех-рынка: итоги I–III кварталов 2025 г. — URL: <https://smartranking.ru/> (дата обращения: 29.05.2026).

**Богатырёв Сергей Индрисович**

заведующий кафедрой экономической экспертизы и финансового мониторинга  
ФГБОУ ВО «МИРЭА – Российский технологический университет»  
Россия, г. Москва

**Моделикова Дарья Михайловна**

**Бакшенова Мария Дмитриевна**

студенты 1 курса  
ФГБОУ ВО «МИРЭА – Российский технологический университет»  
Россия, г. Москва

## **Инновации как ключевой фактор технологического развития**

**Аннотация.** В статье рассматриваются подходы к понятию «Инновации», делается вывод: инновации выступают главным двигателем технологического развития. Анализируются ключевые проблемы и предлагаются пути и решения. Рассматривается влияние инновационных проектов на инновационное развитие страны. Определяются ключевые причины и системные вызовы инновационного развития в России. Проводится оценка динамики затрат на инновационную деятельность и динамики показателей инновационной деятельности предприятий за 2021-2025 гг. Делается вывод о необходимости корректировки государственной политики в инновационной сфере.

**Ключевые слова:** инновации, технологическое развитие, системные вызовы, инновационные проекты, государственной политики.

В современную эпоху, отмеченную геополитической нестабильностью и цифровой трансформацией, технологическое развитие стало ключевым полем глобальной конкуренции. Скорость технологических изменений беспрецедентна, а инновации превратились в важный ресурс экономического суверенитета, национальной безопасности и социального благополучия. Мировые лидеры, такие как США, Китай и страны ЕС (Европейского союза), формируют комплексные национальные стратегии, направленные на захват технологического лидерства.

Для России, чья экономика исторически зависит от сырьевого экспорта, переход на инновационную модель развития является императивным условием для преодоления структурных ограничений, обеспечения устойчивого роста и выполнения стратегических задач в условиях новых вызовов. Пандемия COVID-19 и санкционное давление наглядно продемонстрировали уязвимость экономик, не обладающих собственными передовыми технологиями, и обострили необходимость в ускоренном технологическом развитии и достижении технологического суверенитета.

Понятие «инновация» (от лат. innovatio – обновление, изменение) в современной экономической науке выходит за рамки простого новшества или изобретения. Основоположник теории Йозеф Шумпетер трактовал инновацию как коммерциализированное новшество, обладающее качественной новизной и приводящее к изменению структуры экономики. Ключевой аспект – успешное внедрение на рынок, приносящее практическую и экономическую пользу.

Ряд авторов (Т. А. Аверина, С. А. Баркалов, И. С. Суровцев, И. Ф. Набиуллин) в своей работе «Инновационный менеджмент» делают своеобразный экскурс в историю и приводят ряд определений инновации (табл. 1.1) [15].

Таблица 1  
Подходы к понятию «Инновации»

| Автор, название                                                                                       | Издание                             | Понятие «Инновации»                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Й. Шумпетер.<br>Теория<br>экономического<br>развития                                                  | М. Прогресс,<br>1982                | Изменения с целью внедрения и использования новых видов потребительских товаров, новых производственных и транспортных средств, рынков и форм организации в промышленности [9]                                                                                                                                                                         |
| Хауштайн,<br>Хартманн.<br>Leitung<br>industrieller<br>Forschung und<br>Entwick-lund                   | Берлин, 1979                        | Внедрение в практику, осуществление и использование идеи, предложения, научно-исследовательского решения, модели                                                                                                                                                                                                                                       |
| В. Н. Лапин.<br>Социальные<br>аспекты<br>управления<br>нововведениями                                 | Таллинн,<br>1981                    | Комплексный процесс создания, распространения и использования нового практического средства для лучшего удовлетворения известной потребности людей                                                                                                                                                                                                     |
| В. Л. Макаров.<br>Внедрение<br>нетехнических<br>нововведений                                          | Новосибирск:<br>Наука, 1983,<br>№10 | Есть форма разрешения противоречия, явление прогресса в любой сфере человеческой деятельности, а не только в технике и технологии [11]                                                                                                                                                                                                                 |
| Ф. Валента.<br>Управление<br>инновациями                                                              | М.: Прогресс,<br>1985               | Изменение в первоначальной структуре производственного механизма, т.е. переход его внутренней структуры к новому состоянию: касается продукции, технологии, средств производства, профессиональной и квалификационной структуры рабочей силы, организации; изменения как с положительными, так и отрицательными социально-экономическими последствиями |
| Л. В. Канторович,<br>Системный анализ<br>и некоторые<br>проблемы научно-<br>технического<br>прогресса | М.: Наука,<br>1986                  | Научные открытия или изобретения, имеющие практическое применение и удовлетворяющие социальным, экономическим и политическим требованиям, дающие эффект в соответствующих областях                                                                                                                                                                     |

Согласно Федеральному закону от 23.08.1996 № 127-ФЗ «О науке и государственной научно-технической политике», инновация – это «внедренный новый или значительно улучшенный продукт (товар, услуга) или процесс, новый метод продаж или новый организационный метод в деловой практике, организации рабочих мест или во внешних связях». Это определение гармонизировано с международными стандартами (Руководство Осло ОЭСР) [1].

Технологическое развитие – это процесс качественного совершенствования технологий, средств и методов производства, приводящий к росту производительности труда, повышению эффективности использования ресурсов и созданию новых возможностей для удовлетворения общественных потребностей [4]. Оно носит нелинейный, часто революционный характер, что отражено в теории технологических укладов.

Взаимосвязь этих понятий носит диалектический характер. Инновации выступают главным двигателем технологического развития.

Каждый технологический прорыв, от парового двигателя до искусственного интеллекта, был следствием цепочки взаимосвязанных инноваций. В свою очередь, достигнутый уровень технологического развития создает платформу для генерации следующих поколений инноваций, формируя самоподдерживающийся цикл прогресса.

Правовая база инновационной деятельности в России носит многоуровневый характер. Ее фундаментом являются:

Конституция Российской Федерации (ст. 44 гарантирует свободу научного творчества) [2].

Гражданский кодекс РФ (часть четвертая), регулирующий права на результаты интеллектуальной деятельности [3].

Федеральный закон от 23.08.1996 (Редакция от 24.06.2025) № 127-ФЗ «О науке и государственной научно-технической политике» (определяет основные понятия и меры господдержки).

Федеральный закон от 02.08.2009 № 217-ФЗ (создает правовые условия для создания малых инновационных предприятий при вузах и научных учреждениях) [4].

Ключевые причины существующих проблем в инновационной сфере, согласно анализу, включают:

- монополизацию экономики крупными компаниями, что снижает восприимчивость предприятий к инновациям;
- иррациональную финансовую систему, обслуживающую преимущественно краткосрочный спекулятивный капитал и блокирующую привлечение инвестиций;
- негативный инвестиционный климат и отсутствие спроса у бизнеса на результаты НИОКР;

- отсутствие адекватной государственной научно-технической и промышленной политики в прошлые периоды;
- отсутствие разнообразных форм и механизмов интеграции науки и производства, а также коммерциализации инноваций.

В свою очередь, основными направлениями преодоления этих проблем должны стать:

- создание системы государственной поддержки отечественных предприятий, обеспечивающей их технологический прорыв в новых отраслях;
- формирование эффективной системы коммуникаций в области науки, технологий и инноваций на основе развития сетевых форм организации деятельности;
- государственная поддержка фундаментальной науки;
- разработка широкого спектра гибких форм финансирования и стимулирования инноваций;
- внедрение разнообразных форм частно-государственного партнерства при финансировании НИОКР.

Стратегическое направление задают ключевые программные документы. Указ Президента РФ от 28.02.2024 N 145 "О Стратегии научно-технологического развития Российской Федерации". Это основной документ, определяющий приоритеты и цели. Он фокусируется на «больших вызовах» и необходимости концентрации ресурсов на прорывных направлениях, обеспечивающих национальную безопасность [6].

По указу Президента РФ №309 от 07.05.2024, с 2025 года реализуются 19 национальных проектов, среди которых несколько напрямую связаны с технологическим развитием [7]:

**«Новые материалы и химия».** Направлено на снижение доли импорта химической и биотехнологической продукции, создание производств редких и редкоземельных металлов;

**«Технологическое обеспечение продовольственной безопасности».** Предполагает увеличение выпуска отечественной техники для сельского хозяйства, разработки в области селекции и генетики;

**«Беспилотные авиационные системы».** Развитие разработок и серийное производство БПЛА и комплектующих;

**«Средства производства и автоматизации».** Повышение независимости в области выпуска высокотехнологичных станков;

**«Экономика данных и цифровая трансформация государства».** Совершенствование системы госуслуг и цифровых платформ в ключевых секторах.

Ключевые причины существующих проблем в инновационной сфере: монополизация экономики крупными компаниями; иррациональная финансовая система, обслуживающая краткосрочный спекулятивный капитал; негативный

инвестиционный климат и отсутствие спроса на НИОКР; отсутствие адекватной научно-технической и промышленной политики; отсутствие разнообразных форм интеграции науки и производства. Основные направления преодоления: создание системы господдержки технологического прорыва; формирование эффективной системы коммуникаций в науке и инновациях; поддержка фундаментальной науки; разработка гибких форм финансирования; внедрение частно-государственного партнёрства в финансировании НИОКР.

Особую роль играют институты развития, созданные для финансирования и поддержки инноваций на разных стадиях: Фонд содействия инновациям, (программы «Старт», «УМНИК»), Группа ВЭБ.РФ (финансирование крупных инфраструктурных проектов), АО «РВК» (развитие венчурного рынка) и Сколково (создание экосистемы для стартапов). Правовой статус этих институтов закреплён отдельными федеральными законами, например, Федеральным законом от 28.09.2010 (Редакция от 30.11.2024) № 244-ФЗ «Об инновационном центре «Сколково» [5].

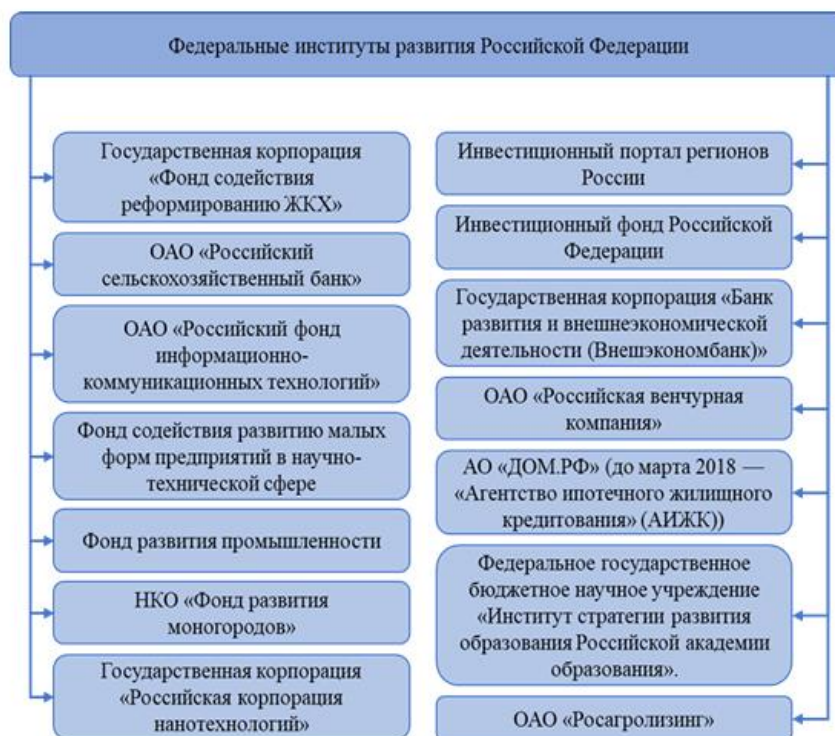


Рисунок 1. Федеральные институты развития Российской Федерации

Национальные проекты России являются целенаправленными драйверами инновационного развития, формируя комплексную стратегию технологического прорыва. Каждый проект концентрируется на ключевом направлении, создавая не только прямые результаты, но и мультипликативный эффект для всей экономики.

Проект **«Новые материалы и химия»** закладывает основу для прорыва в высокотехнологичных отраслях, таких как авиация, космос и медицина.

Параллельно **«Технологическое обеспечение продовольственной безопасности»** трансформирует агропромышленный комплекс через биотехнологии и цифровые решения, обеспечивая устойчивость и технологический суверенитет в производстве продуктов питания.

Развитие **«Беспилотных авиационных систем»** создаёт не просто новую отрасль, а стимулирует смежные области - от искусственного интеллекта до композитных материалов, повышая эффективность в логистике, сельском хозяйстве и мониторинге.

Проект **«Средства производства и автоматизация»** модернизирует промышленный базис страны, делая его более производительным и конкурентоспособным за счёт роботизации и современного оборудования.

Связующей основой выступает **«Экономика данных и цифровая трансформация государства»**, которая создаёт инфраструктуру для работы с большими данными и искусственным интеллектом, ускоряя внедрение инноваций во всех сферах и повышая качество государственного управления. Вместе эти проекты формируют экосистему, в которой инновации становятся системным фактором роста, обеспечивая долгосрочную конкурентоспособность и технологическую независимость России.

Влияние инновационных проектов на инновационное развитие представлено в табл.2.

Таблица 2

Влияние инновационных проектов на инновационное развитие [14]

| Национальный проект                                          | Основной инновационный фокус                                                           | Влияние на инновационное развитие                                                                                 |
|--------------------------------------------------------------|----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| «Новые материалы и химия»                                    | Передовые материалы (композиты, наноматериалы) и химические технологии.                | Развитие высокотехнологичных отраслей, снижение импортозависимости, рост конкурентоспособности.                   |
| «Технологическое обеспечение продовольственной безопасности» | Биотехнологии, умное сельское хозяйство, цифровизация АПК.                             | Повышение производительности АПК, технологический суверенитет в продовольствии.                                   |
| «Беспилотные авиационные системы»                            | Разработка и производство БПЛА, технологии автономного управления.                     | Создание новой отрасли, развитие смежных технологий (ИИ, сенсоры), эффективность в логистике и мониторинге.       |
| «Средства производства и автоматизация»                      | Промышленное оборудование, станки, роботизированные комплексы и системы автоматизации. | Модернизация промышленности, рост производительности, стимулирование спроса на инженерные кадры.                  |
| «Экономика данных и цифровая трансформация государства»      | Инфраструктура для работы с большими данными, ИИ, цифровые госуслуги.                  | Формирование экономики, основанной на данных, повышение эффективности госуправления, среда для цифровых стартапов |

Влияние инноваций на технологическое развитие в рамках сложившейся в России системы осуществляется через несколько ключевых механизмов [8,10]:

1. Повышение производительности и конкурентоспособности. Процессные инновации, стимулируемые нацпроектами (например, «Производительность труда»), напрямую снижают издержки и повышают эффективность российских предприятий. Это является основой для импортозамещения и роста несырьевого экспорта.

2. Создание новых высокотехнологичных рынков. Продуктовые инновации, особенно в сфере сквозных цифровых технологий (нацпроект «Цифровая экономика»), порождают новые отрасли, такие как отечественная робототехника, биотехнологии и фармацевтика.

3. Развитие человеческого капитала. Нацпроект «Наука и университеты» и государственная программа «Научно-технологическое развитие» направлены на подготовку нового поколения ученых, инженеров и технологических предпринимателей, что является долгосрочным инвестированием в основной ресурс инноваций – знания.

4. Формирование инновационной экосистемы. Через институты развития, технопарки и поддержку стартапов создается среда, в которой идеи могут быть доведены до коммерческого продукта. Яркий пример – льготный режим для резидентов Инновационного центра «Сколково» и Территорий опережающего развития (ТОР).

Среди ключевых причин, сдерживающих технологическое развитие, выделяются:

- низкая рентабельность производства в сочетании с высокими ставками по кредитным ресурсам;
- отсутствие механизмов интеграции науки и производства и внедрения инноваций в производство, что сказывается на неэффективности деятельности предприятий;
- невосприимчивость предприятий к инновациям, обусловленная монополизацией отдельных сфер промышленности;
- низкий уровень руководства и топ-менеджеров предприятий, препятствующий внедрению прогрессивных бизнес-моделей развития на основе постоянной разработки и внедрения инноваций в производственный процесс [11].

Однако системные вызовы остаются.

1. Разрыв между наукой и бизнесом: несмотря на меры поддержки, коммерциализация результатов научных исследований остается слабым звеном. Кооперация, особенно между крупными корпорациями и малыми инновационными предприятиями, развита недостаточно.

2. Дефицит кадров: сохраняется нехватка высококвалифицированных инженеров, специалистов в области цифровых технологий и управленцев, способных вести инновационные проекты.

3. Сложность доступа к финансированию: для малого и среднего инновационного бизнеса сохраняются барьеры в получении «длинных» и доступных кредитов на НИОКР, особенно на ранних, наиболее рискованных стадиях [11].

Таблица 3

Системные вызовы инновационного развития в России [11]

| Системный вызов                | Суть проблемы                                                                                                     | Направления решений                                                                                                            |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Сырьевая модель экономики      | Доминирование ТЭК подавляет стимулы для развития высокотехнологичных секторов и инноваций.                        | Диверсификация экономики через целевое инвестирование нефтегазовых доходов в НИОКР и инфраструктуру будущего.                  |
| Разрыв «наука-бизнес»          | Слабый трансфер технологий. Низкий спрос бизнеса на исследования, низкая коммерциализация разработок.             | Создание инфраструктуры трансфера (технопарки, инжиниринговые центры). Налоговые льготы для корпоративных R&D.                 |
| Дефицит «длинных» денег        | Неразвитость венчурного финансирования. Высокие риски и неготовность частного капитала инвестировать в инновации. | Развитие венчурного рынка (фонды фондов, налоговые стимулы). ГЧП для софинансирования высокорисковых проектов                  |
| Кадровый голод и «утечка умов» | Нехватка специалистов нового типа и отток лучших кадров за рубеж.                                                 | Реформа образования (акцент на STEM и гибкие навыки). Создание привлекательных условий для работы ученых и инженеров в России. |

Объем инвестиций российского крупного и среднего бизнеса в инновации в 2023 году достигли 3,5 трлн рублей, что на 23% больше, чем в 2022 году, и в 1,2 раза – чем было в 2019-м (в постоянных ценах). Таковы данные исследования, проведенного Институтом статистических исследований и экономики знаний НИУ ВШЭ [13].

Лидером по затратам стала сфера услуг (1,8 трлн рублей) из-за ухода зарубежных компаний, ускорившим развитие отечественных технологий. Наибольший рост показали рекламная деятельность (рост более чем в 7,2 раза, до 13 млрд рублей), IT (в 4,8 раза, до 78,8 млрд) и разработчики компьютерного ПО (в 3,2 раза, до 291,4 млрд) [13].

Но по абсолютным показателям впереди научные исследования и разработки (771 млрд рублей, с ростом на 15,7%), а также транспортировка и хранение (405 млрд, рост почти на 105%).

Затраты промышленности на разработку и внедрение инноваций превысили 1,56 трлн рублей, в том числе только по обрабатывающим производствам – 1,27 трлн. Интересно, что положительную динамику показали главным образом «среднетехнологичные сектора», а также производство компьютеров, электронных и оптических изделий, напитков, табачных изделий

и кожи, «которые переориентировали свою деятельность в соответствии с возросшим потребительским спросом» (отметили в ИСИЭЗ НИУ ВШЭ). Отрицательные темпы прироста расходов на инновации были зафиксированы в автопроме, металлургии, нефтепереработке, выпуске лекарств и бумажных изделий. Основные направления инвестиций: научные исследования и разработки (771 млрд рублей) и транспортировка/хранение (405 млрд рублей). В промышленности затраты превысили 1,56 трлн рублей, с положительной динамикой в среднетехнологичных секторах. Основным источником финансирования – собственные средства компаний (57,4%), значительна доля бюджетных субсидий (28,5%) [13].

В последние годы в России наблюдается устойчивый рост затрат на инновационную деятельность. Основными драйверами стали цифровизация экономики, импортозамещение, развитие отечественного программного обеспечения и усиление конкуренции за потребительский спрос. По данным Росстата и аналитических материалов НИУ ВШЭ, особенно заметно выросли расходы на разработку новых методов ведения бизнеса, программные решения, маркетинг и дизайн.

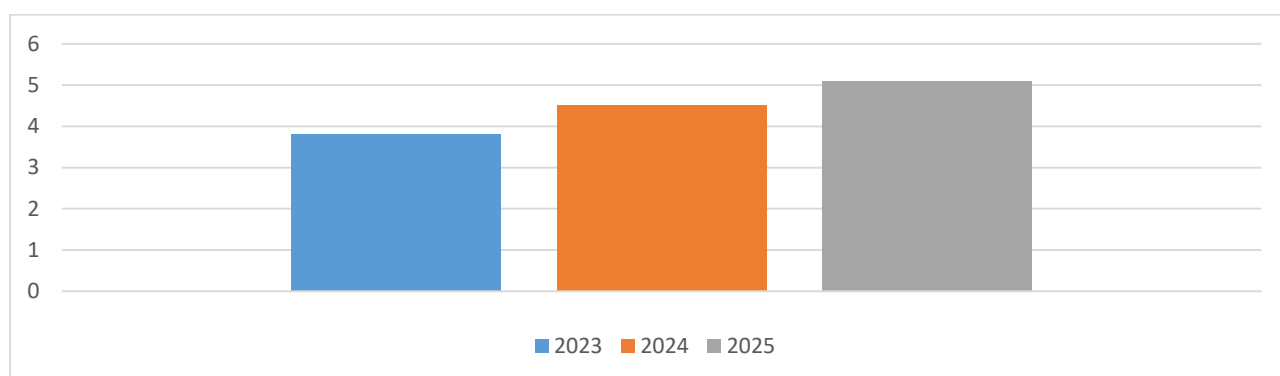


Рисунок 1. Динамика затрат на инновационную деятельность 2023-2025 гг. [13]

По итогам 2024–2025 годов в России продолжился рост расходов на инновационную деятельность. Наиболее высокими темпами увеличивались вложения в цифровые технологии, разработку и внедрение программного обеспечения, новые методы управления бизнесом, а также маркетинг и создание брендов. Это связано с необходимостью адаптации компаний к изменяющимся экономическим условиям, ростом внутреннего спроса и ускорением процессов технологической независимости. Кроме того, предприятия активнее инвестируют в автоматизацию и развитие собственных ИТ-решений, что становится одним из ключевых факторов повышения конкурентоспособности российской экономики.

Данные табл. 4 демонстрируют устойчивый рост всех ключевых показателей инновационной деятельности предприятий в России за период с

2021 по 2025 год. Это говорит о том, что инновации становятся всё более значимым фактором развития как для крупных, так и для малых организаций.

Таблица 4

Динамика показателей инновационной деятельности предприятий  
в РФ (2021–2025 гг.) [13]

| Год                                                                                                                    | 2021 | 2022 | 2023 | 2024 | 2025 |
|------------------------------------------------------------------------------------------------------------------------|------|------|------|------|------|
| Уровень инновационной активности, %                                                                                    | 10,1 | 10,3 | 10,5 | 10,7 | 10,9 |
| Удельный вес организаций, осуществляющих технологические инновации, %                                                  | 9,2  | 9,4  | 9,6  | 9,8  | 10,0 |
| Удельный вес инновационных товаров, работ, услуг в общем объёме отгруженных товаров, работ, услуг, %                   | 7,8  | 8,0  | 8,2  | 8,4  | 8,6  |
| Удельный вес затрат на технологические инновации в общем объёме отгруженных товаров, работ, услуг, %                   | 2,2  | 2,3  | 2,4  | 2,5  | 2,6  |
| Удельный вес малых предприятий, осуществлявших технологические инновации, %                                            | 5,0  | 5,2  | 5,4  | 5,6  | 5,8  |
| Удельный вес инновационных товаров, работ, услуг в общем объёме отгруженных товаров, работ, услуг малых предприятий, % | 5,5  | 5,7  | 5,9  | 6,1  | 6,3  |

Таким образом, инновация – это не просто новшество, а коммерциализированное изменение, приводящее к практическому результату. Технологическое развитие – это процесс совершенствования технологий, движимый инновациями. Их взаимосвязь циклична: инновации двигают технологии, а достигнутый технологический уровень создает основу для новых инноваций.

В Российской Федерации создана разветвленная нормативно-правовая база и система государственного регулирования инновационной деятельности. Ключевыми элементами являются Стратегия НТР, государственная программа «Научно-технологическое развитие РФ» и ряд федеральных законов, регулирующих права на интеллектуальную собственность и деятельность институтов развития. Национальные проекты, прежде всего «Наука и университеты» и «Цифровая экономика», выступают основными практическими инструментами государственной инновационной политики. Они создают целевое финансирование, формируют инфраструктуру (НОЦ, мегасайенс) и стимулируют спрос на технологии со стороны государства и ключевых отраслей, являясь системным драйвером технологического развития.

Инновации влияют на технологическое развитие через повышение производительности, создание новых рынков и развитие человеческого капитала. Однако национальная инновационная система России продолжает сталкиваться с серьезными системными вызовами: низкая рентабельность производства и высокие кредитные ставки, монополизация отраслей, невосприимчивость бизнеса к инновациям, отсутствие эффективной интеграции

науки и производства, негативный инвестиционный климат и дефицит долгосрочного финансирования. Преодоление этих барьеров требует дальнейшей корректировки государственной политики в соответствии с основными направлениями: создание системы господдержки технологического прорыва, развитие сетевых форм коммуникаций в науке и инновациях, поддержка фундаментальной науки, внедрение гибких форм финансирования и частно-государственного партнерства.

Инновации действительно являются ключевым фактором технологического развития России. Государство осознает эту роль и создает комплексную систему ее поддержки через стратегическое планирование, нормативное регулирование и реализацию масштабных национальных проектов. Дальнейший успех будет зависеть от способности преодолеть системные разрывы, усилить кооперацию между наукой, государством и бизнесом и создать гибкую, адаптивную среду для генерации и внедрения прорывных технологий.

### Список литературы

1. Федеральный закон "О науке и государственной научно-технической политике" от 23.08.1996 N 127-ФЗ (редакция от 31.07.2025)  
<https://normativ.kontur.ru/document?moduleId=1&documentId=504647&ysclid=mq18oeu9ggq813625221>
2. Конституция Российской Федерации (редакция от 14.03.2020)  
<https://normativ.kontur.ru/document?moduleId=1&documentId=357694&ysclid=mq18qozooi614272483>
3. Гражданский кодекс Российской Федерации (редакция от 23.07.2025)  
<https://normativ.kontur.ru/document?moduleId=1&documentId=503517&ysclid=mq18sud6vv564611943>
4. Федеральный закон "О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам создания бюджетными научными и образовательными учреждениями хозяйственных обществ в целях практического применения (внедрения) результатов интеллектуальной деятельности" от 02.08.2009 N 217-ФЗ (редакция от 29.12.2012)  
<https://normativ.kontur.ru/document?moduleId=1&documentId=217747&ysclid=mq18umh679169458204>
5. Федеральный закон "О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации" от 29.12.2006 N 244-ФЗ (редакция от 02.05.2026)  
<https://normativ.kontur.ru/document?moduleId=1&documentId=505951&ysclid=mq18xc7a60139035861>

6. Указ Президента РФ от 28.02.2024 N 145 "О Стратегии научно-технологического развития Российской Федерации"  
<https://www.garant.ru/products/ipo/prime/doc/408518353/?ysclid=mq19007q9k513794520>

7. Указ Президента РФ от 07.05.2024 N 309 "О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года" (Редакция от 07.05.2024)  
<https://normativ.kontur.ru/document?moduleId=1&documentId=470566&ysclid=mq1912t9ep865314021>

8. Иванова Н.И. Национальные инновационные системы в условиях глобальных вызовов // Мировая экономика и международные отношения.–2022.  
<http://opac.hse.ru/absopac/index.php?url=/notices/index/IdNotice:32230/Source:default&ysclid=mhss3hhas1234133411>

9. Шумпетер Й.А. Теория экономического развития. – М.: Прогресс, 1982.  
<https://djvu.online/file/JajYWySAMOxto?ysclid=mhss4jkkqa623885913>

10. Голиченко О.Г. Национальная инновационная система России: состояние и пути развития. – М.: Наука, 2021. – 387 с.  
<https://www.vopreco.ru/jour/article/view/1632?ysclid=mhss60iogi684534828>

11. Макаров В.Л., Баклицкая М.В. Технологическое развитие и экономический рост: новые вызовы // Экономика и математические методы. – 2020. – Т. 56.–№4.–С.5-18.  
<https://urss.ru/cgi-bin/db.pl?lang=Ru&blang=ru&page=Book&id=19755&ysclid=mhss71bd7j33649>

12. Государственная программа Российской Федерации «Научно-технологическое развитие Российской Федерации» (утв. постановлением Правительства РФ от 29 марта 2019 г. № 377).  
[https://www.consultant.ru/document/cons\\_doc\\_LAW\\_322380/](https://www.consultant.ru/document/cons_doc_LAW_322380/)

13. Аналитический отчет «Итоги реализации нацпроекта "Наука и университеты" в 2023 году». – М.: Минобрнауки России, 2024.  
<https://gradmsk.ru/video/1789f96faa57679552dae7f9027af8e1/?ysclid=mhss94zmpl869998524>

14. Паспорт национального проекта «Производительность труда».  
[https://www.economy.gov.ru/material/directions/np\\_proizvoditelnost\\_truda/?ysclid=mhssbya3wy545775138](https://www.economy.gov.ru/material/directions/np_proizvoditelnost_truda/?ysclid=mhssbya3wy545775138)

**Бондарчук Наталья Витальевна**  
доктор экономических наук, профессор  
профессор кафедры финансового учета и контроля  
ФГБОУ ВО «МИРЭА – Российский технологический университет»  
Россия, г. Москва

**Назаренко Полина Алексеевна**  
студент 5 курса  
ФГБОУ ВО «МИРЭА – Российский технологический университет»  
Россия, г. Москва

## **Аудит как инструмент выявления и профилактики искажений в финансовой отчетности**

**Аннотация.** В статье рассматривается роль аудита как ключевого инструмента обеспечения достоверности финансовой отчетности. Проанализированы сущность и задачи аудита в контексте выявления фальсификаций, нормативные требования международных стандартов аудита. Описаны методы и инструменты выявления искажения, включая анализ бухгалтерских аномалий, вертикальный и горизонтальный анализ, использование специализированного программного обеспечения модели Бениша.

**Ключевые слова:** аудит, финансовая отчетность, фальсификация отчетности, искажения в отчетности, внутренний контроль, профессиональный скептицизм, бухгалтерские аномалии, модель Бениша, аудиторские процедуры, недобросовестные действия, мошенничество.

Под аудитом понимается независимая проверка финансовой отчетности компании, с целью выражения мнения о достоверности финансовой отчетности [1].

Финансовая отчетность при проведении аудиторской проверки играет ключевую роль и является ключевым источником информации для бушующих инвесторов, кредиторов, партнеров, государственных органов.

Финансовая отчетность представляет собой сведения о финансовом положении компании минимум за 2 года с пояснениями.

В МСА 200 определение финансовой отчетности звучит следующим образом «финансовая отчетность-это структурированное представление финансовой информации прошедших периодов, включая соответствующие примечания, предназначенное для информирования об экономических ресурсах и обязательствах организации на определенный момент или изменения в них за период в соответствии с концепцией подготовки финансовой отчетности» [2].

Однако, случается так, что достоверность финансовой отчетности может быть поставлена под сомнение из-за преднамеренных искажений, которые могут

быть связаны с мошенническими действиями.

Согласно МСА 200 искажение - расхождение между включенной в отчетность суммой, классификацией, представлением или раскрытием информации в финансовой отчетности и суммой, классификацией, представлением или раскрытием информации, которые требуются в соответствии с применимой концепцией подготовки финансовой отчетности. Искажения могут быть следствием недобросовестных действий или ошибок [2].

То есть, под искажениями можно понимать ошибки, случайные или же целенаправленно, которые в конечном итоге окажут существенное или несущественное влияние на финансовую отчетность компании.

В таком случае роль аудита играет важную роль при выявлении и обеспечении прозрачности, а также повышении надежности к финансовым отчетам компании.

Аудит фальсификации финансовой отчетности направлен на выявление и предотвращение умышленных искажений финансовой отчетности, связанных с объектами бухгалтерского учета.

Одной из задач аудита является выявление поддельных учетных записей, документов, регистров и иных первичных документов.

Так же немало важным является обнаружение специального применения неверных принципов ведения бухгалтерского учета.

Помимо вышеперечисленных задач, так же стоит отметить, что аудитор должен перед проверкой произвести оценку рисков существенных искажений, которые будут связаны с фальсификацией данных.

Международный стандарт аудита (МСА) 240 «Обязанности аудитора в отношении недобросовестных действий при проведении аудита финансовой отчетности» устанавливает, что аудитор должен:

- выявлять и оценивать риски существенного искажения вследствие недобросовестных действий на уровне финансовой отчетности и на уровне предпосылок в отношении видов операций, остатков по счетам и раскрытия информации;
- оценивать, может ли выбор и применение организацией той или иной учетной политики служить признаком недобросовестного составления финансовой отчетности;
- разрабатывать и выполнять дополнительные аудиторские процедуры, характер, сроки и объем которых разработаны с учетом оценённых рисков;
- проверять надлежащий характер бухгалтерских записей в основном регистре и прочих корректировок, сделанных при подготовке финансовой отчетности;
- анализировать оценочные значения на предмет предвзятости и оценивать, не свидетельствуют ли о риске существенного искажения вследствие

недобросовестных действий обстоятельства, породившие предвзятость;

- сообщать лицам, отвечающим за корпоративное управление, обо всех фактах, имеющих отношение к недобросовестным действиям, которые, по мнению аудитора, входят в сферу их компетенции;
- определять, существует ли обязанность сообщать о выявленных или подозреваемых недобросовестных действиях лицам за пределами организации [3].

Если аудитором входе проверки были выявлены мошеннические действия, присутствует искажение данных по сравнению с предыдущим периодом, он обязан сначала сообщить руководству о выявленных подозрительных действиях, которые прямо влияют на финансовую отчетность проверяемой компании [8].

Так же немало важным является понимать разницу между ошибкой и недобросовестными действиями. Именно недобросовестные действия предполагают умышленные искажения, которые могут быть в большинстве случаев направлены на получение незаконных преимуществ.

Существует так же такое понятие как бухгалтерские аномалии. Бухгалтерские аномалии- это отклонение в учетных данных, которые могут свидетельствовать о нарушениях в деятельности компании, например, о мошеннических действиях [4].

Такие аномалии могут быть связаны непосредственно с корпоративным управлением. Под корпоративным управлением можно понимать систему взаимодействий между руководителем организации, Советом директоров или акционерами, которые как раз и определяют цели, задачи и планы компании, а также пути контроля за деятельностью компании и ее сотрудников.

Таким образом, именно через бухгалтерские аномалии совершаются нарушения в деятельности компании, которые в свою очередь могут быть связаны с мошенническими действиями, которые требуют контроля со стороны заинтересованных сторон.

Например, формальные отклонения в первичных документах или их полное отсутствие, незаполнение или пропуск обязательных реквизитов, так же отсутствие соответствия данных в экземплярах одного и того же документа.

Помимо этого, могут быть несостыковки в регистрах бухгалтерского учета, то есть ошибки, дублирование номенклатуры, или номенклатура может прерываться.

Необычные проводки, которые в конечном итоге будут существенно влиять на финансовый результат и активы компании, также могут свидетельствовать об ошибках. Так же может быть, что операции вводятся задним числом систематически, например, под конец отчетного периода [4].

Для обнаружения фальсификации аудиторы используют разные методы или же их комплекс:

- анализ финансовых аномалий, например, резкое увеличение дебиторской

задолженности или же стабильный доход при снижении выручки или же большая прибыль при нехватке собственных средств;

- инвентаризация, которая позволяет установить фактическое наличие у компании на складе продукции с данными учета, на дату проведения инвентаризации;

- вертикальный анализ помогает увидеть значительные изменения в каждой статье. Горизонтальный анализ, они позволяют выявить коэффициент роста и прироста относительно предыдущего периода [5];

- использование программных продуктов, которые используются при выявлении искажений в финансовой отчетности. Например, AuditXPPProfessional, ThetaRay, AppZen, Контур. Экстерн - это программы, которые позволяют автоматизировать проверку счетов, проверку операций на правильность корреспонденции, помимо этого формируют генеральную совокупность и делают выборку, выявляют подозрительные операции [6].

Помимо выше перечисленных методов так же используют модель Бениша. Это математическая модель, которая помогает определить манипулирует ли компания своей прибылью и финансовой отдельностью [5].

Аудит, как инструмент выявления искажений финансовой отчетности имеет следующие особенности.

Профилактическая роль аудита, то есть аудит не только выявляет, но и предотвращает фальсификацию.

Проводить оценку службы внутреннего контроля. Эффективная служба внутреннего контроля (СВК) - подразделение в компании, которое занимается контролем за правомерным, целевым и эффективным использованием материалов и финансовых ресурсов, предупреждением, выявлением и пресечением нарушений законодательства и локальных актов [7]. Аудиторы проверяют ее функциональность и дают рекомендации по ее улучшению.

Так же, не мало важным является профессиональный скептицизм. В соответствии с МСА 200, аудитор должен сохранять скептицизм на всех этапах проверки, не принимая на веру предоставленные документы без дополнительной проверки.

Взаимодействие с внешними аудиторами. Частая ротация аудиторов может снижать риски сокрытия нарушений, так как свежий взгляд повышает вероятность нахождения искажений.

Под ротацией понимается смена аудиторской организации в соответствии с принципами законности и целесообразности, общепринятыми стандартами и внутренними документами компании [9].

Несмотря на всю эффективность проведения аудиторской проверки и выявления искажений, аудит имеет ограничения:

- субъективность оценки данных;
- возможность намеренного сокрытия информации руководством

компании;

- недостаточная разработанность методик для оценки нефинансовых показателей.

Аудит является важным инструментом при выявления искажений в финансовых отчетах компании и намеренной ее фальсификации. При проведении аудита используют не только нормативную базу и современные технологии, но и профессиональные навыки, особенно профессиональный скептицизм который помогает трезво смотреть на всю картину в отчетности компании. Однако, его эффективность зависит от качества внутреннего контроля, прозрачности бизнес-процессов и готовности компании к сотрудничеству с аудиторами и готовности здраво оценивать комментарии и рекомендации при проверке. Таким образом, в условиях постоянно изменяющихся современных реалий, увеличивается риск мошеннических махинаций. В этих условиях роль аудита, а также усложнение ведения и проверки финансовых операций будет все большее возрастать.

### Список литературы

1. Федеральный закон от 30.12.2008 N 307-ФЗ (ред. от 26.12.2024) «Об аудиторской деятельности»  
[https://www.consultant.ru/document/cons\\_doc\\_LAW\\_83311/5662200f71fec9b8ab1a6e0615896613d3852b5a/](https://www.consultant.ru/document/cons_doc_LAW_83311/5662200f71fec9b8ab1a6e0615896613d3852b5a/) ( дата обращения 08.11.2025).

2. Международный стандарт аудита 200 «Основные цели независимого аудитора и проведение аудита в соответствии с международными стандартами аудита» (введен в действие на территории Российской Федерации Приказом Минфина России от 09.01.2019 N 2н) (ред. от 16.10.2023)  
[https://www.consultant.ru/document/cons\\_doc\\_LAW\\_317258/8b01883380fec344f044c706161a816e9c86186e/](https://www.consultant.ru/document/cons_doc_LAW_317258/8b01883380fec344f044c706161a816e9c86186e/) (дата обращения 08.11.2025).

3. Международный стандарт аудита 240. «Обязанности аудитора в отношении недобросовестных действий при проведении аудита финансовой отчетности» (введен в действие на территории Российской Федерации Приказом Минфина России от 09.01.2019 N 2н)  
[https://www.consultant.ru/document/cons\\_doc\\_LAW\\_317404/](https://www.consultant.ru/document/cons_doc_LAW_317404/) ( дата обращения 08.11.2025)

4. Обнаружение мошенничества:выявляем информационные шумы и «технические» аномалии в учете данных // Финансовые расследования и судебные экспертизы URL: <https://fi.center/blog/article/104/Obnaruzenie-mosennicestva-vyavlaem-informacionnye-sumy-i-tehnicaskie-anomalii-v-~> (Дата обращения 11.11.2025)

5. ОЦЕНКА ДОСТОВЕРНОСТИ ОТЧЕТНОСТИ ПРИ ПРОВЕДЕНИИ ВНЕШНЕГО АУДИТА // URL: <https://elib.utmn.ru/jspui/bitstream/ru->

[tsu/6952/1/CifEkon2020\\_386\\_391.pdf](https://tsu/6952/1/CifEkon2020_386_391.pdf) (дата обращения: 12.11.2025).

6. Нейросеть для бухгалтеров: автоматизация учета и анализ финансовых данных // ruGPT URL: [https://sroaas.ru/pc/novosti/organizaciya\\_i\\_osuwestvlenie\\_ekonomicheskim\\_sub\\_ektom\\_vnutrennego\\_kontrolya\\_overshaemyh\\_faktov\\_hozy/](https://sroaas.ru/pc/novosti/organizaciya_i_osuwestvlenie_ekonomicheskim_sub_ektom_vnutrennego_kontrolya_overshaemyh_faktov_hozy/) (дата обращения: 10.11.2025).

7. Организация и осуществление экономическим субъектом внутреннего контроля совершаемых фактов хозяйственной жизни, ведения бухгалтерского учета и составления бухгалтерской (финансовой) отчетности // Саморегулируемая Организация Аудиторов Ассоциация «Содружество» URL: [https://sroaas.ru/pc/novosti/organizaciya\\_i\\_osuwestvlenie\\_ekonomicheskim\\_sub\\_ektom\\_vnutrennego\\_kontrolya\\_overshaemyh\\_faktov\\_hozy/](https://sroaas.ru/pc/novosti/organizaciya_i_osuwestvlenie_ekonomicheskim_sub_ektom_vnutrennego_kontrolya_overshaemyh_faktov_hozy/) (дата обращения: 10.11.2025)

8. За что отвечает аудитор ? // Бухгалтерия.ру URL: <https://www.buhgalteria.ru/article/za-chto-otvechaet-auditor> (дата обращения: 10.11.2025)

9. Что происходит при смене аудиторской фирмы? // URL: <https://tenchat.ru/media/2765055-chto-proiskhodit-pri-smene-auditorskoy-firmy> (дата обращения: 11.11.2025)

**Генина Кира Анатольевна**

студент 1 курса

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

Научный руководитель

**Беловицкий Константин Борисович**

кандидат экономических наук, доцент

доцент кафедры экономической экспертизы и финансового мониторинга

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

## **Развитие финансового контроля в условиях цифровизации государственного сектора экономики**

**Аннотация.** В представленных тезисах рассматриваются вопросы цифровизации финансового контроля, риски государственного финансового контроля, меры по их предотвращению. Сделаны выводы о целесообразности и необходимости внедрения современных информационных технологий в целях создания единой цифровой платформы и автоматизированного обмена данными между всеми органами контроля.

**Ключевые слова:** цифровизация, государственный сектор, финансовый контроль, риски.

В условиях постоянного роста объемов государственных финансовых потоков, усложнения бюджетных процессов и усиления требований к прозрачности расходования бюджетных средств, традиционные методы государственного финансового контроля (ГФК) становятся неэффективными.

Актуальность цифровизации обусловлена острой потребностью государства в переходе от постфактум-проверок к непрерывному, превентивному контролю. Внедрение современных информационных технологий позволяет значительно повысить оперативность, снизить человеческий фактор, минимизировать коррупционные риски и обеспечить максимальную целесообразность использования государственных ресурсов в интересах национальной экономики и общества.

**Государственный финансовый контроль (ГФК)** – это инструмент финансовой политики, главной задачей которого, является обеспечение должной системы надзора за соблюдением бюджетного законодательства Российской Федерации.

**Субъектом внешнего ГФК** на федеральном уровне является Счётная палата Российской Федерации, а **субъектом внутреннего ГФК** в нашей стране является Федеральное казначейство.

**Органы внешнего ГФК**, в отличие от органов внутреннего ГФК, находятся вне структуры исполнительной власти и не связаны с контролируемыми исполнительными органами, то есть являются независимым, что чётко определено в нормативном законодательстве.

**Главная задача** контролирующих органов заключается в содействии исполнению политики государства в области финансов путем обеспечения соблюдения законодательства и недопущения нецелевого использования бюджетных и внебюджетных средств. Контроль проводится через многогранную деятельность финансовых органов.

**Риски государственного финансового контроля:**

- необоснованное завышение цен при государственных закупках;
- непрозрачность расчетов на уровнях корпорации между исполнителями государственных контрактов;
- расхождение в учетных данных по государственному имуществу;
- недостоверность данных по государственному имуществу;
- несоответствие результатов исполнения государственных контрактов целям предоставления средств из бюджета;
- значительный объем незавершенного строительства на федеральном и региональном уровнях.

**Меры по предотвращению рисков:**

- разработка и принятие единого Классификатора финансовых нарушений для органов внешнего и внутреннего государственного (муниципального) финансового контроля;
- согласование планов контрольных мероприятий между органами внутреннего и внешнего государственного финансового контроля с целью исключения дублирования и параллелизма;
- оптимизация структуры региональных органов государственного финансового контроля;
- организация обмена информацией о результатах контрольных мероприятий на всех уровнях;
- развитие системы профилактики нарушений в финансово-бюджетной сфере.

Экономический эффект – финансовое измерение результатов выполнения объектами аудита требований представлений, реализации соответствующими органами власти предложений (рекомендаций), содержащихся в информационных письмах, а также результатов рассмотрения обращений Счетной палаты, направленных в правоохранительные органы.

## Экономический эффект и возвраты

### Экономический эффект –

финансовое измерение результатов выполнения объектами аудита требований представлений, реализации соответствующими органами власти предложений (рекомендаций), содержащихся в информационных письмах, а также результатов рассмотрения обращений Счетной палаты, направленных в правоохранительные органы

35,6 %  
иное



148,9  
млрд рублей

64,4 %  
возвраты  
в бюджеты  
всех  
уровней

95,9 млрд рублей

рекорд за всю  
30-летнюю историю  
Счетной палаты

88,2 млрд рублей



Рисунок 1. Экономический эффект и возвраты денежных средств в результате осуществления Счетной палатой контрольных мероприятий за 2017-2024 г.г.

### Выводы

1. Внедрение современных информационных технологий критически важно для минимизации коррупционных рисков и человеческого фактора. Это обеспечивает более высокую прозрачность и максимальную целесообразность использования государственных ресурсов, что отвечает интересам национальной экономики.

2. В Российской Федерации ГФК разделён на внешний (Счетная палата, независимая от исполнительной власти) и внутренний (Федеральное казначейство). Эффективная цифровизация должна обеспечить интеграцию и обмен информацией между этими субъектами для исключения дублирования контрольных мероприятий и повышения общей эффективности надзора.

3. Основные риски в бюджетной сфере (необоснованное завышение цен, непрозрачность расчетов, недостоверность учетных данных, значительный объем незавершенного строительства) могут быть эффективно предотвращены только через автоматизированные системы контроля. Цифровые платформы позволяют выявлять аномалии и несоответствия в режиме реального времени.

4. Предлагаемые меры по повышению эффективности ГФК, такие как разработка единого Классификатора финансовых нарушений, согласование планов контрольных мероприятий и развитие системы профилактики, могут

быть реализованы только при наличии единой цифровой платформы и автоматизированного обмена данными между всеми органами контроля.

### Список литературы

1. Отчет Счетной палаты Российской Федерации о результатах проверки исполнения Федерального закона «О федеральном бюджете на 2024 год и на плановый период 2025 и 2026 годов» и бюджетной отчетности об исполнении федерального бюджета за 2024 год в Федеральном казначействе (Руководитель Федерального казначейства Р.Е. Артюхин). Утвержден Коллегией Счетной палаты Российской Федерации 30 апреля 2025 года. URL:[https://ach.gov.ru/upload/iblock/34f/4ofrijxyloxr6ngna0g6az1h53oqtrvu/GRBS\\_Kaznacheystvo.pdf](https://ach.gov.ru/upload/iblock/34f/4ofrijxyloxr6ngna0g6az1h53oqtrvu/GRBS_Kaznacheystvo.pdf)
2. Отчет о работе Счетной палаты Российской Федерации в 2024 году. URL:<https://ach.gov.ru/upload/iblock/d34/r9je39e5z05455o9ksar608z6j12jwad.pdf>
3. Государственный финансовый контроль и аудит – анализ эффективности и векторы развития. URL:[https://www.vedomosti.ru/press\\_releases/2025/08/25/gosudarstvennii-finansovii-kontrol-i-audit--analiz-effektivnosti-i-vektori-razvitiya](https://www.vedomosti.ru/press_releases/2025/08/25/gosudarstvennii-finansovii-kontrol-i-audit--analiz-effektivnosti-i-vektori-razvitiya)
4. Е. А. Болотнова, А. А. Храмченко, А. В. Анопкин, К. Р. Никитина ЦИФРОВИЗАЦИЯ ГОСУДАРСТВЕННОГО ФИНАНСОВОГО КОНТРОЛЯ В РФ // Вестник Академии знаний. 2021. №4 (45). URL: <https://cyberleninka.ru/article/n/tsifrovizatsiya-gosudarstvennogo-finansovogo-kontrolya-v-rf> (дата обращения: 26.11.2025).
5. Государственный финансовый контроль в условиях цифровой экономики: тенденции, проблемы и пути решения. URL: <https://apni.ru/article/10736-gosudarstvennyj-finansovyy-kontrol-v-usloviyah-cifrovoj-ekonomiki-tendencii-problemy-i-puti-resheniya>

**Дзюба Артем Юрьевич**  
**Каримов Александр Владиславович**  
студенты 5 курса  
ФГБОУ ВО «МИРЭА – Российский технологический университет»  
Россия, г. Москва

Научный руководитель  
**Кузовлева Нина Фёдоровна**  
кандидат экономических наук  
профессор кафедры экономической экспертизы и финансового мониторинга  
ФГБОУ ВО «МИРЭА – Российский технологический университет»  
Россия, г. Москва

## **Роль выездных проверок в системе налогового контроля Российской Федерации**

**Аннотация.** В статье рассматривается место выездных проверок в системе налогового контроля РФ, анализируются их виды, этапы проведения и эффективность. Особое внимание уделяется роли выездных проверок в выявлении крупных схем уклонения от налогообложения, а также их влиянию на налоговую дисциплину и бюджетные поступления.

**Ключевые слова:** налоговый контроль, выездная налоговая проверка, камеральная проверка, налоговые правонарушения, уклонение от уплаты налогов, ФНС России, налоговый мониторинг.

Налоговый контроль в Российской Федерации представляет собой систему мер государственного регулирования, направленных на обеспечение полноты и своевременности уплаты налогов и сборов. Среди форм налогового контроля выделяют камеральные проверки, выездные проверки, налоговый мониторинг и иные мероприятия. Ключевое место в этой системе занимает выездная налоговая проверка, которая проводится непосредственно на территории налогоплательщика и позволяет наиболее глубоко изучить его финансово-хозяйственную деятельность.

Выездная налоговая проверка определяется как форма налогового контроля, осуществляемая уполномоченными должностными лицами налоговых органов по месту нахождения (жительства) налогоплательщика и направленная на проверку правильности исчисления, полноты и своевременности уплаты налогов за определённый период.

Роль выездных проверок в системе налогового контроля определяется несколькими ключевыми функциями.

1. Контрольная функция заключается в непосредственной проверке полноты уплаты налогов.

2. Фискальная функция обеспечивает дополнительные поступления в бюджет за счёт доначисленных недоимок, пеней и штрафов.

3. Превентивная функция сдерживает налогоплательщиков от совершения нарушений налогового законодательства.

4. Аналитическая функция позволяет выявлять новые схемы ухода от налогообложения и отраслевые риски.

5. Правовосстановительная функция направлена на принудительное взыскание выявленных недоимок.

Эффективность выездных проверок неоднородна и зависит от того, насколько глубоко удаётся проникнуть в финансовые потоки проверяемого лица. В лучшем случае проверка приводит к доначислению крупных сумм налогов и выявлению сложных схем уклонения, материалы передаются в правоохранительные органы, а сам факт такой проверки создаёт мощный сдерживающий эффект для других налогоплательщиков.

Однако возможен и более скромный результат, когда обнаруживаются лишь отдельные ошибки в исчислении налоговой базы или неполная уплата по отдельным налогам, и налогоплательщик добровольно устраняет эти недостатки. Худший вариант развития событий с точки зрения государства - это формально проведённая проверка, не выявившая существенных нарушений; в таком случае бюджет недополучает причитающиеся суммы, а превентивный эффект практически отсутствует.

Камеральная проверка, проводимая в налоговой инспекции без выезда к налогоплательщику, эффективна для выявления арифметических и логических ошибок в отчётности, но она почти бессильна против умышленных схем сокрытия доходов. Выездная же проверка позволяет инспекторам физически осмотреть склады, сличить документы с реальным движением товаров, опросить сотрудников и контрагентов.

Именно поэтому выездная налоговая проверка остаётся незаменимым инструментом для выявления таких явлений, как «фирмы-однодневки», «обналичка» через подконтрольные организации, занижение выручки путём ведения «чёрной бухгалтерии» и другие схемы, которые невозможно обнаружить дистанционно.

Выездные налоговые проверки классифицируются по нескольким основаниям.

1. По объёму проверяемых налогов они делятся на комплексные, охватывающие все налоги и сборы, уплачиваемые налогоплательщиком, и тематические, которые проводятся по одному конкретному налогу.

2. По периоду проведения различают первичные проверки и повторные, которые могут проводиться вышестоящим налоговым органом в порядке контроля за деятельностью нижестоящего налогового органа либо в случае реорганизации или ликвидации налогоплательщика.

3. По инициативе выделяют плановые выездные проверки, включённые в ежегодный план ФНС, и внеплановые, которые назначаются, например, при реорганизации или ликвидации организации.

Кроме того, существуют совместные выездные проверки, проводимые налоговыми органами совместно с органами внутренних дел.

Влияние выездных проверок на налоговую безопасность государства проявляется в нескольких ключевых аспектах.

В сфере бюджетных доходов выездные проверки обеспечивают прямое доначисление недоимок, пеней и штрафов, что ежегодно приносит в консолидированный бюджет Российской Федерации десятки миллиардов рублей. В отношении налоговой дисциплины регулярное проведение выездных проверок у крупных налогоплательщиков способствует снижению количества грубых нарушений налогового законодательства.

В сфере противодействия теневому сектору экономики выездные проверки позволяют выявлять фирмы-однодневки и цепочки транзитных платежей. Что касается инвестиционной среды, здесь влияние двойственное: с одной стороны, добросовестные компании получают защиту от недобросовестной конкуренции, с другой стороны, само проведение проверки создаёт определённую административную нагрузку.

В судебной практике решения, принятые по итогам выездных проверок, формируют единообразные подходы к оспариванию актов налоговых органов.

Для наглядности основные сферы и характер влияния выездных налоговых проверок представлены в таблице 1.

Таблица 1

Влияние выездных налоговых проверок на налоговую безопасность

| Сфера влияния            | Характер влияния                                                                                            |
|--------------------------|-------------------------------------------------------------------------------------------------------------|
| Бюджетные доходы         | Прямое доначисление недоимок, пеней, штрафов (миллиарды рублей ежегодно)                                    |
| Налоговая дисциплина     | Снижение количества грубых нарушений у крупных налогоплательщиков                                           |
| Теневой сектор экономики | Выявление фирм-однодневок, цепочек транзитных платежей                                                      |
| Инвестиционная среда     | Защита добросовестных компаний от недобросовестной конкуренции, но при сохранении административной нагрузки |
| Судебная практика        | Формирование единообразных подходов к оспариванию решений налоговых органов                                 |

Выездные проверки обладают и рядом недостатков. Прежде всего, это высокая трудоёмкость: одна проверка может длиться до шести месяцев, а в исключительных случаях - до девяти месяцев. Кроме того, выездная проверка создаёт значительную административную нагрузку даже на добросовестный бизнес, отвлекая ресурсы на подготовку документов и взаимодействие с

инспекторами. Нельзя исключать и риск субъективизма со стороны проверяющих инспекторов, что иногда приводит к судебным спорам.

Для повышения роли выездных проверок в системе налогового контроля и снижение их недостатков предлагается несколько направлений совершенствования. Необходима дальнейшая цифровизация, включающая использование Единого реестра проверок и автоматизированный отбор объектов проверки на основе риск-ориентированного подхода.

1. Следует снижать число малозначительных проверок в пользу глубоких расследований по группам высокого налогового риска.

2. Требуется повышение квалификации инспекторов, особенно в сфере трансфертного ценообразования, международного налогообложения и противодействия агрессивным схемам оптимизации.

3. Целесообразно внедрение постпроверочного анализа, то есть оценки исполнения принятых решений и предотвращения повторных нарушений.

4. Необходимо сокращение сроков проведения проверок за счёт параллельных процедур и активного использования электронного документооборота.

Таким образом, выездная налоговая проверка продолжает играть центральную роль в системе налогового контроля Российской Федерации. Несмотря на рост значения камеральных проверок и налогового мониторинга, именно выездная налоговая проверка остаётся наиболее действенным инструментом выявления крупных налоговых правонарушений, восстановления бюджетных прав государства и формирования общей налоговой культуры. Дальнейшее развитие этого института должно идти по пути интеллектуализации, селективности и снижения нагрузки на добросовестных налогоплательщиков.

### Список литературы

1. Налоговый кодекс Российской Федерации от 31.07.1998 № 146-ФЗ [Электронный ресурс] [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_19671/](https://www.consultant.ru/document/cons_doc_LAW_19671/)
2. Официальный сайт Налоговой службы РФ [Электронный ресурс] - <https://www.nalog.gov.ru/rN77/>
3. Гончаренко Л.И., Вишневская О.В. «Налоговый контроль: современные вызовы и лучшие практики»

**Кузовлева Нина Фёдоровна**

кандидат экономических наук

профессор кафедры экономической экспертизы и финансового мониторинга

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

**Сазонов Кондрат Дмитриевич**

студент 1 курса

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

## **Влияние цифровизации на обеспечение конкурентоспособности промышленных предприятий в условиях современной геополитической среды**

**Аннотация.** В статье исследуется влияние цифровизации на обеспечение конкурентоспособности промышленных предприятий в условиях современной геополитической среды: анализируется роль цифровых технологий в адаптации предприятий к вызовам, связанным с санкционным давлением и проведением специальной военной операции (СВО), оценивается их вклад в формирование экономической модели страны, выявляются ключевые цифровые технологии – цифровые двойники, искусственный интеллект, роботизация, способствующие повышению операционной эффективности и конкурентоспособности. Формулируются практические рекомендации по развитию цифровой инфраструктуры, поддержке импортозамещения и формированию кадрового потенциала в условиях геополитической нестабильности.

**Ключевые слова:** цифровизация, цифровые технологии, конкурентоспособность, промышленные предприятия, кадровый потенциал.

Современные геополитические вызовы, включая санкционное давление и проведение специальной военной операции (СВО), существенно трансформируют условия функционирования промышленных предприятий России. В этих условиях цифровизация выступает ключевым фактором обеспечения их конкурентоспособности и устойчивости.

Цифровизация – многоаспектный процесс распространения цифровых технологий во всех сферах жизни. В промышленности она подразумевает внедрение информационных и коммуникационных технологий в производственные и бизнес-процессы, переход на цифровые форматы хранения и обработки данных, автоматизацию операций, создание единой информационной среды для обмена данными. Это повышает эффективность, снижает издержки и ускоряет принятие решений.

Цифровые технологии играют центральную роль в трансформации промышленности и экономики в рамках четвёртой промышленной революции.

Эти технологии взаимосвязаны и дополняют друг друга, обеспечивая повышение эффективности, снижение издержек и создание новых возможностей для бизнеса и общества. К ключевым цифровым технологиям относятся.

Промышленный интернет вещей (IIoT) – система взаимосвязанных сенсоров, приборов и датчиков, объединённых проводными и беспроводными каналами и подключённых к глобальной сети Интернет.

Цифровые двойники – цифровые копии физических объектов или процессов, используемые для моделирования, анализа и прогнозирования их поведения.

Искусственный интеллект (ИИ) – программные системы и алгоритмы, способные решать определённые задачи аналогично тому, как это делает человек.

Роботизация – внедрение роботизированных систем для выполнения задач, ранее выполняемых человеком.

Большие данные (Big Data) – это массивы данных, которые из-за своего объёма и сложности обработки требуют специальных подходов и инструментов.

Машинное обучение – подраздел искусственного интеллекта, который занимается разработкой алгоритмов, способных обучаться на данных и делать предсказания или принимать решения без явного программирования.

Для подготовки предприятия к трансформации руководителям необходимо определить, на каком из этапов находятся предприятия, насколько развиты и автоматизированы бизнес-процессы, насколько внедрено использование информационных технологий, готова ли компания к преобразованиям, а также созданию новых продуктов/внедрения инновационных продуктов. Ключевые этапы цифровой трансформации предприятия [1]:

1. Автоматизация.

- Перевод аналоговых процессов в автоматизированный формат.
- Ускорение процессов при сохранении их структуры.

2. Цифровизация.

- Создание новых бизнес-процессов и модернизация уже существующих.
- Возможность контроля за процессами производства.
- Создание предпосылок для цифровой трансформации.

3. Цифровая трансформация.

- Масштабные преобразования внутренних процессов за счет активного внедрения информационных технологий;
- Изменения в цепочках создания ценности.

Главным отличием цифровой трансформации от других этапов является интеграция технологий практически во все аспекты деятельности предприятия, увеличивается производительность производства, трудовых ресурсов, а также

принимается во внимание более качественные и взвешенные управленческие решения.

Конкурентоспособность промышленных предприятий в современных условиях – это их способность эффективно функционировать на рынке, опережая конкурентов за счёт оптимального сочетания цены и качества продукции, оперативности реагирования на изменения спроса и рационального использования ресурсов. Ключевые критерии конкурентоспособности включают [2]:

- долю рынка (абсолютную и динамику её прироста) – отражает реальное положение компании среди конкурентов;
- качество продукции (технические характеристики, надёжность, эргономику, экологичность и эстетику);
- цену – конкурентоспособность достигается при оптимальном соотношении цены и потребительской ценности;
- скорость вывода продукта на рынок (Time-to-Market) – чем быстрее предприятие адаптируется к запросам рынка, тем выше его конкурентные преимущества;
- рентабельность и финансовую устойчивость (уровень ликвидности, оборачиваемость активов, доходность продаж и капитала);
- производительность (эффективность труда, капиталовложений и совокупная производительность факторов производства);
- инновационную активность (внедрение новых технологий, модернизация процессов, разработка уникальных продуктов);
- уровень сервиса и послепродажного обслуживания (гарантии, техническая поддержка, инструктаж);
- гибкость и адаптивность – способность оперативно перестраивать производство под новые рыночные условия, санкции, логистические вызовы;
- репутацию и бренд – доверие потребителей, узнаваемость марки, лояльность клиентов;
- эффективность логистики и цепочек поставок – надёжность партнёрских связей, минимизация издержек на транспортировку и хранение.

Цифровизация играет ключевую роль в повышении операционной эффективности промышленных предприятий и снижении издержек, обеспечивая комплексную трансформацию производственных и управленческих процессов. За счёт внедрения цифровых технологий предприятия получают возможность в режиме реального времени собирать, анализировать и использовать данные о состоянии оборудования, загрузке мощностей, расходе ресурсов и качестве продукции.

Цифровизация обеспечивает [2]:

- а) сокращение производственных издержек за счёт оптимизации ресурсов и снижения брака;
- б) уменьшение времени простоя оборудования и затрат на его обслуживание;
- в) ускорение производственных циклов и вывода новых продуктов на рынок;
- г) повышение гибкости и адаптивности производства к изменениям спроса;
- д) улучшение качества продукции и безопасности труда;
- е) более обоснованное и оперативное принятие управленческих решений в реальном времени.

Внедрение цифровых решений не только снижает операционные затраты, но и создаёт устойчивые конкурентные преимущества, позволяя предприятиям быстрее реагировать на рыночные вызовы, эффективнее использовать ресурсы и наращивать общую производительность.

Современная российская промышленность столкнулась с мощным штормом геополитических потрясений, кардинально изменившим условия хозяйствования. Если ограничения 2014 года затронули преимущественно финансовый и сырьевой секторы, то нынешний раунд санкционного давления стал беспрецедентным по масштабу и глубине, затронув практически каждое производственное звено – от доступа к станкам и микрочипам до логистики и международных расчётов.

К началу 2026 года общее количество антироссийских санкций, введённых различными государствами с 2014 года, превысило 31,5 тыс. ограничительных мер. Санкционное давление продолжает нарастать – 23 апреля 2026 года. Европейский союз утвердил 20-й пакет санкций, ставший одним из самых масштабных за последние два года: под ограничения попали более 120 физических и юридических лиц, введён полный запрет на транзакции с 20 российскими банками, расширены экспортные ограничения на товары общей стоимостью свыше 365 млн евро и импортные ограничения на сумму более 530 млн евро. США также продолжают наращивать санкционное давление – в мае 2026 года Минфин США расширил санкционный список, добавив 28 организаций, 19 танкеров и 4 физических лица. Накопленный эффект этих ограничений оказывает существенное влияние на российскую экономику. Динамика ВВП России в 2022-2026 гг. представлена в табл. 1.

Как видно из таблицы, после восстановительного роста в 2023-2024 годах в 2025 году рост ВВП резко замедлился до 1,0 % (с 4,9 % в 2024-м). На 2026 год прогнозы большинства ведомств и организаций сходятся в диапазоне 0,5-1,5 % (Банк России ожидает 0,5-1,5 %, Минэкономразвития – около 1,2 %).

Таблица 1

Темпы прироста ВВП РФ (в % к предыдущему году)

| Год         | 2022 | 2023 | 2024 | 2025 | 2026 (прогноз) |
|-------------|------|------|------|------|----------------|
| Прирост ВВП | -1,2 | +3,6 | +4,9 | +1,0 | +0,5...+1,5    |

Источник: Росстат, Минэкономразвития РФ, прогноз ЦБ РФ (апрель 2026).

Инфляция и ключевая ставка демонстрируют следующую динамику (табл. 2).

Таблица 2

Инфляция и ключевая ставка ЦБ РФ (среднегодовые значения, %)

| Показатель                           | 2022 | 2023 | 2024 | 2025 | 2026 (прогноз) |
|--------------------------------------|------|------|------|------|----------------|
| Инфляция (годовая, на конец периода) | 11,9 | 7,4  | 9,5  | 5,6  | 4,5-5,5        |
| Ключевая ставка (среднегодовая)      | 10,0 | 11,5 | 16,0 | 18,5 | 13,5-14,5      |

Источник: Банк России, Росстат.

Уровень безработицы по итогам 2025 года составил 2,2 % (исторический минимум), прогноз на 2026 год – 2,3 %.

Инвестиционная активность демонстрирует тревожную динамику. По данным Росстата и Института комплексных стратегических исследований (ИКСИ), в 2025 году инвестиции в основной капитал сократились на 2,3 % в годовом выражении это первое падение с 2020 года и самое сильное с 2015 года. Помесячная динамика инвестиций в 2025 году (в % к соответствующему месяцу предыдущего года) выглядела следующим образом:

I квартал: +0,5%

II квартал: -0,8%

III квартал: -4,3%

IV квартал: -5,3%

Абсолютный объём инвестиций в основной капитал по итогам 2025 года составил 42,6 трлн руб. Эксперты ИКСИ охарактеризовали ситуацию как начало новой «инвестиционной зимы». На 2026 год Минэкономразвития прогнозирует дальнейшее снижение инвестиций (ориентировочно на 1,5-2,0%).

Промышленное производство в 2025 году выросло лишь на 1,3%. Однако уже в январе 2026 года промышленное производство снизилось на 0,8% в годовом сравнении, а обрабатывающие производства сократились на 3,0%. Прогноз роста обрабатывающей промышленности на 2025-2026 годы неоднократно пересматривался в сторону понижения: согласно актуальному прогнозу Минэкономразвития (сентябрь 2025 года), в 2025 году рост составит 3,1 %, в 2026 году – 2,9 % (изначально ожидалось 4,3% и 3,4% соответственно). Тем не менее в отдельных высокотехнологичных сегментах сохраняется положительная динамика: в январе-феврале 2026 года производство компьютеров, электроники и оптики выросло на 7,3% в годовом выражении.

Таблица 3  
Динамика инвестиций в основной капитал РФ  
(прирост в % к предыдущему году)

| Год                | 2020 | 2021 | 2022 | 2023 | 2024 | 2025 |
|--------------------|------|------|------|------|------|------|
| Прирост инвестиций | -1,4 | +6,0 | +4,7 | +9,8 | +7,6 | -2,3 |

Источник: Росстат

Экономическое давление реализуется через комбинацию инструментов от прямых торговых эмбарго до вторичных санкций, угрожающих любым иностранным контрагентам, сохраняющим связи с Россией. Особую проблему представляет зависимость от импортного станочного парка. До 2022 года импорт покрывал около 90 % парка металлообрабатывающих станков, к 2025 году зависимость сократилась лишь до ~75 %, причём в основном не за счёт локализации, а благодаря резкому росту поставок из КНР, занявших до трёх четвертей импорта. До 60 % станков в России изношено, а доступность китайских аналогов пока не решает проблему технологического суверенитета. Одновременно финансовая блокада – отключение от SWIFT, арест активов, угрозы для банков-корреспондентов – существенно осложнила платежи за импорт. По состоянию на начало 2026 года западными странами заморожены российские активы на общую сумму около 590 млрд. долларов, включая золотовалютные резервы ЦБ России (около 300 млрд долларов) и активы частных лиц и компаний.

Параллельный импорт, легализованный как экстренная мера, по итогам 2025 года составил 23,1 млрд. долларов, что соответствует среднемесячному объёму около 1,9 млрд. долларов. Динамика объёмов параллельного импорта представлена в табл. 4.

За январь-ноябрь 2025 года объём параллельного импорта сократился на 45% - с 37,9 до 20,9 млрд. долларов (накопленным итогом). Основные причины: ужесточение таможенного контроля, угроза вторичных санкций для стран-посредников, а также постепенное импортозамещение по отдельным позициям [3].

Импортная составляющая в затратах промышленности за 2021-2024 годы сократилась почти вдвое. Количество производственных компаний в России увеличилось на 3% в 2025 году, достигнув 504 тыс. В IT-секторе реализуется 175 особо значимых проектов по импортозамещению ПО общей стоимостью 187 млрд. руб., 120 из них уже завершены, выполнено 70% от запланированного в 2022 году. Степень локализации ПО в России достигает 77% (аппаратного обеспечения – 40%). За зиму 2025-2026 годов в промышленности и машиностроении запущено более 30 крупных производств с инвестициями свыше 130 млрд. руб.

Таблица 4  
Динамика параллельного импорта в Россию  
(среднемесячный объём, млрд. долл.)

| Период                          | Среднемесячный объём | Примечание             |
|---------------------------------|----------------------|------------------------|
| Начало 2022 (после легализации) | ~4,0                 | Пиковые значения       |
| 2023                            | ~3,2                 | Постепенное снижение   |
| 2024                            | ~2,5                 | Ужесточение контроля   |
| 2025 (в среднем)                | ~1,9                 | Снижение на 45% за год |
| Январь 2026                     | ~1,0                 | Исторический минимум   |

Источник: Росстат

Однако в станкостроении зависимость от импорта остаётся критической: в 2024 году доля импорта вновь превысила 98% из-за неспособности отечественных производителей в короткие сроки закрыть возросший рыночный спрос. Национальный проект «Средства производства и автоматизация» ставит целью достичь технологической независимости на уровне 95% по высокотехнологичным станкам и доли отечественной продукции на внутреннем рынке 60%, но пока эти цели далеки от реализации.

Главным стратегическим вызовом остаётся критическая зависимость от импортных технологий и компонентов. Для промышленности сегодня приоритетны не столько тактические схемы обхода санкций, сколько долгосрочные инвестиции в НИОКР, перестройка производственных цепочек с ориентацией на дружественные страны и активная государственная поддержка технологического суверенитета. Только комплекс мер от льготного кредитования до целевых программ по локализации позволит предприятиям не просто выживать, но и наращивать конкурентоспособность в новых геополитических реалиях [4].

Российские промышленные предприятия выработали комплекс стратегий адаптации, позволяющих не только компенсировать потери от санкций, но и использовать новые возможности для технологического рывка.

Импортозамещение стало центральной стратегией адаптации. Особенно наглядно это проявилось в станкостроении – отрасли, являющейся «базой для базовых» и критически важной для технологического суверенитета. По итогам 9 месяцев 2025 года доля российской станкоинструментальной продукции на внутреннем рынке достигла порядка 32%. Количество предприятий в реестре российской станкоинструментальной продукции выросло с примерно 40 в 2021 году до порядка 120.

Ключевым механизмом поддержки стал национальный режим в госзакупках, когда заявки на импорт отклоняются при наличии российского аналога. В 2025 году было отклонено почти 40% заявок на приобретение импортной продукции, что обеспечило более 90 млрд. рублей для закупки отечественных станков и инструментов. Правительство рассчитывает, что

национальный проект «Средства производства и автоматизации» позволит к 2030 году увеличить долю отечественных станков до 60% внутреннего рынка.

В рамках реализации Стратегии цифровой трансформации обрабатывающих отраслей промышленности исследования среди российских промышленных предприятий выявили основные цели цифровой трансформации (рис. 1).



Рисунок 1. Цели цифровой трансформации промышленных предприятий РФ (2025 год, в % от числа опрошенных компаний)

Источник: исследование РФРИТ и НАФИ «Цифровая зрелость российских предприятий», 2025 г.

Как показывают данные рис. 1, 45% компаний называют приоритетной целью повышение операционной и экономической эффективности, 20% – повышение качества продукции, 15% – импортозамещение и адаптацию к новым условиям, 10% – снижение затрат и рисков. Другие цели («увеличение объёмов производства», «выполнение контрактов», «получение стратегического преимущества») упоминаются лишь в 5% случаев каждый.

Важно отметить, что кадровые ограничения остаются одним из главных препятствий для цифровой трансформации (рис.2).

Согласно опросу предприятий, недостаток финансирования отметили 25% респондентов; нехватку квалифицированных кадров 20%, проблемы с ИТ-системами и технологиями ещё 20%, трудности, связанные с цифровизацией бизнес-процессов 15%. Другие барьеры (организационная культура и стратегия, цифровая грамотность сотрудников) назвали 10% респондентов каждый. Уровень цифровой зрелости российских предприятий остаётся неравномерным: по данным исследования СКБ Контур, 2,58% предприятий находятся в очень

высокой степени цифровой зрелости, 10,57% на базовом уровне.



Рисунок 2. Основные барьеры цифровой трансформации промышленных предприятий РФ (2025 год, в % от числа опрошенных компаний)

Источник: исследование РФРИТ и НАФИ «Цифровая зрелость российских предприятий», 2025 г.

Проведённый анализ позволяет сделать вывод, что российская промышленность, столкнувшись с беспрецедентными вызовами, продемонстрировала высокую адаптивность. Ключевым фактором успеха стало сочетание стратегий импортозамещения, цифровизации и переориентации на внутренний и дружественные внешние рынки. Представленные кейсы подтверждают, что цифровая трансформация и оптимизация процессов позволяют не только компенсировать потери от санкций, но и создавать новые конкурентные преимущества.

### Список литературы

1. Николаев Д. А., Крупнов Ю. А. Этапы цифровой трансформации в организации [https://ecsn.ru/wp-content/uploads/202511\\_355.pdf](https://ecsn.ru/wp-content/uploads/202511_355.pdf)
2. Синцова Е. А., Воскресенская О. В. О влиянии цифровой экономики на конкурентоспособность промышленных предприятий // Экономика и управление. 2020. Т. 26. № 9. С. 986–992. <http://doi.org/10.35854/1998-1627-2020-9-986-992>
3. Городнова Наталья Васильевна ИНДУСТРИАЛЬНЫЙ ИНТЕРНЕТ ВЕЩЕЙ В РОССИИ: СУЩНОСТЬ И ПЕРСПЕКТИВЫ // Вопросы инновационной экономики. 2022. №3. URL:

<https://cyberleninka.ru/article/n/industrialnyy-internet-veschey-v-rossii-suschnost-i-perspektivy> (дата обращения: 09.06.2026).

4. Панова Екатерина Андреевна ВЛИЯНИЕ САНКЦИЙ НА ДЕЯТЕЛЬНОСТЬ РОССИЙСКИХ ПРОИЗВОДСТВЕННЫХ ПРЕДПРИЯТИЙ // Государственное управление. Электронный вестник. 2023. №96. URL: <https://cyberleninka.ru/article/n/vliyanie-sanktsiy-na-deyatelnost-rossiyskih-proizvodstvennyh-predpriyatiy> (дата обращения: 09.06.2026).

**Кузовлева Нина Фёдоровна**

кандидат экономических наук

профессор кафедры экономической экспертизы и финансового мониторинга

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

**Попова Анастасия Владимировна**

**Поневенкина Анна Андреевна**

студенты 1 курса

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

## **Использование биометрии в финансовых услугах: технологии и вопросы безопасности**

**Аннотация.** В статье проводится комплексный анализ технологий биометрической аутентификации, применяемых при оказании финансовых услуг, выявляются основные угрозы безопасности, разрабатываются рекомендации по защите биометрических данных и соблюдению регуляторных требований для обеспечения безопасного и эффективного внедрения таких систем при проведении финансовых операций.

**Ключевые слова:** биометрическая аутентификация; финансовые услуги; цифровые технологии; экономическая безопасность.

В настоящее время традиционные способы подтверждения личности в финансовой сфере – пароли, ПИН-коды и SMS-сообщения – потеряли свою надежность. Они регулярно поддаются перехвату, фишингу или социальной инженерии, что подтверждается растущей статистикой кибератак и хищений средств с банковских карт и счетов. Внедрение биометрических технологий (отпечаток пальца, распознавание лица или голоса) позволяет значительно повысить экономическую безопасность, поскольку подделать такие данные сложнее, а процесс проверки занимает доли секунды.

Финансовые организации заинтересованы в повышении удобства и скорости обслуживания: биометрия сокращает время транзакций, снижает нагрузку на колл-центры и уменьшает операционные издержки. Кроме того, сами биометрические данные обладают важной особенностью – в отличие от пароля, их невозможно изменить при утечке. Если злоумышленник получит отпечаток пальца или запись голоса клиента, этот клиент останется уязвимым пожизненно. При этом методы защиты биометрических шаблонов (например, их хэширование или криптографическое преобразование) пока не стали стандартом для банковской отрасли, а развитие технологий подделки (Deepfake) создает новые угрозы.

Правовое регулирование в этой области отстает от темпов внедрения: законодательство о персональных данных (включая российское законодательство и европейский GDPR) не всегда содержит четкие и единообразные требования к сбору, хранению и обработке биометрии именно в финансовом секторе. Таким образом, изучение баланса между технологическими возможностями биометрии и рисками для безопасности клиентов является своевременным и практически значимым.

Биометрическая аутентификация — это процесс подтверждения личности человека с использованием его уникальных физиологических или поведенческих характеристик. Цель — проверить, действительно ли пользователь является тем, за кого себя выдаёт, и предоставить ему доступ к определённому ресурсу или услуге.

Биометрические технологии аутентификации классифицируются по типу распознаваемых признаков.

- Распознавание лица (Face ID). Технология используется для быстрого входа в мобильное приложение банка, подтверждения транзакций, а также при оплате товаров и услуг через биометрические терминалы. Например, в России доступны сервисы FacePay, которые позволяют оплачивать покупки по изображению лица.
- Голосовая биометрия. Системы распознают голос по интонации, тембру и манере речи. Применяется в колл-центрах для верификации клиентов, а также для подтверждения операций при звонке в банк.
- Отпечатки пальцев. Используются в банкоматах, мобильных приложениях банков и для аутентификации в платёжных сервисах (например, в приложениях вроде MTS Pay, Mir Pay, СБП).
- Сканирование радужки глаза. Более сложный рисунок радужной оболочки делает эту технологию надёжной для идентификации личности.
- Идентификация по рисунку вен ладони. Применяется в некоторых банковских системах, например, для доступа к банковским ячейкам.
- Мультимодальная биометрия. Комбинирование нескольких методов (например, использование лица и голоса одновременно) повышает уровень безопасности и позволяет решать несколько задач одновременно.

Согласно данным российских исследований, отпечатки пальцев занимают значительную долю рынка биометрических технологий в банковском секторе, при этом наиболее востребованными являются распознавание лица и голоса, что обусловлено их бесконтактностью и возможностью использования на стандартных устройствах [1, с. 84].

Важно отметить, что сравнение ведется не по исходным изображениям или записям голоса, а по вычисленным математическим векторам признаков, что позволяет не хранить чувствительные биометрические данные в открытом виде.

Как отмечают исследователи, ключевым трендом цифровой трансформации банковской отрасли является интеграция биометрических решений в процессы идентификации клиентов, а уровень затрат на IT-решения в данной сфере ежегодно возрастает [4, с. 108].

Приведем примеры реального применения биометрии в российских финансовых услугах, такие как вход в мобильный банк по лицу или отпечатку пальца, система оплаты по биометрии Сбера, ВТБ ID, а также удаленное открытие счетов через фотографию паспорта и селфи [3, с. 555].

Рассмотрим структуру внедрения биометрических систем в российскую финансовую инфраструктуру, центральным элементом которой выступает Единая биометрическая система (ЕБС) – государственная информационная система, оператором которой является Центр биометрических технологий [1, с. 84]. ЕБС обеспечивает централизованный сбор, хранение и обработку биометрических данных граждан, причем с вступлением в силу Федерального закона № 572-ФЗ хранение биометрических данных стало возможным исключительно через ЕБС, что заменило децентрализованную модель, при которой банки могли самостоятельно разрабатывать сервисы для сбора биометрии [1, с. 85].

На конец июля 2025 года система насчитывает порядка 12 тысяч точек очной регистрации и 17 действующих сервисов, включая оплату покупок и проезда, дистанционное открытие банковского счета и бизнеса, оформление усиленной квалифицированной электронной подписи и SIM-карт [2].

Одним из наиболее значимых является биоэквайринг – платформа, связывающая решения банков и позволяющая совершать биометрические транзакции независимо от банка клиента. В этой архитектуре ЕБС отвечает за биометрическую идентификацию, Национальная система платежных карт (НСПК) – за маршрутизацию и расчеты, банк-эквайер – за точку входа на стороне розничного продавца, а пользователь просто подтверждает оплату своей биометрией без карты и телефона [2]. Кроме того, биометрия интегрируется в процессы удаленной идентификации клиентов, трансформируя традиционные процедуры КУС в электронные eКУС, что позволяет открывать банковские счета и оформлять продукты без личного присутствия, но при условии, что клиент уже зарегистрировал свои биометрические данные в ЕБС [1, с. 84].

В 2025 году был реализован сервис выездной регистрации подтвержденной биометрии с использованием планшетов на базе российской операционной системы «Аврора» [5]. Данное решение обеспечивает полный цикл размещения биометрических данных в Единой системе идентификации и аутентификации (ЕСИА) и ГИС ЕБС, включая получение согласия клиента, подтверждение учетной записи и регистрацию уникальных физических характеристик – фото лица и записи голоса [5]. До этого финансовые организации использовали для регистрации только стационарные устройства,

размещенные в отделениях банков, поэтому переход к мобильным решениям стал важным этапом развития инфраструктуры [5].

Основные технические сложности интеграции.

- Необходимость обеспечения совместимости различных информационных систем через унифицированные API.
- Соблюдение жестких требований информационной безопасности (сертификация ФСТЭК и ФСБ).
- Обеспечение би-модальности (использование одновременно лица и голоса) для повышения устойчивости к ошибкам и атакам [2].

Ключевым вопросом остается выстраивание «системы доверия», при которой клиент остается активным субъектом, способным управлять своими данными, видеть, где они используются, и при необходимости отзывать согласие на их обработку [2].

Анализ актуальных источников позволяет выделить несколько категорий угроз, каждая из которых обладает своей спецификой в контексте финансовых операций. Первая и наиболее известная категория – атаки подмены, или презентационные атаки. Злоумышленник предъявляет датчику не реальный биометрический признак, а его подделку: фотографию или маску для системы распознавания лиц, слепок из желатина или силикона для датчика отпечатков пальцев, аудиозапись для голосовой аутентификации.

Вторая категория угроз, приобретающая критическое значение в 2025 – 2026 годах, связана с генеративным искусственным интеллектом и deepfake-технологиями. Злоумышленник больше не нуждается в физической подделке отпечатка или в краже фотографии высокого разрешения из закрытой базы. Достаточно публично доступных изображений из социальных сетей, на основе которых нейросеть способна синтезировать видео, имитирующее естественные микродвижения лица, моргание, артикуляцию речи. По данным отчета Entrust, deepfake-атаки составляют уже одно из пяти (20%) попыток биометрического мошенничества, а количество случаев использования deepfake-селфи увеличилось на 58% в 2025 году [6].

Третья категория угроз относится не к процессу предъявления биометрии, а к инфраструктурному уровню – это атаки на этапе обработки и передачи данных. Атаки внедрения выросли на 40% в годовом исчислении, позволяя злоумышленникам обходить процесс live-захвата путем прямой подачи манипулированных изображений или видео в системы верификации [7].

Четвертая, принципиально важная угроза – это смещение фокуса мошенничества с этапа регистрации на этап аутентификации. Долгое время финансовые платформы концентрировали свои системы безопасности на этапе создания учетной записи, требуя от новых пользователей предъявления удостоверения личности и селфи для верификации. Однако злоумышленники

сместили свое внимание на моменты доступа к уже существующим счетам: попытки входа, сброса пароля или смены устройства [8].

Наконец, еще одним значимым фактором уязвимости является человеческий фактор, а точнее – социальная инженерия. Как отмечается в статье Полины Кобзевой, злоумышленники все чаще используют психологическую манипуляцию: фишинг, имперсонацию и принуждение для того, чтобы убедить жертв использовать их подлинную идентичность для несанкционированных операций или добровольно передать чувствительные данные [16].

Перед лицом описанных угроз финансовая индустрия выработала комплекс защитных мер, которые можно разделить на несколько уровней. Первый и наиболее очевидный уровень – liveness-детекция (или определение живости), то есть проверка того, что предъявленный биометрический образец получен от живого человека в режиме реального времени, а не является статической подделкой, видеозаписью или deepfake-синтезом. Определение живости бывает активной, требующей от пользователя произвольных действий вроде моргания, поворота головы или произнесения случайной фразы, и пассивной, работающей незаметно для пользователя и анализирующей текстуру кожи, микродвижения, пульс по изменению цвета лица или даже рефлекс зрачков. Пассивное определение живости предпочтительнее с точки зрения пользовательского опыта, поскольку не создает дополнительных барьеров, но она технологически сложнее и требует более мощных вычислительных ресурсов на устройстве [9].

Стоит также упомянуть, что современные системы все чаще переходят к двухуровневой проверке: сначала универсальный алгоритм определения живости, а затем специализированная нейросетевая модель форензического анализа deepfake, обученная выявлять специфические артефакты, которые генеративные модели неизбежно вносят в синтезированное изображение. Это особенно важно в свете данных о том, что deepfake-атаки становятся все более изощренными и массовыми.

Второй уровень защиты, который считается сегодня одним из наиболее перспективных, – это отменяемая биометрия. Исходный биометрический образец подвергается необратимому преобразованию, в результате которого получается шаблон, не позволяющий восстановить исходную биометрию. Причем для одного и того же человека можно создать множество различных шаблонов, применяя разные преобразования. Если один из таких шаблонов скомпрометирован, система просто переходит к другому, ранее не использовавшемуся преобразованию того же самого биометрического признака. Таким образом, проблема неотзываемости биометрии получает элегантное решение: система становится возобновляемой, подобно системе паролей, но без необходимости хранить эталонный образец в открытом виде [10].

Третий уровень защиты – аппаратный. Данный уровень представляет собой изолированную область процессора, которая обрабатывает биометрические данные и выполняет операцию сравнения, не передавая сырые шаблоны в основную операционную систему или в приложения. Даже если операционная система устройства полностью скомпрометирована, злоумышленник не может получить доступ к биометрическим данным, обрабатываемым внутри этой защищенной области. В финансовых системах, особенно в банкоматах и платежных терминалах нового поколения, внедряются аппаратные модули безопасности, отвечающие за криптографическую защиту биометрических каналов и хранение ключей [11].

Важным направлением защиты также является переход от вероятностной аутентификации к детерминированной криптографической. Традиционная биометрическая система отвечает на вопрос: «С какой вероятностью предъявленный образец принадлежит заявленному пользователю?» В случае ошибки система может либо пропустить злоумышленника, либо заблокировать легитимного клиента. Новый подход предполагает, что биометрия используется не для прямого сравнения с шаблоном, а для разблокировки криптографического ключа, который надежно привязан к аппаратному корню доверия на устройстве пользователя. Этот подход также находит отражение в требовании российского законодательства, согласно которому биометрические данные представляют собой особую категорию персональных данных, обработка которых строго регламентирована, а основным риском их использования является утечка, способная привести к мошенничеству, краже личности и нарушению конфиденциальности [12].

Технологические возможности защиты биометрии имеют значение только в той мере, в какой они трансформируются в доверие конечных пользователей. Финансовая сфера уникальна тем, что здесь пользователь ежедневно принимает решения о безопасности своих средств, и даже самая совершенная система не будет эффективной, если клиенты отказываются ее использовать из-за недоверия.

Наиболее свежие эмпирические данные по этому вопросу предоставлены исследованием ВТБ, проведенным в апреле 2026 года среди 1500 респондентов – жители крупных российских городов. Согласно результатам, почти семьдесят процентов опрошенных (69%) заявили о готовности использовать биометрию в финансовых операциях [17].

Это довольно высокий показатель, особенно если учесть, что массовое внедрение биометрии в российском финансовом секторе насчитывает лишь несколько лет. Примечательно, что при выборе между биометрической аутентификацией и традиционными методами вроде СМС-кодов или PIN-паролей треть опрошенных (33%) отдали предпочтение биометрии, еще 39% сочли все способы равноценными, и только 28% предпочли подождать СМС-код.

То есть для абсолютного большинства пользователей биометрия уже не воспринимается как нечто экзотическое или рискованное, а рассматривается как равноправный инструмент наряду с привычными способами подтверждения операций [13].

Эти данные согласуются с результатами опроса ВЦИОМ и Центра биометрических технологий на конец 2025 года, согласно которым биометрия занимает первое место (20%) в списке надежных способов подтверждения личности при использовании цифровых устройств. Более половины респондентов (53%) рассматривают биометрию как инструмент защиты от кредитного мошенничества и поддерживают ее использование при онлайн-оформлении займов [14].

Анализируя предпочтения в сценариях использования, исследование ВТБ выявило, что наиболее востребованным применением биометрии является вход в онлайн-банк – это указали 44% респондентов. Столько же опрошенных хотели бы подтверждать финансовые операции по лицу, воспринимая такую аутентификацию как дополнительную защиту от несанкционированного списания, поскольку лицо трудно подделать в реальном времени, а мошенник не может просто перехватить СМС-код. Тридцать один процент (31%) видят ценность в подписании документов без визита в офис, 29% – в получении кредита, и столько же (29%) – в оплате покупок и проезда. Таким образом, биометрия воспринимается не как универсальная замена всем методам аутентификации, а как инструмент для конкретных, наиболее ответственных или наиболее частых операций [18].

Ключевым фактором, определяющим доверие, является безопасность: каждый второй респондент назвал ее самым важным критерием при выборе метода оплаты или подтверждения операции. Удобство и скорость оказались на втором месте, но с заметным отрывом. Люди готовы терпеть определенные неудобства, если уверены в защите своих средств. В качестве конкретного преимущества биометрии респонденты называли возможность «забыть дома и карту, и телефон» – биометрия воспринимается как встроенная, всегда доступная, неотчуждаемая форма идентификации, которая не может быть потеряна или забыта.

Четверть респондентов (25%) за последний год стали больше доверять банковской биометрии, причем ключевым фактором, по их собственному признанию, стало отсутствие в их информационном поле новостей об успешных атаках на биометрические системы. Люди склонны доверять технологии, если они не слышат о ее компрометациях, что подтверждает важность контроля репутационных рисков в финансовой сфере. Почти 18% респондентов уже используют биометрию в повседневных финансовых операциях, а 38% отмечают, что стали чаще наблюдать использование биометрии другими людьми и оценивают это как удобное решение. Воспринимаемая социальная норма —

если другие используют, значит, это безопасно и приемлемо — оказывает сильное влияние на индивидуальное доверие. Вместе с тем, остается значимая группа пользователей (около 28%), которые предпочитают традиционные методы вроде СМС-кодов. Гипотетические причины этого можно реконструировать на основе качественных комментариев. Наиболее вероятные причины: страх утечки биометрических данных с осознанием их неотзываемости, консервативное неприятие новых технологий, недостаточная информированность о том, что современные системы не хранят сырые биометрические данные, а работают с необратимыми преобразованиями, либо наличие негативного опыта использования биометрии в нефинансовых контекстах [15].

Биометрические системы в российском финансовом секторе достигли критической точки доверия, позволяющей их масштабное внедрение. Технологическая защита сама по себе перестала быть лимитирующим фактором, потому что на первый план вышли психологические и информационные аспекты. Для дальнейшего роста доверия необходимо не только совершенствовать защиту, но и активно информировать пользователей о невозможности восстановления «сырых» биометрических данных при взломе, а также строго контролировать репутационные риски (не допускать публичных инцидентов с компрометацией). Основной вызов на ближайшие годы – не убедить большинство, а ответить на страхи устойчивого меньшинства, для которого риски утечки биометрии перевешивают выгоды от удобства.

Проведенное исследование позволяет сделать следующие выводы.

Во-первых, биометрические технологии (распознавание лица, голоса, отпечатков пальцев) активно внедряются в российский финансовый сектор, наиболее востребованными являются распознавание лица и голоса благодаря бесконтактности и совместимости со стандартными устройствами.

Во-вторых, центральным элементом инфраструктуры выступает Единая биометрическая система (ЕБС), которая на конец июля 2025 года насчитывает порядка 12 тысяч точек регистрации и 17 сервисов, включая биоэквайринг и удаленное открытие счетов, однако интеграция сопряжена с техническими сложностями: необходимость совместимости систем через API, соблюдение требований ФСТЭК и ФСБ, обеспечение би-модальности.

В-третьих, выявлены основные угрозы: презентационные атаки (подделки), deepfake-атаки (до 20% попыток мошенничества), атаки на этапе передачи данных (рост 40%), социальная инженерия.

В-четвертых, определены методы защиты: liveness-детекция (проверка живости), отменяемая биометрия (необратимые шаблоны), аппаратная защита (Secure Enclave), переход к криптографической аутентификации.

В-пятых, согласно исследованию ВТБ (апрель 2026, 1500 респондентов), 69% готовы использовать биометрию, 33% предпочитают ее традиционным

методам, ключевым фактором доверия является безопасность (50%), а основным барьером – страх утечки данных. Основной вызов – ответ на страхи устойчивого меньшинства (около 28%) и информирование клиентов о невозможности восстановления сырых биометрических данных при компрометации.

### Список литературы

1. Серов Е. Р. Применение технологий биометрии в российском банковском бизнесе // Проблемы современной экономики. — 2025. — № 3 (95). — С. 83–86
2. Биометрия в России. Новые ID-технологии, архитектура доверия и биоэквайринг // PLUSworld.ru. — 2025. — 1 сентября. — URL: <https://plusworld.ru/articles/67032/>
3. Булатова Э. И., Матерова Е. С., Коновалова М. Е., Белов А. В., Батталова А. А. Опыт и перспективы использования биометрических технологий в банковском секторе // Экономика и предпринимательство. — 2024. — № 3 (164). — С. 554–557
4. Гуртовая К. А., Окунева А. Г. Актуальные проблемы безопасности хранения персональных данных клиентов // Вестник Самарского государственного экономического университета. — 2025. — № 1 (243). — С. 106–113
5. ПСБ и «Открытая мобильная платформа» предоставят населению сервис выездной регистрации подтвержденной биометрии // ПСБ. — 2025. — 9 октября. — URL: <https://www.psbank.ru/bank/press/news/2025/10/09-03>
6. Entrust: технологии GenAI и дипфейки усиливают рост подделок и подрывают биометрическую идентификацию <https://cisoclub.ru/entrust-tehnologii-genai-i-dipfejki-usilivajut-rost-poddelok-i-podryvajut-biometricheskuju-identifikaciju/?ysclid=mq8capsk1484932250>
7. Entrust: Генеративный ИИ и дипфейки интенсифицируют фрод <https://ib-bank.ru/bisjournal/news/22987?ysclid=mq8cds78e2383970892>
8. Информационная безопасность банков: угрозы, решения и стратегии защиты <https://www.gazprombank.ru/pro-finance/safety/informacionnaya-bezopasnost-bankov/?ysclid=mq8cgj4lo310653717>
9. Технология liveness в биометрии: что это и как работает <https://trends.rbc.ru/trends/industry/64f93a379a794730d0d8b498?ysclid=mq8crakh63651672661&from=copy>
10. Ленская Д. А. ОТМЕНЯЕМАЯ БИОМЕТРИЧЕСКАЯ СИСТЕМА БЕЗОПАСНОСТИ, ОСНОВАННАЯ НА ХАОТИЧЕСКИХ ФУНКЦИЯХ // Auditorium. 2022. №2 (34). URL: <https://cyberleninka.ru/article/n/otmenyaemaya-biometricheskaya-sistema-bezopasnosti-osnovannaya-na-haoticheskikh-funktsiyah> (дата обращения: 10.06.2026).

11. Свой-чужой. Как работает биометрия и Secure Enclave в современных телефонах <https://xakep.ru/2026/03/05/secure-enclave/>
12. ЭЦП и аутентификация: сделано в России <https://www.osp.ru/lan/2014/09/13042709?ysclid=mq8d19zn6o292953274>
13. Россияне стали больше доверять биометрии в финансах <https://finance.mail.ru/article/rossiyane-stali-bolshe-doveryat-biometrii-v-finansah-69209565/?ysclid=mq8ddsji6s919683453>
14. Оплата налицо: какие риски несут платежи по биометрии <https://kiberboloid.ru/analitika/oplata-nalitso-kakie-riski-nesut-platezhi-po-biometrii/?ysclid=mq8dhaq8cl522268136>
15. Банк выяснил, что предпочитают россияне в биометрических сервисах <https://perm.aif.ru/society/details/bank-vyyasnil-chto-predpochitayut-rossiyane-v-biometricheskih-servisah?ysclid=mq8drpr1c6801583619>
16. <https://moshousing.ru/psihologicheskie-ulovki-i-tehniki-manipulyacii-v-sovremennyh-moshennicheskikh-skhemah/>
17. <https://volgograd.bezformata.com/listnews/biometriya-ili-paroli/159846453/>
18. <https://www.banki.ru/news/lenta/?id=11024318&ysclid=mpvr21cfpq520288624>

**Курашова Анна Андреевна**

кандидат экономических наук, доцент

доцент кафедры экономической экспертизы и финансового мониторинга

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

**Кузнецова Полина Игоревна**

**Лысенко Маргарита Андреевна**

студенты 4 курса

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

## **Интеграция искусственного интеллекта и больших данных в аудиторскую практику**

**Аннотация.** В статье исследуется трансформация аудиторской практики под влиянием интеграции технологий искусственного интеллекта (ИИ) и Больших данных (Big Data). Показано, что данные технологии знаменуют переход от выборочного, ретроспективного аудита к сплошному, предиктивному анализу и непрерывному мониторингу. Выявлены ключевые модели интеграции, среди которых наиболее перспективными являются гибридные системы, сочетающие экспертные знания и машинное обучение. Анализ международного опыта свидетельствует о лидерстве развитых стран, тогда как в России и странах СНГ процесс носит асинхронный характер и сталкивается с инфраструктурными и кадровыми вызовами. Несмотря на комплекс проблем, таких как «эффект черного ящика» и недостаток регулирования, авторы доказывают, что интеграция ИИ и Больших данных является необратимым этапом эволюции аудита, кардинально повышающим его качество, эффективность и стратегическую ценность.

**Ключевые слова:** аудит, искусственный интеллект, Большие данные, машинное обучение, гибридные системы, профессиональный скептицизм, аудиторские риски.

Актуальность данной работы заключается в том, что интеграция искусственного интеллекта и Больших данных в нынешнюю аудиторскую практику меняет подход к проведению проверок. Традиционные методы, основанные на выборочном анализе, становятся недостаточно эффективными при больших объемах информации. Использование алгоритмов машинного обучения и аналитических систем позволяет автоматизировать обработку данных, выявлять аномалии и риски в режиме реального времени. Это в свою очередь, повышает точность, скорость и объективность аудита, а также снижает влияние человеческого фактора и усиливает контроль за достоверностью финансовой отчетности.

Искусственный интеллект представляет собой совокупность технологий и методов, направленных на моделирование когнитивных функций человека, таких как обучение, анализ, прогнозирование и принятие решений. Основная особенность ИИ заключается в способности алгоритмов самостоятельно адаптироваться и улучшать результаты на основе накопленного опыта. Технология Больших данных охватывает процессы сбора, хранения, обработки и анализа колоссальных объемов разнообразной информации, которые невозможно обработать традиционными средствами. Для аудита эти категории являются ключевыми, поскольку позволяют переходить от выборочного анализа к полному охвату всех хозяйственных операций. Взаимосвязь ИИ и Больших данных формирует основу цифрового аудита, где интеллектуальные системы способны выявлять закономерности и аномалии, ранее недоступные традиционным методам анализа.

Обработка большого количества информации в короткие сроки является затруднительной. Технологии, основанные на ИИ, на сегодняшний момент способны реализовать задачи, которыми раньше занимались аудиторы. Применение ИИ в аудите могут выявлять закономерности, прогнозировать вероятные искажения и оценивать риски мошенничества. Незаменимые технологии на основе ИИ выступают, если необходимо выявить аномалии или рискованные транзакции. Также на основе инструментов, использующих искусственные нейронные связи, может позволить более эффективно выявлять несоответствия, области риска, что в условиях больших объемов финансовой и нефинансовой информации способно значительно ускорить проведение аудиторской проверки. Это в свою очередь, обосновывает переход от ручных процедур к автоматизированным системам анализа, способным обрабатывать миллионы операций за считанные секунды [10].

Большие данные становятся основной доказательной базой современного аудита, предоставляя аудитору доступ к полным массивам финансовой и нефинансовой информации. Это позволяет перейти от анализа выборок к исследованию всех транзакций, что значительно повысит достоверность аудиторских заключений. Большие данные вместо проверки на соответствие отчетности нормам переносят акцент на выявление аномалий и прогнозирование рисков. Использование Больших данных позволяет проводить комплексный анализ в режиме реального времени, что ранее не было возможно в рамках классического подхода [7].

Внедрение ИИ и Больших данных изменяет саму теоретическую парадигму аудита. Если ранее аудит рассматривался как инструмент подтверждения достоверности финансовой отчетности, то на сегодняшний день он приобретает функции прогнозирования, анализа эффективности и предупреждения рисков.

Теоретические исследования выделяют несколько моделей интеграции ИИ и Больших данных в аудиторскую практику: автоматизированные экспертные системы, алгоритмические платформы анализа и гибридные системы поддержки решений (табл. 1) [11].

Таблица 1

Сравнительная таблица моделей интеграции ИИ и Big Data  
в аудиторскую практику

| Критерий               | Автоматизированные экспертные системы                                                                                                                 | Алгоритмические платформы анализа (на основе ИИ)                                                                                                   | Гибридные системы поддержки решений                                                                                                                                                         |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Сущность и описание    | Программы, основанные на базе знаний и формализованных правилах, имитирующие рассуждения эксперта-аудитора в конкретной предметной области.           | Системы, использующие методы машинного обучения, нейронные сети и анализ больших данных для выявления закономерностей, аномалий и прогнозирования. | Интегрированные решения, сочетающие элементы экспертных систем и алгоритмических моделей (нейронные сети, генетические алгоритмы, нечеткая логика) для решения слабо формализованных задач. |
| Основные технологии    | Базы знаний, логический вывод, формализованные правила и сценарии принятия решения.                                                                   | Машинное обучение (с учителем и без), глубокое обучение, анализ больших данных, обработка естественного языка (NLP), компьютерное зрение.          | Комбинация экспертных правил, нейронных сетей, нечеткой логики, эволюционных и генетических алгоритмов.                                                                                     |
| Примеры задач в аудите | Оценка системы внутреннего контроля, анализ рисков, предварительная идентификация мошеннических факторов, структурирование аудиторских доказательств. | Выявление мошенничества, прогнозирование банкротства и непрерывности деятельности, построение аналитических процедур и кластеризация операций.     | Комплексная оценка рисков в условиях неопределённости, прогнозирование финансовых показателей, моделирование сценариев развития предприятия.                                                |
| Преимущества           | Высокая объяснимость решений и прозрачность логики вывода, опора на экспертные знания и стандарты аудита.                                             | Способность к самообучению и адаптации, работа с большими массивами данных, выявление скрытых взаимосвязей и нелинейных зависимостей.              | Гибкость и универсальность, возможность решать сложные и слабо формализованные задачи, объединяя экспертные и обучающиеся компоненты.                                                       |

Продолжение таблицы 1

|                            |                                                                                                                                                                 |                                                                                                                                                                |                                                                                                                                                                    |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Недостатки/<br>Ограничения | Ограниченность<br>областью<br>формализованных<br>знаний, отсутствие<br>механизма<br>самообучения,<br>необходимость<br>постоянного<br>обновления базы<br>знаний. | Сложность<br>интерпретации<br>решений («эффект<br>чёрного ящика»),<br>зависимость от<br>качества обучающих<br>данных, риск<br>алгоритмической<br>предвзятости. | Высокая сложность<br>проектирования и<br>верификации,<br>необходимость<br>междисциплинарной<br>интеграции технологий и<br>значительных<br>вычислительных ресурсов. |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Проведённое сравнение показывает, что каждая модель интеграции ИИ и Больших данных в аудиторскую практику имеет собственную функциональную нишу. Экспертные системы обеспечивают формализованный и объяснимый анализ, алгоритмические платформы — высокую адаптивность и масштабируемость, а гибридные решения объединяют преимущества обоих подходов, создавая основу для интеллектуального и предиктивного аудита. Наиболее перспективным направлением развития выступают именно гибридные системы, способные сочетать экспертное знание и машинное обучение в едином аналитическом контуре.

Таким образом, технологические аспекты интеграции ИИ и Больших данных в аудиторскую практику выходят за рамки простого применения отдельных программных решений. Речь идёт о построении комплексной цифровой экосистемы, в которой технологии обеспечивают непрерывный мониторинг, прогнозирование рисков и поддержку решений аудитора. Такая интеграция формирует основу для перехода аудита к новому уровню — интеллектуальному, автоматизированному и предиктивному контролю, обеспечивающему более высокое качество и прозрачность финансовой отчётности.

Рассмотрим современное состояние внедрения ИИ и Больших данных в аудиторскую практику.

Бесспорными лидерами в применении ИИ и Больших данных в аудиторской сфере являются США и Великобритания. Их крупнейшие аудиторские фирмы, такие как Deloitte, PwC, EY и KPMG, активно используют эти технологии для автоматизации рутинных процессов, повышения точности и сокращения времени на выполнение задач. Например, в статье «Is Artificial Intelligence Improving the Audit Process?» (2022) рассмотрено использование ИИ для анализа больших объемов данных и улучшения качества проверки бухгалтерских записей. Исследование показало, что внедрение ИИ снижает вероятность ошибок и помогает аудиторам более эффективно выявлять аномалии в финансовых отчетах [8].

Кроме того, в Великобритании Financial Reporting Council (FRC) также активно следит за внедрением новых технологий в аудиторской практике. Регулятор отмечает, что технологии Большие данные и аналитика данных в реальном времени позволяют повысить точность оценки финансовых рисков и эффективность аудита, особенно в таких сферах, как тестирование финансовых операций и оценка рисков мошенничества. Однако, несмотря на успешные примеры внедрения технологий, FRC также подчеркивает необходимость дальнейшего улучшения мониторинга и оценки качества таких аудиторских процедур. Наряду с Великобританией в США также есть регулирующий орган, ответственный за аудиторскую практику. Public Company Accounting Oversight Board (PCAOB) рассматривает использование технологий как ключевой элемент в повышении прозрачности и качества аудиторских проверок.

Помимо того, в некоторых странах, таких как Австралия и Германия, разрабатываются конкретные стандарты для использования ИИ в аудите, что предполагает обязательное соблюдение прозрачности в процессах обработки и анализа данных. Это способствует созданию более безопасной и регулируемой среды для внедрения новых технологий в аудиторскую практику.

В странах с развивающимися рынками внедрение ИИ и Больших данных сталкивается с определенными трудностями, связанными с нехваткой квалифицированных специалистов, ограниченными ресурсами и проблемами доступа к качественным данным. Например, в Малайзии исследование, проведенное в 2019 году, показало, что внешние аудиторы сталкиваются с барьерами в виде недостаточной подготовленности кадров и технологической инфраструктуры для полноценного использования аналитики данных. Однако исследование также показало, что при наличии должного обучения и поддержки со стороны крупных фирм, малые и средние аудиторские компании могут успешно интегрировать базовые аналитические инструменты в свою практику [9].

В Палестине также было проведено исследование, в котором изучалась роль обучения в принятии технологий Большие данные аудиторами. Результаты показали, что обучение и повышение квалификации имеют решающее значение для успешного внедрения аналитики данных. Аудиторы, прошедшие специальное обучение, значительно чаще принимали решение о внедрении новых технологий, что приводило к улучшению качества аудита и повышению его точности [4].

На основе анализа мирового опыта внедрения ИИ и Больших данных в аудиторскую практику можно выделить несколько ключевых моментов: несмотря на значительный прогресс в развитых странах, в развивающихся странах остаются вызовы, связанные с недостатком квалификации специалистов и доступом к качественным данным. Тем не менее, даже в этих условиях успешные примеры внедрения технологий Большие данные и ИИ показывают их

потенциал для улучшения качества аудита и повышения эффективности работы. Важно, чтобы в будущем компании и регуляторы продолжали развивать и адаптировать стандарты, направленные на повышение прозрачности и безопасности использования данных и ИИ в аудиторской практике.

Современный аудит активно трансформируется благодаря внедрению технологий искусственного интеллекта, выходя за рамки простой автоматизации рутинных задач. На практике это выражается в конкретных инструментах применения (табл. 2).

Таблица 2

Примеры применения технологий ИИ в аудите

| № | Инструменты                                                      | Применение в аудите                                                                                                                                                                |
|---|------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | NLP (обработка естественного языка)                              | Анализ неструктурированных данных (договоров, финансовых отчетов, писем) с целью выявления риск-контролей, несоответствий, слабых мест.                                            |
| 2 | Машинное обучение (ML) / анализ аномалий                         | Обучение моделей на исторических данных аудита/транзакций для выявления необычных шаблонов, ошибок, мошенничества; оптимизация распределения ресурсов аудита.                      |
| 3 | Роботизация/автоматизация (RPA)                                  | Автоматизация рутинных этапов аудита — сбор данных, подготовка рабочей документации, первичная проверка транзакций — что позволяет оптимизировать работу аудиторов                 |
| 4 | Планирование/Прогнозирование аудита и оценка рисков с помощью ИИ | Использование ИИ для анализа больших массивов данных (в том числе внешних источников: новости, соцсети, регуляторные сообщения) и определения зон, требующих повышенного внимания. |
| 5 | Непрерывный аудит / мониторинг в реальном времени                | Благодаря ИИ процессы аудита могут переходить от точечных проверок к постоянному мониторингу транзакций и рисков, что повышает эффективность и качество аудита.                    |
| 6 | Улучшение качества аудита / снижение ошибок                      | ИИ уменьшает вероятности корректировок отчётности и снижает количество аудиторских сборов.                                                                                         |

Таким образом, ИИ не просто ускоряет аудит, а кардинально меняет его глубину и фокус, превращая его из ретроспективной проверки в инструмент сквозного анализа и прогнозирования [6].

Схожие моменты с инструментами ИИ имеет аналитика больших данных в оценки рисков и формирования выборок для аудита. Это позволяет аудиторам анализировать большие объёмы данных, выявлять закономерности, аномалии и потенциальные риски, а также формировать выборки для проверки элементов, связанных с предметом аудита. Аналитика Больших данных включает как структурированные (например, финансовые отчёты), так и неструктурированные данные (электронные письма, посты в социальных сетях) [1, 5].

Представить техники и инструменты аналитике больших данных можно в таблице 3.

Таблица 3

Техники и инструменты, применяемые в аудите с использованием аналитики  
Больших данных

| № | Техника/<br>инструмент                                                 | Как она применяется в аудите (оценка рисков / выборка)                                                                                                                                                           |
|---|------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Анализ выбросов и аномалий (Outlier detection)                         | Автоматически выявление транзакций или записей, которые резко отличаются от нормальной истории или от контрольной группы – такие записи считаются высоким риском и подлежат дополнительной проверке.             |
| 2 | Машинное обучение для выборки (ML-для выборки)                         | Применение алгоритмов классификации или прогнозирования, чтобы выбрать из большой совокупности данные с высоким риском для тестирования – улучшает таргетинг выборки, уменьшая менее рискованные случаи.         |
| 3 | Визуализация и аналитика данных (Data Visualization + Dashboarding)    | Использование визуализаций и панелей мониторинга для выявления трендов, отклонений, паттернов в больших наборах данных – в ранней фазе аудита помогает оценить риск, наметить зоны высокого риска.               |
| 4 | Аналитика всей совокупности данных (100 % тестирование вместо выборки) | Вместо выборки — анализируются все записи/транзакции в данных (или значительная их часть) –повышается охват и снижается риск пропуска существенных искажений.                                                    |
| 5 | Процессный майнинг (Process Mining) и цифровые следы                   | Анализ логов, цифровых записей (ERP-систем), чтобы сопоставить фактический процесс с ожидаемым, выявить отклонения или несанкционированные шаги – помогает оценить контрольные риски, операционные риски.        |
| 6 | Прогнозная/предиктивная аналитика (Predictive Analytics)               | Использование исторических данных и моделей (регрессии, временные ряды, ML) для прогнозирования возможных искажений, финансовых затруднений, оценки непрерывности деятельности клиента – важна для оценки риска. |
| 7 | Интеграция внешних и нефинансовых данных                               | Помимо финансовых данных клиента, подключаются внешние данные (рынок, соцсети, сетевые данные) – помогает выявить дополнительные риски, которые не очевидны из финансовых отчётов.                               |

Таким образом, применение аналитики Больших данных, включая такие техники, как машинное обучение и анализ аномалий, знаменует переход аудита от выборочных проверок на основе усреднённых рисков к глубокому, сплошному и предиктивному анализу. Эти инструменты позволяют перераспределить ресурсы аудитора, целенаправленно фокусируясь на зонах повышенного риска, которые выявляются алгоритмически. В результате повышается как эффективность аудита (за счёт автоматизации рутинного отбора), так и его качество (за счёт увеличения вероятности обнаружения существенных искажений).

Особое внимание стоит уделить уровню цифровизации аудита в России и стран Содружества Независимых Государств (СНГ).

Текущий этап цифровизации аудита в России и странах СНГ

характеризуется активным, но асинхронным развитием. В Российской Федерации данный процесс приобрел характер системной государственной политики, в то время как в странах СНГ он остается в значительной степени фрагментированным и находится на стадии институционального становления.

В России цифровизация аудита реализуется по нескольким ключевым направлениям. На уровне внешнего государственного финансового контроля наблюдается наиболее значительный прогресс. Ярким примером служит деятельность Счётной палаты Российской Федерации, которая в 2024 году запустила проекты по созданию единой цифровой платформы и переходу к принципам «data-centricity» (ориентации на данные). Это подразумевает проведение аудита на основе качественных и полных данных с применением аналитических инструментов и методов, включая искусственный интеллект. Значительные бюджетные ассигнования (в 2022 году на создание цифровой платформы было запланировано 1,78 млрд рублей на период до 2024 года) свидетельствуют о высокой приоритетности этого направления. Результатом данной трансформации, по официальным заявлениям, стал рекордный возврат средств в бюджет и существенный экономический эффект [13, 14, 16].

Параллельно развивается цифровизация в сфере корпоративного бухгалтерского учета и аудита. Цифровая трансформация ведет к автоматизации рутинных операций, повышению оперативности и точности обработки информации, что, в свою очередь, закономерно меняет профессиональную роль бухгалтера и аудитора. Смещается фокус с выполнения контрольных процедур в сторону аналитики и работы с большими данными. Аналогичные процессы затрагивают и сферу внутреннего аудита и управления рисками, где автоматизация бизнес-процессов создает технологический фундамент для цифровизации контрольных функций, хотя и сопровождается ростом значимости рисков кибербезопасности [2, 3].

Таким образом, в России цифровизация аудита является не перспективой, а текущей реальностью, сопровождаемой реальными проектами, бюджетными инвестициями и трансформацией профессиональных парадигм.

В странах СНГ ситуация имеет иной характер. Наблюдаются позитивные институциональные инициативы, такие как проведение семинаров Совета руководителей высших органов аудита государств-участников СНГ по обмену практиками ИТ-аудита и заседания Координационного совета по бухгалтерскому учёту, на которых принимаются решения о развитии национальных систем на основе международных стандартов. Уровень зрелости, масштабы внедрения и стандартизация цифрового аудита в странах Содружества варьируются и находятся в стадии формирования [12, 15].

Ключевыми вызовами для стран СНГ остаются проблемы интеграции и обеспечения качества данных, дефицит кадров с необходимыми цифровыми компетенциями, отсутствие унифицированных стандартов и методик для

цифрового аудита, а также обеспечение безопасности и доверия к применяемым технологическим решениям. Несмотря на общую тенденцию к цифровой трансформации, Россия и страны СНГ демонстрируют «догоняющую» модель развития, где темпы и глубина изменений значительно отличаются.

Важно добавить, что с развитием ИИ и технологий Больших данных профессия аудитора претерпевает значительные изменения, которые касаются как технических, так и межличностных компетенций. Традиционные навыки, такие как бухгалтерская отчетность и анализ финансовых документов, становятся дополнением к новым обязанностям, связанным с управлением и интерпретацией больших объемов данных, а также использованию автоматизированных систем для аудита. Аудиторам необходимо овладеть основами программирования, машинного обучения и работы с аналитическими инструментами, которые позволяют обрабатывать и анализировать данные в реальном времени.

Компетенции в области информационных технологий становятся неотъемлемой частью работы современного аудитора, поскольку они позволяют эффективно интегрировать ИИ в процесс аудита и принимать обоснованные решения на основе данных, полученных с использованием алгоритмов. В то же время, важной частью работы аудитора остается способность оценивать и интерпретировать результаты, а также понимать возможные риски и ограничения технологий. Это требует от специалистов нового уровня критического мышления, способного учитывать не только количественные, но и качественные аспекты предоставленных данных.

Цифровая трансформация кардинально меняет роль аудитора, который становится не только исполнителем проверок, но и стратегическим консультантом, способным предложить бизнесу эффективные пути оптимизации и повышения прозрачности на всех уровнях управления. Аудиторы, использующие ИИ и Большие данные, могут предложить более точные прогнозы финансового состояния организации, выявлять скрытые риски и предоставлять рекомендации по улучшению бизнес-процессов.

В условиях цифровой трансформации аудиторы должны стать экспертами в области технологических изменений, а также уметь взаимодействовать с различными системами и инструментами, которые активно внедряются в корпоративную среду.

Важно отметить, что хотя ИИ и автоматизация процессов могут значительно повысить эффективность и точность аудита, роль человеческого фактора в принятии окончательных решений остается важной. Аудитор продолжает выполнять функцию оценки и контроля, не заменяемую машинными алгоритмами, особенно в вопросах, касающихся этики, стратегического анализа и взаимодействия с клиентами [10].

Можно выделить следующие преимущества интеграции ИИ и Больших данных в аудит (табл. 4).

Таблица 4

Преимущества интеграции ИИ и Больших данных в аудит [11]

| Область преимуществ                   | Пояснение                                                                 | Практический эффект                                                                                      |
|---------------------------------------|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Повышение эффективности и скорости    | Автоматизация рутинных операций (проверка транзакций, сверка документов). | Сокращение времени проверки на 30-50%, возможность проводить сплошной анализ вместо выборочного.         |
| Углубление аналитических возможностей | Выявление сложных аномалий, недоступных традиционным методам.             | Обнаружение скрытых рисков и схем мошенничества, повышение вероятности выявления существенных искажений. |
| Улучшение качества и точности         | Минимизация человеческого фактора, снижение субъективности в оценках.     | Повышение достоверности аудиторских заключений, сокращение количества ошибок.                            |
| Расширение горизонта анализа          | Использование внешних данных (соцсети, новости, рыночные индикаторы).     | Комплексная оценка рисков, прогнозирование финансового состояния компаний.                               |
| Непрерывность контроля                | Возможность мониторинга в режиме реального времени.                       | Своевременное выявление проблем, переход от периодического аудита к постоянному мониторингу.             |
| Оптимизация ресурсов                  | Автоматизация 60-70% рутинных операций.                                   | Высвобождение аудиторов для аналитических и консультационных задач.                                      |
| Стратегическая ценность               | Прогнозная аналитика и моделирование сценариев.                           | Консультации по оптимизации бизнес-процессов, повышение прозрачности управления.                         |

Таким образом, интеграция ИИ и Больших данных в аудит приносит комплексный эффект, а именно повышает скорость и точность проверок за счет автоматизации рутинных операций, расширяет аналитические возможности благодаря работе с разнородными данными и обеспечивает переход к непрерывному мониторингу. Это не только сокращает временные затраты на 30-50% и минимизирует человеческий фактор, но и преобразует роль аудитора - от контролера к стратегическому консультанту, способному прогнозировать риски и оптимизировать бизнес-процессы.

Однако на пути этой технологической трансформации возникает комплекс методологических, технических и нормативных барьеров, требующих системного решения (табл. 5).

Таким образом, интеграция ИИ и Больших данных в аудит, при всей ее перспективности, требует системного подхода, включающего дальнейшие научные исследования, адаптацию международных стандартов аудита и

разработку надежных методов валидации и контроля за интеллектуальными системами.

Таблица 5

Проблемы и ограничения интеграции ИИ и Больших данных в аудит [11]

| Категория проблем             | Конкретные ограничения                                                                                                    | Возможные последствия                                                                                           |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Методологические проблемы     | Высокая степень не структурированности аудиторских задач, сложность формализации профессионального суждения.              | Невозможность полной алгоритмизации аудита, ограниченность применения ИИ для задач, требующих опыта и интуиции. |
| Проблемы качества данных      | Недостаточная репрезентативность выборок, риск унаследованной предвзятости алгоритмов.                                    | Смещенные результаты, ошибочные выводы, воспроизводство субъективности разработчиков.                           |
| Технические ограничения       | Проблема «черного ящика» в сложных моделях, необходимость обработки больших объемов разнородной информации.               | Нарушение принципа профессионального скептицизма, трудности получения надлежащих аудиторских доказательств.     |
| Нормативные и этические риски | Не разработанность нормативной базы, вопросы конфиденциальности данных, неопределенность в разграничении ответственности. | Риски нарушения конфиденциальности, необходимость разработки новых этических стандартов и процедур контроля.    |
| Новые аудиторские риски       | Риски, связанные с несовершенством ИИ, целенаправленным обходом роботизированных средств контроля.                        | Появление новых схем мошенничества, адаптированных под слабые места алгоритмов.                                 |

Исходя из вышеуказанных преимуществ и проблем можно предложить некоторые рекомендации для аудиторских организаций по интеграции ИИ и Больших данных (табл. 6).

Внедрение этих рекомендаций позволит аудиторским организациям не только повысить операционную эффективность, но и значительно усилить ценность своих услуг для клиентов, превратившись из проверяющих в стратегических партнеров, способных прогнозировать риски и предлагать решения по оптимизации бизнеса.

Таким образом можно сделать вывод, что интеграция технологий искусственного интеллекта и Больших данных является не просто тенденцией, а фундаментальным фактором трансформации современной аудиторской практики. Эта интеграция знаменует переход от традиционного, ретроспективного и выборочного аудита к интеллектуальному, предиктивному и сплошному контролю.

Таблица 6

**Рекомендации для аудиторских организаций  
по интеграции ИИ и Больших данных**

| Рекомендация                      | Конкретные действия и мероприятия                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Ожидаемый результат / Выгода                                                                                                                                                                                                                               |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Поэтапное внедрение технологий | <p>Этап 1 - Пилотные проекты:</p> <ul style="list-style-type: none"> <li>• Автоматизация рутинных операций с использованием RPA.</li> <li>• Внедрение анализа аномалий для выявления подозрительных операций.</li> </ul> <p>Этап 2 - Масштабирование и углубление:</p> <ul style="list-style-type: none"> <li>• Внедрение гибридных систем поддержки решений, сочетающих экспертные правила и машинное обучение.</li> <li>• Использование ML для оценки рисков и прогнозирования.</li> </ul> | <ul style="list-style-type: none"> <li>• Снижение трудозатрат и количества рутинных ошибок.</li> <li>• Повышение скорости выполнения аудиторских процедур.</li> <li>• Более точная и обоснованная оценка рисков, проактивное выявление проблем.</li> </ul> |
| 2. Развитие кадрового потенциала  | <ul style="list-style-type: none"> <li>• Организация регулярного обучения для аудиторов.</li> <li>• Формирование кросс-функциональных команд для реализации проектов.</li> </ul>                                                                                                                                                                                                                                                                                                             | <ul style="list-style-type: none"> <li>• Формирование команды специалистов, способных эффективно работать с технологиями ИИ и Big Data.</li> <li>• Успешная интеграция технологий в аудиторские процессы благодаря синергии экспертиз.</li> </ul>          |
| 3. Качество и безопасность данных | <ul style="list-style-type: none"> <li>• Внедрение строгих процедур валидации, очистки и стандартизации данных.</li> <li>• Разработка и внедрение усиленных политик кибербезопасности и защиты конфиденциальной информации клиентов в соответствии с требованиями ФСБ и Банка России.</li> </ul>                                                                                                                                                                                             | <ul style="list-style-type: none"> <li>• Минимизация рисков алгоритмической предвзятости и получения некорректных результатов.</li> <li>• Соблюдение регуляторных требований, укрепление доверия клиентов и репутации компании.</li> </ul>                 |
| 4. Объяснимость и контроль        | <ul style="list-style-type: none"> <li>• Приоритет на внедрение решений с прозрачными алгоритмами.</li> <li>• Закрепление в внутренних стандартах принципа финальной ответственности аудитора-человека за заключение, а ИИ — инструмент поддержки.</li> </ul>                                                                                                                                                                                                                                | <ul style="list-style-type: none"> <li>• Возможность обосновать и защитить выводы, сделанные с помощью ИИ, перед клиентами и регуляторами.</li> <li>• Сохранение профессионального суждения и этических норм в аудите.</li> </ul>                          |
| 5. Участие в регулировании        | <ul style="list-style-type: none"> <li>• Инициация диалога с Институтом профессиональных бухгалтеров и аудиторов России, регуляторами для разработки отечественных стандартов по применению ИИ в аудите.</li> <li>• Разработка внутренних этических стандартов, регламентирующих вопросы ответственности, конфиденциальности и скептицизма при работе с ИИ.</li> </ul>                                                                                                                       | <ul style="list-style-type: none"> <li>• Формирование благоприятной и предсказуемой нормативной среды.</li> <li>• Управление юридическими и репутационными рисками, связанными с использованием ИИ.</li> </ul>                                             |

*Продолжение таблицы 6*

|                                      |                                                                                                                                                                                            |                                                                                                                                                                                                                              |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6.<br>Непрерывный аудит и мониторинг | <ul style="list-style-type: none"> <li>Разработка систем непрерывного мониторинга ключевых транзакций и показателей клиентов в режиме, близком к реальному времени, на базе ИИ.</li> </ul> | <ul style="list-style-type: none"> <li>Оперативное выявление аномалий и рисков, а не постфактум.</li> <li>Смещение фокуса с периодических проверок на постоянный контроль, повышение ценности аудита для клиента.</li> </ul> |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

ИИ и Большие данные кардинально меняют саму парадигму аудита. Аудит перестает быть лишь инструментом подтверждения достоверности отчетности, приобретая функции прогнозирования рисков, комплексного анализа эффективности бизнес-процессов и обеспечения непрерывного мониторинга. Анализ показал, что наиболее перспективной моделью интеграции выступают гибридные системы, которые сочетают в себе строгость экспертных знаний и адаптивность машинного обучения, что позволяет решать сложные, слабо формализованные задачи.

Сравнительный анализ международного опыта выявил асинхронность этого процесса: в то время как развитые страны (США, Великобритания) демонстрируют зрелые примеры внедрения, в России и странах СНГ цифровизация аудита находится на активной, но неравномерной стадии развития, требующей преодоления инфраструктурных и кадровых вызовов.

Несмотря на очевидные преимущества — такие как рост эффективности, глубины анализа и достоверности заключений — внедрение данных технологий сопряжено с комплексом методологических, технических и нормативных проблем. К ним относятся проблема «черного ящика», риски качества данных, недостаточная развитость регулирования и новые формы аудиторских рисков.

В этой связи, предложенные в работе рекомендации для аудиторских организаций — такие как поэтапное внедрение, развитие кадрового потенциала, обеспечение объяснимости решений и активное участие в формировании нормативной базы — носят практико-ориентированный характер. Их реализация позволит не только минимизировать сопутствующие риски, но и максимально использовать потенциал технологий для перехода от роли контролера к роли стратегического консультанта, повышающего прозрачность и устойчивость бизнеса.

Таким образом, интеграция ИИ и Больших данных представляет собой закономерный и необратимый этап эволюции аудита. Его успешная реализация будет определяться способностью профессионального сообщества адаптироваться к новым условиям, превращая технологические вызовы в возможности для повышения качества, ценности и общественного доверия к аудиторской профессии.

## Список литературы

1. Казакова Н. А., Мельник М. В., Дудорова Е. В. Перспективы внедрения аналитики больших данных в аудиторскую профессию // GAAP.RU. 2021. № 3. URL: [https://gaap.ru/articles/Perspektivy\\_vnedreniya\\_analitiki\\_bolshikh\\_dannykh\\_v\\_auditorskuyu\\_professiyu/?ysclid=mhmcrrh7742787381470](https://gaap.ru/articles/Perspektivy_vnedreniya_analitiki_bolshikh_dannykh_v_auditorskuyu_professiyu/?ysclid=mhmcrrh7742787381470)
2. Каламанова Е. Н., Проданова Н. А. Перспективы развития внутреннего аудита в условиях цифровизации экономики // Панорама. - 2025. Бухучет в здравоохранении № 1. URL: <https://panor.ru/articles/perspektivy-razvitiya-vnutrennego-audita-v-usloviyakh-tsifrovizatsii-ekonomiki/110004.html?ysclid=mhmdcty08i903259590#>
3. Лымарь А. И., Каурова О. В. Цифровая трансформация бухгалтерского учета и аудита в России: тенденции и перспективы // OpenScience. - 2025. - Т. 7. - №1. - С. 131-142. URL: <https://journals.rcsi.science/2658-7939/article/view/305164?ysclid=mhmda6jckm515865561>
4. Моат Абу А. Р., Мохд Назли М. Н., Залайла С. Роль обучения во внедрении аналитики больших данных: эмпирическое исследование аудиторов с использованием модели принятия технологий // EJBRM. 2024. – Т. 22. № 2. URL: <https://academic-publishing.org/index.php/ejbrm/article/view/3752?>
5. Парамонов П. В. Развитие методики аудита в условиях цифровизации с помощью аналитики аудиторских данных / П. В. Парамонов. — Текст : непосредственный // Молодой ученый. — 2021. — № 19 (361). — С. 131-133. — URL: <https://moluch.ru/archive/361/80850>.
6. Титков Д. И., Резниченко С. А. Революция в аудите информационной безопасности: искусственный интеллект // Вестник науки. 2024. №4 (73). URL: <https://cyberleninka.ru/article/n/revolyutsiya-v-audite-informatsionnoy-bezopasnosti-iskusstvennyy-intellekt>
7. Урусов А. Т. Особенности интеграции аналитики больших данных в аудиторские процедуры // StudNet. 2020. №5. URL: <https://cyberleninka.ru/article/n/osobennosti-integratsii-analitiki-bolshih-dannyh-v-auditorskie-protsedury>
8. Федик А., Ходсон Д., Химич Н., Федик Т. Улучшает ли искусственный интеллект процесс аудита? // Springer Nature Link. 2022. – Т. 27. С. 938-985. URL: <https://link.springer.com/article/10.1007/s11142-022-09697-x>
9. Че Хуссейн Н. Х., Инь К. В., Ленг Л. В., Фонг Л. С., Ва Х. К. Изучение внедрения анализа аудиторских данных среди внешних аудиторов в Малайзии // Информационный менеджмент и обзор бизнеса. 2025. – Т. 17. № 2(I)S. С. 84-95. URL: [https://doi.org/10.22610/imbr.v17i2\(I\)S.4568](https://doi.org/10.22610/imbr.v17i2(I)S.4568)
10. Элоян Н. В., Какосьян Р. М. Инновационные подходы в аудите:

использование искусственного интеллекта и машинного оборудования // Электронная наука. 2023. №1. URL: <https://cyberleninka.ru/article/n/innovatsionnye-podhody-v-audite-ispolzovanie-iskusstvennogo-intellekta-i-mashinnogo-oborudovaniya>

11. Якимова В. А. Возможности и перспективы использования цифровых технологий в аудиторской деятельности // Вестник Санкт-Петербургского университета. Экономика. – Санкт-Петербург: 2020. – Т. 36. Вып. 2. С. 287-318. URL: <https://economicsjournal.spbu.ru/article/download/7764/5705>

12. ВОА СНГ обменялись опытом проведения аудита государственных информационных систем // ИНТОСАИ: сайт. 2024. – URL: <https://intosairussia.org/ru/novosti-media/novosti/voa-sng-obmenyalis-opytom-provedeniya-audita-gosudarstvennykh-informatsionnykh-sistem.html?ysclid=mhmdlqzq14600705055>

13. В России строят цифровую платформу государственного аудита за 1,78 миллиарда // Cnews: сайт. 2022. – URL: [https://www.cnews.ru/news/top/2022-02-01\\_vlasti\\_potratyat\\_178\\_mlrdrub?ysclid=mhmd4h4wcm848529947](https://www.cnews.ru/news/top/2022-02-01_vlasti_potratyat_178_mlrdrub?ysclid=mhmd4h4wcm848529947)

14. Информационные технологии в Счетной палате Российской Федерации // T Adviser.com: сайт. 2024. – URL: [https://tadviser.com/index.php/Article:Information\\_technologies\\_in\\_the\\_Accounts\\_Chamber\\_of\\_the\\_Russian\\_Federation?ysclid=mhmcxc6gov962425143](https://tadviser.com/index.php/Article:Information_technologies_in_the_Accounts_Chamber_of_the_Russian_Federation?ysclid=mhmcxc6gov962425143)

15. Национальные системы бухучета и аудита в странах СНГ продолжают развивать на основе международных стандартов // РСПП.РУ: сайт. 2022. – URL: <https://rspp.ru/events/news/natsionalnye-sistemy-bukhucheta-i-audita-v-stranakh-sng-prodolzhat-razvivat-na-osnove-mezhdunarodnykh-standartov-636402a32752c/?ysclid=mhmdo5cziw920123160>

16. Цифровизация помогла Счетной палате поставить рекорд по возвратным средствам // Comnews: сайт. 2025. – URL: <https://www.comnews.ru/content/238225/2025-03-13/2025-w11/1008/cifrovizaciya-pomogla-schetnoy-palate-postavit-rekord-vozvratnym-sredstvam?ysclid=mhmd6vreig152118406>

**Курашова Анна Андреевна**

кандидат экономических наук, доцент

доцент кафедры экономической экспертизы и финансового мониторинга

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

**Кармашов Максим Сергеевич**

**Чумичёв Виктор Алексеевич**

студенты 4 курса

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

## **Кибербезопасность в цифровом аудите: теоретико-методологические аспекты защиты данных**

**Аннотация.** В контексте глобальной цифровой трансформации происходит теоретическое переосмысление парадигмы аудиторской деятельности. Статья посвящена исследованию концептуальных основ кибербезопасности как неотъемлемого элемента методологии цифрового аудита. Анализируется теоретическая база, определяющая взаимосвязь между цифровой трансформацией аудита и эволюцией киберугроз. Рассматриваются методологические подходы к интеграции принципов информационной безопасности в теоретические конструкции современного аудита. Особое внимание уделяется концептуальным аспектам применения технологий распределенного реестра и искусственного интеллекта с позиций теоретического осмысления их роли в обеспечении достоверности аудиторских процедур.

**Ключевые слова:** цифровой аудит, кибербезопасность, теоретическая парадигма, методология, киберугрозы, информационная безопасность, блокчейн, искусственный интеллект, аудиторские стандарты.

Современная экономическая теория констатирует фундаментальную трансформацию природы аудиторской деятельности в условиях цифровой экономики. Теоретическое осмысление цифрового аудита требует выхода за рамки традиционных представлений о аудите как о ретроспективной верификации отчетности. Цифровой аудит представляет собой сложную многоуровневую систему непрерывного мониторинга и анализа данных, основанную на принципиально новых методологических подходах [6].

Теоретическая значимость проблемы кибербезопасности в цифровом аудите обусловлена необходимостью концептуального осмысления новых видов рисков, порождаемых цифровой средой. Если в традиционной аудиторской парадигме риски были связаны преимущественно с человеческим фактором и системами внутреннего контроля, то в цифровой среде на первый план выходят

риски, связанные с уязвимостью информационных систем и целостностью данных [8].

Концептуальный анализ проблем кибербезопасности в цифровом аудите позволяет выявить методологические противоречия между требованием открытости и прозрачности данных и необходимостью обеспечения их конфиденциальности и защиты. Теоретическое разрешение этого противоречия требует разработки новых концептуальных подходов к организации аудиторской деятельности.

Теоретическая платформа цифрового аудита основывается на синтезе нескольких научных направлений: теории аудита, кибернетики, теории информации и компьютерных наук. С методологической точки зрения, цифровой аудит можно рассматривать как информационную систему, предназначенную для снижения информационного риска пользователей финансовой отчетности [7].

Кибербезопасность в данном контексте выступает не как внешняя по отношению к аудиту функция, а как неотъемлемый элемент его теоретической конструкции. Это требует пересмотра традиционных аудиторских концепций и принципов. Принцип профессионального скептицизма, например, должен распространяться не только на действия персонала проверяемого субъекта, но и на надежность информационных систем и алгоритмов обработки данных [10].

Теоретический анализ позволяет выделить три основных уровня интеграции кибербезопасности в методологию цифрового аудита:

1. концептуальный уровень (определение целей и принципов);
2. методологический уровень (разработка процедур и методик);
3. технологический уровень (реализация технических решений).

С теоретической точки зрения, угрозы кибербезопасности в цифровом аудите могут быть классифицированы на основе нарушения фундаментальных принципов информационной безопасности. Концепция CIA-триады (Confidentiality, Integrity, Availability) получает новое звучание в контексте цифрового аудита [9].

Нарушение конфиденциальности в цифровом аудите имеет не только техническое, но и концептуальное измерение. Теоретически, утечка аудиторских данных подрывает саму сущность аудита как доверительной процедуры. Конфиденциальность становится не просто техническим требованием, а методологическим принципом, определяющим этические и профессиональные основы аудиторской деятельности [6].

Теоретическое осмысление угроз целостности данных требует рассмотрения не только внешних атак, но и внутренних уязвимостей алгоритмов обработки данных. С методологической точки зрения, целостность данных должна обеспечиваться на всех этапах аудиторского процесса – от сбора доказательств до формирования заключения.

Концептуальный анализ применения технологии блокчейн в цифровом аудите показывает, что ее значение выходит за рамки простого технического решения. Блокчейн теоретически может служить основой для создания новой парадигмы аудита, основанной на принципах неизменяемости и прозрачности [7].

С теоретической точки зрения, блокчейн позволяет реализовать концепцию "аудита как процесса" в противовес традиционной модели "аудита как моментальной проверки". Это открывает новые методологические перспективы для развития теории непрерывного аудита и мониторинга.

Искусственный интеллект и машинное обучение также требуют теоретического осмысления с позиций аудиторской методологии. Концептуальный вопрос заключается в том, как интегрировать алгоритмическую прозрачность в традиционные аудиторские процедуры. Теоретически, использование AI ставит новые вопросы относительно профессионального суждения аудитора и его взаимодействия с интеллектуальными системами [8].

С методологической точки зрения, интеграция кибербезопасности в цифровой аудит сталкивается с несколькими концептуальными проблемами. Во-первых, существует методологический разрыв между языком и понятийным аппаратом специалистов по информационной безопасности и аудиторов. Это требует разработки единой теоретической платформы и понятийного аппарата [9].

Во-вторых, методологическую проблему представляет собой согласование международных стандартов аудита и стандартов информационной безопасности. Теоретически, это требует пересмотра и расширения традиционных аудиторских стандартов с учетом новых рисков цифровой среды.

В-третьих, концептуальной проблемой является определение границ ответственности аудитора в области кибербезопасности. Теоретическое решение этой проблемы требует четкого разграничения между оценкой рисков кибербезопасности как элемента аудита финансовой отчетности и специализированным аудитом информационной безопасности.

Теоретическое развитие цифрового аудита в контексте кибербезопасности видится в нескольких направлениях. Перспективным представляется развитие теории «киберустойчивого аудита», которая бы интегрировала концепции устойчивости и адаптивности в методологию аудиторской деятельности [10].

Другим направлением теоретического развития является концепция «доверительных вычислений», которая позволяет теоретически переосмыслить подходы к обеспечению конфиденциальности данных в процессе их обработки.

Теоретическую ценность представляет также разработка концепции «цифрового аудиторского доказательства», которая бы учитывала особенности электронных доказательств и специфику их защиты в цифровой среде.

Теоретический анализ проблем кибербезопасности в цифровом аудите позволяет сделать вывод о необходимости фундаментального пересмотра методологических основ аудиторской деятельности. Кибербезопасность не может рассматриваться как внешний по отношению к аудиту фактор; она должна быть интегрирована в саму теоретическую конструкцию цифрового аудита.

Концептуальное осмысление современных технологий, таких как блокчейн и искусственный интеллект, открывает новые перспективы для развития теории аудита. Однако их внедрение требует решения методологических проблем, связанных с интеграцией новых понятий и подходов в существующую теоретическую парадигму.

Дальнейшее теоретическое исследование должно быть направлено на разработку целостной концепции цифрового аудита, которая бы органично интегрировала принципы кибербезопасности в методологию аудиторской деятельности. Это потребует междисциплинарного подхода, объединяющего достижения теории аудита, компьютерных наук и теории информации.

Теоретическая разработка этих вопросов будет способствовать не только развитию методологии аудита, но и укреплению доверия к институту аудита в условиях цифровой экономики, обеспечивая теоретическую основу для практической реализации принципов кибербезопасности в аудиторской деятельности.

### Список литературы

1. ISO/IEC 27001:2013. Информационные технологии. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности. Требования. — Введен 2014-01-01.
2. ГОСТ Р ИСО/МЭК 27001-2021. Информационные технологии. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности. Требования. — Введен 2022-01-01.
3. ГОСТ Р 57580.1-2017. Защита информации. Требования к системам информационной безопасности финансовых организаций. Часть 1. Оценка соответствия и отчетность. — Введен 2018-01-01.
4. СТО БР ИББС-1.1-2007. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности. — Утвержден Центральным банком РФ от 28.04.2007.
5. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О защите персональных данных». — Действует с 1 января 2021 г.
6. Фишинг и вредоносное ПО как основные угрозы при цифровой трансформации / IBM X-Force Threat Intelligence Index 2025. — Электронный ресурс. — Режим доступа: <https://www.ibm.com/thought-leadership/institute->

---

[business-value/en-us/report/2025-threat-intelligence-index](https://business-value/en-us/report/2025-threat-intelligence-index) (дата обращения: 21.11.2025).

7. Аудит информационной безопасности: определение, виды и рекомендации / DDoS-Guard. — Электронный ресурс. — Режим доступа: <https://ddos-guard.ru/blog/audit-kiberbezopasnosti> (дата обращения: 21.11.2025).

8. Кибербезопасность и защита данных: аудиты соответствия / BradyWare. — Электронный ресурс. — Режим доступа: <https://bradyware.com/cybersecurity-data-privacy-audits/> (дата обращения: 21.11.2025).

9. ГОСТы по аудиту информационной безопасности: принципы и требования / RosGOSTS. — Электронный ресурс. — Режим доступа: <https://rosgosts.ru/blog/gosty-po-auditu-informaczionnoj-bezopasnosti/> (дата обращения: 21.11.2025).

10. Методология COBIT и ITIL в аудите информационной безопасности / Innostage Group. — Электронный ресурс. — Режим доступа: <https://innostage-group.ru/press/media/metodichnyy-kiberbez-vzglyad-na-til-i-cobit-pod-prizmoy-zashchity-informatsii/> (дата обращение: 21.11.2025).

11. Угрозы информационной безопасности в эпоху цифровой трансформации / Habr. — Электронный ресурс. — Режим доступа: <https://habr.com/ru/articles/544932/> (дата обращения: 21.11.2025).

12. Двухфакторная аутентификация и сквозное шифрование в защите данных / Secuteck. — Электронный ресурс. — Режим доступа: <https://www.secuteck.ru/articles/skvoznoe-shifrovanie-i-dvuhfaktornaya-autentifikaciya-v-sovremennom-internete> (дата обращения: 21.11.2025).

**Кушарев Дмитрий Владимирович**

студент 5 курса

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

Научный руководитель

**Кузовлева Нина Фёдоровна**

кандидат экономических наук

профессор кафедры экономической экспертизы и финансового мониторинга

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

## **Совершенствование системы противодействия легализации преступных доходов в банковской сфере**

**Аннотация.** В статье рассматриваются актуальные проблемы противодействия легализации (отмыванию) доходов, полученных преступным путем, в российской банковской системе. Анализируются изменения нормативно-правового регулирования 2025–2026 гг., включая исключение института банковских платежных агентов из системы идентификации, внедрение цифровых инструментов контроля и новые требования Банка России. Предлагается комплексная модель совершенствования AML-системы на основе технологической платформы «Знай своего клиента» и искусственного интеллекта, направленная на снижение регуляторной нагрузки при одновременном повышении эффективности выявления сомнительных операций. Формулируются выводы о парадоксальной ситуации, при которой ужесточение внутреннего контроля сопровождается внешнеполитическими рисками включения России в «черные списки» ФАТФ.

**Ключевые слова:** легализация доходов, ПОД/ФТ, банковский сектор, 115-ФЗ, идентификация клиентов, дропперство, риск-ориентированный подход, цифровой рубль, AML/CFT, Банк России.

Актуальность проблемы противодействия легализации преступных доходов (ПОД/ФТ) в банковском секторе России обусловлена одновременным действием разнонаправленных факторов. С одной стороны, национальная платежная система сталкивается с усложнением мошеннических схем: распространение «дропперства», нелегальный оборот криптовалют и вывод капиталов за рубеж требуют адекватного ответа регулятора. С другой стороны, сами банки испытывают повышенную нагрузку из-за требований по идентификации клиентов и предоставлению отчетности, что нередко приводит к комплаенс-эксцессам, необоснованным блокировкам счетов добросовестных предпринимателей.

Ситуация осложняется внешним контекстом. В конце января 2026 года Европейский союз включил Россию в свой «черный список» юрисдикций с недостаточными мерами по борьбе с отмыванием денег. Это решение носит во многом политический характер, однако оно создает репутационные риски и затрудняет корреспондентские отношения с банками из «дружественных» стран. В связи с этим поиск внутренних резервов для повышения прозрачности финансовых потоков становится не просто задачей ведомственного контроля, а фактором сохранения международной платежеспособности страны.

Нормативно-правовую базу исследования составили ключевые акты, регулирующие сферу ПОД/ФТ в РФ. Основополагающим является Федеральный закон от 07.08.2001 № 115-ФЗ, в который в феврале 2026 года были внесены изменения. Данным актом из статьи 7 закона исключены положения, позволявшие банковским платежным агентам (Далее – БПА) проводить идентификацию и упрощенную идентификацию физических лиц. Одновременно были скорректированы нормы Федерального закона «О национальной платежной системе» (161-ФЗ), возвращающие БПА к их исходной функции – приему и выдаче наличных денежных средств без права комплаенс-оценки клиентов.

Подзаконное регулирование представлено Положением Банка России № 860-П, детализирующим правила внутреннего контроля (ПВК) для кредитных организаций. Важным источником стали «Основные направления развития финансового рынка РФ на 2026–2028 годы», где ЦБ РФ декларирует переход к «умному надзору» с акцентом на проактивное выявление рисков и широкое использование искусственного интеллекта (Далее – ИИ).

Анализ современного состояния системы ПОД/ФТ в банковском секторе России позволяет выделить три ключевых вектора трансформации: централизация идентификации, цифровизация мониторинга и ребалансировка ответственности.

1. Реформа идентификации клиентов. Принятый 10 февраля 2026 года Федеральный закон №44-ФЗ («О внесении изменений в статью 7 Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма» и Федеральный закон «О национальной платёжной системе»») исключил возможность привлечения банковских платёжных агентов (БПА) для проведения идентификации (в том числе упрощённой) физических лиц. Исключение данных субъектов из цепочки комплаенса, по оценкам экспертов Data Sapience, должно привести к сокращению числа «номинальных» кошельков, используемых дропперами. Однако в краткосрочной перспективе это создает риски для микрофинансовых организаций (МФО) и онлайн-агрегаторов, которым придется либо интегрироваться с банками на новом техническом уровне, либо покинуть рынок.

2. Внедрение «цифрового следа». Банк России совместно с Минцифрой запускает систему обязательной привязки ИНН ко всем банковским счетам физических лиц и создание единого реестра идентификационных номеров устройств (IMEI-кодов смартфонов). Это позволяет банкам автоматически «сшивать» данные: клиент, использующий 10 разных сим-карт на одном телефоне для обналичивания денег, будет мгновенно идентифицирован системой финмониторинга. Параллельно регулятор готовит введение с 1 сентября 2026 года ограничение на количество карт в одном банке, а в 2027 году – на общее количество банковских карт, выпускаемых на одного человека.

3. Совершенствование системы риск-ориентированного подхода «Знай своего клиента» (ЗСК). На сегодняшний день ЦБ РФ присваивает юридическим лицам «цветовые» уровни риска: «зеленый» (низкий), «желтый» (средний) и «красный» (высокий). Однако большая часть жалоб бизнеса касаются необоснованного попадания в «красную» зону из-за формальных критериев, например, работа с наличностью по роду деятельности.

Предлагается внедрить «презумпцию добросовестности» в алгоритмы автоматического скоринга.

3.1. Для «зеленой» зоны – полное освобождение от обязательного репортинга по операциям с недвижимостью и отмена ежеквартальной подачи формализованных сведений.

3.2. Для «желтой» зоны – введение «периода реабилитации» (6 месяцев): если за это время не зафиксировано новых странных транзакций, банк обязан перевести клиента в «зеленую» зону без участия ЦБ, что снизит административное давление.

3.3. Для борьбы с «дропперами» – введение обязательного скоринга через Единую биометрическую систему для физлиц при попытке получить онлайн-кредит или открыть счет, если по его паспорту уже были блокировки.

В качестве иллюстрации эффективности предлагаемых мер рассмотрим таблицу 1, в которой проведен анализ новых инструментов ПОД/ФТ в банковской сфере Российской Федерации.

Технологический базис этих изменений уже заложен. 22 апреля 2026 года на форуме «ФИНМОНИТОР» обсуждались VI-driven подходы к выявлению R2P-дроппов (переводы между физлицами в целях обналичивания) и использование ИИ для верификации происхождения криптовалют [4].

В ответ на антироссийские санкции ЦБ РФ ускорил пилотирование цифрового рубля, который, благодаря программируемости, позволяет отслеживать целевое использование средств на уровне смарт-контрактов, устраняя саму возможность легализации через цепочки подставных фирм.

Таблица 1

Анализ новых инструментов ПОД/ФТ в банковской сфере РФ

| Инструмент контроля        | Суть нововведения                                        | Целевая нагрузка на банки (изменение)                            |
|----------------------------|----------------------------------------------------------|------------------------------------------------------------------|
| Единый идентификатор (ИНН) | Обязательная привязка ИНН ко всем счетам (физлица)       | Снижение целевой нагрузки на банки, автоматизация дедубликации   |
| Контроль номеров банкнот   | Сканирование серийных номеров купюр в банкоматах         | Высокая целевая нагрузка на банки требует модернизации устройств |
| Реестр устройств           | Запрет мобильного банка на незарегистрированных гаджетах | Средняя целевая нагрузка на банки, интеграция с базами Минцифры  |

Кроме того, заслуживает отдельного внимания кадровая составляющая системы ПОД/ФТ. Даже самые совершенные алгоритмы остаются бесполезными при отсутствии квалифицированных специалистов. В настоящее время в России наблюдается дефицит AML-аналитиков (по оценкам АРБ, не менее 3 тыс. вакансий по стране), при этом типичный банк тратит до 40% бюджета комплаенс-подразделения на обучение персонала работе с обновляющимися требованиями.

Проведенное исследование позволяет сформулировать следующие выводы о состоянии и перспективах совершенствования системы ПОД/ФТ в банковской сфере России.

1. Законодательный тренд на централизацию. Устранение банковских платежных агентов из процесса идентификации является вынужденной и своевременной мерой. Она закрывает главную лазейку для дропперов, но требует от регулятора создания переходного периода для легальных агрегаторов, чтобы избежать коллапса в сегменте микроплатежей.

2. Технологическая гонка. Банк России и Росфинмониторинг создали одну из самых технологичных систем финмониторинга в мире (сквозная идентификация по ИНН, контроль номеров банкнот, реестр устройств). Однако парадокс заключается в том, что санкционное давление и политические решения ухудшают эти усилия на международной арене. В этой связи приоритетом должно стать не столько международное признание, сколько экономический эффект в виде сокращения теневого сектора внутри страны.

3. Рекомендации по совершенствованию. Для банков целесообразно внедрение «адаптивного комплаенса»: переход от тотального контроля к превентивному. Кредитным организациям рекомендуется сократить долю ручного труда AML-аналитиков путем внедрения нейросетей для выстраивания связей между транзакциями.

## Список литературы

1. Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 07.08.2001 N 115-ФЗ [Электронный ресурс] - [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_32834/](https://www.consultant.ru/document/cons_doc_LAW_32834/)
2. Банк России. Положение № 860-П «О требованиях к правилам внутреннего контроля в целях ПОД/ФТ» РФ [Электронный ресурс] - <https://base.garant.ru/412480152/>
3. Минцифры РФ / Росфинмониторинг. Перспективы развития удаленной идентификации и ЕБС. Доклад на ФИНМОНИТОР 2026 / А. Смирнов [Электронный ресурс] - <https://cbr.ru/press/event/?id=21066>
4. Форум «ФИНМОНИТОР» [Электронный ресурс] - <https://sdlinfo.ru/?p=22581>

**Лашинская Наталья Викторовна**

доцент кафедры экономической экспертизы и финансового мониторинга  
ФГБОУ ВО «МИРЭА – Российский технологический университет»  
Россия, г. Москва

**Кемпи Анна Дмитриевна**

студент 5 курса  
ФГБОУ ВО «МИРЭА – Российский технологический университет»  
Россия, г. Москва

## **Актуальные методы контроля расчетов по заработной плате с целью повышения системы экономической безопасности страховых компаний**

**Аннотация.** В статье исследованы и раскрыты особенности расчетов по оплате труда страховых компаний. Обоснована важность контрольных функций, связанных с начислением заработной платы и проведением анализа начисления заработной, исследована система методов постпроверки основных начислений. Все эти вопросы связаны напрямую с обеспечением финансовой и экономической безопасности страховых компаний.

**Ключевые слова:** контроль расчетов по заработной плате, экономическая безопасность, страховые компании, комплекс методов контроля, система контроля расчета заработной платы (СКРЗП), нештатные сотрудники.

В современных экономических условиях, характеризующихся высокой волатильностью финансовых рынков, усилением санкционного давления и ростом требований со стороны регуляторов (в частности, Банка России), вопросы обеспечения экономической безопасности страховых компаний приобретают первостепенное значение. Страховой рынок, оперирующий значительными объемами денежных средств населения и корпораций, является одной из ключевых подсистем финансовой безопасности государства. В этой связи особую уязвимость представляют собой зоны внутреннего контроля, и одним из наиболее чувствительных участков являются вопросы действующей системы оплаты труда

Ошибки, злоупотребления или мошеннические действия в области оплаты труда влекут за собой не только прямые финансовые потери, но и репутационные риски, снижение лояльности персонала и, как следствие, падение эффективности бизнеса. В соответствии с этим, актуальность данной темы подтверждается высокой долей переменной части вознаграждения (бонусов, комиссионных), свойственная страховому сектору, объемом нештатных сотрудников, а также усложненной системой учета начисления заработной платы.

Проведение анализа системы контроля расчета заработной платы (далее – СКРЗП) является ключевым параметром в системе операционного бизнеса

любой компании. Для проведения анализа выделим следующие характеристики, обуславливающие показатель сложности СКРЗП страховых компаний.

1. 60-65% страховых агентов являются штатными сотрудниками, расчет заработной платы которых – это процесс с объективными особенностями (учет НДФЛ и страховых взносов; порядок оплаты вознаграждения, совместно с ревизией корректности договора гражданско-правового характера (далее – договора ГПХ); особенности предоставления налоговых документов физическим лицам, работающим по договорам ГПХ и т.д.).

2. Особенности сдачи налоговой и статистической отчетности, учитывая особенности бизнеса (П-4; П-4 НЗ; 6-НДФЛ; СЗВ-ТД; РСВ и т.д.).

3. Особенности учета заработной платы самозанятых.

Стоит отметить, что основная угроза некорректного расчета заработной платы, а также ошибки сопровождающего функционала обусловлены не совершенностью используемой информационной системы. Многие расчетные программы, которые используются бизнесом, адаптируются под саму модель бизнеса разработчиками. В основном, разработчики данных систем – это внутренние сотрудники компании, основной функционал которых достаточно близок к тому, чтобы создать адаптивную информационную систему.

Однако, во многом, такие программы, как 1С:ЗУП, 1С:Предприятие достаточно адаптивны, но несовершенны. Например, при расчете заработной платы в 1С:ЗУП существуют ресурсы для разработки индивидуальных проверочных отчетов. Основная проблема состоит не в процессе и методике разработки отчета для проверки начислений, а в самой информационной базе: платформа 1С:ЗУП недостаточно совершенна для формирования точного безошибочного расчета.

Таким образом, большинство страховых компаний используют ручные методы проверки расчетов с 20-30% автоматизации.

Рассмотрим основные характеристики, приведенные выше, усложняющие процесс проверки заработной платы. Так, для штатных сотрудников страховая компания выступает налоговым агентом. Удержание НДФЛ (обычно 13% или 15% при превышении порога доходов) производится с каждой суммы выплаченного вознаграждения.

Важным показателем является корректность применения ст. 221 НК РФ [2]. Агенты имеют право на профессиональный налоговый вычет в сумме фактически произведенных и документально подтвержденных расходов, связанных с оказанием услуг. Контроль за обоснованностью этих вычетов – критическая зона для предотвращения налоговых рисков компании [2].

Так, основная особенность НДФЛ по страховым агентам заключается в том, что страховым агентом в данном случае выступает работодатель, то есть страховая компания, являющаяся заказчиком по договору ГПХ [1;3].

Также с 1 января 2023 года в России введен единый платеж по страховым

вносам на обязательное пенсионное, социальное и медстрахование. Это следует из пункта 3 статьи 425 НК РФ. Значит, вознаграждения по договорам гражданско-правового характера теперь облагаются по единому тарифу, а также по взносам от временной нетрудоспособности и материнству (ВНиМ) [1;2; 6].

Внедренная система Единого налогового платежа (ЕНП), радикально изменила механизм исполнения фискальных обязательств. Данный порядок предполагает консолидацию всех налогов и сборов в рамках единого платежного документа с последующим зачислением средств на Единый налоговый счет (ЕНС). Распределение ресурсов по конкретным видам обязательств осуществляется налоговыми органами самостоятельно на базе представленной отчетности и уведомлений. Ключевым следствием реформы стала унификация налогового календаря: в частности, предельный срок перечисления страховых взносов (включая выплаты по договорам ГПХ) был смещен с 15-го на 28-е число месяца, следующего за отчетным.

В 2026 году система отчетности, формируемая бухгалтером по заработной плате, структурируется по четырем ключевым направлениям. Периодичность и полнота предоставляемых сведений находятся в прямой зависимости от численности персонала организации. К указанным категориям относятся.

1. Фискальная отчетность: комплект документации, направляемый в адрес Федеральной налоговой службы (ИФНС).

2. Отчетность перед Социальным фондом России: информация, касающаяся застрахованных лиц и начислений на травматизм.

3. Статистические наблюдения: данные, предоставляемые в органы госстатистики, где сроки сдачи регламентированы штатной численностью сотрудников.

4. Иные сведения: данные, подготавливаемые по мере поступления индивидуальных запросов от уполномоченных министерств и ведомств [3].

В табл. 1 представлены актуальные сроки сдачи отчетности по заработной плате в 2026г.

С 1 марта 2024 года зарплатным комиссиям открыт доступ к налоговой тайне [7]. В состав новых зарплатных комиссий входят представители региональных властей, ФНС, СФР, Роструда, МВД, объединений работодателей и профсоюзов. Заседания комиссий проводятся не менее одного раза в квартал, на заседание могут быть приглашены представители прокуратуры. Заседания могут проводиться как очно, так и по видео-конференцсвязи. По результатам заседаний комиссии принимают решения, которые оформляются протоколом, и являются обязательными для всех, включая работодателей.

На комиссии могут вызывать работодателей, у которых обнаружили факты или признаки нелегальной занятости (серые зарплаты, подмену трудовых отношений гражданско-правовыми и т. п.).

Таблица 1

Сроки сдачи отчетности по заработной плате в 2026 году для работодателей

| Наименование отчета                                                                                                              | Контролирующий орган | Сроки подачи                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Расчет по страховым взносам                                                                                                      | ИФНС                 | Ежеквартально, до 25-го числа месяца, следующего за отчетным периодом                                                                                                                                                                                                                                      |
| Персонифицированные сведения о физлицах                                                                                          |                      | Ежемесячно, до 25-го числа следующего месяца                                                                                                                                                                                                                                                               |
| Расчет 6-НДФЛ                                                                                                                    |                      | Ежеквартально, до 25-го числа месяца, следующего за отчетным периодом. Годовой отчет сдают до 25 февраля следующего года                                                                                                                                                                                   |
| Подраздел 1.1 отчета ЕФС-1 — сведения о трудовой деятельности                                                                    | СФР                  | Только при наступлении кадрового события. При увольнении или приеме сотрудника, заключении или расторжении договора ГПХ, приостановлении или возобновлении трудового договора с мобилизованным — на следующий рабочий день. До 25-го числа месяца, следующего за отчетным, — при переводе на другую работу |
| Подраздел 1.2 отчета ЕФС-1 — сведения о страховом стаже, совместно с подразделом 2                                               |                      | Ежегодно, до 25 января года, следующего за отчетным                                                                                                                                                                                                                                                        |
| Подраздел 3 отчета ЕФС-1 — сведения о застрахованных лицах, за которых перечислили дополнительные взносы на накопительную пенсию |                      | Ежеквартально, до 25-го числа следующего месяца после отчетного периода                                                                                                                                                                                                                                    |
| Раздел 2 отчета ЕФС-1 — сведения о начисленных страховых взносах на травматизм                                                   |                      | Ежеквартально, до 25-го числа следующего месяца после отчетного периода                                                                                                                                                                                                                                    |
| Статотчет П-4 (НЗ)                                                                                                               | Росстат              | Ежеквартально. За 1–3-й квартал отчитываемся с 1-го рабочего дня по 8-е число после отчетного квартала, а за 4-й квартал — с 1-го рабочего дня по 10-е число                                                                                                                                               |
| Статотчет П-4                                                                                                                    | Росстат              | Ежемесячно, с 1-го рабочего дня по 15-е число после отчетного периода. Микро — ежеквартально, с 1-го рабочего дня по 15-е число после отчетного периода.                                                                                                                                                   |

Данные для вызова на комиссию берутся в ИФНС, Социального фонда и других ведомств. Большинство сведений в комиссии передают налоговые органы. Список сведений для передачи в комиссию утвержден в приказе Минтруда от 02.02.2024 года № 40н [8].

В соответствии с этим, основной и необходимой функцией бухгалтера по расчету заработной платы является не только корректное ведение

бухгалтерского учета, но и последующий контроль расчетов, начислений и перечислений.

В соответствии с этим, для корректного начисления расчетов по оплате труда страховыми компаниями экономистами-бухгалтерами разрабатывается внутренняя система методов постпроверки основных начислений на базе 1С:ЗУП, учитывающая все особенности этой сферы деятельности [5].

В настоящее время в страховых компаниях существуют следующие стандартизированные отчеты:

1. Отражение зарплаты в бухгалтерском учете. Данный отчет запускается для ежедневной проверки и особенно актуален в дни начисления заработной платы в страховых компаниях, а также в последующие три дня после выплаты заработной платы. Отчет содержит в себе все дневные начисления по сотрудникам, включая сотрудников региональных подразделений.

2. Ошибки отражения (компиляторная проверка отчета отражения зарплаты). Данный отчет является компилятором обнаружения ошибок начисления заработной платы, исчисления НДФЛ, а также задвоения начислений в программе. Он запускается после формирования основного отчета «Отражения зарплаты в бухгалтерском учете» и на основании представленных данных, выявляет ошибки в программе.

3. Анализ зарплаты по сотрудникам – по категориям штатного производственного состава и на дату утверждения расчета. Данный отчет создается для формирования общего свода начислений. В дальнейшем он может использоваться сотрудниками для ручной проверки начислений.

4. Свод по видам расчета ЗУП-АИС – это внутренний отчет страховых компаний, который содержит в себе данные по начислениям из двух бухгалтерских информационных систем: 1С:ЗУП и АИС (административная информационная система страховой компании). Данный отчет собирает в себе данные по банковским выпискам, которые попали в АИС на выплату, и данные, рассчитанные в 1С:ЗУП. Контрольная функция данного отчета – это сопоставлении начисленной суммы заработной платы и выплаченной суммы заработной платы по каждому сотруднику.

То есть бухгалтер по расчету заработной платы страховой компании не только производит постконтрольные функции, но и предоставляет точную методологию разработки внутренних контрольных отчетов.

Каждый из разработанных отчетов является отдельным методом контроля расчетов по заработной плате. Разновидность отчетов варьируется относительно предметной цели контроля.

1. Контроль корректности исчисления НДФЛ, относительно начисленного сотрудникам дохода за налоговый период (прогрессивная шкала НДФЛ с учетом стандартных налоговых вычетов).

2. Контроль корректности исчисления страховых взносов.

3. Проверка корректности выплаты агентского вознаграждения страховым агентам.

4. Контроль корректности удержаний по исполнительным листам штатных и нештатных сотрудников.

5. Корректность статистического учета сотрудников компании (формы П4 и П4-НЗ) и т.д.

В ходе проведенного исследования было установлено, что система контроля расчетов по заработной плате в страховых компаниях, представляет собой многофакторный комплекс, требующий особого внимания в рамках обеспечения экономической безопасности. Специфика страхового сектора, выражающаяся в высокой доле нештатных сотрудников (агентов), сложной системе мотивации и жестких требованиях фискальных органов, создает повышенную зону риска для возникновения ошибок и злоупотреблений.

Проведенное исследование показало, что существующие программные продукты, такие как 1С:ЗУП, обладают достаточной адаптивностью, однако их базовый функционал не позволяет в полной мере автоматизировать процесс выявления ошибок. В связи с этим, ключевым элементом системы экономической безопасности становится разработка собственных (внутренних) методов постконтроля. В связи с чем страховыми компаниями эффективно применяется комплекс стандартизированных отчетов, которые позволяют минимизировать риски некорректных начислений, задвоения выплат и ошибок в исчислении НДФЛ и страховых взносов.

Таким образом, повышение уровня экономической безопасности страховых компаний в части расчетов с персоналом по оплате труда достигается не столько за счет тотальной автоматизации, сколько за счет грамотного симбиоза стандартного бухгалтерского функционала и специализированных контрольных отчетов, разработанных компанией с учетом методологии расчета и специфики бизнес-процессов. Дальнейшее совершенствование системы видится в направлении увеличения доли автоматической верификации данных (до 50-60%) и интеграции контрольных процедур непосредственно в процесс начисления заработной платы, а не только на этапе постпроверки. Это позволит снизить нагрузку на бухгалтерскую службу и оперативно реагировать на изменения в налоговом законодательстве, что позволит повысить уровень экономической безопасности страховых компаний.

### **Список литературы**

1. Трудовой кодекс Российской Федерации (ТК РФ) от 30.12.2001 №197-ФЗ (ред. от 29.12.2025, с изм. От 15.05.2026): [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_34683/](https://www.consultant.ru/document/cons_doc_LAW_34683/)
2. Налоговый кодекс Российской Федерации часть 2 (НК РФ ч.2) URL:

[https://www.consultant.ru/document/cons\\_doc\\_LAW\\_28165/](https://www.consultant.ru/document/cons_doc_LAW_28165/). (дата обращения: 23.02.2026).

3. Какую отчетность по заработной плате нужно сдавать в 2026 году URL: <https://ppt.ru/art/buh-uchet/otchetnost-po-zp>. (дата обращения: 23.02.2026).

4. Изменения по договору ГПХ с 2023 года URL: <https://buhexpert8.ru/zkn-bu/kadry-buhuchet/izmeneniya-po-dogovoru-gph-s-2023-goda.html>. (дата обращения: 23.02.2026).

5. Все изменения в расчете НДФЛ. Разбор новых правил для вас и ваших работников. Акцион-диджитал, Группа Акцион, 2026 Главный редактор С.А. Шилкин URL: <https://e.zarplata-online.ru/?mid=45338>. (дата обращения: 23.02.2026).

6. Договоры ГПХ: уплата страховых взносов в 2023 году. URL: <https://www.zarplata-online.ru/art/163256-dogovory-gph-uplata-strahovyh-vznosov-v-2023-godu>. (дата обращения: 23.02.2026).

7. Федеральный закон «О занятости населения в Российской Федерации от 12.12.2023 № 565-ФЗ (ред. От 28.11.2025): [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_464093/](https://www.consultant.ru/document/cons_doc_LAW_464093/)

8. Приказ Минтруда РФ от 02.02.2024 N 40н "Об утверждении перечня сведений и информации, в том числе составляющих налоговую тайну, передаваемых налоговыми органами Российской Федерации в Межведомственные комиссии субъектов Российской Федерации по противодействию нелегальной занятости, а также в территориальные органы Федеральной службы по труду и занятости в порядке межведомственного взаимодействия": <https://minjust.consultant.ru/special/documents/document/51240>

**Лашинская Наталья Викторовна**

доцент кафедры экономической экспертизы и финансового мониторинга  
ФГБОУ ВО «МИРЭА – Российский технологический университет»  
Россия, г. Москва

**Захарчук Михаил Сергеевич**

**Кузьменко Илья Артемович**

студенты 3 курса  
ФГБОУ ВО «МИРЭА – Российский технологический университет»  
Россия, г. Москва

### **Теневой бизнес и коррупция: взаимосвязь и последствия для экономической безопасности государства**

**Аннотация.** В статье исследованы и раскрыты вопросы взаимосвязи теневого сектора экономики и коррупции, которые замедляют национальный экономический рост и представляют собой взаимообусловленные угрозы экономической безопасности российского государства.

**Ключевые слова:** теневой бизнес, коррупция, теневая экономика, нелегальные экономические отношения, меры противодействия теневому бизнесу.

В условиях современной геополитической ситуации теневая экономика совместно с коррупцией все чаще затрагивают различные сферы деятельности граждан. Данная взаимосвязь порождает процессы, оказывающие негативное влияние на уровень жизни населения, замедляет национальный экономический рост и снижает уровень экономической безопасности государства.

Теневая экономика и коррупция неразделимы, они порождают и взаимно обуславливают друг друга. Теневой сектор выступает благодатной почвой для разрастания коррупции, поскольку находится вне поля правового контроля. Он формирует устойчивый спрос на коррупционные услуги и, по сути, программирует необходимое для своего функционирования число коррумпированных чиновников. При этом сама коррупционная деятельность является неотъемлемой частью теневой экономики. То есть, борьба с коррупцией не может быть эффективной без одновременного противодействия теневой экономике.

В рамках данной взаимосвязи выделяются две основные проблемы, требующие безотлагательного вмешательства. Первая проблема связана с так называемыми коррупционными услугами в широком смысле, что предполагает совпадение предмета коррупционной деятельности с предметом теневой экономической активности; материальный эффект от коррупции в таком случае становится частью теневого дохода. Вторая проблема, также обусловлена необходимостью борьбы с коррупцией в контексте теневой экономики, касается

макроэкономических финансовых решений государства, которые объективно продуцируют разрастание теневого сектора.

Как видим, теневая экономика объединяет в себе понятие любых нелегальных экономических отношений во всех сферах экономической деятельности. Однако, в настоящее время отсутствует четко закреплённое понятие теневой экономики, в то время как определение коррупции закреплёно в ФЗ «О противодействии коррупции» [1].

Выделяется три основные группы деяний, попадающих под определение «теневая экономика» представленные в табл.1.

Таблица 1  
Сегменты теневой экономики

| Сегмент теневой экономики                  | Характеристика (пример) сегмента                                                                                                                                                                |
|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Неформальная (неофициальная)               | - организация предприятия по производству алкоголя и продуктов питания, добычи драгметаллов и драгоценных камней;<br>- товары и услуги, производимые частным образом и не облагаемые налогами   |
| Фиктивная (серая)                          | - вывод капитала по фиктивным договорам и контрактам<br>- уклонение от уплаты налогов                                                                                                           |
| Черная экономика (нелегальная, подпольная) | - полностью криминальные виды деятельности, включающие наркоторговлю, кражи и грабежи, вымогательство и другие виды преступлений;<br>- в некоторых случаях – действия монополистов и рейдерство |

По данным Росстата и Генпрокуратуры число занятых в неформальном секторе экономики на конец 2024 года составило 15,8 млн человек, а рост за 2024 год составил 11,7%. Необходимо отметить то, что в реальной жизни бывает сложно отнести какое-то явление к конкретной форме теневой экономики.

Стоит подчеркнуть, что специалисты отдельно выделяют теневую экономику в сфере цифровых технологий, включающую киберпреступления, кражу личных данных, теневой труд, теневой рынок недвижимости и другие.

Причинами появления теневого оборота в экономике можно назвать: высокий уровень налогообложения субъектов рыночных отношений; состояние нестабильности в экономической сфере государства; отсутствие стабильного правового регулирования; отток высококвалифицированных кадров; низкий уровень доходов населения и другие.

Теневой бизнес проникает практически во все сферы деятельности, принимая специфические для каждой сферы формы.

Как уже было сказано, теневая экономика непосредственно связана с экономическими, правовыми, социальными и политическими коррупционными факторами, среди которых выделяют внутренние и внешние факторы, представленные в табл. 2.

Таблица 2

Внутренние и внешние факторы роста теневого оборота в экономике

| Группа факторов | Факторы роста теневого оборота                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                     |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | Внутренние                                                                                                                                                                                                                                                                                                                   | Внешние                                                                                                                                                                                                                                             |
| Экономические   | <ul style="list-style-type: none"> <li>- производственные проблемы российской экономики</li> <li>- низкий уровень защищенности малого и среднего бизнеса</li> <li>- отсутствие здоровой конкурентной среды</li> <li>- бесконтрольность деятельности значительного числа предприятий социального сектора экономики</li> </ul> | <ul style="list-style-type: none"> <li>- санкционная политика иностранных государств;</li> <li>- уход значительного числа иностранных компаний с российского рынка;</li> <li>- сокращение инвестиционных вложений в российскую экономику</li> </ul> |
| Правовые        | <ul style="list-style-type: none"> <li>- устаревание нормативной базы</li> <li>- запоздалое формирование законодательного регулирования ответственности за преступления коррупционной направленности</li> </ul>                                                                                                              |                                                                                                                                                                                                                                                     |
| Социальные      | <ul style="list-style-type: none"> <li>- неравенство различных групп населения (на фоне безграничного богатства одних выделяется значительная группа населения, живущая за чертой бедности)</li> </ul>                                                                                                                       |                                                                                                                                                                                                                                                     |
| Политические    | <ul style="list-style-type: none"> <li>- коррумпированность власти</li> <li>- слабое развитие демократических институтов</li> <li>- отстранение граждан от управления делами государства</li> </ul>                                                                                                                          |                                                                                                                                                                                                                                                     |

Достаточно часто бизнес в теневой экономике не обнаруживался государственными органами, то есть бывал скрыт. В таких условиях теневая экономика и коррупция, вероятнее всего, будут усиливать друг друга, поскольку коррупция необходима для расширения деятельности теневой экономики, в то время как теневой экономике для расширения и процветания требуются нелегальные денежные поступления.

Механизмы такого взаимодействия теневой экономики и коррупции-могут проявляться в следующем:

- теневая экономика может существовать и развиваться в значительных масштабах в условиях коррумпированности всех систем государственной власти;
- теневая экономика формирует коррупционные отношения в тех сфера политики и экономики, от которых зависит ее благополучное существование;
- коррупция «вынуждает» теневую экономику оставаться в «тени» и вести нелегальный бизнес;
- коррупция создает основу для формирования новых сфер и видов теневой экономики;
- теневая экономика является финансовой основой коррупции, а коррупция – финансовая основа теневой экономики.

Как видим, говоря о теневой экономике, не стоит забывать, что она, безусловно, порождает коррупцию, а коррупция, в свою очередь, создает основу расцвета теневой экономики. При этом коррупция и теневая экономика настолько сильно переплетены и взаимосвязаны, что невозможно определить, что является причиной, а что следствием.

Определив взаимодействие теневой экономики и коррупции, остановимся на их последствиях, которые представляют непосредственную угрозу экономической безопасности нашего государства, среди которых выделяют экономические, социальные и политические, что представлено в табл. 3.

Таблица 3  
Последствия коррупции и теневой экономики  
для экономической безопасности государства

| Группа последствий | Результаты                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Экономические      | <ul style="list-style-type: none"> <li>- рост издержек бизнеса</li> <li>- упущенные возможности</li> <li>- снижение уровня благосостояния людей</li> <li>- потеря доверия к власти</li> <li>- неэффективное и нецелевое использование бюджетных средств</li> <li>- замедление (снижение) экономического роста</li> </ul>                                                |
| Социальные         | <ul style="list-style-type: none"> <li>- усугубление социального неравенства</li> <li>- подрыв единства общества</li> <li>- трудности в получении доступа к услугам здравоохранения, качественному образованию и пр.</li> <li>- распространение незаконной деятельности и преступности в обществе</li> </ul>                                                            |
| Политические       | <ul style="list-style-type: none"> <li>- усиление ресурсного обеспечения коррупции, что приводит к увеличению ее масштабов</li> <li>- усиление теневых структур государственной политики, СМИ и избирательных компаний на различных уровнях;</li> <li>- падение престижа государства на международной арене, угроза ее экономической и политической изоляции</li> </ul> |

Согласно Стратегии экономической безопасности Российской Федерации на период до 2030 года, экономическая безопасность - состояние защищенности национальной экономики от внешних и внутренних угроз, при котором обеспечиваются экономический суверенитет страны, единство ее экономического пространства, условия для реализации стратегических национальных приоритетов Российской Федерации.

Учитывая вероятность негативных последствий для ЭБ РФ была проведена, и в настоящее время продолжает проводиться многопрофильная работа по противодействию теневому бизнесу и коррупции.

Меры противодействия теневому бизнесу и коррупции в виде законодательных инициатив, подготовленных на государственном уровне, а также мероприятий, осуществляемых бизнес-сообществами представлены в табл. 4.

Таблица 4

Меры противодействия теневому бизнесу и коррупции

| Законодательные инициативы                                                                                                                                                                                                                                                                           | Роль государственных и частных институтов                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>- Федеральный закон "О противодействии коррупции" от 25.12.2008 N 273-ФЗ является фундаментальным нормативным актом</li> <li>- Конституция РФ</li> <li>- Международные договоры</li> <li>- Указы президента</li> <li>- Постановления правительства</li> </ul> | <ul style="list-style-type: none"> <li>- На государственном уровне координацию деятельности осуществляет Президент РФ, определяющий основные направления политики, а также Федеральное Собрание, Правительство, Генеральная прокуратура и Счетная палата</li> <li>- Примером успешной частной инициативы является Антикоррупционная хартия российского бизнеса, разработанная Российским союзом промышленников и предпринимателей (РСПП)</li> <li>- Государство уделяет приоритетное внимание формированию в обществе нетерпимости к коррупционному поведению, что закреплено в статье 6 Федерального закона № 273-ФЗ как одна из основных мер профилактики</li> </ul> |

В заключение подчеркнем, что теневой бизнес и коррупция представляют собой взаимосвязанные явления, формирующие устойчивую деструктивную систему, которая несёт серьёзные угрозы экономической безопасности государства. Коррупция создаёт благоприятные условия для функционирования теневой экономики, обеспечивая ей «защиту» и доступ к ресурсам, а теневой бизнес, в свою очередь, генерирует финансовые потоки, подпитывающие коррупционные схемы. Эта взаимозависимость порождает замкнутый круг, где каждое явление усиливает другое, затрудняя эффективное противодействие.

Негативные последствия данной взаимосвязи носят многоаспектный и долгосрочный характер, теневая экономика тормозит технологическое развитие, ориентируясь на краткосрочную прибыль, а коррупция размывает правовые нормы и снижает качество государственного управления. Для нейтрализации этих угроз необходим комплексный подход, включающий ужесточение финансового контроля, совершенствование антикоррупционного и налогового законодательства, повышение эффективности правоохранительных органов, стимулирование легализации бизнеса и формирование антикоррупционной культуры в обществе.

Таким образом, борьба с теневым бизнесом и коррупцией – это не просто локальная административная задача, а стратегический приоритет, от реализации которого зависит устойчивость экономической системы, инвестиционный климат и долгосрочное развитие государства. Только системная работа по разрыву взаимосвязи этих явлений способна создать условия для обеспечения экономической безопасности и повышения благосостояния общества.

## Список литературы

1. О противодействии коррупции: Федеральный закон от 25 декабря 2008 г. № 273-ФЗ // Официальный интернет-портал правовой информации. – URL: <http://pravogovru/proxy/ips/?docbody=&nd=102125976> (дата обращения: 18.02.2026).
2. О Стратегии экономической безопасности Российской Федерации на период до 2030 года: Указ Президента РФ от 13 мая 2017 г. № 208 // Официальный интернет-портал правовой информации. – URL: <http://pravogov.ru/proxy/ips/?docbody=&nd=102431385> (дата обращения: 18.02.2026).
3. Имиев И. М., Дикажев М. М. Экономические и социальные последствия коррупции // Право и управление. – 2023. – № 12. – С. ... – URL: <https://cyberleninka.ru/article/n/ekonomicheskie-isotsialnye-posledstviya-korrupsii> (дата обращения: 18.02.2026).
4. Генпрокуратура раскрыла данные о коррупции в России // РБК: [сайт]. – 16 июня 2025. – URL: <https://www.rbc.ru/society/16/06/2025/6837ed979a79471aa4b6c83d> (дата обращения: 18.02.2026).
5. Новости // Audit-it.ru: [сайт]. – URL: <https://www.audit-it.ru/news/finance/1119277.html> (дата обращения: 12.02.2026).
6. Теневая экономика России // TAdviser: [сайт]. – URL: [https://www.tadviser.ru/index.php/Статья:Теневая\\_экономика\\_России](https://www.tadviser.ru/index.php/Статья:Теневая_экономика_России) (дата обращения: 11.02.2026).

**Лебедева Екатерина Сергеевна**

кандидат экономических наук, доцент

доцент кафедры экономической экспертизы и финансового мониторинга

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

**Назаренко Полина Алексеевна**

студент 5 курса

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

## **Цифровой аудит и аналитика данных как инструменты противодействия киберрискам и фальсификации финансовой отчетности**

**Аннотация.** В статье рассматривается трансформация аудита в условиях цифровой экономики. Финансовая отчетность анализируется как критически важный информационный актив, целостность которого напрямую зависит от уровня кибербезопасности компании. Исследуется роль современных технологий – ИИ, анализа больших данных, непрерывного мониторинга - в выявлении цифровых манипуляций и кибермошенничества. Особое внимание уделяется симбиозу правовых норм, экономических требований и технологических решений в построении устойчивой системы обеспечения достоверности финансовых данных.

**Ключевые слова:** цифровой аудит, финансовая отчетность, кибербезопасность, аналитика данных, искусственный интеллект в аудите, фальсификация отчетности, кибермошенничество, непрерывный аудит, целостность данных, информационные риски, искажения в отчетности, профессиональный скептицизм, бухгалтерские аномалии, недобросовестные действия, мошенничество, экономическая безопасность.

В контуре «новой реальности» финансовая отчетность перестала быть исключительно бухгалтерским результатом, превратившись в сложный цифровой продукт. Ее формирование, хранение и передача происходят в информационных системах, что создает принципиально новые риски. Угроза сместилась от случайных ошибок к целенаправленным кибератакам, целью которых является хищение средств, манипуляция рыночной стоимостью или сокрытие реального положения дел. В этом контексте аудит эволюционирует, становясь междисциплинарной деятельностью на стыке экономики, права и информационных технологий.

Согласно МСА 200, финансовая отчетность представляет собой структурированное представление финансовой информации [2]. В современном понимании, это структурированные данные, уязвимые ко всем угрозам

информационной безопасности. Искажения, определяемые тем же стандартом как расхождения с требуемыми принципами учета [2], все чаще являются следствием не человеческой ошибки, а внедрения в системы учета (ERP, CRM) или подделки электронных документов и цифровых подписей.

Таким образом, достоверность отчетности становится производной от двух факторов: корректности методологии учета и целостности данных в информационных системах компании. Нарушение конфиденциальности (утечка) или доступности (блокировка) финансовых данных также наносит прямой экономический ущерб, влияя на репутацию и капитализацию.

Классические методы аудита приобретают новое звучание в цифровой среде, трансформируясь в инструменты, позволяющие прогнозировать будущие события и тенденции задолго до их наступления.

Непрерывный аудит и мониторинг: вместо выборочных проверок по итогам периода реализуется постоянный анализ потоков транзакций в реальном времени. Это позволяет выявлять аномалии мгновенно.

Горизонтальный и вертикальный анализ перерастают в сравнительную аналитику больших данных, включая аудит качества с отраслевыми показателями и выявление статистически маловероятных отклонений.

Предиктивная аналитика и моделирование: Математические модели, подобные модели Бениша для выявления манипуляций прибылью, дополняются алгоритмами машинного обучения. Нейросети обучаются на исторических данных (в том числе – о выявленных случаях мошенничества) для прогнозирования рискованных операций и сегментов.

Аудит цифровых следов: Проверке подлежат не только проводки, но и метаданные: логин доступа к критически важным системам (кто, когда, с какого IP-адреса), история изменений в документах, временные штампы создания и модификации файлов. Систематический ввод операций «задним числом» становится легко обнаружимым техническим артефактом.

Специализированное ПО:

- AppZen. Платформа использует нейросети для автоматической проверки счетов и отчётов о расходах. Система анализирует данные, выявляет возможные ошибки и несоответствия, а также предлагает рекомендации по их исправлению [6].

- ThetaRay. Платформа анализирует финансовые данные и выявляет аномалии, связанные с мошенничеством. Система анализирует транзакции в режиме реального времени, выявляя подозрительные операции и предупреждая о них бухгалтеров и руководителей компании [6].

- AuditXP Professional. Программа автоматизирует практически все рутинные операции, которые выполняют аудиторы на проверках. Она делает сложные расчёты, расшифровывает и сверяет показатели отчетности с бухгалтерской базой клиента, анализирует генеральную совокупность и строит

выборку [6].

– «Проверка бухгалтерского учёта». Бесплатная Excel-программа, которая позволяет на регулярной основе выявлять операции, отражённые с нарушением корреспонденций, предусмотренных в инструкциях к плану счетов.

– «Контур.Экстерн». Сервис предоставляет подробный финансовый анализ деятельности организации. Он моментально формирует детальный аналитический отчёт, который даёт понятные ответы о финансовом состоянии компании [6].

Данные программы позволят автоматизировать проверку всей генеральной совокупности транзакций, выявляя сложные, замаскированные взаимосвязи, невидимые при выборочной проверке.

Международный стандарт аудита МСА 240 обязывает аудитора оценивать риски существенного искажения вследствие недобросовестных действий [3]. В новой реальности эта оценка обязательно включает аудит систем информационной безопасности (СИБ).

Оценка ИБ-контролей: аудитор должен понимать, как организован доступ к финансовым системам, как защищены каналы передачи данных, существует ли система управления инцидентами ИБ. Слабость внутреннего контроля в сфере ИБ (например, отсутствие сегрегации обязанностей в (Т-системах) создает среду для злоупотреблений.

Соответствие регуляторным требованиям: обеспечение достоверности данных напрямую связано с соблюдением требований 152-ФЗ «О персональных данных», стандартов ЦБ РФ (например, СТО БР ИББС), а для международных компаний — GDPR, SOX. Профессиональный скептицизм аудитора теперь распространяется и на эту область.

Ротация аудиторов и «цифровая» свежесть взгляда: частая смена аудиторских команд, помимо традиционных преимуществ, позволяет привлекать специалистов с новейшими компетенциями в области кибербезопасности и анализа данных, что повышает шансы обнаружения сложных и изощренных кибератак.

Несмотря на мощный технологический инструментарий, аудит сталкивается с новыми сложностями:

– сложность аудита облачных и распределенных систем: при использовании облачных сервисов (SaaS для бухгалтерии) физический контроль над инфраструктурой данных отсутствует. Аудитор должен полагаться на отчеты независимых аудиторов облачного провайдера (SOC-отчеты);

– намеренное сокрытие с применением продвинутых IT-средств: руководство или злоумышленники внутри компании могут использовать изощренные, высокотехнологичные методы для маскировки манипуляций, включая техники, направленные на противодействие цифровому расследованию и сокрытию следов;

– «Человеческий фактор» в технологической среде: социальная инженерия остается одним из самых эффективных способов обхода любых технических защит;

– недостаточная разработанность стандартов для аудита алгоритмов искусственного интеллекта, принимающих все больше финансовых решений.

В заключении отметим, что аудит в контуре новой реальности перестает быть ретроспективной финансовой проверкой. Он трансформируется в киберустойчивый аудит, главная задача которого – обеспечить доверие к цифровым финансовым данным. Это достигается через симбиоз:

- права (соблюдение нормативов в сфере ИБ и защиты данных);
- технологий (внедрение AI, аналитики и непрерывного мониторинга);
- экономики (оценка и минимизация финансовых последствий киберинцидентов и искажений).

Эффективность противодействия фальсификациям в современном мире определяется способностью аудиторов и специалистов по экономической безопасности говорить на одном языке с IT-архитекторами и экспертами по кибербезопасности. Надежность финансовой отчетности начинается с целостности данных, а ее обеспечение – это комплексная междисциплинарная задача, актуальность которой будет только возрастать.

### Список литературы

1. Федеральный закон от 30.12.2008 № 307-ФЗ «Об аудиторской деятельности» URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_83311/5662200f71fec9b8ab1a6e0615896613d3852b5a/](https://www.consultant.ru/document/cons_doc_LAW_83311/5662200f71fec9b8ab1a6e0615896613d3852b5a/).

2. Международный стандарт аудита 200 «Основные цели независимого аудитора и проведение аудита в соответствии с международными стандартами аудита» (введен в действие на территории Российской Федерации Приказом Минфина России от 09.01.2019 № 2н) (ред. от 16.10.2023) URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_317258/8b01883380fec344f044c706161a816e9c86186e/](https://www.consultant.ru/document/cons_doc_LAW_317258/8b01883380fec344f044c706161a816e9c86186e/).

3. Международный стандарт аудита 240. «Обязанности аудитора в отношении недобросовестных действий при проведении аудита финансовой отчетности» (введен в действие на территории Российской Федерации Приказом Минфина России от 09.01.2019 № 2н) URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_317404/](https://www.consultant.ru/document/cons_doc_LAW_317404/).

4. Обнаружение мошенничества: выявляем информационные шумы и «технические» аномалии в учете данных // Финансовые расследования и судебные экспертизы URL: <https://fi.center/blog/article/104/Obnaruzenie-mosennicestva-vyavlaem-informacionnye-sumy-i-tehniceskie-anomalii-v-~>.

5. Оценка достоверности отчетности при проведении внешнего аудита //

URL: [https://elib.utmn.ru/jspui/bitstream/ru-tsu/6952/1/CifEkon2020\\_386\\_391.pdf](https://elib.utmn.ru/jspui/bitstream/ru-tsu/6952/1/CifEkon2020_386_391.pdf).

6. Нейросеть для бухгалтеров: автоматизация учета и анализ финансовых данных // ruGPT URL: [https://sroaas.ru/pc/novosti/organizaciya\\_i\\_osuwestvlenie\\_ekonomicheskim\\_sub\\_ektom\\_vnutrennego\\_kontrolya\\_overshaemyh\\_faktov\\_hozy/](https://sroaas.ru/pc/novosti/organizaciya_i_osuwestvlenie_ekonomicheskim_sub_ektom_vnutrennego_kontrolya_overshaemyh_faktov_hozy/).

7. Организация и осуществление экономическим субъектом внутреннего контроля совершаемых фактов хозяйственной жизни, ведения бухгалтерского учета и составления бухгалтерской (финансовой) отчетности // Саморегулируемая Организация Аудиторов Ассоциация «Содружество» URL: [https://sroaas.ru/pc/novosti/organizaciya\\_i\\_osuwestvlenie\\_ekonomicheskim\\_sub\\_ektom\\_vnutrennego\\_kontrolya\\_overshaemyh\\_faktov\\_hozy/](https://sroaas.ru/pc/novosti/organizaciya_i_osuwestvlenie_ekonomicheskim_sub_ektom_vnutrennego_kontrolya_overshaemyh_faktov_hozy/).

8. За что отвечает аудитор? // Бухгалтерия.ру URL: <https://www.buhgalteria.ru/article/za-chto-otvechaet-auditor>.

9. Что происходит при смене аудиторской фирмы? // URL: <https://tenchat.ru/media/2765055-chto-proiskhodit-pri-smene-auditorskoy-firmy>.

**Лебедева Екатерина Сергеевна**

кандидат экономических наук, доцент

доцент кафедры экономической экспертизы и финансового мониторинга

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

**Рыбакова Екатерина Дмитриевна**

студент 5 курса

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

### **Администрирование налогов в Российской Федерации: от налогообложения в условиях цифровой реальности до судебно-налоговой экспертизы**

**Аннотация.** В статье комплексно исследуются актуальные аспекты налогового администрирования в РФ в контексте цифровой трансформации экономики и развития судебно-налоговой экспертизы. Особое внимание уделяется влиянию цифровизации на эффективность налогового контроля, снижение издержек администрирования и повышение прозрачности налоговых отношений. В статье рассматриваются преимущества цифровых решений и связанные с ними вызовы (защита информации, необходимость адаптации законодательства, риски кибербезопасности). Также в статье рассматриваются вопросы проведения судебно-налоговой экспертизы и ее роли в разрешении налоговых споров, в том числе в уголовном судопроизводстве.

**Ключевые слова:** налоговое администрирование, цифровизация, цифровая экономика, судебно-налоговая экспертиза, налоговый контроль, Федеральная налоговая служба (ФНС) России.

Цифровая эпоха требует от государства проведения трансформации налоговых отношений. Этот процесс, обусловленный динамичным развитием технологий, предполагает совершенствование нормативно-правовой базы и общественных институтов.

Ключевым документом, регулирующим цифровизацию экономики, является Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы». Согласно ему, «цифровая экономика – хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг» [1]. Таким образом, цифровая экономика основывается на плотных сетевых взаимодействиях между людьми,

предприятиями, устройствами и данными.

Исходя из этой сущности, определяется и связь цифровой экономики с налоговым администрированием. Её трансформация в России представляет собой объединение множества информационных потоков от физических и юридических лиц в единую систему для последующего анализа и контроля с применением современных технологий. Активную работу в этом направлении ведет ФНС России, которая на протяжении последних лет создает и развивает специализированные информационные системы.

Далее рассмотрим налоговое администрирование на примере конкретного налога – налог на добавленную стоимость (НДС).

НДС – это один из основных налогов, составляет внушительную долю доходной части федерального бюджета Российской Федерации, он интересен с точки зрения анализа его администрирование и исследование при помощи инструментов и методик экономической судебной экспертизы.

НДС является косвенным налогом, включаемым в стоимость товаров, работ или услуг. Его уплачивают на каждом этапе производства и реализации продукции, а также является входным налогом при покупке товара у иностранного поставщика (импортера) при ввозе товара в Россию.

Налоговое администрирование НДС за последние 10 лет претерпевает значительные изменения в сторону автоматизации данного процесса, что позволяет управлять процессом налогового контроля НДС без непосредственного участия налогового инспектора на достаточно высоком уровне.

Автоматизация контроля и администрирования налога на добавленную стоимость начинается с первого квартала 2014 года. Именно с указанного периода налогоплательщики обязаны предоставлять декларацию по НДС только в электронном виде.

После этого, начиная с налоговой отчетности за 1 квартал 2015 года, электронному декларированию подлежит не только декларация по НДС, но и сведения книг покупок и книг продаж, включаемые в новую форму налоговой декларации [2].

С этими нововведениями ФНС приняло соответствующие меры, способные упростить администрирование налогового контроля, а также повысить его эффективность и всеобъемлемость. В 2014 году создается автоматизированная система контроля за исчислением НДС – АСК НДС-2, позволяющая оперативно выявлять разрывы в цепочках контрагентов.

Указанная система использует 84 критерия риска, такие как: налоговая нагрузка, рентабельность, уплата налогов плательщиком за три года, задолженность, сведения об учредителях, директоре, в соответствии с которыми распределяет все объекты налогового контроля на три уровня: низкий, средний и высокий риск.

Однако, автоматизация системы налогового контроля совершенствуется не только на внутреннем уровне. Россия и Беларусь предприняли шаги по интеграции контроля за уплатой НДС в рамках Союзного государства. В октябре 2022 года был подписан договор, регулирующий общие принципы налогообложения по косвенным налогам, включая НДС. Целью соглашения стало упрощение трансграничной торговли, формирование единого информационного пространства и создание целостной фискальной базы. Для реализации этих целей была разработана интегрированная система администрирования косвенных налогов (ИСА КН), введенная в промышленную эксплуатацию в январе 2023 года. Система обеспечивает автоматический обмен данными о транзакциях налогоплательщиков обеих стран, выявляет разрывы по НДС и анализирует цепочки добавленной стоимости, позволяя фокусировать контроль на недобросовестных плательщиках [3].

Кроме технологической интеграции, в рамках сотрудничества планируется создание наднационального налогового комитета, который координирует налоговую политику двух стран и контролирует реализацию положений договора. Система ИСА КН уже показала экономический эффект: снижена административная нагрузка на добросовестный бизнес, увеличена точность выявления схем уклонения от уплаты НДС и обеспечен рост налоговых поступлений. Кроме того, интеграция способствует гармонизации правил начисления налогов и льгот, унификации ставок и повышает прозрачность трансграничных операций, что укрепляет налоговую дисциплину в рамках Союзного государства.

С помощью указанных непубличных баз данных, налоговыми органами выявляются особая группа контрагентов – «технические» организации и фирмы-однодневки, используемые недобросовестными налогоплательщиками для искажения данных отчетности по налогу на добавленную стоимость.

Налоговые органы пользуются автоматической программой «АСК НДС-2», которая отслеживает разрывы в уплате НДС по принципу «Каждый счет-фактура найдет свою пару». Разрывы – это ситуация, когда сторона сделки не заплатила налоги. Когда инспекторы видят разрыв, они проверяют контрагента и могут провести встречную проверку в компании. При чем программы ищут и сложные разрывы, когда, например, в схеме увеличивается количество фирм.

Если выяснится, что компания знала о недобросовестном поведении контрагента и все равно заключила с ним договор, налоговый орган откажет в налоговом вычете и доначислит пени и штрафы на сумму неуплаченного НДС [4].

Отметим, что, если налоговая проверка позволяет предполагать, что в организации совершено налоговое преступление, данные об этом должны быть переданы в органы внутренних дел. На основе этих данных представители органов внутренних дел будут решать вопрос о возбуждении уголовного дела и

о привлечении должностных лиц к уголовной ответственности.

В уголовном судопроизводстве в таком уголовном деле пострадавшая сторона – это государство, представителем которого в указанном случае является налоговый орган.

И здесь судебная экономическая экспертиза является процессуальным действием, состоящим из проведения экономического исследования и дачи заключения экспертом по вопросам, которые требуют специальных знаний в области экономической науки.

Развитие автоматизации контроля НДС оказывает значительное влияние на отрасль судебной экономической экспертизы, способствуя повышению её эффективности и точности. Современные автоматизированные системы позволяют отслеживать движение товаров и денежных средств с минимальным количеством ошибок, создавая достоверную базу данных для анализа хозяйственных операций.

Основное преимущество, которое приносит отрасли автоматизация контроля НДС – это предоставление на исследование обширного круга объектов исследования в рациональном для быстрой обработки формате, чем исключает человеческий факт при ручной проверке документов и ускоряет судебный процесс, в рамках которого назначена судебная экономическая экспертиза.

Как следствие эффективной работы автоматизированных систем налогового контроля, количество проверок и объем доначислений по НДС начал снижаться уже в 2019 году. Начиная с 2018 года потребителей бумажного НДС стало в разы меньше. Система автоматического контроля обеспечила устойчивый рост поступлений по НДС и способствовало обелению экономики, и одновременно усовершенствовала методику производства судебных экономических экспертиз, сделав их выводы более точными, оперативными и всеобъемлющими.

### Список литературы

1. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_216363/](https://www.consultant.ru/document/cons_doc_LAW_216363/).

2. Как успокоить контрагента, если ФНС усомнилась в надежности вашей компании. Материал из БСС «Система Главбух». URL: <https://1gl.ru/#/recommendations/found/fixedregioncode=55&isUseHints=false&phrase=%D0%B0%D1%81%D0%BA&sort=Relevance&status=actual/?of=copy-c3fdf66f73>.

3. «Договор между Российской Федерацией и Республикой Беларусь об общих принципах налогообложения по косвенным налогам» (Подписан в г. Москве 03.10.2022) (ред. от 20.09.2024) URL:

[https://www.consultant.ru/document/cons\\_doc\\_LAW\\_438910/4241573a9b3ff2eb81f7a568222f9744e2524e0c/](https://www.consultant.ru/document/cons_doc_LAW_438910/4241573a9b3ff2eb81f7a568222f9744e2524e0c/).

4. «Как пояснить разрывы и ошибки в декларации по НДС». Валентина Сухомлинова, Сергей Тараканов, Виталий Сазанский © Материал из Системы Главбух URL: <https://1gl.ru/#/document/16/211448/dfas8gi284/>.

**Паленова Юлия Андреевна**

студент 5 курса

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

Научный руководитель

**Няргинен Виктория Анатольевна**

кандидат экономических наук

доцент кафедры экономической экспертизы и финансового мониторинга

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

### **Оценка экономической безопасности сектора малого и среднего предпринимательства во взаимосвязи с развитием региона (на примере г. Москва)**

**Аннотация.** В статье анализируется состояние сектора малого и среднего предпринимательства (МСП) г. Москвы за период 2020–2025 гг., вклад в валовой региональный продукт, занятость и налоговые поступления. Представлена апробация методики оценки экономической безопасности субъектов МСП во взаимосвязи с экономической безопасностью региона, основанной на индикаторном подходе и индексном методе нормирования. Выявлены ключевые угрозы, включая низкий уровень инновационной активности и дефицит квалифицированных кадров. Обосновано, что устойчивое развитие МСП является фактором укрепления экономической безопасности мегаполиса. Предложены направления совершенствования мониторинга индикаторов для своевременного реагирования на возникающие риски.

**Ключевые слова:** экономическая безопасность, малое и среднее предпринимательство, валовой региональный продукт, индикаторный подход, пороговые значения, обобщенный индекс, Москва, угрозы развития, инновационная активность.

Город Москва – столица Российской Федерации и крупнейший экономический, научно-производственный и социально-культурный центр страны. Москва представляет собой сложный многофункциональный комплекс, в котором сочетаются производственные и непроизводственные виды деятельности: торговля, финансовый сектор, сфера услуг, наука, здравоохранение. Москва входит в состав Центрального федерального округа, занимает одну из ключевых ролей в формировании макроэкономических показателей страны и выступает центром деловой активности и концентрации инвестиционных ресурсов. Высокий уровень экономического развития, развитая инфраструктура и значительный человеческий капитал определяют особое значение города в системе обеспечения экономической безопасности (ЭБ)

Российской Федерации и ее регионов.

Сектор малого и среднего бизнеса играет решающую роль как один из ключевых факторов стратегического развития Москвы. Как было отмечено ранее, малое и среднее предпринимательство способствует созданию рабочих мест, развивает конкуренцию, формирует налоговую базу, вносит вклад в создание валового регионального продукта [4]. В условиях современных геополитических и экономических вызовов оценка экономической безопасности сектора МСП приобретает особую актуальность, поскольку именно малый и средний бизнес выступает амортизатором экономических потрясений и обеспечивает социальную стабильность.

Проведенный анализ развития сектора МСП в Москве за период 2020–2025 гг. показывает, что за это время МСП претерпел значительные изменения, связанные с пандемией COVID-19, экономическими санкциями, логистическими срывами и валютной нестабильностью. Указанные факторы внешней среды оказали разнонаправленное воздействие: с одной стороны, они привели к сокращению спроса и разрыву цепочек поставок; с другой – стимулировали процессы импортозамещения и поиск новых рыночных ниш.

По статистическим данным Федеральной налоговой службы (ФНС) и столичного Департамента предпринимательства, количество зарегистрированных субъектов МСП в Москве увеличилось с 721 тыс. в 2020 г. до 906 тыс. к концу 2025 г., что эквивалентно приросту 26% за 5 лет (рис. 1). Данная динамика свидетельствует о высокой адаптивности московского предпринимательского сообщества и эффективности мер государственной поддержки, включая льготные кредитные программы, гранты и налоговые каникулы.

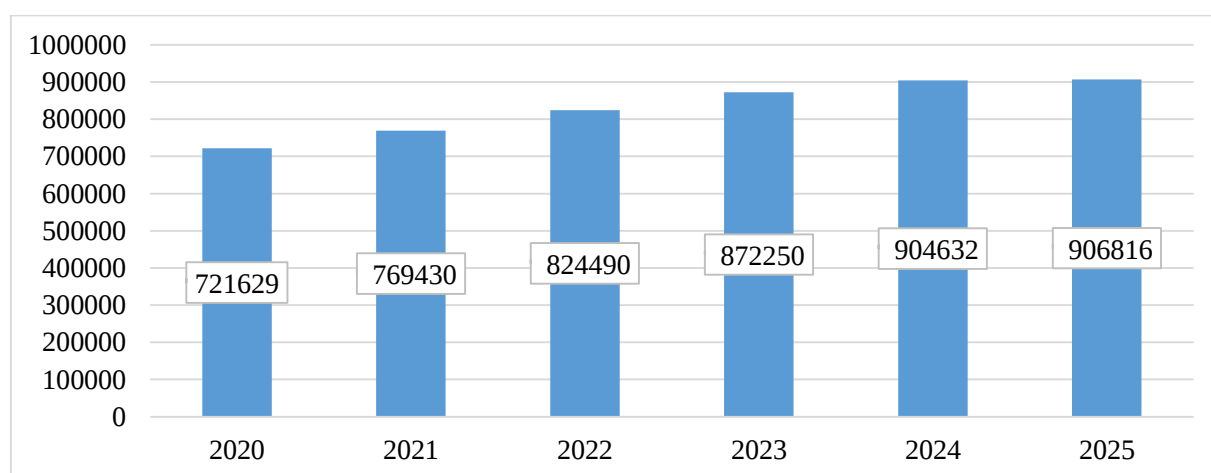


Рисунок 1. Динамика количества МСП в г. Москва на период 2020-2025 гг. [6]

По итогам 2025 года в Российской Федерации общее количество субъектов малого и среднего предпринимательства превысило 6,7 млн, при этом в Москве их численность на аналогичный период составила более 900 тыс. субъектов МСП, что составило 13,4% от общего количества субъектов МСП России. Таким образом, каждый восьмой субъект МСП страны работает в московском регионе, что подчеркивает концентрацию предпринимательской активности в столице.

Исходя из данных, представленных на рис. 1, можно отметить, что с 2020 по 2025 год наблюдается положительная тенденция. Прирост с каждым годом в усредненном значении составляет 5%, что в количественном эквиваленте примерно 37 037 субъектов МСП в год. Суммарное количество МСП в 2025 году составило 906 816 субъектов, большую долю которых составляют индивидуальные предприниматели (ИП) – 53,2% и микропредприятия – 41,6%; остальные 5,2% распределены между малым и средним бизнесом. Детальная структура представлена в табл. 1.

Таблица 1  
Количество субъектов МСП в Москве [6]

| Период     | Всего    | Микро   | Малый  | Средний | ИП       |
|------------|----------|---------|--------|---------|----------|
| 10.12.2020 | 721 629  | 386 187 | 33 381 | 3 507   | 298 554  |
| 10.12.2025 | 906 816  | 377 949 | 40 939 | 5 377   | 482 551  |
| Прирост    | +185 187 | -8 238  | +7 558 | +1 870  | +183 997 |

Проведенный анализ данных показал, что за рассматриваемый пятилетний период (2020 и 2025 гг.) наблюдается рост числа ИП и общего числа субъектов малого и среднего предпринимательства, в то время как количество микропредприятий сократилось на 8 238 единиц или 2,1%. Данная ситуация объясняется следующими факторами: ужесточением фискальной политики в отношении юридических лиц, простотой ведения бизнеса в статусе ИП (по сравнению с юридическими лицами), а также целенаправленной поддержкой малых инновационных компаний со стороны государства. Следует отметить, что рост числа ИП также обусловлен привлекательностью упрощенной системы налогообложения, минимальной бюрократией и значительно более низкими административными расходами.

Одной из особенностей экономической сферы Москвы является высокая степень диверсификации, которая проявляется в отсутствии какой-либо одной доминирующей отрасли. В сфере МСП к лидирующим отраслям можно отнести: розничную и оптовую торговлю (31%), профессиональную и научную деятельность (13%), деятельность по операциям с недвижимым имуществом (10%) и строительство (8%) (рис. 2). Структура видов деятельности МСП Москвы отражает постиндустриальный характер экономики столицы, где доминируют услуги и высокотехнологичные сектора.

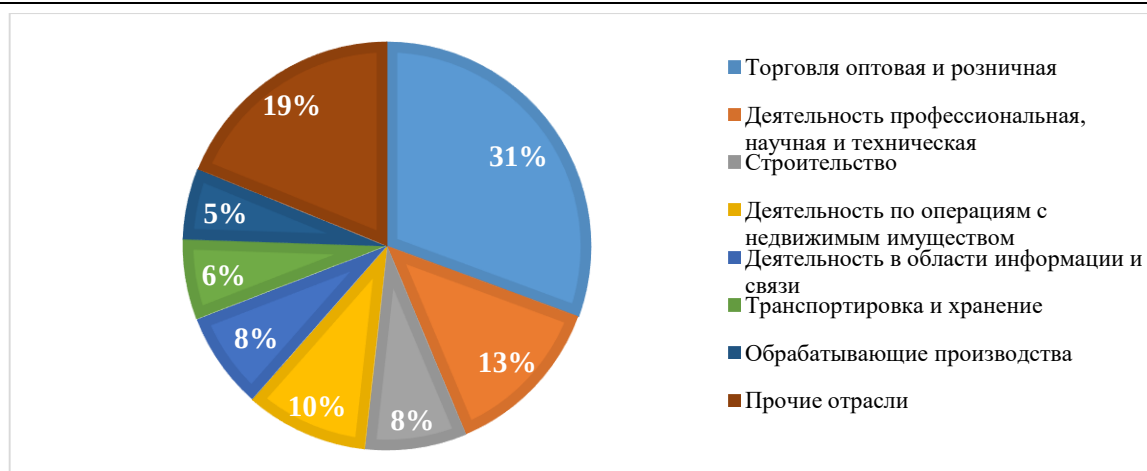


Рисунок 2. Доля субъектов МСП в разрезе видов деятельности [8]

Валовой региональный продукт Москвы – один из основных показателей, характеризующих развитие и размеры экономики города. За последние 5 лет прирост ВРП составил 79,6%, и в 2024 году он превысил 41 трлн рублей. Экономическая сфера Москвы является крупнейшей среди субъектов Российской Федерации по объему ВРП: на долю столицы приходится почти 21% суммарного ВРП страны. Динамика ВРП Москвы за 2020–2024 гг. отражена в табл.2.

Таблица 2  
Динамика ВРП г. Москвы 2020-2024 гг. [8]

| Период        | 2020         | 2021         | 2022         | 2023         | 2024         |
|---------------|--------------|--------------|--------------|--------------|--------------|
| ВРП, млн руб. | 22 821 980,4 | 27 287 345,8 | 30 542 556,2 | 36 523 200,1 | 41 003 635,6 |

Доля МСП в ВРП Москвы в 2024 году составила 25%, что в денежном эквиваленте равно 10,2 трлн руб. Сектор МСП является крупным работодателем: в 2024 году в нем было занято 2,3 млн человек – 28% от общей численности занятых в Москве (рис. 3).

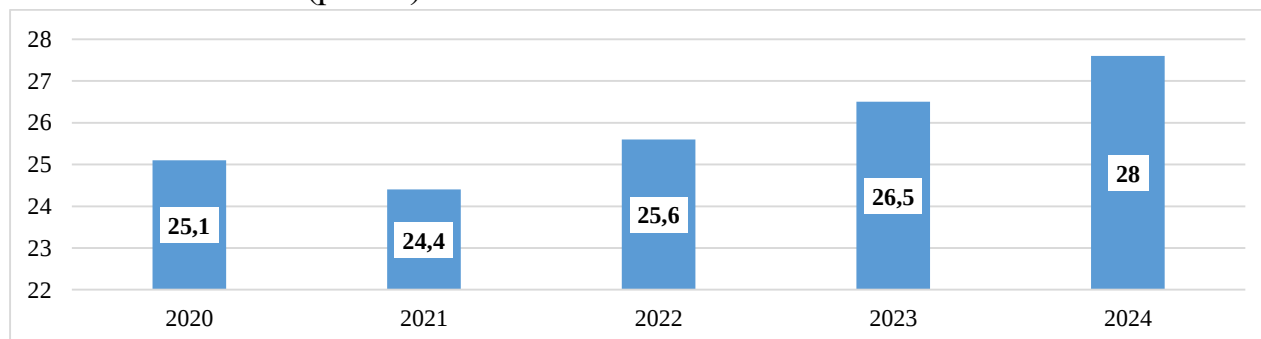


Рисунок 3. Доля занятых в секторе МСП в разрезе общей занятости в г. Москва [5,8]

Общий объем налоговых поступлений от субъектов МСП в бюджет города составил в 2025 году 1,2 трлн руб., или 27% от налоговых доходов бюджета Москвы (рис. 4).

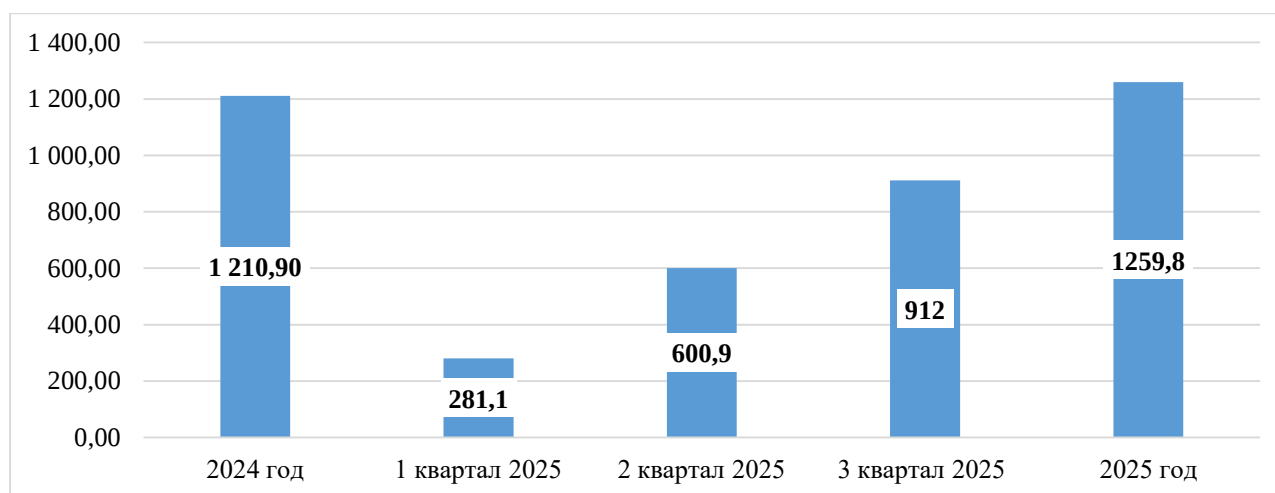


Рисунок 4. Динамика налоговых отчислений от субъектов МСП в бюджет г. Москва [5]

Для оценки экономической безопасности субъектов МСП во взаимосвязи с безопасностью региона использована методика Няргинен В.А. [20], основанная на интегральном подходе. Первый этап – идентификация ключевых показателей и сбор данных за 2020–2024 гг. Пороговые значения взяты из паспортов национального проекта «Малое и среднее предпринимательство» и данных Росстата (табл. 3).

Таблица 3  
Пороговые значения ключевых показателей развития МСП [1,2,8]

| Показатель                                                 | Пороговое значение | Факт 2024 | Оценка  |
|------------------------------------------------------------|--------------------|-----------|---------|
| Доля МСП в ВРП, %                                          | 32,5 [16]          | 24,9      | хорошо  |
| Численность работников на 1 субъекта МСП                   | 3,16 [16]          | 2,6       | хорошо  |
| Доля занятых в МСП в общей занятости, %                    | 35 [44]            | 27,6      | хорошо  |
| Доля МСП в инвестициях в основной капитал, %               | 15* [44]           | 19,8      | отлично |
| Удельный вес предприятий с технологическими инновациями, % | 30 [44]            | 42,4      | отлично |
| Ежегодный рост выручки на 1 субъекта (юридическое лицо), % | 103,76 [16]        | 129,6     | отлично |

Второй этап – нормирование значений с использованием индексного метода Сенчагова–Митякова [3] по формуле (1) для «эффективных» показателей. Зоны экономического риска определяются по табл. 2.4.

Таблица 4  
Зоны экономического риска [2]

| Стабильность | Умеренный риск | Значительный риск | Критический риск | Катастрофический риск |
|--------------|----------------|-------------------|------------------|-----------------------|
| более 1      | 0,75 – 1       | 0,50 – 0,75       | 0,25 – 0,50      | менее 0,25            |

Результаты расчета индексов показателей за 2020–2024 гг. представлены в табл. 5.

Таблица 5  
Индексы показателей развития МСП [2]

| Показатель                                                                                                       | 2020 | 2021 | 2022 | 2023 | 2024 |
|------------------------------------------------------------------------------------------------------------------|------|------|------|------|------|
| Доля МСП в ВРП, %                                                                                                | 0,71 | 0,78 | 0,84 | 0,85 | 0,86 |
| Численность работников в расчете на 1 субъекта МСП                                                               | 0,98 | 0,92 | 0,91 | 0,89 | 0,90 |
| Доля занятых в секторе малого и среднего предпринимательства в общей численности занятых, %                      | 0,83 | 0,81 | 0,84 | 0,85 | 0,87 |
| Доля малого и среднего предпринимательства в общем объеме инвестиций в основной капитал, %                       | 1,06 | 1,09 | 1,15 | 1,14 | 1,15 |
| Удельный вес малых и средних предприятий, осуществляющих технологические инновации в общем объеме предприятий, % | 0,56 | 0,56 | 0,57 | 0,53 | 1,18 |
| Ежегодный рост выручки в расчете на 1 субъекта МСП, юридическое лицо                                             | 1,08 | 1,12 | 1,03 | 1,10 | 1,12 |

К 2024 году в зоне стабильности находятся показатели доли инвестиций, инновационной активности (с переходом из зоны значительного риска) и роста выручки. Показатели доли МСП в ВРП, численности работников и занятости находятся в зоне умеренного риска, но имеют тенденцию к росту.

Третий этап – визуализация с помощью лепестковой диаграммы (рис. 5). Наиболее нестабильным показателем является удельный вес инновационных предприятий.

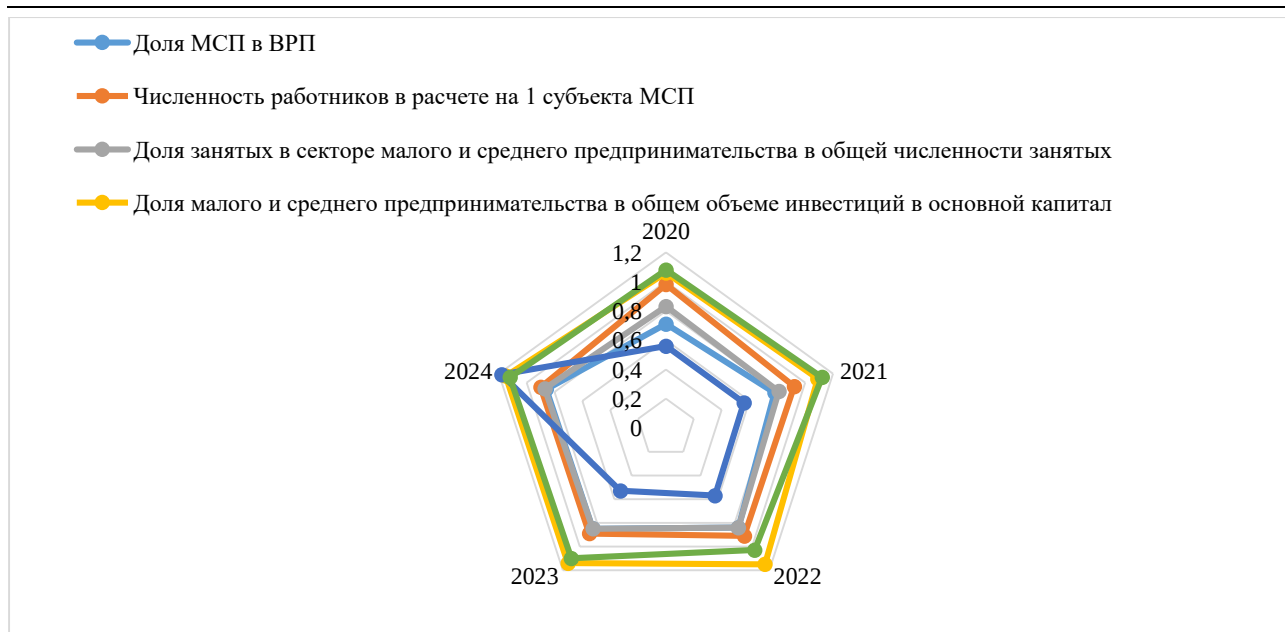


Рисунок 5. Лепестковая диаграмма нормированных значений индикаторов МСП в контексте экономической безопасности региона за 2020–2024 год [2,7]

Далее рассчитан обобщенный индекс экономической безопасности (ОЭБ) по формуле (2). Результаты представлены на рис. 6.

$$I = \frac{\sum_{i=1}^N y_i}{N} \quad (1)$$

где:  $I$  – обобщенный индекс ОЭБ;  
 $i$  – индексы показателей развития МСП;  
 $N$  – число индексов показателей развития МСП.

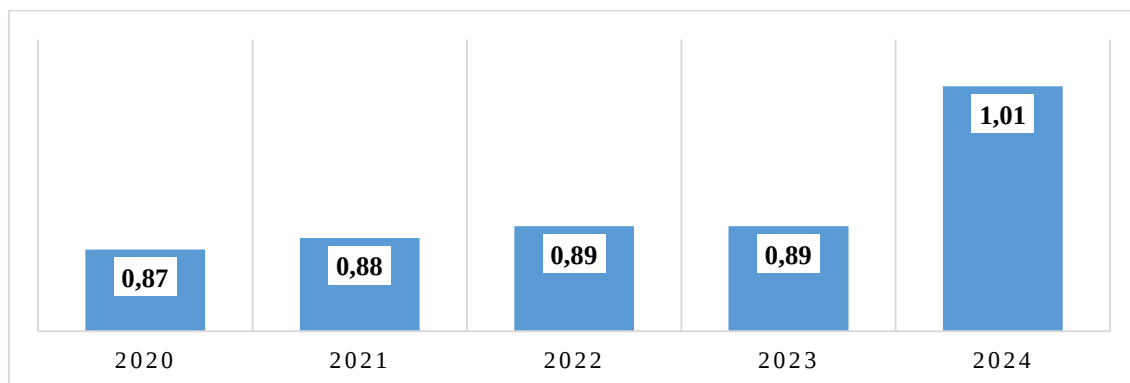


Рисунок 6. Обобщенный индекс обеспечения ЭБ субъектов МСП  
г. Москва 2020-2024 гг.

В 2020–2023 гг. обобщенный индекс находился в зоне умеренного риска (0,87–0,92), в 2024 году он вошел в зону стабильности (1,01). Однако индекс неустойчив из-за высокой волатильности показателя инновационной активности.

Заключительный этап – частотный анализ попадания индикаторов в зоны риска (табл. 6).

Таблица 6

Число попадания индикаторов показателей развития МСП в зоны риска экономической безопасности согласно индексной методике оценки

| Индикатор                                                                                                        | Диапазоны вариации |        |          |          |        |
|------------------------------------------------------------------------------------------------------------------|--------------------|--------|----------|----------|--------|
|                                                                                                                  | >1                 | 0,75-1 | 0,5-0,75 | 0,25-0,5 | 0-0,25 |
| Доля МСП в ВРП, %                                                                                                | 0                  | 4      | 1        | 0        | 0      |
| Численность работников в расчете на 1 субъекта МСП                                                               | 0                  | 5      | 0        | 0        | 0      |
| Доля занятых в секторе малого и среднего предпринимательства в общей численности занятых, %                      | 0                  | 5      | 0        | 0        | 0      |
| Доля малого и среднего предпринимательства в общем объеме инвестиций в основной капитал, %                       | 5                  | 0      | 0        | 0        | 0      |
| Удельный вес малых и средних предприятий, осуществляющих технологические инновации в общем объеме предприятий, % | 1                  | 0      | 4        | 0        | 0      |
| Ежегодный рост выручки в расчете на 1 субъекта МСП, юридическое лицо                                             | 5                  | 0      | 0        | 0        | 0      |

Анализ показал, что основными угрозами развития МСП в контексте экономической безопасности региона являются:

- низкий уровень инновационной активности (4 года в зоне значительного риска);
- недостаток рабочей силы в сфере МСП (стабильно в зоне умеренного риска);
- недостаток квалифицированных работников.

Проведенный анализ свидетельствует, что сектор МСП Москвы обладает огромным потенциалом: большинство показателей имеют тенденцию к росту, обобщенный индекс экономической безопасности в 2024 году вошел в зону стабильности, что положительно сказывается на обеспечении экономической безопасности региона. Вклад МСП в ВРП, занятость и налоговые поступления устойчиво растут. Однако такие угрозы, как низкая инновационная активность и дефицит квалифицированных кадров, требуют постоянного мониторинга и

дополнительных мер государственной поддержки. Рекомендуются проведение регулярной оценки индикаторов для предотвращения возврата в зону умеренного риска.

### Список литературы

1. Паспорт национального проекта «Малое и среднее предпринимательство и поддержка индивидуальной предпринимательской инициативы»: утвержден Министерством экономического развития России, апрель 2021. – Текст: электронный // СПС «Гарант». – URL: <https://base.garant.ru/400664238/> (дата обращения 15.04.2026).

2. Няргинен, В. А. Инструменты обеспечения экономической безопасности субъектов малого и среднего предпринимательства: диссертация ... кандидата экономических наук: 5.2.3 / Няргинен Виктория Анатольевна; место защиты: ФГБОУ ВО «МИРЭА – Российский технологический университет». – Москва, 2024. – 178 с. – Текст: непосредственный.

3. Сенчагов, В. К. Использование индексного метода для оценки уровня экономической безопасности / В. К. Сенчагов, С. Н. Митяков. – Текст: непосредственный // Вестник Академии экономической безопасности МВД России. – 2011. – № 5. – С. 41–50.

4. Анофриков, С. П. Экономическая безопасность регионов / С. П. Анофриков. – Текст: электронный // ЕГИ. – 2023. – № 5 (49). – URL: <https://cyberleninka.ru/article/n/ekonomicheskaya-bezopasnost-regionov-1> (дата обращения 10.03.2026).

5. Департамент предпринимательства и инновационного развития города Москвы: официальный сайт. – Москва. – URL: <https://www.mos.ru/dpir/> (дата обращения 01.05.2026). – Текст: электронный.

6. Единый реестр субъектов малого и среднего предпринимательства: официальный сайт. – Москва. – URL: <https://rmsp.nalog.ru/> (дата обращения: 10.03.2026). – Текст: электронный.

7. Сенчагов, В. К. Использование индексного метода для оценки уровня экономической безопасности / В. К. Сенчагов, С. Н. Митяков. – Текст: электронный // Вестник экономической безопасности. – 2011. – № 5. – URL: <https://cyberleninka.ru/article/n/ispolzovanie-indeksnogo-metoda-dlya-otsenki-urovnya-ekonomicheskoy-bezopasnosti> (дата обращения 17.04.2026).

8. Хирунцев, С. В. Роль малого и среднего бизнеса в экономике Москвы: анализ текущего состояния и тенденций развития / С. В. Хирунцев. – Текст: электронный // Вестник Академии права и управления. – 2024. – № 4 (79). – URL: <https://cyberleninka.ru/article/n/rol-malogo-i-srednego-biznesa-v-ekonomike-moskvy-analiz-tekuschego-sostoyaniya-i-tendentsiy> (дата обращения 20.03.2026).

**Перанов Михаил Борисович**

студент 5 курса

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

Научный руководитель

**Няргинен Виктория Анатольевна**

кандидат экономических наук

доцент кафедры экономической экспертизы и финансового мониторинга

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

## **Роль финансового мониторинга в системе противодействия нецелевому использованию бюджетных средств**

**Аннотация.** В статье рассматривается роль финансового мониторинга в системе противодействия нецелевому использованию бюджетных средств. Обосновывается, что эффективное функционирование системы невозможно без применения специализированных механизмов сбора, анализа и оценки финансовых операций, обладающих признаками нарушений. Особое внимание уделяется взаимодействию Росфинмониторинга с иными контрольными и правоохранительными органами.

**Ключевые слова:** финансовый мониторинг, нецелевое использование бюджетных средств, Росфинмониторинг, маркеры риска, экономическая безопасность, бюджетный контроль, противодействие легализации доходов.

Современная система противодействия нецелевому использованию бюджетных средств не может эффективно функционировать без применения специализированных механизмов выявления, анализа и оценки финансовых операций, обладающих признаками нарушений. Ключевое место среди таких механизмов занимает финансовый мониторинг, представляющий собой совокупность мер по сбору, обработке, анализу информации о финансовых операциях и их участниках в целях противодействия неправомерному использованию финансовых ресурсов. В обеспечении экономической безопасности государства финансовый мониторинг выступает не просто вспомогательным инструментом, а самостоятельным и чрезвычайно значимым элементом институциональной системы, позволяющим выявлять нарушения, прослеживать движение бюджетных средств на всех этапах и своевременно предотвращать их нецелевое использование.

В узком смысле под финансовым мониторингом понимается деятельность Росфинмониторинга и иных субъектов (кредитных организаций, профучастников рынка ценных бумаг, страховых организаций) по сбору, анализу и передаче информации об операциях, подлежащих обязательному контролю, а

также об операциях, в отношении которых возникают подозрения. В широком смысле финансовый мониторинг охватывает всю совокупность государственных и негосударственных институтов, обеспечивающих прозрачность финансовых потоков.

Система субъектов финансового мониторинга имеет сложную, многоуровневую структуру, включающую как государственные органы, так и негосударственные организации. Система субъектов, их функции и роли финансового мониторинга представлены на рис. 1.

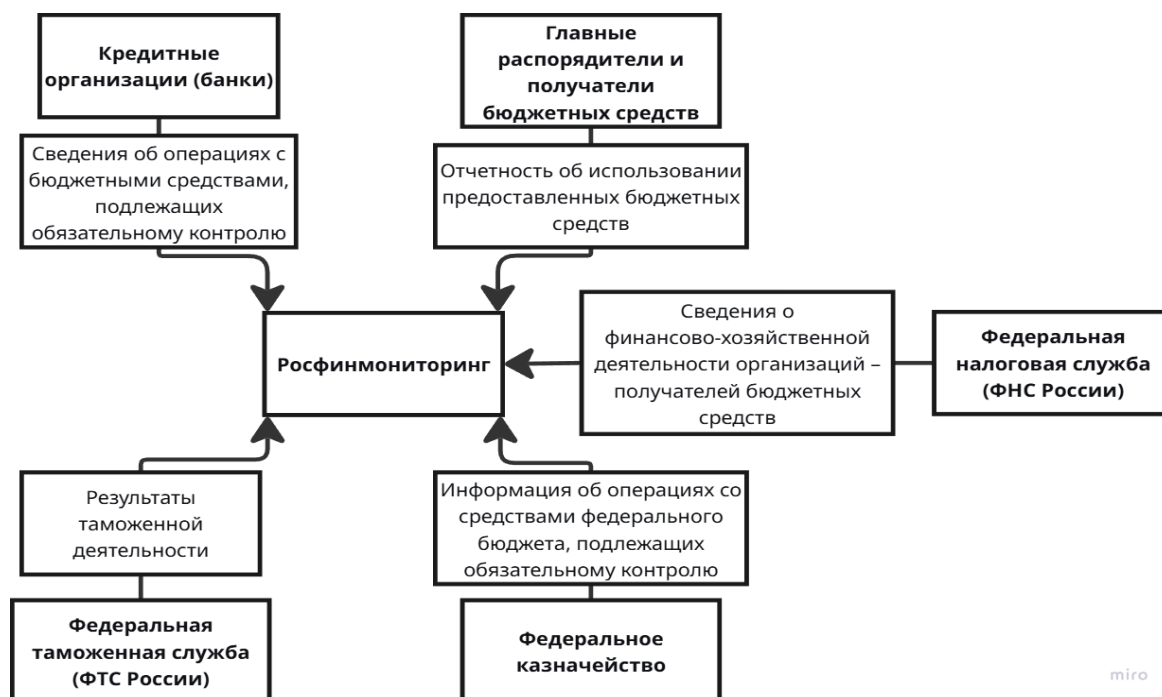


Рисунок 1. Система субъектов, их функции и роли, финансового мониторинга

Центральным элементом системы является Росфинмониторинг, выполняющий функции национального центра, по оценке угроз. Его ключевые функции: сбор и анализ информации об операциях с бюджетными средствами, выявление операций с признаками нецелевого использования, формирование межведомственной информационной системы, направление информации о нарушениях в правоохранительные органы [1].

Федеральное казначейство выступает одновременно субъектом бюджетного контроля и участником финансового мониторинга, осуществляя санкционирование операций и представляя информацию в Росфинмониторинг. Кредитные организации выполняют функции первичного финансового мониторинга: идентифицируют клиентов, выявляют операции, подлежащие обязательному контролю, и направляют информацию в Росфинмониторинг. Главные распорядители и получатели бюджетных средств являются одновременно объектами мониторинга и субъектами внутреннего контроля.

В практике финансового мониторинга используется широкий арсенал инструментов и методик, позволяющих выявлять операции с бюджетными средствами, обладающие признаками нецелевого использования. Классификация методик финансового мониторинга представлена в табл. 1.

Таблица 1

Классификация методик финансового мониторинга [2,3,4]

| Основание                        | Методика                      | Характеристика                                                                                                                                                                                                                                                                                  |
|----------------------------------|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| По стадии применения             | Предварительный мониторинг    | Осуществляется до совершения операции с бюджетными средствами.                                                                                                                                                                                                                                  |
|                                  | Текущий мониторинг            | Проводится непосредственно в момент совершения финансовой операции.                                                                                                                                                                                                                             |
|                                  | Последующий мониторинг        | Выполняется после завершения операции на основе отчетных данных.                                                                                                                                                                                                                                |
| По характеру используемых данных | Документарный мониторинг      | Анализ документов-оснований (сметы, контракты, платежные поручения). Проверяется наличие реквизитов, соответствие сумм лимитам и соблюдение процедурных требований (например, порядка принятия обязательств).                                                                                   |
|                                  | Аналитический мониторинг      | Использование методов экономического и финансового анализа:<br>Горизонтальный анализ (сравнение динамики расходов).<br>Вертикальный анализ (оценка структуры расходов).<br>Коэффициентный анализ (расчет ликвидности, рентабельности).<br>Сравнительный анализ (сопоставление цен с рыночными). |
|                                  | Электронный мониторинг        | Осуществляется через Единую информационную систему (ЕИС) Росфинмониторинга. Обеспечивает сбор данных, отслеживание цепочек транзакций и установление взаимосвязей между участниками операций.                                                                                                   |
| По степени автоматизации         | Ручной мониторинг             | Проверка документов и данных осуществляется специалистом вручную, без использования специальных программ.                                                                                                                                                                                       |
|                                  | Автоматизированный мониторинг | Использование программных комплексов и баз данных (например, ЕИС) для сбора и первичного анализа информации.                                                                                                                                                                                    |
|                                  | Интеллектуальный мониторинг   | Применение алгоритмов машинного обучения для:<br>Выявления аномалий в движении средств.<br>Прогнозирования рисков нецелевого использования.<br>Поиска скрытых связей между контрагентами.<br>Классификации нарушений по степени опасности.                                                      |

Для систематизации работы по выявлению признаков нецелевого использования активно используются «маркеры риска» – это совокупность критериев, позволяющих идентифицировать подозрительные операции. Система маркеров риска нецелевого использования бюджетных средств в практике финансового мониторинга представлена в табл. 2.

Таблица 2

Система маркеров риска нецелевого использования бюджетных средств  
в практике финансового мониторинга [2,3,4,5,6]

| Группа маркеров | Конкретные индикаторы                                                                                            | Источники информации                        |
|-----------------|------------------------------------------------------------------------------------------------------------------|---------------------------------------------|
| Операционные    | Снятие наличных вскоре после поступления средств, транзитные операции, несоответствие операций виду деятельности | Выписки по счетам, платежные поручения      |
| Субъектные      | Контрагенты с признаками номинальности, аффилированность, оффшорная регистрация                                  | ЕГРЮЛ, реестры недобросовестных поставщиков |
| Ценовые         | Завышение цен, дробление контрактов, неоднократное увеличение цены                                               | Реестр контрактов, коммерческие предложения |
| Количественные  | Закупки сверх потребности, наличие неиспользуемого имущества                                                     | Отчетность, инвентаризационные описи        |
| Временные       | Платежи в выходные дни, «штурмовщина» в конце периода                                                            | Платежные поручения, контракты              |

Эффективность финансового мониторинга во многом определяется налаженностью механизмов взаимодействия Росфинмониторинга с иными государственными органами. Данное взаимодействие осуществляется в формах информационного, оперативного, аналитического и координационного взаимодействия. Особое значение имеет взаимодействие с органами прокуратуры на основании совместного приказа Генеральной прокуратуры РФ и Росфинмониторинга.

Практика деятельности свидетельствует о высокой эффективности применяемых инструментов. По информации Росфинмониторинга, ежегодно выявляется несколько тысяч операций с бюджетными средствами, обладающих признаками нецелевого использования. Объем таких операций исчисляется десятками миллиардов рублей. Типичными схемами являются: обналичивание бюджетных средств, вывод средств за рубеж через оффшорные компании, фиктивные сделки, завышение цен, дробление контрактов, а также использование средств, выделенных на конкретные проекты, на иные цели.

Теоретико-методологический анализ позволяет сделать вывод, что нецелевое использование бюджетных средств представляет собой системную угрозу экономической безопасности, оказывающую комплексное деструктивное воздействие на фискальную, экономическую, социальную и институциональную сферы. Финансовый мониторинг является важнейшим элементом системы противодействия данному явлению, обеспечивающим выявление латентных нарушений и прослеживание движения средств на всех этапах. Правовую основу составляет Федеральный закон № 115-ФЗ. Система субъектов включает Росфинмониторинг, Федеральное казначейство, кредитные организации и

получателей средств. Разработанный инструментарий, включающий документарный, аналитический и автоматизированный мониторинг, а также систему маркеров риска, позволяет своевременно выявлять и пресекать нарушения. Дальнейшее совершенствование механизмов взаимодействия между уполномоченными органами и внедрение технологий интеллектуального анализа данных будут способствовать повышению эффективности противодействия нецелевому использованию бюджетных средств.

### Список литературы

1. Указ Президента РФ от 13.06.2012 № 808 «Вопросы Федеральной службы по финансовому мониторингу» (ред. от 25.02.2025) // Собрание законодательства РФ. — 2012. — № 25. — Ст. 3346.
2. Публичный отчет о работе Федеральной службы по финансовому мониторингу за 2022 год / Росфинмониторинг. — М., 2023. — 38 с.
3. Годовой отчет о работе Федеральной службы по финансовому мониторингу. 2023 / Росфинмониторинг. — М., 2024. — 37 с.
4. Годовой отчет о работе Федеральной службы по финансовому мониторингу. 2024 / Росфинмониторинг. — М., 2025. — 40 с.
5. Состояние преступности в России за январь – декабрь 2022 года: статистический сборник / ФКУ «Главный информационно-аналитический центр» МВД России. — М., 2023. — 68 с.
6. Состояние преступности в России за январь – декабрь 2023 года: статистический сборник / ФКУ «Главный информационно-аналитический центр» МВД России. — М., 2024. — 66 с.
7. Состояние преступности в России за январь – декабрь 2024 года: статистический сборник / ФКУ «Главный информационно-аналитический центр» МВД России. — М., 2025. — 67 с.

**Петрова Дарья Ивановна**

студент 5 курса

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

Научный руководитель

**Шеверева Елена Александровна**

кандидат экономических наук, доцент

доцент кафедры экономической экспертизы и финансового мониторинга

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

## **Четырехуровневая система налоговых паспортов как фактор снижения налоговых рисков и роста бюджетных доходов**

**Аннотация.** В статье рассматриваются вопросы обеспечения налоговой безопасности государства как базового элемента его экономической стабильности. В ходе исследования выявлен критический рост вертикального дисбаланса бюджетной системы. Также зафиксировано снижение операционной эффективности выездных налоговых проверок. Для минимизации выявленных рисков предложено внедрение цифрового инструмента — четырехуровневой системы налоговых паспортов. Паспорт спроектирован как аналитический модуль в составе АИС «Налог-3». Данное решение позволит автоматизировать комплекс и выявлять теневые схемы в режиме реального времени.

**Ключевые слова:** налоговая безопасность, налоговые риски, налоговый паспорт, фискальный эффект, угрозы.

Ключевым элементом системы экономической безопасности государства является налоговая безопасность. Поскольку налоговая система государства является важнейшим инструментом перераспределения ВВП, она является зоной повышенного риска, где сталкиваются фискальные интересы государства и интересы добросовестных налогоплательщиков. Для эффективного управления налоговыми рисками необходим постоянный мониторинг показателей налоговой безопасности, отражающих как фискальную эффективность налоговой системы, так и уровень напряжённости в отношениях между государством и налогоплательщиками (рис. 1).

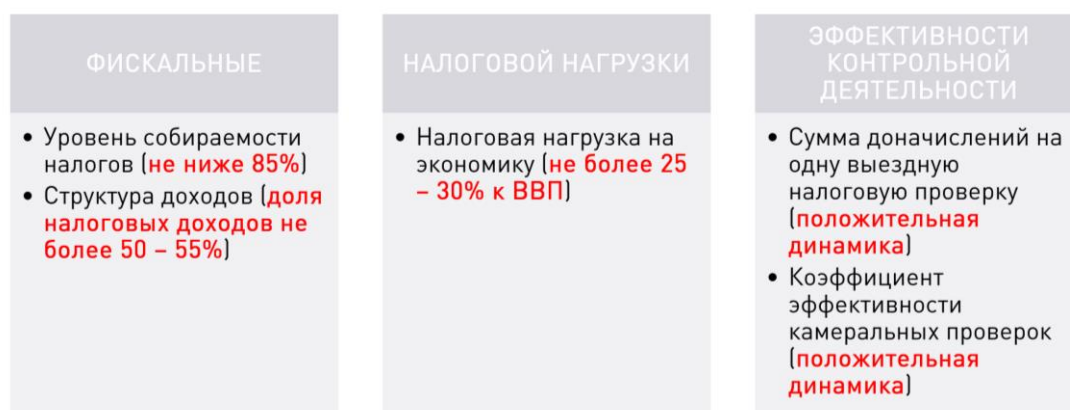


Рисунок 1. Показатели налоговой безопасности

Анализ динамики этих показателей позволяет выявить дисбаланс в системе, оценить результативность контрольной работы ФНС России и определить перспективные направления минимизации рисков (табл. 1).

Таблица 1  
Оценка соответствия параметров налоговой безопасности пороговым значениям

| Показатель                                         | Фактическое значение (2020–2025 гг) | Пороговое значение     | Соответствие     | Оценка риска                     |
|----------------------------------------------------|-------------------------------------|------------------------|------------------|----------------------------------|
| Уровень собираемости налогов                       | 107,6–102,9%                        | не ниже 85%            | Соответствует    | Низкий                           |
| Доля налоговых доходов федерального бюджета        | 72,53–79,61%                        | не более 50 – 55%      | Не соответствует | Высокий (вертикальный дисбаланс) |
| Сумма доначислений на одну ВВП (млн. руб.)         | 31,95 – 17,4                        | положительная динамика | Не соответствует | Высокий (риск администрирования) |
| Эффективность камеральных проверок (руб./проверку) | 853 – 15 030                        | положительная динамика | Соответствует    | Низкий                           |

В частности, исследование параметров налоговой безопасности за период с 2020 – по 2025 годы позволил сделать следующие выводы.

1. **Уровень собираемости налогов** превышает пороговое значение, что свидетельствует о низком фискальном риске недополучения бюджетных доходов.

2. Доля налоговых доходов федерального бюджета выросла с 72 с

половиной % до почти 80 % при пороговом значении до 55%, что создаёт высокий риск усиления вертикального дисбаланса бюджетной системы и снижения финансовой самостоятельности регионов.

3. **Внедрение риск-ориентированного подхода** позволило сократить количество выездных проверок в 2024 году, но в 2025 году их количество опять выросло практически в 2 раза, при этом доначисления на одну проверку сократились с тем же темпом. Все это характеризует наличие критического операционного и стратегического риска снижения эффективности налогового администрирования. В реальной практике ФНС такой сценарий считается негативным, так как согласно риск-ориентированному подходу на выездную налоговую проверку инспекторы налоговой службы выходят только тогда, когда скрытые бенефициары и точная сумма неуплаченных налогов уже фактически определены на этапе предпроверочного анализа.

Все это позволило сделать вывод о том, что налоговые органы нуждаются в дополнительных инструментах, которые позволяют в режиме реального времени обрабатывать огромные массивы данных о финансово-хозяйственной деятельности налогоплательщиков, выявлять отклонения и осуществлять прогнозирование возможных нарушений. В последние годы ФНС России внедрила ряд прогрессивных аналитических инструментов (АСК НДС-2, АИС «Налог-3» и др.), которые основаны на цифровых технологиях, но изменение экономической ситуации, появление новых способов минимизации налоговых обязательств, а также необходимость соблюдения баланса между фискальным давлением и стимулированием деловой активности требуют постоянного совершенствования подходов к анализу и минимизации налоговых рисков.

В качестве наиболее перспективного направления развития налогового администрирования можно предложить внедрение **налогового паспорта всех уровней (от** юридического лица, индивидуального предпринимателя, физического лица до муниципального образования и региона в целом) как инструмента, объединяющего в себе функции идентификации, оценки, мониторинга и прогнозирования налоговых рисков.

Налоговый паспорт организации представляет собой структурированный электронный документ (а именно модуль в составе АИС «Налог-3»), который аккумулирует все значимые сведения о налоговой истории налогоплательщика, включая его текущее состояние и прогнозируемые риски. В отличие от «досье налогоплательщика», носящего преимущественно информационный характер, налоговый паспорт должен стать **активным инструментом управления рисками**, который позволяет в режиме реального времени оценивать уровень добросовестности организации и прогнозировать вероятность совершения налоговых правонарушений.

Предлагаемый налоговый паспорт существенно повышает прозрачность взаимодействия бизнеса и государства, предоставляя налогоплательщику

полный доступ к конкретным критериям риска, отклонениям и пороговым значениям в личном кабинете. В отличие от закрытой Системы управления рисками (СУР), новый формат позволяет компаниям самостоятельно устранять нарушения, прогнозировать вероятность проверок и суммы доначислений, а также оперативно реагировать на риски благодаря учету отраслевых индикаторов и интеграции с внешними данными в режиме реального времени, что, в свою очередь, позволяет ФНС видеть зарождение серых схем не через год-два, а непосредственно в момент совершения операций.

Для государства налоговый паспорт — это инструмент создания цифровой экосистемы, где бизнес контролирует себя сам, а налоговые органы выполняют роль ИТ-платформы, собирающей налоги автоматически и с максимальным уровнем добровольного комплаенса со стороны бизнеса.

По расчетам экономический эффект от внедрения налоговых паспортов может составить 39 млрд.руб. Исходными данными для исследования послужили официально публикуемые материалы Федеральной Налоговой Службы РФ (табл. 2).

Таблица 2  
Расчет экономического эффекта

| Параметр                                                     | Значение |
|--------------------------------------------------------------|----------|
| <b>Исходные данные (по итогам 2025 года, форма 2-НК ФНС)</b> |          |
| Выездные проверки, всего                                     | 7 617    |
| Из них не выявили нарушений                                  | 3 780    |
| Доначисления по результативным проверкам, млрд.руб.          | 132,6    |
| Количество результативных проверок                           | 3 837    |
| <b>Расчет параметров результативности</b>                    |          |
| Средняя результативность одной проверки, млн.руб.            | 34,55    |
| Фискальный эффект, млрд.руб.                                 | 39,18    |

Для практического использования налогового паспорта необходимо предпринять меры правового и кадрового характера. А именно, включить новую статью в НК РФ «Налоговый паспорт», законодательно исключить «зелёную» категорию риска из плана выездных проверок, утвердить открытую методику оценки рисков приказом ФНС. Помимо этого, эффективными могут быть меры кадрового характера, которые позволят оптимизировать оплату труда

инспекторов, в том числе посредством использования сбалансированной системы KPI, ориентированной на качественные показатели и системы непрерывного обучения работе с большими данными и ИИ.

### Список литературы

1. Официальный сайт Федеральной налоговой службы России. – URL: <https://www.nalog.ru/> (дата обращения: 15.03.2026).
2. Клерк.ру: какие программы использует ФНС для выявления налоговых рисков по НДС: принцип их работы и меры безопасности для бизнеса. – URL: <https://www.klerk.ru/razbory/kakie-programmy-ispolzuets-fns-dlya-vyyavleniya-nalogovyh-riskov-po-nds-princip-ih-raboty-i-mery-bezopasnosti-dlya-biznesa/> (дата обращения: 20.03.2026).
3. Официальный сайт ФНС России: сервис «Прозрачный бизнес». – URL: [https://www.nalog.gov.ru/rn77/service/proz\\_biz/](https://www.nalog.gov.ru/rn77/service/proz_biz/) (дата обращения: 21.03.2026).

**Сигунова Татьяна Анатольевна**  
кандидат экономических наук  
профессор кафедры финансового учета и контроля  
ФГБОУ ВО «МИРЭА – Российский технологический университет»  
Россия, г. Москва

**Клюев Александр Владиславович**  
студент 4 курса  
ФГБОУ ВО «МИРЭА – Российский технологический университет»  
Россия, г. Москва

## **Цифровизация системы государственных закупок: эффективность антикоррупционного контроля и технологические вызовы**

**Аннотация.** В статье рассматривается влияние цифровизации на систему государственных закупок в Российской Федерации с акцентом на эффективность антикоррупционного контроля и технологические уязвимости цифровой инфраструктуры. Анализируются правовые основы закупок по 44-ФЗ и 223-ФЗ, роль Единой информационной системы и электронных торговых площадок на основных стадиях закупочного цикла. Выявляются типичные схемы искажения конкуренции и оцениваются масштабы сохраняющихся коррупционных рисков на основе эмпирических данных. Сформулированы направления совершенствования системы: унификация технических заданий, развитие риск-ориентированных аналитических инструментов на базе больших данных и искусственного интеллекта, а также усиление ответственности заказчиков за формирование конкурентных условий закупки.

**Ключевые слова:** система государственных закупок, единая информационная система, антикоррупционный контроль, эффективности цифровизации в сфере закупок.

Сфера государственных закупок Российской Федерации вслед за другими отраслями экономики активно внедряет инструменты цифровизации. Это связано с необходимостью более эффективного расходования бюджетных средств и развитием конкурентной среды. Переход к электронным форматам заметно изменил как характер взаимодействия государства с бизнесом, так и саму организацию закупочного процесса.

Единая информационная система в сфере закупок и электронные торговые площадки расширили доступ участников к информации о торгах, сделали процедуры более прозрачными и усилили возможности бюджетного контроля. Исследователи отмечают, что электронные торги, автоматизированный документооборот и открытые данные действительно способствуют росту конкуренции, снижению транзакционных издержек и сокращению части

коррупционных рисков, прежде всего связанных с личными контактами между заказчиком и поставщиком.

Одновременно практика показывает, что вместе с преимуществами цифровой среды сохраняются и новые проблемы: технические, правовые и институциональные. Даже при развитии цифровых решений остаются устойчивые недобросовестные практики, включая подготовку документации под конкретного исполнителя и использование формально законных, но фактически ограничивающих конкуренцию условий закупки.

В этих условиях возрастает значение анализа того, насколько эффективен антикоррупционный контроль в цифровой системе закупок и какие технологические уязвимости сохраняются в действующей инфраструктуре. Цель статьи состоит в анализе государственных закупок в условиях цифровизации с акцентом на результативность антикоррупционных механизмов и технологические уязвимости действующей инфраструктуры.

В Российской Федерации на практике выделяют три вида закупок: закупки по 44-ФЗ, закупки по 223-ФЗ и коммерческие закупки, регулируемые нормами гражданского законодательства. В рамках настоящего исследования рассматриваются только закупки, регулируемые федеральными законами, поскольку в коммерческих закупках перечень процедур в значительной части определяется самим заказчиком.

Федеральный закон № 44-ФЗ регулирует закупки для обеспечения государственных и муниципальных нужд и отличается высокой степенью формализации процедур. Федеральный закон № 223-ФЗ применяется к закупкам отдельных видов юридических лиц и предоставляет заказчикам больше свободы через положение о закупке при сохранении общих принципов открытости и недопустимости ограничения конкуренции (табл. 1).

Таблица 1

Сравнение законодательства в сфере государственных закупок

| Критерий            | Закупки по 44-ФЗ                                                                               | Закупки по 223-ФЗ                                                                                                                                                                          |
|---------------------|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Основное назначение | Обеспечение государственных и муниципальных нужд в рамках контрактной системы                  | Закупки товаров, работ и услуг отдельными видами юридических лиц, включая компании с государственным участием и естественные монополии                                                     |
| Типичные заказчики  | Органы государственной власти, органы местного самоуправления, казённые и бюджетные учреждения | Госкорпорации, хозяйственные общества с долей государства не менее 50%, их дочерние общества, естественные монополии и отдельные бюджетные учреждения при расходовании собственных средств |

|                      |                                                                                                                         |                                                                                                                                                   |
|----------------------|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Степень формализации | Подробно регламентируются этапы закупочного цикла, способы определения поставщика, требования к документации и контролю | Общие принципы закреплены в законе, а конкретные процедуры устанавливаются положением о закупке заказчика                                         |
| Контроль             | Развитый многоуровневый контроль, включая ФАС России, Федеральное казначейство, финансовый контроль и прокуратуру       | Контроль в большей мере сосредоточен на соблюдении процедурных принципов; значительная часть рисков связана с внутренними регламентами заказчиков |

Оба вида закупок фактически встроены в единую электронную среду, в которой информация размещается, обрабатывается и контролируется с использованием государственных информационных систем и электронных площадок. Это обеспечивает публичность процедур, упорядочивает документооборот и формирует цифровой след на всех основных этапах закупочного цикла — от планирования до исполнения контракта.

Таким образом, оба закона различаются по кругу субъектов-заказчиков и, соответственно, по степени государственного контроля. Кроме того, в закупках по 223-ФЗ часть документов может подаваться по корпоративным шаблонам конкретной компании, тогда как в закупках по 44-ФЗ формы и требования более унифицированы.

Ключевым элементом современной закупочной системы выступает Единая информационная система в сфере закупок, размещённая на портале [zakupki.gov.ru](http://zakupki.gov.ru). Через ЕИС публикуются извещения и документация, размещаются сведения о контрактах, жалобах, недобросовестных поставщиках, независимых гарантиях и других юридически значимых событиях.

Для поставщика ЕИС выполняет не только информационную, но также является местом, где происходит регистрация. В системе она служит основой для последующей аккредитации на электронных торговых площадках. Она является обязательной для заказчика, так как здесь раскрываются сведения о нём и подтверждается законность прохождения закупочных стадий. Именно за счёт централизации информации и формализации действий участников ЕИС формирует цифровой каркас закупочной системы.

Непосредственное проведение конкурентных процедур связано не только с ЕИС, но и с сопутствующими федеральными электронными торговыми площадками (РТС-тендер, Сбербанк-АСТ, Фабрикант, Газпромбанк ЭТП и так далее). Они обеспечивают подачу заявок, проведение ценовой конкуренции, обмен юридически значимыми электронными документами и фиксацию результатов торгов, а сведения о поставщиках и итогах процедур синхронизируются между площадками и ЕИС. Вдобавок, некоторые эксперты в

отрасли утверждают, что информации о торгах там больше, сам торги актуальнее.

Кроме классических площадок, в системе применяются агрегаторы, в том числе сервисы для закупок малого объёма. Они расширяют доступ малого бизнеса к государственному заказу и ускоряют проведение простых закупок, но одновременно усложняют техническую архитектуру системы и создают дополнительные точки потенциального сбоя или манипулирования условиями отбора. Но главной их целью является сбор информации о торгах с разных ЭТП и поиск/аналитика. Сами заявки подаются уже на исходной площадке

Функционирование закупок в ЕИС строится по логике закупочного цикла, который охватывает планирование, публикацию извещения, подачу заявок, проведение торгов, заключение и исполнение контракта. Такая модель обеспечивает формирование единого цифрового следа закупки и позволяет фиксировать действия заказчика, поставщиков и операторов электронных площадок на всех стадиях процедуры.

На стадии планирования заказчик определяет потребность в товарах, работах или услугах, соотносит её с лимитами бюджетного финансирования и отражает будущую закупку в плановых документах. Здесь же задаются базовые параметры процедуры: предмет закупки, ориентировочная цена, сроки и предполагаемый способ определения поставщика.

После этого в ЕИС публикуются извещение и закупочная документация, в которых раскрываются характеристики объекта закупки, условия участия, требования к заявке, проект контракта и сроки проведения процедуры. Открытый характер публикации имеет принципиальное значение для конкуренции, поскольку формально обеспечивает равный доступ к информации для всех потенциальных поставщиков.

Подача заявок осуществляется в электронной форме через аккредитованные электронные торговые площадки. Электронная форма подачи заявок сокращает временные и организационные издержки, а также снижает влияние территориального фактора на участие в закупках.

На этапе торгов осуществляется рассмотрение заявок, сопоставление предложений и определение победителя в зависимости от вида процедуры. Площадка технически фиксирует ценовые предложения, временные параметры и итоговые протоколы, а ЕИС выполняет функцию централизованного хранения и отображения результатов.

После определения победителя контракт заключается в электронной форме, а сведения о его заключении отражаются в реестрах и информационных блоках системы. На стадии исполнения в цифровой среде фиксируются поставка товара, приёмка результатов, оплата, изменение условий и при необходимости расторжение контракта, что обеспечивает прослеживаемость исполнения обязательств.

Одним из основных аргументов в пользу цифровизации закупок выступает усиление антикоррупционного контроля за счёт открытости информации, электронного документооборота и снижения доли неформальных контактов между заказчиком и потенциальным поставщиком. Цифровая фиксация действий участников и доступность данных о процедурах повышают выявляемость нарушений и упрощают надзор за соблюдением закупочного законодательства.

Таблица 2

Положительные и отрицательные эффекты от ведения торгов  
в электронной среде

| Элемент цифровой среды      | Антикоррупционный эффект                                  | Сохраняющаяся уязвимость                                                     |
|-----------------------------|-----------------------------------------------------------|------------------------------------------------------------------------------|
| ЕИС и открытые реестры      | Повышение прозрачности закупок и доступности данных       | Формальная открытость не исключает скрытого ограничения конкуренции          |
| Электронный документооборот | Фиксация действий и снижение неформального вмешательства  | Возможность манипуляций на этапе подготовки документации сохраняется         |
| ЭТП                         | Автоматизация процедур и фиксирование результатов торгов. | Возможны сговоры участников и техническая зависимость от платформ.           |
| Автоматизированный контроль | Выявление аномалий и риск-индикаторов                     | Ограниченная способность распознавать сложные содержательные злоупотребления |

Однако формальная цифровая прозрачность не устраняет проблему недобросовестного поведения полностью, а лишь меняет формы её проявления. На практике сохраняются ситуации, при которых документация составляется так, чтобы соответствовать характеристикам конкретного поставщика, хотя внешне процедура остаётся конкурентной и размещённой в открытом доступе.

По оценке Института государственного и муниципального управления НИУ ВШЭ, при объёме закупок 29,1 трлн руб. в 2020 году совокупный объём неформальных выплат в сфере госзаказа превышал 6,5–6,6 трлн руб., что составляло около 6% ВВП и было сопоставимо с третьей доходной части федерального бюджета. Средний размер «отката», по данным опроса поставщиков, достигал 22,5% цены контракта, а в отдельных случаях участники указывали на неформальные платежи до 60–65% стоимости договора.

Существенные масштабы нарушений фиксировались и финансовой разведкой. Согласно приведённым в статье данным, Росфинмониторинг сообщил, что только в 2024 году при реализации госконтрактов и национальных проектов были выявлены нарушения на сумму свыше 39 млрд руб., связанные с нецелевым использованием средств, завышением стоимости работ и иными

злоупотреблениями. По результатам анализа государственных контрактов и расходования бюджетных средств в 2024 году было возбуждено свыше 1300 уголовных дел.

Эти оценки показывают, что даже при развитой цифровой инфраструктуре закупок коррупционные и иные недобросовестные практики сохраняют значительный масштаб и адаптируются к условиям электронной среды. Это повышает значимость риск-ориентированных подходов, аналитических инструментов и правоприменительной практики, направленных на выявление формально законных, но, по существу, моделей поведения, направленных против конкуренции

Одной из наиболее распространённых схем остаётся включение в документацию условий, которые формально соответствуют требованиям закона, но фактически ориентированы на конкретного поставщика. Речь идёт о специально составленных технических заданиях, в которых чрезмерно детализируются характеристики товара или устанавливаются специфические требования к опыту, ресурсам и срокам исполнения.

Другой характерной практикой является участие в закупке только одного поставщика. Сам по себе факт подачи единственной заявки не всегда означает нарушение, но в совокупности с избыточными требованиями документации, узкими сроками или повторяемостью результатов по однотипным закупкам он может указывать на формальный характер открытости процедуры и недостаточный уровень конкуренции.

К числу распространённых практик относятся и нереалистичные сроки подачи заявок или исполнения контракта. Формально заказчик соблюдает процедуру размещения извещения, однако сокращённые сроки объективно ограничивают возможность участия добросовестных поставщиков, особенно если закупка требует сложной подготовки заявки или привлечения субподрядчиков.

Отдельно выделяется дробление потребности на несколько закупок меньшего объёма. Такая схема позволяет избегать более жёстких конкурентных процедур, снижать заметность закупочной активности и упрощать выбор фактически предпочтительного исполнителя, тогда как автоматическое выявление взаимосвязанных закупок требует более высокого уровня аналитической обработки данных.

Оценка эффективности цифровизации в сфере закупок показывает, что её влияние носит двойственный характер. С одной стороны, внедрение ЕИС, электронных площадок, цифровых реестров и электронного документооборота действительно повысило прозрачность процедур, расширило возможности мониторинга и сократило пространство для части традиционных коррупционных практик. С другой стороны, сама по себе цифровизация не гарантирует добросовестную конкуренцию, поскольку значительная часть нарушений

переносится на этап подготовки документации и конструирования условий закупки.

В качестве основных направлений совершенствования целесообразно выделить унификацию технических заданий по типовым товарам, работам и услугам. Более высокая степень стандартизации описания объекта закупки может сократить пространство для субъективной настройки условий под конкретного исполнителя и упростить сравнение закупок между собой.

Не менее важным направлением является развитие аналитических инструментов на базе искусственного интеллекта и больших данных, которые способны выявлять повторяющиеся аномалии, нестандартные параметры закупок, устойчивые связи между заказчиками и поставщиками, а также признаки дробления закупочной деятельности. Дополнительного внимания требует усиление контроля за аномальными характеристиками закупок: чрезмерно короткими сроками, устойчиво низким числом участников, повторяемостью победителей и нестандартными требованиями документации.

Идея внедрения смарт-контрактов на основании блокчейна так же может способствовать в выявлении нарушений законодательства. Каждому участнику торгов будет присваиваться уникальный идентификационный номер, с помощью которого можно будет отслеживать его участие в тендерах в автоматическом режиме (в нынешних условиях отслеживание так же возможно). Если один и тот же подрядчик на протяжении многих лет получает статус исполнителя у одного и того же заказчика – это может стать поводом для проверки данного контрагента.

Также необходимо повышать ответственность заказчиков за формирование дискриминационных условий закупки, поскольку именно на стадии подготовки документации закладывается значительная часть будущих ограничений конкуренции. В совокупности такие меры способны повысить не только техническую прозрачность закупок, но и их реальную конкурентность.

Таким образом, цифровая трансформация системы государственных закупок в Российской Федерации привела к формированию многоуровневой электронной инфраструктуры, включающей ЕИС, сеть электронных торговых площадок, цифровые реестры и электронный документооборот. Это обеспечило рост прозрачности процедур и управляемости контрактной системы, а также расширило возможности аналитического контроля за расходованием бюджетных средств.

Вместе с тем проведённый анализ показывает, что цифровизация сама по себе не устраняет коррупционные и иные недобросовестные практики, а скорее меняет характер соответствующих рисков. Наиболее уязвимым остаётся подготовительный этап закупок аспекты закупок: формирование технических заданий, установление избыточных требований к участникам, манипулирование

сроками и объёмами закупок, а также согласованное поведение поставщиков при внешне корректном прохождении процедур.

Следовательно, цифровая среда государственных закупок является необходимым, но недостаточным условием повышения эффективности антикоррупционного контроля. Её потенциал реализуется в полной мере только при сочетании с совершенствованием нормативного регулирования, развитием аналитических инструментов, стандартизацией закупочной документации и усилением контроля за аномальными закупочными практиками.

### Список литературы

1. Федеральный закон от 05.04.2013 № 44-ФЗ (ред. от 28.12.2025) «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» [Электронный ресурс] // КонсультантПлюс (справочно-правовая система) (дата обращения: 05.06.2026).
2. Федеральный закон от 18.07.2011 № 223-ФЗ (ред. от 08.08.2024) «О закупках товаров, работ, услуг отдельными видами юридических лиц» [Электронный ресурс] // Правительство России. URL: <http://government.ru/docs/all/100084/> (дата обращения: 05.06.2026).
3. Мосеева Л. С., Львова М. И. Digital transformation of the public procurement system in the Sverdlovsk region as a factor in increasing the effectiveness of budget policy // Economics and Management: Problems, Solutions. 2025. Vol. 7, No. 6. P. 230–235.
4. Ибрагимова Г. М., Нуртдинов А. Р. The dynamics of digitalization of state and municipal procurement in the Republic of Tatarstan: an empirical study // The Eurasian Scientific Journal. 2025. Vol. 17, Iss. S1.
5. Цифровизация закупок: современные тенденции и проблемы [Электронный ресурс] // Научный журнал (статья). URL: <https://cyberleninka.ru/article/n/tsifrovizatsiya-zakupok-sovremennyye-tendentsii-i-problemy> (дата обращения: 05.06.2026).
6. Цифровые закупки в государственном секторе [Электронный ресурс] // Научный журнал (статья). URL: <https://cyberleninka.ru/article/n/tsifrovye-zakupki-v-gosudarstvennom-sektore> (дата обращения: 05.06.2026).
7. Блокчейн в государственных закупках и управлении контрактными обязательствами [Электронный ресурс] // Научный журнал (статья). URL: <https://cyberleninka.ru/article/n/blokcheyn-v-gosudarstvennyh-zakupkah-i-upravlenii-kontraktnymi-obyazatelstvami> (дата обращения: 05.06.2026).
8. Государственный контроль за размещением заказов в рамках 44-ФЗ: проблемы и перспективы [Электронный ресурс] // Научный журнал (статья). URL: <https://cyberleninka.ru/article/n/gosudarstvennyy-kontrol-za-razmescheniem-zakazov-v-ramkah-44-fz-problemy-i-perspektivy> (дата обращения: 05.06.2026).

9. Тенденции развития управления государственными закупками в условиях цифровизации [Электронный ресурс] // Научный журнал (статья). URL: <https://cyberleninka.ru/article/n/tendentsii-razvitiya-upravleniya-gosudarstvennymi-zakupkami-v-usloviyah-tsifrovizatsii> (дата обращения: 05.06.2026).
10. Государственные закупки как инструмент повышения эффективности бюджетных расходов [Электронный ресурс] // Научный журнал (статья). URL: <https://cyberleninka.ru/article/n/gosudarstvennye-zakupki-kak-instrument-povysheniya-effektivnosti-byudzhethnyh-rashodov> (дата обращения: 05.06.2026).
11. Цифровизация контрактной системы закупок как составляющей цифровой трансформации общественного сектора [Электронный ресурс] // Монография / коллектив авторов. 2024. URL: (по месту опубликования монографии, при наличии точного URL) (дата обращения: 05.06.2026).
12. Анализ институционального изоморфизма в условиях цифровизации публичных закупок [Электронный ресурс] // CyberLeninka. URL: <https://cyberleninka.ru/article/n/analiz-institutsionalnogo-izomorfizma-v-usloviyah-tsifrovizatsii-publichnyh-zakupok> (дата обращения: 05.06.2026).
13. Единая информационная система в сфере закупок (ЕИС) [Электронный ресурс]. Официальный сайт. URL: <https://zakupki.gov.ru/> (дата обращения: 05.06.2026).
14. Исследование 2021 года об уровне коррупции в государственных закупках [Электронный ресурс] // Исследования в сфере антикоррупции. URL: (точный адрес публикации исследования ВШЭ / Фонда «Норматив») (дата обращения: 05.06.2026).
15. Эксперты оценили средний размер откатов при госзакупках [Электронный ресурс] // РБК. 2021. 20 дек. URL: <https://www.rbc.ru/economics/20/12/2021/61bc5d059a794770833e7b51> (дата обращения: 05.06.2026).
16. МВД РФ сообщило о почти двукратном росте числа преступлений в сфере госзакупок [Электронный ресурс] // Интерфакс. 2023. 23 окт. URL: <https://www.interfax.ru/russia/927204> (дата обращения: 05.06.2026).
17. Росфинмониторинг выявил нарушения на 39 млрд рублей при реализации госконтрактов и нацпроектов в 2024 г. [Электронный ресурс] // Ведомости. 2025. 8 июля. URL: <https://www.vedomosti.ru/society/articles/2025/07/09/1123047-rosfinmonitoring-viyavil-narusheniya> (дата обращения: 05.06.2026).
18. В России пресекли незаконные торги на госзакупках на 39 миллиардов рублей [Электронный ресурс] // РИА Новости. 2025. 8 июля. URL: <https://ria.ru/20250708/goszakupki-2027893905.html> (дата обращения: 05.06.2026).

**Соколова Мария Сергеевна**

студент 1 курса

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

**Кузовлева Нина Федоровна**

кандидат экономических наук

профессор кафедры экономической экспертизы и финансового мониторинга

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

## **Развитие национальной платежной системы на основе цифровых технологий**

**Аннотация.** В статье рассматривается сущность понятия «национальная платежная система», анализируются перспективы использования цифровых технологий для повышения эффективности и безопасности национальной платежной системы.

**Ключевые слова:** платежная система; стабильность; цифровые технологии; инновации.

### **1. Сущность понятия «национальная платежная система»**

Платежная система – это механизм выполнения денежных обязательств, возникающих в результате выполнения экономической деятельности ее участников [1]. Из него следует сущность национальной платежной системы в правовом понимании прописана в Федеральном законе № 161-ФЗ и сформулирован следующим образом: «совокупность операторов по переводу денежных средств (включая операторов электронных денежных средств), банковских платежных агентов (субагентов), платежных агентов, организаций федеральной почтовой связи при оказании ими платежных услуг в соответствии с законодательством Российской Федерации, операторов платежных систем, операторов услуг платежной инфраструктуры, операторов услуг информационного обмена, иностранных поставщиков платежных услуг, операторов иностранных платежных систем, поставщиков платежных приложений, операторов электронных платформ (субъекты национальной платежной системы)» [2].

Таким образом, национальная платёжная система представляет собой не просто институциональную проекцию абстрактного платежного механизма, а сложную, иерархически и функционально связанную среду. Эффективность такой системы определяется перечнем входящих в неё субъектов и качеством коммуникаций, стандартов обмена и степенью технологической интеграции между ними.

## 2. Основные направления развития национальной платёжной системы

В течение длительного периода российская экономика функционировала в режиме глубокой инфраструктурной зависимости от нерезидентных платёжных операторов, прежде всего от систем Visa и Mastercard. Авторизация, клиринг и процессинг карточных транзакций осуществлялись исключительно зарубежной технологической инфраструктурой, что означало передачу управления расчётными потоками во внешние юрисдикции.

Подобная модель, обеспечивая банкам-эквайерам краткосрочное снижение капитальных и операционных расходов, одновременно формировала фундаментальные системные уязвимости национальной финансовой системы. К числу таких уязвимостей относились бесконтрольная передача транзакционных данных за рубеж, устойчивый отток доходов от эксплуатации платёжных систем в пользу иностранных корпораций и риск принудительной блокировки расчётных потоков по решению внешних регуляторов.

Практическая реализация санкционных ограничений в 2014 и 2022 годах наглядно продемонстрировала ограниченность частноправовых гарантий. Стало очевидно, что финансовая независимость государства не может обеспечиваться исключительно договорными соглашениями между коммерческими структурами, поскольку такие механизмы стремительно утрачивают силу в условиях политического конфликта.

Следовательно, для обеспечения технологической независимости и минимизации внешних угроз необходима системная модернизация национального расчётного контура, что определяет следующие приоритетные направления развития национальной платёжной системы (табл. 1).

Таблица 1

Приоритетные направления развития национальной платёжной системы

| Направления развития              | Задачи                                                                                                    | Ожидаемые результаты                                                          |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Совершенствование регулирования   | Создание понятных правил для новых технологий (открытые API, цифровые сервисы); защита прав пользователей | Развитие инноваций безопасно; потребители получают прозрачные условия         |
| Развитие платёжной инфраструктуры | Развитие СБП; запуск цифрового рубля                                                                      | Платежи проходят мгновенно; появляются удобные способы оплаты (QR, биометрия) |
| Развитие платёжного рынка         | Поддержка новых участников рынка; упрощение подключения к платёжным сервисам                              | Снижение стоимости услуг; больше выбора для пользователей                     |

|                                  |                                                                                            |                                                                                   |
|----------------------------------|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Развитие трансграничных платежей | Расширение использования СБП и СПФС для международных переводов; расчеты в цифровых рублях | Бесперебойность от иностранных платежных систем; непрерывные расчеты с партнерами |
|----------------------------------|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|

Источник: составлено авторами [3, с.34].

Документ фиксирует переход от зависимости от зарубежной инфраструктуры к построению суверенной, технологически независимой платёжной экосистемы. Ключевыми факторами развития являются — цифровизация (цифровой рубль, Открытые API), обеспечение бесперебойности расчётов в режиме реального времени, и адаптация трансграничных механизмов к новым геоэкономическим условиям.

### 3. Цифровые технологии национальной платёжной системы

При развитии инноваций в НПС Банк России стремится обеспечить предоставление доступных и востребованных платежных сервисов всем категориям потребителей, содействовать развитию конкуренции и внедрению возможностей новых технологий при обеспечении бесперебойности и безопасности оказания платежных услуг. Внедрение передовых технологических решений формирует новые возможности и одновременно актуализирует комплекс системных вызовов.

Основная часть покупок в России оплачивается безналично

Рис. 5

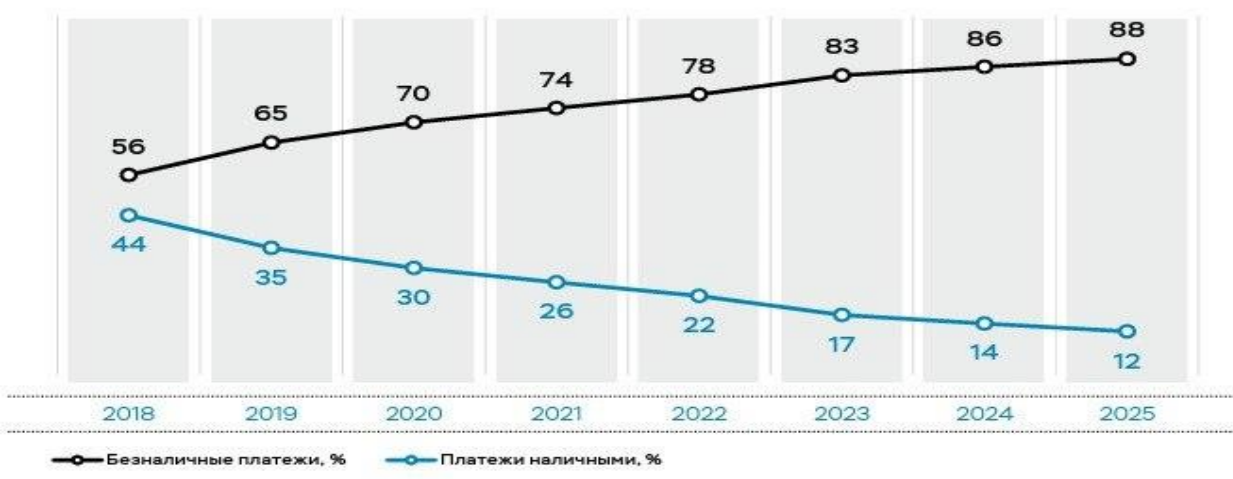


Рисунок 1. Платежное поведение населения России [4]

Указанные тенденции (рис. 1) демонстрируют структурный сдвиг в платёжном поведении населения, обусловленный внедрением цифровых технологий национальной платёжной системы. Согласно эмпирическим данным, к 2025 году показатель безналичных расчётов достиг 88%, что подтверждает

эффективность стратегии Банка России. Это один из самых высоких показателей в мире [4].

Первым ключевым фактором выступает Система быстрых платежей (СБП). СБП представляет собой платформенное решение для мгновенных переводов по QR-коду, мобильному телефону или биометрии без комиссии в пределах установленного лимита. С момента запуска в 2019 году СБП обеспечила снижение транзакционных издержек, особенно в сегменте микроплатежей (до 1000 рублей), где ранее безналичные инструменты были нерентабельны из-за комиссий эквайринга. Интеграция QR-кодов СБП в торгово-сервисных предприятиях позволила отказаться от терминального оборудования в мелком ритейле, что критически важно для малых населённых пунктов. К 2025 году доля наличных платежей сократилась до 14%, чему способствовали низкие тарифы СБП (0,4–0,7% против 1–3% по банковским картам).

Вторым фактором является Национальная платёжная карта «Мир». Эмитируемая с 2015 года, карта «Мир» стала базовым инфраструктурным элементом НПС, обеспечив суверенный канал обработки внутрироссийских транзакций в условиях санкционных рисков и отключения от международных систем. Карта выполняет также социальную функцию: через неё зачисляются пенсии, пособия, реализуются программы льготного проезда и кешбэка. К 2025 году доля операций по картам «Мир» в социально значимых сегментах превысила 75%. Технологическая совместимость «Мир» с СБП и биометрической платформой создала синергетический эффект, позволяя держателю карты совершать оплату разными способами.

Третьим фактором выступают биометрическая аутентификация и удалённая идентификация. Внедрение Единой биометрической системы (ЕБС) и соответствующей нормативной базы (ФЗ № 572-ФЗ) позволило преодолеть необходимость физического присутствия клиента в отделении банка для юридически значимых операций. Биометрические данные приравнены к собственноручной подписи, что даёт возможность дистанционно открывать счета, оформлять кредиты и осуществлять переводы на суммы свыше 100 тыс. рублей. Особое значение этот механизм имеет для сельской местности и удалённых территорий. По данным Банка России, объём дистанционных платежей с использованием биометрии вырос в 4,2 раза по сравнению с 2023 годом.

Дополнительно следует выделить цифровой рубль как третью форму денег (наряду с наличными и безналичными), находящуюся в стадии пилотного тестирования. К 2025 году он показал работоспособность в сценариях «умных контрактов» и целевых платежей, однако его массовое внедрение потребует решения вопросов конфиденциальности и адаптации законодательства.

Таким образом, в настоящее время все большее количество платежных операций стало проводиться в цифровом пространстве, этому способствует развитие всевозможных технологических инноваций, повышение финансовой и технологической грамотности пользователей финансовых услуг, увеличение доступности и качества сети Интернет, удобство проведения операций. Таким образом, дальнейшее развитие инфраструктуры безналичных расчётов, включая сервисы быстрых платежей и цифровой рубль, остаётся стратегическим приоритетом для обеспечения технологического суверенитета и удобства граждан.

### Список литературы

1. Рабаданова Д. А. К вопросу о понятии национальной платежной системы // Региональная и отраслевая экономика. – 2023. – № 6. – С. 180–184. doi:10.47576/2949-1916\_2023\_6\_180 URL: <https://cyberleninka.ru/article/n/k-voprosu-o-ponyatii-natsionalnoy-platezhnoy-sistemy/viewer>
2. Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» // Справочно-правовая система Консультант Плюс. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_115625/](https://www.consultant.ru/document/cons_doc_LAW_115625/)
3. Основные направления развития национальной платежной системы на период 2025 – 2027 годов // Банк России URL: [https://cbr.ru/Content/Document/File/170680/onrnps\\_2025-27.pdf](https://cbr.ru/Content/Document/File/170680/onrnps_2025-27.pdf)
4. Доля безналичных платежей в российской экономике и популярность платежных QR-кодов выросла <https://www.comnews.ru/content/244447/2026-03-27/2026-w13/1008/dolya-beznalichnykh-platezhey-rossiyskoy-ekonomike-i-populyarnost-platezhnykh-qr-kodov-vyroslo>

**Тарасова Наталия Валентиновна**

кандидат экономических наук, доцент

доцент кафедры экономической экспертизы и финансового мониторинга

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

**Генина Кира Анатольевна**

студент 1 курса

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

## **Перспективы и риски внедрения цифрового рубля для российской экономики**

**Аннотация.** В статье рассматривается проблема внедрения цифрового рубля в экономику страны; раскрываются понятие и причины введения цифрового рубля в экономику страны, включая усиление конкуренции в финансовой сфере, снижение зависимости от международных платежных систем, борьба с теневой экономикой. Проводится сравнение этапов внедрения цифровой национальной валюты по отдельным странам. Анализируются плюсы и минусы цифрового рубля, перспективы внедрения цифрового рубля, использование цифрового рубля при выплате зарплаты

**Ключевые слова:** цифровая экономика; цифровой рубль; финансовый суверенитет; смарт-контракты; транзакционные издержки; импортозамещение; платёжная система; кибербезопасность; теневая экономика; экономическая безопасность.

Внедрение цифрового рубля — третьей формы российской национальной валюты наряду с наличной и безналичной — является одним из наиболее значимых проектов цифровой трансформации финансовой системы России. Согласно официальной позиции Банка России, цифровой рубль призван стать дополнительным средством платежа, сочетающим преимущества безналичных расчётов (скорость) и наличных денег (надёжность).

С сентября 2026 года в России стартует этап массового внедрения цифрового рубля, в связи с чем вопросы его влияния на экономическую безопасность страны приобретают особую актуальность и требуют всестороннего научного анализа [1,2,3].

### **1. Понятие цифрового рубля**

Цифровой рубль — это электронная форма российской национальной валюты, выпускаемая Центральным банком Российской Федерации.

В отличие от безналичных денег, которые хранятся на счетах коммерческих банков, цифровой рубль представляет собой уникальный цифровой код, размещенный на специальной платформе Банка России.

Таким образом, в современной денежной системе России будут существовать три формы рубля:

- наличные деньги;
- безналичные деньги;
- цифровой рубль.

Основные особенности цифрового рубля:

- выпускается исключительно Центральным банком;
- имеет одинаковую стоимость с обычным рублем;
- может использоваться как для онлайн-, так и для офлайн-платежей;
- обеспечивает высокий уровень контроля и безопасности операций.

Цифровой рубль не является криптовалютой. В отличие от биткоина и других децентрализованных цифровых активов, цифровой рубль полностью контролируется государством и обеспечивается Центральным банком [4].

## **2. Причины внедрения цифрового рубля [4].**

Внедрение цифрового рубля связано с несколькими важными экономическими и технологическими факторами.

### **2.1 Развитие цифровой экономики**

Современное общество активно использует электронные сервисы, мобильные приложения и интернет-платежи. Люди все реже пользуются наличными деньгами, а скорость финансовых операций становится важнейшим фактором экономики.

### **2.2 Усиление конкуренции в финансовой сфере**

Многие государства уже занимаются разработкой собственных цифровых валют. Китай тестирует цифровой юань, Европейский союз обсуждает цифровой евро, а другие страны изучают возможности внедрения CBDC.

Россия также стремится сохранить финансовую независимость и технологическую конкурентоспособность.

### **2.3 Снижение зависимости от международных платежных систем**

После введения международных санкций вопрос финансового суверенитета России стал особенно актуальным. Цифровой рубль рассматривается как инструмент укрепления национальной платежной системы.

### **2.4 Борьба с теневой экономикой**

Использование цифровой валюты позволяет повысить прозрачность денежных операций и снизить масштабы незаконных финансовых схем.

Аналитики финансового рынка прогнозируют, что после полноценного запуска количество пользователей цифрового рубля достигнет 15-20 млн человек в первые годы (рис.1). [5,6].

### Прогноз внедрения цифрового рубля до 2030 года

Прогнозируемая доля цифрового рубля в общем объеме платежей (%)

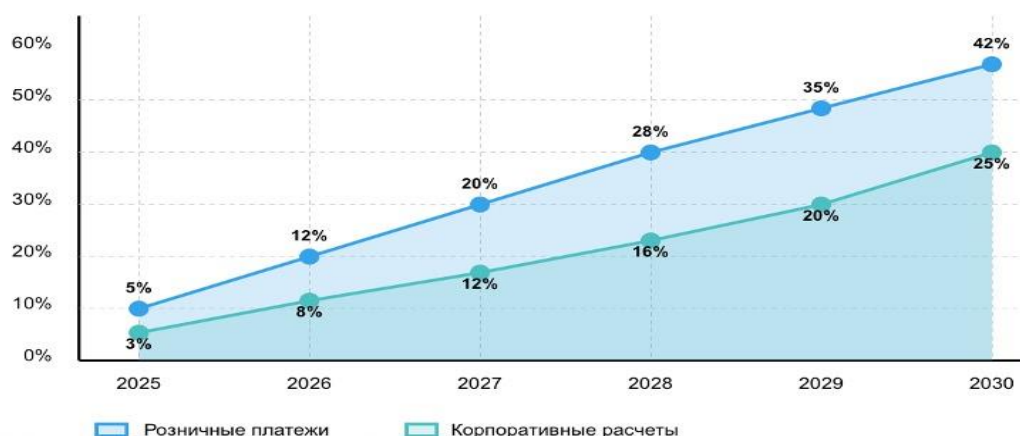


Рисунок 1. Прогноз внедрения цифрового рубля

Для коммерческого сектора разработан четкий график принятия цифрового рубля: предприятия с годовым оборотом свыше 30 млн рублей начнут работу с июля 2025 года, компании с выручкой от 20 млн рублей — с июля 2026 года, все остальные — с июля 2027 года. Такое постепенное внедрение призвано избежать потрясений на рынке и обеспечить плавный переход к использованию новой формы денег.

Экономический эффект от использования цифрового рубля в России может быть значительным — по оценкам Банка России, потенциальное сокращение затрат на денежное обращение может составить до 1,5-2% ВВП в долгосрочной перспективе (рис.2). [5,6].

### Экономический эффект внедрения цифрового рубля

Долгосрочный прогноз (% от ВВП)

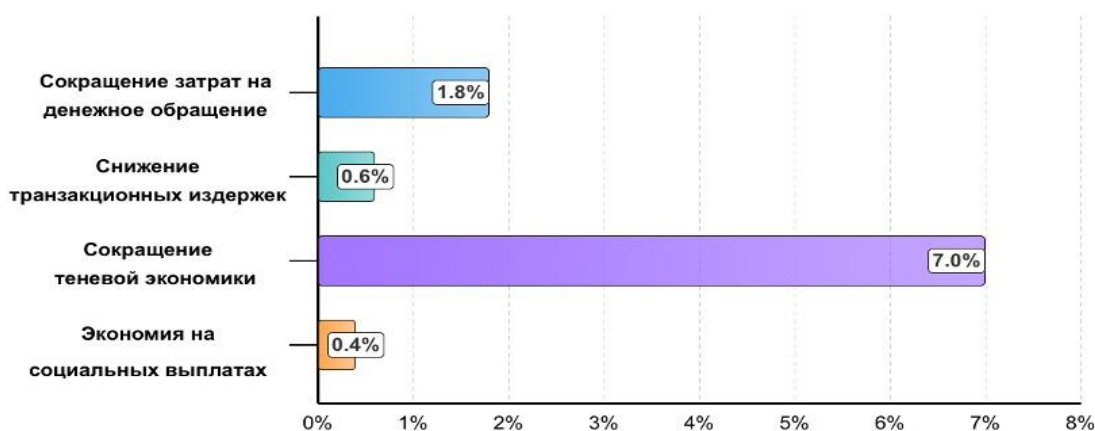


Рисунок 2. Экономический эффект внедрения цифрового рубля

Данные, представленные на рис. 2 показывают, что экономический эффект внедрения цифрового рубля выразится в сокращении затрат на денежное обращение — 1,8%, снижении транзакционных издержек — 0,6%, сокращении теневой экономики — 7,0%, экономии на социальных выплатах — 0,4% (горизонтальная столбчатая диаграмма, показывающая долгосрочный прогноз в % от ВВП)

### **3. Китай – стадия масштабного пилота и частичного внедрения цифровой валюты центрального банка**

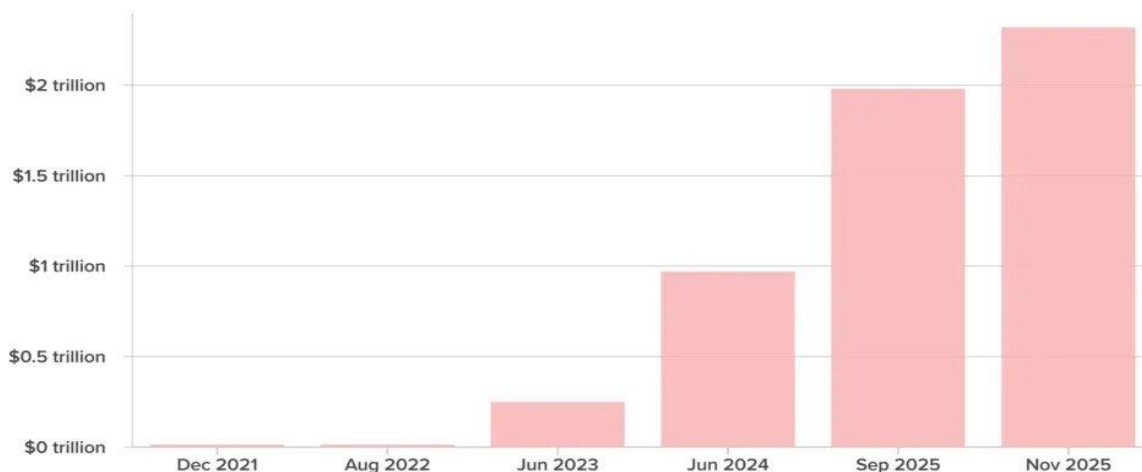
Китай является мировым лидером среди крупных экономик по внедрению цифровой валюты центрального банка (CBDC). Что уже сделано:

- цифровой юань (e-CNY) тестируется с 2020 года (рис.3) [7];
- действует в десятках городов и провинций;
- используется для оплаты транспорта, товаров, коммунальных услуг и государственных выплат;
- открыты сотни миллионов цифровых кошельков;
- проводятся международные эксперименты по трансграничным платежам через проект mBridge.

#### **e-CNY transaction volume exceeds two trillion dollars**

Cumulative transaction volumes for select months (2021–2025)

Atlantic Council  
GEOECONOMICS CENTER



Source: People's Bank of China • PBoC releases data sporadically. PBoC did not release official data in 2022

Рисунок 3. Объем транзакций e-CNY

### **4. США – стадия исследований и политических споров по внедрению цифровой валюты.**

США находятся на более раннем этапе внедрения цифровой валюты. На сегодняшний день [8,9,10]:

- Федеральная резервная система изучает технологию CBDC;
- ведутся исследования и эксперименты;

- решение о запуске цифрового доллара не принято;
- многие политики выступают против CBDC из-за рисков контроля над финансами граждан.

В последние годы руководство ФРС неоднократно заявляло, что не планирует запуск цифрового доллара без одобрения Конгресса. Более того, в США появились инициативы по ограничению или запрету CBDC.

Таблица 1

#### Этапы внедрения цифровой национальной валюты

| Страна | Этап внедрения                                                  |
|--------|-----------------------------------------------------------------|
| Китай  | Масштабный пилот, частичное использование населением и бизнесом |
| Россия | Пилотное тестирование цифрового рубля с банками и гражданами    |
| США    | Исследования и обсуждение, запуск не утвержден                  |

### 5. Плюсы и минусы цифрового рубля [11]

#### Плюсы

1. Один кошелек — доступ через любой банк. Цифровой кошелек открывается на платформе Банк России. Коммерческие банки выступают посредниками и обязаны обеспечивать к нему доступ через свои приложения — то есть при смене банка доступ к цифровым рублям сохраняется.

2. Моментальные переводы. Поскольку цифровые рубли хранятся на единой платформе ЦБ, переводы происходят внутри одной системы. Не нужно «гонять» деньги между разными банками — операция не проходит через цепочку корреспондентских счетов. Платежи будут проходить быстрее.

3. Платежи без интернета. Заявлена возможность офлайн-расчётов. Это полезно в ситуациях, когда нет устойчивого соединения — например, на выездной торговле или в удалённых локациях. Правда, сам механизм ещё тестируют и будут внедрять постепенно.

4. Экономия на комиссиях. Для малого бизнеса это, пожалуй, самый ощутимый плюс. ЦБ обещал, что до 31 декабря 2026 года все операции с цифровым рублём будут бесплатны. С 1 января 2027 года с предпринимателей за приём платежей от физлиц будут брать 0,3% от суммы перевода, но не более 1500 Р за одну операцию. Для физических лиц переводы останутся бесплатными.

#### Минусы

1. Узкая сфера применения. Цифровой рубль — это исключительно средство платежей и переводов. Его нельзя разместить на вкладе, использовать для получения кредита или инвестировать. Держать крупные суммы в цифровом кошельке экономически невыгодно — деньги не работают. Более того, они не защищены даже от инфляционных потерь.

2. Риск обязательного применения. Пока использование цифрового рубля добровольное. Но постепенно государство может обязать применять его в

отдельных сферах — например, при расчётах по госконтрактам или при получении бюджетных средств. Если компания работает с государством, к этому сценарию стоит быть готовыми заранее.

3. Географические ограничения. На текущем этапе цифровой рубль функционирует внутри российской финансовой системы под управлением Центробанка. Для международных расчётов он пока не используется. Возможности трансграничных операций рассматриваются как перспектива, а не как действующий инструмент.

## **6. Возможные риски и проблемы**

Несмотря на значительные преимущества, внедрение цифрового рубля связано с рядом серьезных рисков [11].

### **6.1 Угроза кибератак**

Любая цифровая система может стать объектом хакерских атак. Поэтому особое значение имеет защита данных и создание надежной инфраструктуры.

### **6.2 Снижение роли коммерческих банков**

Если граждане начнут хранить средства непосредственно на платформе Центрального банка, коммерческие банки могут потерять часть клиентов и ресурсов.

### **6.3 Контроль над финансовыми операциями**

Некоторые эксперты считают, что цифровой рубль может усилить государственный контроль над личными финансами граждан.

### **6.4 Технические сложности**

Для полноценного внедрения цифрового рубля потребуются модернизация банковской инфраструктуры, развитие цифровых сервисов и повышение уровня цифровой грамотности населения.

### **6.5 Риски ограничения конфиденциальности**

Повышенная прозрачность платежей может вызвать опасения у граждан по поводу сохранения банковской тайны и персональных данных.

## **7. Перспективы внедрения цифрового рубля в России**

На сегодняшний день Банк России проводит тестирование цифрового рубля с участием коммерческих банков и отдельных пользователей [12,13].

Предполагается, что в будущем цифровой рубль сможет использоваться:

- для оплаты товаров и услуг;
- при получении государственных выплат;
- в международных расчетах;
- в системе государственных контрактов;
- для автоматических платежей с использованием смарт-контрактов.

Эксперты считают, что внедрение цифрового рубля станет одним из важнейших этапов модернизации российской финансовой системы.

Однако успех проекта будет зависеть от надежности технологий, доверия населения и эффективности государственного регулирования.

## **8. Будет ли обязательным цифровой рубль при выплате зарплаты?**

Пока нет. Во всяком случае, поправок в Трудовой кодекс под обязательную цифровую зарплату не вносили. Формат выплаты остаётся прежним — наличными или безналом по договорённости между работодателем и сотрудником.

Скорые изменения вероятны прежде всего в бюджетной системе. Федеральный закон от 31.07.2025 № 303-ФЗ позволяет использовать цифровой рубль в расчётах через счёт Федерального казначейства. Государство тестирует механизм бюджетных выплат в цифровых рублях и выстраивает инфраструктуру.

Центробанк объяснял, что использование цифрового рубля добровольно: гражданин открывает цифровой кошелек через банк-участник платформы по собственному желанию. Поэтому в 2026 году корректно говорить не о всеобщем переводе зарплат и пособий, а о постепенном расширении сценариев — в первую очередь в бюджетных выплатах [14].

Это значит, что бизнесу, во всяком случае малому, обязательства срочно перестраивать зарплатные процессы нет. Но присматриваться к тому, что происходит, точно надо: как только бюджетники начнут получать зарплату и пособия в цифровых рублях, бизнесу надо готовиться к переходу.

### **Заключение**

Цифровой рубль представляет собой новую форму национальной валюты, которая способна существенно изменить финансовую систему России. Его внедрение может повысить скорость и безопасность платежей, сократить издержки и укрепить финансовый суверенитет страны. Одновременно цифровой рубль создает новые вызовы, связанные с кибербезопасностью, защитой персональных данных и изменением роли банковской системы.

Таким образом, цифровой рубль является важным элементом цифровой трансформации экономики России. При грамотной реализации данный проект способен стать значительным шагом в развитии современной финансовой инфраструктуры государства.

## **Список литературы**

1. О внесении изменений в отдельные законодательные акты Российской Федерации в связи с введением цифрового рубля: Федеральный закон от 23.07.2025 № 248-ФЗ [Электронный ресурс]. — URL: <https://www.pnp.ru/politics/putin-podpisal-zakon-o-massovom-vnedrenii-cifrovogo-rublya.html> (дата обращения: 17.05.2026).
2. О внесении изменений в отдельные законодательные акты Российской Федерации в связи с введением цифрового рубля: Федеральный закон от

24.07.2023 № 340-ФЗ [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 17.05.2026).

3. О внесении изменений в отдельные законодательные акты Российской Федерации в связи с введением цифрового рубля: Федеральный закон от 24.07.2023 № 339-ФЗ [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 17.05.2026).

4. Банк России. Цифровой рубль: официальный сайт / Банк России. – Москва, 2020–2026. – URL: [https://cbr.ru/analytics/d\\_ok/dig\\_ruble/](https://cbr.ru/analytics/d_ok/dig_ruble/) (дата обращения: 17.05.2026).

5. Банк России. Решение Совета директоров Банка России о продлении льготного периода на платформе цифрового рубля (тарифы на услуги, размеры вознаграждений) от 21.11.2025 [Электронный ресурс] / Банк России. – URL: [https://cbr.ru/rbr/dir\\_decisions/rsd\\_2025-11-21\\_45\\_01/](https://cbr.ru/rbr/dir_decisions/rsd_2025-11-21_45_01/) (дата обращения: 17.05.2026).

6. Банк России. Опубликованы промежуточные результаты внедрения цифрового рубля: по состоянию на май 2025 г. [Электронный ресурс] // Банк России. – URL: <https://cbr.ru/> (дата обращения: 17.05.2026).

7. Леднев, М. В. Перспективы развития и внедрения цифровых финансовых активов в странах БРИКС / М. В. Леднев, С. П. Морозов, В. И. Карпова // Инновации и инвестиции. – 2025. – № 4. – С. 108–112. – DOI отсутствует.

8. Михайлишин, А. Ю. О роли мультивалютных шлюзов цифровых валют центральных банков в трансграничных расчетах / А. Ю. Михайлишин // Банковское дело. – 2025. – № 3. – С. 12–21.

9. Хомутова, Е. В. Цифровой рубль как инструмент трансформации национальной финансовой системы и международных расчетов / Е. В. Хомутова // Финансовая экономика. – 2026. – № 2. – С. 187–191.

10. Дюдикова, Е. И. В контексте глобального парадигмального сдвига в сторону цифровизации финансовых систем / Е. И. Дюдикова, И. А. Ризванова // Ведомости. – 2025. – 6 нояб. – URL: [https://www.vedomosti.ru/press\\_releases/2025/11/06/tsifrovoy-rubl-evolyutsiya-a-ne-revolvyutsiya-v-koshelke-rossiyan](https://www.vedomosti.ru/press_releases/2025/11/06/tsifrovoy-rubl-evolyutsiya-a-ne-revolvyutsiya-v-koshelke-rossiyan) (дата обращения: 17.05.2026).

11. Национальное рейтинговое агентство (НРА). Цифровой рубль принесет экономике РФ до 260 млрд рублей в год к 2031 году: аналитический обзор / НРА. – Москва, 2025. – URL: [https://minfin.gov.ru/ru/press-center/?id\\_4=39861-nra-tsifrovoy-rubl-prineset-ekonomike-rf-do-260-mlrd-rublei-v-god-k-2031-godu](https://minfin.gov.ru/ru/press-center/?id_4=39861-nra-tsifrovoy-rubl-prineset-ekonomike-rf-do-260-mlrd-rublei-v-god-k-2031-godu) (дата обращения: 17.05.2026).

12. Кухарчак, С. Как цифровой рубль формируют новую платежную инфраструктуру для бизнеса / С. Кухарчак // РБК Компании. – 2026. – 14 мая. –

URL: <https://companies.rbc.ru/news/AqzjZMFFNq/kak-tsifrovoj-rubl-formiruyut-povuyu-platezhnuyu-infrastrukturu-dlya-biznesa/> (дата обращения: 17.05.2026).

13. Цифровой рубль стал стандартом расчетов бизнеса с Азией в 2026 году // РБК Компании. – 2026. – 23 апр. –

URL: <https://companies.rbc.ru/amp/news/4b7fef0d-0480-4147-97a1-84c7c83d7189/> (дата обращения: 17.05.2026).

14. Аитов, Т. Цифровой рубль: миссия невыполнима? / Т. Аитов; интервьюер Национальный банковский журнал // Национальный банковский журнал. – 2026. – 16 февр. –

URL: [http://nbj.ru/pubs/timur\\_aitov\\_ekspert\\_nbj\\_tsifrovoy\\_rubl\\_mis/72132/](http://nbj.ru/pubs/timur_aitov_ekspert_nbj_tsifrovoy_rubl_mis/72132/) (дата обращения: 17.05.2026).

**Фильчева Лариса Ивановна**

студент 5 курса

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

Научный руководитель

**Няргинен Виктория Анатольевна**

кандидат экономических наук

доцент кафедры экономической экспертизы и финансового мониторинга

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

## **Анализ тенденций осуществления внешнеэкономической деятельности компаний на современном этапе**

**Аннотация.** В статье анализируются ключевые тенденции развития внешнеэкономической деятельности российских компаний в 2024–2026 гг. Выявлены основные факторы макроэкономической нестабильности, изменения географической и товарной структуры экспорта и импорта. Рассмотрены последствия продовольственного эмбарго, санкционного давления и переориентации торговых потоков на страны Азии, Африки и Ближнего Востока. Определены основные вызовы для участников ВЭД и направления адаптации.

**Ключевые слова:** внешнеэкономическая деятельность, экспорт, импорт, санкции, продовольственное эмбарго, переориентация торговых потоков, сырьевой экспорт, экономическая безопасность.

В 2025 году в качестве главной угрозы для внешнеэкономической деятельности (ВЭД) российских компаний определена макроэкономическая нестабильность. Традиционные логистические коридоры, ориентированные на Запад, стали недоступны или экономически невыгодны, что потребовало экстренной переориентации маршрутов, пересмотра поставщиков и адаптации внутренних производственных цепочек. Анализ внешнеторговой статистики за 2024–2026 гг. позволяет выявить ряд фундаментальных сдвигов в структуре и динамике российской внешней торговли, непосредственно влияющих на экономическую безопасность компаний-участников ВЭД.

В 2025 году вступило в силу несколько важных актов в сфере внешней торговли. Прежде всего речь идет об обновлении перечня товаров для параллельного импорта и отмене ряда таможенных пошлин. Также продолжили действовать запреты, введенные ранее, включая те, что были приняты еще 10 лет назад.

Так называемое «продовольственное эмбарго» в России было введено в 2014 году и обосновывалось как ответная мера по отношению к западным санкциям. Оно неоднократно продлевалось, и в сентябре 2024 года было в

очередной раз продлено по 31 декабря 2026 года. В силу Указа Президента РФ от 06.08.2014 № 560 (ред. от 15.11.2021, с изм. от 18.09.2024) «О применении отдельных специальных экономических мер в целях обеспечения безопасности Российской Федерации» запрещается либо ограничивается осуществление внешнеэкономических операций, предусматривающих ввоз на территорию РФ отдельных видов сельскохозяйственной продукции, сырья и продовольствия, страной происхождения которых является государство, принявшее решение о введении экономических санкций в отношении российских юридических и физических лиц или присоединившееся к такому решению [1].

В ответ на санкции недружественных стран Россия с 2014 года ввела продовольственное эмбарго. Под запрет на импорт попали мясо, рыба, моллюски, молоко и молочная продукция, овощи и фрукты из ЕС, США, Канады, Австралии и Норвегии. Впоследствии список был расширен за счёт Албании, Черногории, Исландии, Лихтенштейна, Украины и других государств.

Экспорт товаров и услуг играет ключевую роль для российской экономики. Он стимулирует производство, ускоряет рост ВВП, обеспечивает приток иностранного капитала, пополняет федеральный бюджет, укрепляет позиции национальной валюты и благоприятно влияет на социально-экономическое развитие регионов. Товарную основу российского экспорта составляют: продукция топливно-энергетического комплекса (нефть, газ), вооружение, продовольственные и сельскохозяйственные товары, продукция металлургической, химической и машиностроительной промышленности, а также драгоценные металлы [3].

В условиях беспрецедентного санкционного давления со стороны недружественных стран российский экспорт претерпевает значительные изменения [2]. По итогам 2024 года, по данным Федеральной таможенной службы, внешнеторговый оборот России сократился до 716,9 млрд долл. США, что на 0,9% больше, чем годом ранее. Экспорт снизился до 433,9 млрд долл. США, а импорт составил 283–294 млрд долл. США. В 2025 году внешнеторговый оборот продолжил сокращаться, составив 697,3 млрд долл. США (–2,8% к 2024 году). Экспорт снизился на 3,7%, до 418,3 млрд долл. США, а импорт – на 1,4%, до 279,0 млрд долл. США [2].

Основой российского экспорта в 2025 году являлись минеральные продукты (нефть, газ, уголь, руда, продукты нефтепереработки), удельный вес которых в товарной структуре экспорта составил 53,9% (в 2024 году – 60,9%). Экспорт металлов и изделий из них в 2025 году составил 17,9% от общего стоимостного объема экспорта (в 2024 году – 14,7%), продовольственных товаров и сырья – 9,8% (на уровне 2024 года), продукции химической промышленности – 8,0% (в 2024 году – 6,4%), машин и оборудования – 7,1% (в 2024 году – 5,4%), лесоматериалов – 2,5% (в 2024 году – 2,3%) [2].

В товарной структуре импорта наибольший удельный вес приходился на

машины, оборудование и другие товары – 48,6% (в 2024 году – 51,9%). Удельный вес продукции химической промышленности в импорте в 2025 году составил 19,9% (в 2024 году – 18,9%), продовольственных товаров – 15,5% (в 2024 году – 13,3%), металлов и изделий – 6,3% (на уровне 2024 года), текстильных изделий – 6,6% (в 2024 году – 6,4%), минеральных продуктов – 1,5% (в 2024 году – 1,6%) [2].

Таблица 1

Динамика внешнеторгового оборота России в 2024–2025 гг. [2]

| Показатель                            | 2024 год | 2025 год | Изменение, % |
|---------------------------------------|----------|----------|--------------|
| Внешнеторговый оборот, млрд долл. США | 716,9    | 697,3    | –2,8         |
| Экспорт, млрд долл. США               | 433,9    | 418,3    | –3,7         |
| Импорт, млрд долл. США                | 283–294  | 279,0    | –1,4         |

Основными торговыми партнерами Российской Федерации в 2025 году были: страны Азиатского региона, на которые приходилось 73,4% от общего объема товарооборота (снижение по сравнению с 2024 годом на 1,6%), европейские страны – 18,6% (снижение на 8,6%), страны Американского континента – 4,1% (рост на 6,3%), страны Африки – 3,9% (снижение на 2,4%).

География экспортных поставок из России претерпела фундаментальные изменения, сместившись с Запада на Восток и Юг. По итогам 2025 года доля стран Азиатско-Тихоокеанского региона в совокупном товарообороте России достигла 73,4% против 72,6% годом ранее, тогда как удельный вес европейских государств сократился до 18,6% (с 19,7% в 2024 году). В абсолютных цифрах экспорт в Азию за 2025 год составил 326 млрд долл. США, тогда как поставки в Европу сократились до 57,4 млрд долл. США, снизившись на 16,5%. Доля африканского континента стабилизировалась на уровне 3,9%, а американского – выросла до 4,1%. Более детальную картину дают данные за 2025 год, согласно которым доля Азии в российском экспорте достигла 80% (с 77% в 2024 году) при сокращении доли Европы до 12% [2].

Значительные изменения затронули и отраслевую структуру экспорта. Если в 2024 году доля минеральных продуктов составляла 60,9%, то в 2025 году она снизилась до 53,9%, что является одним из минимальных значений за последние годы. Параллельно наблюдается активный рост несырьевого неэнергетического экспорта: по итогам 2025 года его объём достиг около 150 млрд долл. США, что на 18% выше уровня 2024 года (127 млрд долл. США). В частности, экспорт металлов и изделий из них увеличился на 17,4%, составив 74,7 млрд долл. США, химической продукции — на 21,6%, машин и оборудования — на 26,6% [2].

Изменения затронули и продовольственный сектор: 90% российского агроэкспорта в 2024 году пришлось на дружественные страны (ранее – две трети). Параллельно доля расчётов в национальных валютах во внешнеторговом обороте в 2025 году обновила исторический максимум, достигнув 54% [2].

Освоение новых рынков происходит на Ближнем Востоке, в Африке, странах Персидского залива и Юго-Восточной Азии. В Евразийском экономическом союзе (ЕАЭС) доля несырьевого неэнергетического экспорта удерживается на уровне двух третей, что отражает сложившийся уровень промышленной кооперации. Три четверти российского товарооборота приходится на дружественные страны. Эксперты прогнозируют к 2030 году рост доли ЕАЭС в общем объеме российского экспорта до 10–11%, в несырьевом неэнергетическом экспорте – до 20% [3].

В условиях санкций часть компаний прекратила свою экспортную деятельность либо снизила объемы экспорта. Причем ослабление экспорта происходит по направлению поставок как в недружественные страны, так и на другие рынки сбыта под влиянием вторичных санкций. Так, в 2022 году по сравнению с досанкционным периодом число экспортеров сократилось с 58 до 52%, в том числе в недружественные государства – с 21 до 15%. У основной массы предприятий доля производимой продукции, ориентированной на экспорт, не превышает 10%. Но если ранее 19% предприятий имели более высокую степень ориентации на внешние рынки, то после введения санкций их число упало до 7% [2].

Сильнее всего от экспорта зависят деревообработка, а также производства химической продукции, резины и пластмассы: в 2021 году здесь экспортировали более 70% компаний, из них свыше 30% работали на рынках недружественных стран. Эти же отрасли, за исключением лесопромышленного сектора, наиболее остро потеряли сбыт в государствах, введших антироссийские санкции. Для половины экспортёров (51%) санкции напрямую не повлияли на экспортную деятельность. Сложности чаще испытывали производители химической продукции и готовых изделий. Из-за формальных и неформальных санкций 16% экспортёров были вынуждены искать новые транспортные коридоры [2].

Таким образом, ключевыми тенденциями 2024–2026 гг. стали.

1. Переориентация внешнеторговых потоков на Азию (доля АТР достигла 73,4% в товарообороте).
2. Рост доли несырьевого неэнергетического экспорта (до 150 млрд долл. США в 2025 году).
3. Увеличение доли расчётов в национальных валютах (54% в 2025 году).
4. Сокращение числа активных экспортёров (с 58% до 52%).
5. Усиление зависимости от ограниченного круга дружественных стран.

Указанные изменения носят долгосрочный характер и требуют от компаний – участников ВЭД пересмотра подходов к управлению экономической

безопасностью, особенно в валютной и логистической сферах. Особое внимание следует уделять диверсификации рынков сбыта, развитию инструментов страхования экспортных рисков и адаптации к новым условиям международных расчётов.

### Список литературы

1. О применении отдельных специальных экономических мер в целях обеспечения безопасности Российской Федерации: Указ Президента РФ от 06.08.2014 № 560 (ред. от 15.11.2021, с изм. от 18.09.2024). – Текст: электронный // СПС «КонсультантПлюс». – URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_166927/](https://www.consultant.ru/document/cons_doc_LAW_166927/) (дата обращения: 14.06.2026)
2. Данные Федеральной таможенной службы о внешнеторговом обороте Российской Федерации за 2024–2025 гг. – Текст: электронный // ФТС России: официальный сайт. – URL: <https://customs.gov.ru/> (дата обращения: 14.06.2026)
3. Аналитические материалы РЭЦ (Российский экспортный центр) о развитии несырьевого неэнергетического экспорта. – Текст: электронный // РЭЦ: официальный сайт. – URL: <https://www.exportcenter.ru/> (дата обращения: 14.06.2026)
4. Обзоры Центрального банка РФ о динамике расчётов в национальных валютах. – Текст: электронный // Банк России: официальный сайт. – URL: <https://cbr.ru/> (дата обращения: 14.06.2026)

**Хусаинов Манон Камарович**

доктор экономических наук, доцент  
профессор кафедры экономической экспертизы и финансового мониторинга  
ФГБОУ ВО «МИРЭА – Российский технологический университет»  
Россия, г. Москва

**Вартапетов Даниил Рубенович**

студент 1 курса  
ФГБОУ ВО «МИРЭА – Российский технологический университет»  
Россия, г. Москва

### **Робо-эдвайзинг (robo-advisory): автоматизация управления инвестициями**

**Аннотация.** В статье рассматривается возможность управления инвестициями на основе использования современных финансовых технологий – Робо-эдвайзинга, представляющий программно-алгоритмический комплекс в сфере финтеха. Рассматривается технология использования Робо-эдвайзинга, его целевая функция, ключевые элементы сопровождения. Обращается внимание на ограничения и проблемы, связанные с системными рисками и рисками получения доходности. Эффективность обусловлена низкой стоимостью, масштабируемостью алгоритмов и нейтрализацией поведенческих искажений.

**Ключевые слова:** долгосрочные сбережения, Робо-эдвайзинг, управление капиталом.

В современных условиях формирования долгосрочных сбережений традиционные банковские инструменты зачастую не обеспечивают опережающего роста капитала относительно инфляции, а прямое участие розничных инвесторов на фондовом рынке сопряжено с высокими информационными и поведенческими рисками. Исторически профессиональное управление капиталом было доступно преимущественно состоятельным клиентам. Развитие финансовых технологий трансформировало данную парадигму, сделав алгоритмическое управление инвестициями массовым явлением. Данный феномен получил название робо-эдвайзинг.

Робо-эдвайзинг представляет собой программно-алгоритмический комплекс в сфере финтеха, направленный на автоматизацию процессов формирования, сопровождения и оптимизации инвестиционных портфелей. Технология выступает инструментом цифровой трансформации управления капиталом, устраняя необходимость в ежедневном ручном контроле и обеспечивая доступ к профессиональным инвестиционным стратегиям для широкого круга инвесторов. [1]

Исследование фокусируется на трёх ключевых аспектах: механизмах адаптации алгоритмических моделей под индивидуальные параметры

инвестора; сравнительной эффективности автоматизированных решений и традиционного консультационного подхода; методологических принципах безопасного внедрения робо-эдвайзинга в инвестиционную практику.

Технологическая архитектура робо-эдвайзинга строится на последовательной обработке данных и строгом соблюдении инвестиционных правил. [2] На первичном этапе осуществляется скоринг инвестора посредством стандартизированного анкетирования, фиксирующего финансовые цели, инвестиционный горизонт и толерантность к риску. На основе полученных параметров алгоритм формирует диверсифицированный портфель, включающий различные классы активов (акции, облигации, биржевые фонды, альтернативные инструменты). Диверсификация обеспечивает снижение несистематических рисков за счёт отрицательной или слабой корреляции доходностей отдельных сегментов.

Ключевым элементом сопровождения является автоматическая ребалансировка: система регулярно корректирует вес активов, фиксируя прибыль по переоцененным позициям и перераспределяя средства в недооцененные, тем самым возвращая портфель к целевому профилю риска[3]. Данный подход исключает влияние поведенческих факторов и обеспечивает строгое соблюдение инвестиционной дисциплины, не зависящее от рыночной конъюнктуры.

Целевая функция робо-эдвайзинга заключается в демократизации доступа к управлению активами, снижении операционных издержек и минимизации поведенческих ошибок инвесторов [4,5]. Автоматизация позволяет снизить комиссии до 0,2–0,8% годовых против 1–3% при традиционном управлении. К преимуществам технологии относятся низкий порог входа, прозрачность алгоритмов, круглосуточный мониторинг и автоматическая налоговая оптимизация.

Однако технология обладает рядом ограничений: зависимость от исторических данных и модельный риск в условиях структурных рыночных сдвигов; ограниченная кастомизация под нестандартные жизненные сценарии; необходимость базовой финансовой грамотности пользователя. Программа не обладает жизненным опытом и интуицией, что делает её неэффективной при решении комплексных задач (налоговое планирование, работа с семейным капиталом, реакция на форс-мажорные обстоятельства). В связи с этим современная индустрия демонстрирует переход к гибридным моделям, где алгоритм отвечает за рутинное управление базовой частью капитала, а человеческий консультант подключается для стратегического сопровождения.

Внедрение робо-эдвайзинга генерирует многоуровневый экономический эффект [6]. На микроуровне наблюдается повышение вовлеченности розничных инвесторов в долгосрочное накопление и снижение эмоциональной нагрузки. На мезоуровне (финансовый рынок) фиксируется приток стабильного «длинного»

капитала, стандартизация продуктов и повышение требований к прозрачности операций. На макроуровне технология способствует росту финансовой грамотности населения, перераспределению сбережений из неформального сектора в регулируемую инвестиционную инфраструктуру и стимулированию развития смежных финтех-сервисов.

Несмотря на автоматизацию, робо-эдвайзинг не устраняет системные рыночные риски и не гарантирует абсолютной доходности [7]. В условиях макроэкономических шоков стоимость портфеля подвержена временной коррекции. Безопасное использование технологии требует соблюдения ряда принципов: верификации регуляторного статуса платформы и лицензий управляющих компаний; анализа методологии ребалансировки и исторических сценариев просадок; исключения краткосрочных или заёмных средств из инвестируемого капитала. Технология функционирует как вспомогательный инструмент, требующий периодического аудита соответствия портфеля изменяющимся жизненным целям инвестора.

В практической реализации робо-эдвайзинг редко выступает как изолированное решение. Он интегрируется в виде модуля в существующие финансовые экосистемы: мобильные приложения банков, брокерские терминалы, пенсионные и страховые платформы, корпоративные программы управления благосостоянием сотрудников. Ключевыми субъектами внедрения выступают кредитные и брокерские организации (обладающие клиентской базой и лицензиями), финтех-стартапы (разрабатывающие алгоритмическое ядро и пользовательский интерфейс), а также регуляторные органы, обеспечивающие стандартизацию алгоритмической логики и защиту прав инвесторов [8].

Таким образом, робо-эдвайзинг представляет собой не универсальный инструмент быстрого обогащения, а дисциплинированную технологию долгосрочного управления капиталом. Его эффективность обусловлена низкой стоимостью, масштабируемостью алгоритмов и нейтрализацией поведенческих искажений. Ограничения связаны с отсутствием адаптивности к сложным жизненным ситуациям и зависимостью от качества исходных математических моделей. Успешное применение технологии требует осознанного выбора платформы, регулярного мониторинга стратегии и, при необходимости, комбинирования алгоритмического управления с экспертным консультированием. Дальнейшее развитие направления связано с углублением интеграции в цифровые экосистемы, повышением прозрачности алгоритмической логики и развитием гибридных моделей обслуживания.

### Список литературы

1. Робо-эдвайзер для инвестиций. <https://blog.mts.investments/articles/robo-adviser?ysclid=mq5ib466ai531689624>

2. Робот-советник и никакого волшебства: как устроен робоэдвайзинг <https://www.banki.ru/news/columnists/?id=10957779>

3. Как ускорить свой портфель простой ребалансировкой <https://bcs-express.ru/novosti-i-analitika/kak-uskorit-svoi-portfel-prostoi-rebalansirovkoj>

4. Что такое робоэдвайзер: как работает и может ли он помочь достигнуть финансовых целей [https://finance.rambler.ru/investicii/56099273/?utm\\_content=finance\\_media&utm\\_medium=read\\_more&utm\\_source=copylink](https://finance.rambler.ru/investicii/56099273/?utm_content=finance_media&utm_medium=read_more&utm_source=copylink)

5. Робоэдвайзинг: что это и работает ли в России [https://finuslugi.ru/navigator/investirovat/stat\\_roboehdvajzing-chto-ehto-takoe-kak-rabotayut-roboehdvajzery-i-ikh-preimushchestva](https://finuslugi.ru/navigator/investirovat/stat_roboehdvajzing-chto-ehto-takoe-kak-rabotayut-roboehdvajzery-i-ikh-preimushchestva)

6. Инвестиции на автомате <https://www.kommersant.ru/doc/6918241>

7. Может ли робот-советник помочь с инвестициями <https://sbersova.ru/sections/invest/mozhet-robot-sovetnik-pomoch-s-investitsiyami>

8. Яцевич Ф. Г. РОБОЭДВАЙЗИНГ КАК НОВАЯ БИЗНЕС-МОДЕЛЬ В ИНВЕСТИЦИОННОМ КОНСУЛЬТИРОВАНИИ // Экономика и социум. 2022. №6-1 (97). URL: <https://cyberleninka.ru/article/n/roboedvayzing-kak-novaya-biznes-model-v-investitsionnom-konsultirovaniii> (дата обращения: 08.06.2026).

**Цебикова Амина Романовна**

студент 1 курса

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

Научный руководитель

**Кузовлева Нина Фёдоровна**

кандидат экономических наук

профессор кафедры экономической экспертизы и финансового мониторинга

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

## **RegTech и SupTech: технология для регулирования национальной платежной системы**

**Аннотация.** В статье рассматривается возможность использования технологий RegTech и SupTech в целях формирования новой экосистемы непрерывного цифрового контроля. Для этого уточняется понятийный аппарат и разграничиваются технологии RegTech и SupTech по субъектам и целям; анализируются системные проекты, формирующие единый цифровой контур, выявляются ключевые риски и барьеры, сдерживающие внедрение.

**Ключевые слова:** цифровые технологии RegTech и SupTech; финансовый рынок; надзор и контроль; экономическая безопасность.

Финансовый рынок переживает фундаментальный сдвиг в системе регулирования, обусловленный стремительным ростом объёмов данных и сквозной цифровизацией бизнес-процессов. Традиционные методы надзора, основанные на периодической бумажной отчётности и выездных проверках, стремительно утрачивают эффективность перед лицом усложняющихся финансовых инструментов и гибридных бизнес-моделей. На передний план закономерно выходят два технологических направления: RegTech (регулятивные технологии, применяемые поднадзорными организациями) и SupTech (надзорные технологии, используемые самим регулятором). В совокупности они формируют в России новую экосистему непрерывного цифрового контроля, в которой обмен данными между Банком России и участниками рынка становится бесшовным и практически мгновенным.

Актуальность темы подтверждается тем, что российский финансовый сектор находится на этапе масштабного внедрения указанных решений. Действующие «Основные направления развития финансовых технологий на 2025–2027 годы» прямо закрепляют внедрение SupTech- и RegTech-инструментов в качестве самостоятельной стратегической задачи [1].

Методология Банка России, изложенная в докладе «Основные направления развития технологий SupTech и RegTech», даёт строгие определения: SupTech

(Supervisory Technology) – это технологии, используемые регулятором для повышения эффективности контроля и надзора за деятельностью участников финансового рынка, тогда как RegTech (Regulatory Technology) – технологии, применяемые финансовыми организациями для оптимизации исполнения регуляторных требований [2]. Различие заключается не столько в технологическом стеке, сколько в целевом назначении и субъекте внедрения.

На функциональном уровне эти две области отчётливо разграничиваются. Для RegTech ключевыми сферами выступают автоматизация процедур идентификации клиентов (KYC) и противодействия отмыванию доходов (AML), мониторинг мошенничества, комплаенс-контроль и подготовка отчётности, то есть всё то, что позволяет банкам с минимальными издержками встраивать обязательные требования в собственные бизнес-процессы [2, 3]. SupTech, напротив, концентрируется на автоматизированном сборе и валидации отчётных данных, предиктивной аналитике рисков, стресс-тестировании, выявлении недобросовестных практик и аффилированных связей – то есть на задачах, непосредственно выполняемых надзорным блоком Центрального банка [1, 2]. При этом в России оба направления институционализированы в рамках единой стратегии, зафиксированной в уже упомянутых «Основных направлениях развития финансовых технологий на 2025–2027 годы», что создаёт предпосылки для их последующей конвергенции. Будучи различными по субъектам, RegTech и SupTech технологически смыкаются в единую экосистему, где данные циркулируют без организационных разрывов.

Архитектура взаимодействия строится на двустороннем потоке данных: от поднадзорных организаций в надзорные информационные системы Банка России и обратно – в форме обязательных к использованию цифровых сервисов. Регулятор перестаёт быть исключительно получателем отчётности и становится поставщиком инфраструктурных платформ, к которым банки подключаются для выполнения собственных регуляторных процедур. Такая логика наглядно проявляется в трёх флагманских проектах.

Первым примером служит Единая биометрическая система (ЕБС), которая выполняет роль межбанковского RegTech-инструмента удалённой идентификации. Предоставляя участникам рынка унифицированный сервис верификации клиентов по биометрическим данным, ЕБС позволяет кредитным организациям исполнять требования законодательства без необходимости создавать собственные дорогостоящие решения, одновременно обеспечивая единый стандарт безопасности и достоверности идентификации [1]. Таким образом, регулятор, создав платформу, реализует RegTech-подход, передавая готовый сервис на аутсорсинг финансовому рынку.

Второй проект, автоматизированная система сбора отчётности на базе таксономии XBRL, олицетворяет центральный SupTech-канал. Банк России реализовал машиночитаемое регулирование, при котором требования к

содержанию, структуре и административным правилам представления отчётных данных некредитных финансовых организаций воплощены в открытой таксономии. Результатами стали кратное сокращение времени подготовки и обработки отчётности, устранение дублирования данных, снижение ошибок за счёт автоматической валидации на стороне отправителя и рост прозрачности регуляторных требований для всех участников рынка [3, 4]. При этом формат XBRL сегодня всё активнее используется не только для обмена с регулятором, но и для прямого информационного взаимодействия между самими участниками, что ещё глубже интегрирует стандарт в ткань рынка.

Третий и наиболее показательный проект – платформа «Знай своего клиента» (ЗСК), которая реализует сквозную логику: SupTech-оценка риска поднадзорного лица встраивается непосредственно в RegTech-процессы банка. Платформа агрегирует данные из ЕГРЮЛ, ФНС, правоохранительных органов и самих кредитных организаций, после чего аналитическое ядро на основе алгоритмов машинного обучения присваивает каждому юридическому лицу и индивидуальному предпринимателю один из трёх цветовых индикаторов риска. Банки через API получают доступ к этой оценке и обязаны учитывать её при проведении операций, что разрывает цепочку миграции недобросовестных клиентов между различными кредитными организациями [5]. Экономический эффект выражается в радикальном снижении нагрузки на комплаенс-службы и повышении результативности борьбы с отмыванием доходов.

Координацию этих инициатив обеспечивает дорожная карта SupTech и RegTech Банка России, которая синхронизирует сроки и функциональные требования к десяткам проектов. Успех подобной интеграции, однако, выводит обсуждение на новый уровень: столь глубокая технологическая связанность создаёт не только преимущества, но и новые уязвимости, требующие пристального анализа.

Цифровой переход в регулировании сопровождается комплексом рисков и барьеров, которые целесообразно систематизировать по трём уровням: технологическому, кадровому и регуляторно-правовому.

Технологический уровень характеризуется недостаточной зрелостью ИТ-инфраструктуры у значительной части поднадзорных организаций, особенно обладающих базовой лицензией. Переход к непрерывному обмену машиночитаемыми данными требует не только модернизации автоматизированных банковских систем, но и решения задачи импортозамещения ключевых компонентов, что в текущих условиях наталкивается на дефицит доверенных программно-аппаратных комплексов [6]. Кроме того, сами алгоритмы машинного обучения, используемые в SupTech-решениях для оценки рисков, несут в себе модельные риски: некорректные допущения или ошибки в обучающих выборках способны приводить к

систематическим искажениям, вплоть до ложной квалификации клиентов на платформе ЗСК.

Кадровый барьер выражается в острой нехватке специалистов, одновременно владеющих компетенциями в области финансов, права и анализа данных. Разработка и валидация моделей оценки кредитного риска, настройка процессов автоматизированного мониторинга и интерпретация результатов предиктивной аналитики требуют именно такого междисциплинарного профиля, дефицит которого пока не преодолен [3].

Регуляторно-правовой уровень связан с необходимостью адаптации законодательства к машиночитаемым нормам. Действующее регулирование по-прежнему во многом ориентировано на документооборот, а не на формально описанные алгоритмы контроля. Отсутствие единого нормативного документа, чётко разграничивающего ответственность за ошибки, неточности и неверные предположения при разработке и эксплуатации SupTech- и RegTech-систем, создаёт зону правовой неопределённости. В практической плоскости это порождает дилемму «квазирегуляторов»: крупные банки, активно внедряющие собственные RegTech-решения, начинают де-факто задавать отраслевые стандарты, что при отсутствии легитимной рамки может повлечь перекося конкурентной среды. Одновременно малые участники рынка сталкиваются с проблемой доступности технологий: затраты на интеграцию с SupTech-платформами требуют инвестиций, не всегда пропорциональных масштабу бизнеса, что способно усиливать рыночную концентрацию.

Преодоление перечисленных барьеров является императивом дальнейшего развития. Система, в которой технологическая мощь регулятора опережает готовность поднадзорной среды и нормативной базы, неизбежно будет сталкиваться с накоплением скрытых уязвимостей, чреватых дискредитацией самой идеи непрерывного цифрового контроля.

Проведённый анализ позволяет сформулировать три синтезирующих вывода.

Во-первых, разграничение RegTech и SupTech по субъектно-целевому принципу является не академической формальностью, а практической необходимостью: RegTech оптимизирует исполнение требований внутри финансовых организаций, тогда как SupTech вооружает регулятора инструментами автоматизированного надзора и предиктивной аналитики.

Во-вторых, проекты Единой биометрической системы, XBRL-отчётности и платформы «Знай своего клиента» наглядно демонстрируют формирование интегрированной экосистемы, в которой регулятор выступает одновременно и получателем данных, и поставщиком инфраструктурных сервисов. Складывается двусторонний цифровой контур, где RegTech- и SupTech-компоненты функционально дополняют друг друга.

В-третьих, риски и барьеры носят системный характер, охватывая технологический, кадровый и регуляторно-правовой уровни, и требуют комплексных решений – от стимулирования импортозамещения и подготовки междисциплинарных специалистов до разработки специального законодательства о машиночитаемых нормах и распределении ответственности.

Таким образом, в России складывается беспрецедентная модель «надзора в реальном времени», где грань между комплаенсом и надзором размывается в пользу общего цифрового контура «Банк России – участники рынка». С одной стороны, такая модель резко повышает прозрачность и предсказуемость рынка, снижает совокупные издержки на соблюдение требований и практически блокирует наиболее грубые формы регуляторного арбитража. С другой стороны, она предъявляет принципиально новые требования к технологической зрелости всех без исключения сторон, концентрация потоков данных усиливает риски кибербезопасности, а цена ошибки алгоритмов становится общесистемной. Дальнейший прогресс будет определяться не столько самими технологиями, сколько способностью государства и рынка выработать единые стандарты доверенного обмена данными, а также сбалансированно распределить риски внедрения решений на основе искусственного интеллекта в контрольно-надзорную деятельность.

### Список литературы

1. Основные направления развития финансовых технологий на период 2025–2027 годов (утв. Банком России). - URL: <https://cbr.ru/fintech/>
2. Доклад Банка России «Основные направления развития технологий SupTech и RegTech на период 2021–2023 годов». - URL: <https://cbr.ru/analytics/>
3. Регулятивные технологии (RegTech) и надзорные технологии (SupTech): опыт Банка России // Вестник финансовых технологий. - 2025. - № 2. - URL: <https://vestnikfintech.ru/>
4. XBRL-отчётность для некредитных финансовых организаций // Официальный сайт Банка России. - URL: <https://cbr.ru/fintech/xbrl/>
5. Платформа «Знай своего клиента»: принципы функционирования // Банковское обозрение. - 2025. - № 12. - URL: <https://bosfera.ru/>
6. Импортозамещение в финансовых технологиях: текущее состояние и перспективы // GIEF Journal. - 2026. - № 1. - URL: <https://giefjournal.ru/>

**Шакунас Юлия Николаевна**

студент 5 курса

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

Научный руководитель

**Богатырёв Сергей Индрисович**

заведующий кафедрой экономической экспертизы и финансового мониторинга

ФГБОУ ВО «МИРЭА – Российский технологический университет»

Россия, г. Москва

## **Роль и значение риск-ориентированного подхода в системе экономической безопасности аудиторской организации**

**Аннотация.** В статье рассматривается риск-ориентированный подход как ключевой элемент обеспечения экономической безопасности аудиторской организации. Проведён сравнительный анализ системного, процессного, сценарного, комплексного и риск-ориентированного подходов к управлению рисками. Обосновано, что риск-ориентированный подход позволяет оптимально распределять ресурсы, концентрируя усилия на наиболее значимых угрозах. Раскрыты практические аспекты применения данного подхода в аудиторской деятельности, включая контроль рабочих документов и обеспечение конфиденциальности.

**Ключевые слова:** экономическая безопасность, риск-ориентированный подход, аудиторская организация, управление рисками, системный подход, процессный подход, сценарный подход, комплексный подход.

Обеспечение экономической безопасности является одной из приоритетных задач любой организации, функционирующей в условиях рыночной неопределенности и динамично меняющейся внешней среды. Особую актуальность данная проблема приобретает для аудиторских организаций, деятельность которых сопряжена с высокими требованиями к качеству услуг, доверием со стороны клиентов и регуляторов, а также с необходимостью обработки конфиденциальной информации. Без непрерывного функционирования эффективной системы экономической безопасности предприятие становится уязвимым для широкого спектра внутренних и внешних угроз.

Для эффективного управления рисками необходима систематизация и анализ рисков на основе ряда факторов, включая сроки реализации, характер последствий и источник возникновения. Это позволяет компании не только выявлять потенциальные риски, но и разрабатывать стратегии их минимизации, что способствует повышению устойчивости и конкурентоспособности бизнеса [2].

В научной литературе выделяются следующие основные подходы к управлению рисками.

*Системный подход* построен на группировке и категоризации рисков. Он позволяет рассматривать организацию как целостную систему взаимосвязанных элементов, где риски в одной сфере влияют на другие. Преимуществом является достижение синергии и целостности, однако существует сложность в определении реальных взаимосвязей между элементами [2].

*Процессный подход* подразумевает системное управление деятельностью организации как совокупностью взаимосвязанных процессов, направленных на достижение определённых целей. Он строится на выделении основных процессов, необходимых для достижения целей организации. К преимуществам относится встроенность в повседневную деятельность, к ограничениям – снижение гибкости и жёсткие временные рамки [6].

*Сценарный подход* осуществляется путём формирования сценариев управления рисками, охватывающих все этапы риск-менеджмента. Процесс управления целесообразно формировать как непрерывный и неизменный во времени. Основное преимущество – учёт неопределённости через проработку различных вариантов развития событий, недостаток – высокая трудоёмкость [5].

*Комплексный подход* основывается на том, что оценка риска начинается с момента определения площади, подверженной негативным последствиям. В процессе планирования данный метод предполагает определение конкретной цели, достижение которой необходимо организации. Преимущество – полнота охвата всех аспектов, ограничения – высокая стоимость и сложность управления [4]. Для удобства сравнения указанные подходы систематизированы в табл. 1.

Несмотря на имеющееся многообразие существующих методологий, в современных условиях ведения аудиторского бизнеса особое значение приобретает такой подход, который позволяет не просто классифицировать или описывать риски, но выстраивать на основе их оценки приоритеты защитной деятельности и оптимально распределять ограниченные ресурсы. Подобными свойствами обладает риск-ориентированный подход.

Риск-ориентированный подход предполагает системную оценку вероятности возникновения событий, возможных вредных последствий для организации и их результатов [3]. Полученная оценка позволяет спрогнозировать как наиболее вероятные сценарии развития негативных событий, так и критические точки уязвимости в бизнес-процессах предприятия. Это открывает возможности заблаговременно определить приоритетные направления системы защиты, направив ресурсы именно в те области, где потенциальный ущерб был выявлен как максимальный.

Таблица 1

Сравнительный анализ подходов к управлению рисками

| Наименование подхода | Основной вопрос                      | Объект фокуса             | Преимущества                | Ограничения                             |
|----------------------|--------------------------------------|---------------------------|-----------------------------|-----------------------------------------|
| Системный подход     | Как связаны рассматриваемые элементы | Структура и взаимосвязи   | Целостность и синергия      | Сложность в определении взаимосвязей    |
| Процессный подход    | Как организовать работу              | Действия, процессы        | Встроенность в деятельность | Снижение гибкости, временные рамки      |
| Сценарный подход     | Что может произойти                  | Варианты развития событий | Учет неопределенности       | Трудоемкость                            |
| Комплексный подход   | Как охватить все                     | Все аспекты               | Полнота охвата              | Высокая стоимость, сложность управления |

В отличие от системного, процессного, сценарного или комплексного подходов, риск-ориентированный подход акцентирует внимание не столько на структуре или организации управления, сколько на селекции угроз по степени их опасности и концентрации усилий на наиболее значимых направлениях.

Согласно Федеральному закону № 294-ФЗ от 26.12.2008 «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля», риск-ориентированный подход представляет собой метод организации и осуществления государственного контроля, при котором выбор интенсивности проведения мероприятий определяется отнесением деятельности юридического лица к определённой категории риска [1].

Интерпретируя данное определение применительно к аудиторской деятельности, риск-ориентированный подход – это способ организации и осуществления контроля на предприятии, включающий мероприятия по профилактике нарушения требований, необходимых для обеспечения безопасности организации. Принципиальным отличием данного подхода от традиционных моделей контроля является его предупреждающий характер. Вместо реагирования на уже свершившиеся факты нарушений и ликвидации последствий система устроена так, чтобы не допустить самого возникновения условий, благоприятствующих реализации угроз.

Данный подход актуален для рисков, которые могут возникать непрерывно в процессе функционирования предприятия, причём единичная реализация риска не исключает его повторного возникновения. Поэтому организации при планировании должны учитывать не только вероятность возникновения рисков, но и их цикличность и объём потенциального ущерба.

Применение риск-ориентированного подхода в аудите позволяет:

- планировать аудиторские процедуры с приоритетом процессов с наибольшей вероятностью риска;
- снижать вероятность ошибок и объёмы потерь;
- повышать качество управленческих решений.

В современных исследованиях отмечается, что интеграция риск-ориентированного аудита во внутренний аудит способствует повышению финансовой устойчивости, эффективности бизнес-процессов и сохранению доверия со стороны собственников, инвесторов и регуляторов [3]. Описанный подход помогает предотвратить наступление репутационного риска, а избежание репутационных потерь, в свою очередь, позволяет предотвратить и другие риски, например, финансовые. Затраты, направленные на определение и минимизацию ещё не реализованных угроз, не превышают ущерб, который может понести компания.

Тем самым риск-ориентированный подход выступает действенным инструментом обеспечения экономической безопасности аудиторской организации, поскольку он выстраивает защиту не путём сплошного перекрытия всех возможных направлений рисков, что крайне затратно, а на основе конкретных объективных данных о том, какие риски действительно представляют опасность, а какие являются малозначительными. Благодаря такому выборочному и одновременно системному воздействию достигается главная цель системы экономической безопасности – поддержание устойчивости функционирования организации в условиях неопределённости при оптимальном, экономически обоснованном уровне затрат на защиту.

Например, согласно руководству по оказанию аудиторских услуг, руководство компаний определяет ряд необходимых действий для предотвращения наступления рисков. Чтобы гарантировать соответствие необходимого уровня качества, все задания, обеспечивающие уверенность, должны быть выполнены, а процедуры задокументированы с использованием определённых программ. В данном примере риск-ориентированный подход предполагает достижение определённого уровня качества выполненных работ, заранее устанавливая обязательные контрольные процедуры для предотвращения репутационного и регуляторного рисков.

Одним из элементов, обосновывающих необходимость применения риск-ориентированного подхода, является контроль за рабочими документами. Аудиторские рабочие документы – это любые материалы, подготовленные работниками или клиентом, подтверждающие аудиторское мнение. Проведение процедур для обеспечения конфиденциальности и сохранности рабочих документов выступает примером требований, выполнение которых обеспечивает защиту коммерческой и государственной тайны. Подобный подход обучения и регулярного напоминания сотрудникам позволяет предотвратить

реализацию ряда рисков или минимизировать их последствия, что особенно важно, поскольку аудиторская деятельность представляет собой обмен значимой информацией, утечка которой может иметь необратимые последствия.

Таким образом, хозяйствующим субъектам любой сферы деятельности важно обеспечивать свою экономическую безопасность, в том числе и предприятиям сферы аудиторских услуг. Полноценная и всесторонняя защита компании невозможна без правильного подхода к её обеспечению. Риск-ориентированный подход позволяет минимизировать возможность возникновения рисков как таковых, концентрируя ресурсы на наиболее значимых угрозах и обеспечивая предупреждающий характер контрольных мероприятий. Для закрепления теоретических положений целесообразен переход к практической оценке необходимости внедрения новых мер контроля или совершенствования, уже имеющихся в конкретной аудиторской организации.

### Список литературы

1. О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля: Федеральный закон от 26.12.2008 № 294-ФЗ (ред. от 29.12.2025). – Текст: электронный // СПС «КонсультантПлюс». – URL: [http://consultant.ru/document/cons\\_doc\\_LAW\\_83079/](http://consultant.ru/document/cons_doc_LAW_83079/) (дата обращения: 14.06.2026). [4]
2. Тубалец, А. А. Системный подход к риск-менеджменту в деятельности предприятия / А. А. Тубалец, А. А. Бедакова, М. С. Саркисян, В. В. Ивахно. – Текст: электронный // ЕГИ. – 2025. – № 2 (58). – URL: <https://cyberleninka.ru/article/n/sistemnyy-podhod-k-risk-menedzhmentu-v-deyatelnosti-predpriyatiya> (дата обращения: 14.06.2026). [8]
3. Кабиева, Л. К. Применение риск-ориентированного подхода в современном внутреннем аудите / Л. К. Кабиева. – Текст: электронный // Проблемы Науки. – 2025. – № 12 (211). – URL: <https://cyberleninka.ru/article/n/primenenie-risk-orientirovannogo-podhoda-v-sovremennom-vnutrennem-audite> (дата обращения: 14.06.2026). [20]
4. Логинова, А. Д. Комплексный подход к анализу рисков в управлении проектами / А. Д. Логинова, О. В. Дюдина. – Текст: электронный // Вестник науки. – 2025. – № 1 (82). – URL: <https://cyberleninka.ru/article/n/kompleksnyy-podhod-k-analizu-riskov-v-upravlenii-proektami> (дата обращения: 14.06.2026). [26]
5. Миллер, А. Е. Сценарный подход к управлению рисками в контексте экономической безопасности организации / А. Е. Миллер. – Текст: электронный // Вестник СИБИТа. – 2025. – № 1. – URL: [https://cyberleninka.ru/article/n/stsenarnyy-podhod-k-upravleniyu-riskami-v-](https://cyberleninka.ru/article/n/stsenarnyy-podhod-k-upravleniyu-riskami-v)

[kontekste-ekonomicheskoy-bezopasnosti-organizatsii](#) (дата обращения: 14.06.2026). [28]

6. Титов, Д. А. Управление рисками на основе методологий Lean и процессного подхода / Д. А. Титов, Е. В. Бондарева. – Текст: электронный // Вестник науки. – 2025. – № 6 (87). – URL: <https://cyberleninka.ru/article/n/upravlenie-riskami-na-osnove-metodologiy-lean-i-protsessnogo-podhoda> (дата обращения: 14.06.2026). [34]

**Янушкина Юлия Игоревна**

старший преподаватель кафедры экономической экспертизы и финансового мониторинга  
ФГБОУ ВО «МИРЭА – Российский технологический университет»  
Россия, г. Москва

**Одушкин Павел Юрьевич**

студент 5 курса  
ФГБОУ ВО «МИРЭА – Российский технологический университет»  
Россия, г. Москва

## **Цифровые технологии в судебной финансово-экономической экспертизе: перспективы анализа финансового состояния организаций**

**Аннотация.** В статье рассматривается применение цифровых технологий и аналитики Big Data на практике в судебной финансово-экономической экспертизе. Анализируется влияние применения машинного обучения, Big Data и цифрового документооборота на изменение методов оценки финансового состояния организаций и повышение достоверности экспертных заключений. Особое внимание уделяется перспективам дальнейшего развития финансовой составляющей организаций.

**Ключевые слова:** судебная финансово-экономическая экспертиза, цифровые технологии, Big Data, финансовый анализ, цифровизация.

В настоящее время судебно-экономическая экспертиза сталкивается с рядом нерешенных вопросов и методических проблем. Преодоление этих трудностей позволит значительно усовершенствовать практику судебно-экспертной деятельности. Среди наиболее значимых задач можно выделить необходимость разработки единых стандартов анализа финансовых данных, унификации подходов к оценке доказательств и интеграции цифровых технологий в экспертные процедуры. Важную роль приобретает создание комплексных методик выявления экономических правонарушений в условиях цифровизации финансовой сферы [1].

Отсутствие унифицированных методических подходов приводит к недостаткам в современной судебной экономической экспертной практике, таким как:

- использование ограниченного набора аналитических показателей, не позволяющего провести комплексную оценку финансового состояния;
- нарушение принципа единообразия и достоверности;
- преобладание формальных расчетных процедур над качественным анализом факторов формирования финансовых показателей;
- смещение акцента в сторону формальных расчетов при недостаточном внимании к анализу факторов, определяющих финансовые результаты;

– отсутствие системного подхода к трактовке результатов коэффициентного анализа.

Одним из перспективных направлений развития в современной судебной экономической экспертной деятельности является использование Big Data. Цифровая инфраструктура организаций формирует значительные объемы информации: данные электронных платежей, автоматизированные записи бухгалтерских операций, лог-файлы действий пользователей, облачные архивы документов и учет взаимодействия с контрагентами. Методы Big Data позволяют определять статистические несоответствия, выявлять взаимосвязи между транзакциями и определять признаки искусственного искажения финансовых потоков. Это существенно повысит достоверность сделанных выводов на базе практических данных, так как вероятность допущения пропуска критически значимых операций значительно снижается [2].

Важное значение имеет развитие системы электронного документооборота. Переход предприятий на цифровые подписи соглашений, облачное хранение документации и автоматизированное формирование отчетности создает для эксперта комплексную и достоверную цифровую среду [3].

Специализированное программное обеспечение для анализа массивов информации может применяться для обнаружения существенных расхождений или фальсификации данных, позволяя выявлять закономерности в исследуемом экономическом массиве данных. Особое значение приобретают технологии распределенных реестров, включая Blockchain, которые обеспечивают прозрачность и неизменность данных. Для анализа информации таких источников как, система «1С: Предприятие», квалификация эксперта не должна ограничиваться познаниями в сфере бухгалтерской учета, но и навыками применения автоматизированных средств обработки больших баз данных. Часто встречаются случаи, когда объем хозяйственных операций крайне велик, особенно если данные изъяты за несколько лет и обработать такой массив быстро с помощью стандартных средств Программы Excel не представляется возможным, поскольку этот процесс займет продолжительное время и потребует значительных трудозатрат. Однако развитие цифровых технологий в судебной системе сталкивается с регуляторными барьерами. Так, попытка Судебного департамента закупить системы видеоконференц-связи для ГАС «Правосудие» на 745 млн рублей была заблокирована из-за спорных требований к обязательной регистрации встроенного программного обеспечения в реестре российских программ. Жалоба поставщика демонстрирует ключевую проблему: формальное применение норм о промышленной продукции к устройствам, где ПО является неотъемлемой частью оборудования, фактически приводит к запрету на закупку не только иностранных, но и соответствующих российских решений. Этот пример иллюстрирует наличие проблемы регулирования госзакупок, создавая

серьезные барьеры для реализации проектов по цифровизации в государственной судебной сфере и требует корректировки в нормативно правовой базе.

В заключение, проведенный анализ перспективы развития судебной финансово-экономической экспертизы в условиях цифровизации требует комплексного внедрения современных технологий, включая Big Data, распределённые реестры и системы электронного документооборота. Эти инструменты позволяют повысить достоверность и глубину анализа финансового состояния организаций, обеспечивая выявление скрытых взаимосвязей и признаков искажения данных. Однако вместе с технологическими возможностями сохраняются значимые проблемы: отсутствие унифицированных подходов, недостаточная системность анализа и ограниченность используемых показателей, а также нормативно-правовые барьеры, препятствующие развитию цифровой инфраструктуры судебной системы. Таким образом, дальнейшее совершенствование судебной финансово-экономической экспертизы связано не только с внедрением цифровых технологий, но и с модернизацией методической базы и устранением нормативных препятствий, что позволит обеспечить более высокую точность, объективность и эффективность экспертных заключений.

### Список литературы

1. Владимир А.П. Роль экономико-математических моделей и современных информационных технологий в методическом обеспечении судебно-экономических экспертиз // Вестник Московского университета МВД России. 2018. №4.
2. Горбачева А.В., Леонов А.И., Мамкин А.Н., Соловьев О.Д., Софьин А.А. АКТУАЛЬНЫЕ ПРОБЛЕМЫ НАЗНАЧЕНИЯ И ПРОИЗВОДСТВА СУДЕБНО-ЭКОНОМИЧЕСКИХ ЭКСПЕРТИЗ // Право и практика. 2024. №2.
3. Саркисян А. А. Цифровые базы данных в судебно экспертной деятельности // Вестник Университета имени О. Е. Кутафина. 2020. №6 (70). URL: <https://cyberleninka.ru/article/n/tsifrovye-bazy-dannyh-v-sudebno-ekspertnoy-deyatelnosti>.

**Янушкина Юлия Игоревна**

старший преподаватель кафедры экономической экспертизы и финансового мониторинга  
ФГБОУ ВО «МИРЭА – Российский технологический университет»  
Россия, г. Москва

**Полушкин Илья Александрович**

студент 5 курса  
ФГБОУ ВО «МИРЭА – Российский технологический университет»  
Россия, г. Москва

### **Диагностика финансовой несостоятельности: аналитический инструментарий на основе бухгалтерской отчетности**

**Аннотация.** Бухгалтерская отчетность служит основным источником информации, дающим комплексное представление о финансовом состоянии предприятия, результатах деятельности и уровне ее финансовой устойчивости. Информация, содержащаяся в отчетности, является основой для выявления признаков финансовой несостоятельности. На фоне нестабильности внешней среды и ужесточения требований к финансовой дисциплине, своевременная диагностика несостоятельности выходит на передний план. В данной статье рассматривается аналитический инструментарий диагностики финансовой несостоятельности на основе бухгалтерской отчетности.

**Ключевые слова:** финансовая несостоятельность, диагностика финансового состояния, бухгалтерская отчетность, аналитический инструментарий, финансовая устойчивость.

Современный этап экономического развития, характеризующийся процессами глубокой цифровизации, оказывает трансформационное воздействие на все сферы финансовой безопасности, включая область диагностики и прогнозирования финансовой несостоятельности (банкротства). Традиционные методы анализа, основанные на ретроспективных данных бухгалтерской отчетности, уступают место комплексным системам, функционирующим в режиме, близком к реальному времени, что кардинально меняет парадигму антикризисного управления. Цифровизация способствует эволюции диагностики по нескольким ключевым направлениям. Во-первых, происходит переход от статического анализа к динамическому прогнозированию. Классические модели Альтмана, Таффлера, Сайфуллина и др., опирающиеся на ограниченный набор коэффициентов, эффективны для констатации сложившегося финансового положения, но обладают ограниченной прогнозной силой. Внедрение технологий больших данных (Big Data) и машинного обучения (Machine Learning) позволяет анализировать неструктурированные информационные потоки: новостные ленты, отзывы

клиентов, данные с кассовых аппаратов, транзакционную активность, активность в социальных сетях. Алгоритмы выявляют сложные, неочевидные для человеческого восприятия корреляции, что значительно повышает точность и заблаговременность прогноза о вероятности наступления финансовой несостоятельности. Во-вторых, цифровизация обеспечивает принципиально новый уровень детализации и скорости получения информации. Платформы электронного документооборота, системы ERP (Enterprise Resource Planning) и CRM (Customer Relationship Management) формируют единое цифровое пространство, предоставляя аналитикам доступ к оперативным данным о состоянии дебиторской и кредиторской задолженности, движении денежных средств, уровне запасов и исполнении контрактов. Это позволяет осуществлять мониторинг финансового здоровья организации не по итогам отчетного периода, а постоянно, выявляя негативные тенденции на стадии их возникновения. Технологии распределенных реестров (блокчейн) могут быть использованы для ведения прозрачной и неизменяемой истории финансовых операций, что повышает достоверность информации для диагностики. В-третьих, развиваются системы предиктивной аналитики и стресс-тестирования [2].

На основе цифровых двойников компании – комплексных математических моделей, имитирующих ее финансовые процессы, – можно проводить сценарный анализ.

Менеджмент получает возможность оценить, как изменения ключевых рыночных параметров (курсы валют, ставки, спрос) или внутренние шоки (потеря крупного контрагента) отразятся на финансовой устойчивости, и своевременно принять превентивные меры

Однако цифровая трансформация диагностики создает и новые вызовы. Возрастают требования к качеству и структуре данных, их защите от киберугроз.

Существует риск «зашумленности» анализа из-за избыточности информации, а также проблема «черного ящика» некоторых сложных алгоритмов, когда решение системы не поддается простой интерпретации. Кроме того, эффективность цифровых моделей зависит от компетенций персонала, способного не только собирать данные, но и корректно интерпретировать результаты анализа.

Двухфакторная модель Альтмана является самым простым методом выявления вероятности банкротства. Формула двухфакторной модели Альтмана имеет следующий вид:

$$Z = -03877 - 1,0736X_1 + 0,579(X_2/X_3),$$

где:  $X_1$  – коэффициент текущей ликвидности;

$X_2$  – заемный капитал;

$X_3$  – пассивы.

При значении коэффициента  $Z > 0$  – вероятность банкротства высока.

Очевидным преимуществом данной модели является её простота, а также очень малый объём информации, необходимой для анализа. Основным недостатком двухфакторной модели Альтмана – низкая точность прогноза, особенно в российских условиях экономической нестабильности.

Пятифакторная модель Альтмана является наиболее популярной.

Модель объединяет пять финансовых показателей, каждый из которых характеризуют финансовое положение и результаты деятельности предприятия:

$$Z = 1,2X_1 + 1,4X_2 + 3,3X_3 + 0,6X_4 + X_5,$$

где:  $X_1$  – оборотный капитал / сумма активов предприятия;

$X_2$  – нераспределённая прибыль / сумма активов предприятия;

$X_3$  – прибыль до налогообложения / общая стоимость активов;

$X_4$  – рыночная стоимость собственного капитала / бухгалтерская (балансовая) стоимость всех обязательств;

$X_5$  – объём продаж / общая величина активов предприятия.

Значение  $Z$  интерпретируется следующим образом:

1.  $Z < 1,81$  – вероятность банкротства составляет от 80% до 100%;
2.  $Z = 1,81 - 2,77$  – средняя вероятность краха компании – от 35% до 50%;
3.  $Z = 2,77 - 2,99$  – вероятность банкротства невелика и составляет от 15% до 20%;
4.  $Z > 2,99$  – ситуация на предприятии стабильна, риск неплатёжеспособности в течение ближайших двух лет крайне мал [3].

Семифакторная модель Альтмана дает возможность оценить риск утраты платежеспособности компании на горизонте нескольких лет – примерно до пятилетнего периода, обеспечивая при этом около 70 % точности прогноза. Однако из-за громоздкости вычислений и сложности применения на практике эта методика не получила широкого распространения.

Проведем анализ банкротства в ЗАО ОПХ «Центральное» на основе пятифакторной модели Альтмана (табл. 1). Показатели рассчитываются на основании «Бухгалтерского баланса» и «Отчета о прибылях и убытках».

Подставим полученные данные в формулу и получим результат:

$$Z = 1,2*0,024 + 1,4*0,018 + 3,3*(-0,027) + 0,6*2,802 + 0,452 = 2,098$$

Таблица 1

Расчет показателей по пятифакторной модели Альтмана

| Показатель | Способ расчета                                                                                    | Значение |
|------------|---------------------------------------------------------------------------------------------------|----------|
| X1         | Оборотный капитал / сумма активов предприятия                                                     | 0,024    |
| X2         | Нераспределённая прибыль / сумма активов предприятия                                              | 0,018    |
| X3         | Прибыль до налогообложения / общая стоимость активов                                              | -0,027   |
| X4         | Рыночная стоимость собственного капитала / бухгалтерская (балансовая) стоимость всех обязательств | 2,802    |
| X5         | Объём продаж / общая величина активов предприятия                                                 | 0,452    |

На основе проведённых расчётов по пятифакторной модели Альтмана для ЗАО ОПХ «Центральное» можно сделать вывод, что финансовое положение предприятия остаётся неоднозначным. Итоговый показатель Z равен 2,098, что попадает в так называемую «серую зону». Это промежуточный диапазон, где сложно уверенно прогнозировать дальнейшее развитие событий: риск банкротства нельзя назвать критическим, однако и говорить о стабильности компании также не приходится. Вероятность наступления финансовых трудностей в ближайшие годы оценивается как средняя – примерно от 35 до 50%. Иными словами, предприятие находится в состоянии неопределённости. С одной стороны, показатели не свидетельствуют о неизбежном крахе в ближайшие два – три года. С другой – текущая структура активов и прибыльность бизнеса не дают уверенности в его надёжности и долгосрочной устойчивости.

В заключении отметим, цифровизация не просто автоматизирует традиционные методы диагностики финансовой несостоятельности, а порождает качественно новую, более эффективную методологию. Она смещает акцент с констатации факта кризиса на его упреждающее прогнозирование и профилактику, превращая диагностику из инструмента экстренного реагирования в элемент системы непрерывного стратегического контроля и управления стоимостью компании. Успешность антикризисного управления в современной экономике напрямую связана со способностью хозяйствующих субъектов интегрировать передовые цифровые инструменты в процессы финансового анализа.

### Список литературы

1. Федеральный закон от 06.12.2011 № 402-ФЗ (ред. от 26.12.2024) «О бухгалтерском учете» [Электронный ресурс] – URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_122855/5864bb6f56b1eb0fb1ada8aac90fa2990e8ef58b](https://www.consultant.ru/document/cons_doc_LAW_122855/5864bb6f56b1eb0fb1ada8aac90fa2990e8ef58b)

2. Вадим Супрун «Финансовый анализ при банкротстве предприятия» [Электронный ресурс] – URL: <https://b2b.ooooeos.ru/articles/kak-provoditsya-finansoviy-analiz-pri-bankrotstve-predpriyatiya>

3. Петрова Е.В., Наговицына В.П. Диагностика Вероятности банкротства: зарубежные и отечественные модели прогнозирования, 2023.

**Актуальные проблемы обеспечения экономической безопасности и противодействия  
коррупции и теневой экономике**

**Выпуск 6**

Сборник научных трудов публикуется в авторской редакции

Сетевое издание

Редакционная коллегия:  
Богатырёв С.И., Кузовлева Н.Ф.

Ответственный за выпуск – Алимова Н.К.

Научное издание

**Системные требования:**  
операционная система Windows XP или новее, macOS 10.12 или новее, Linux.  
Программное обеспечение для чтения файлов PDF.

Объем данных 4,1 Мб

Принято к публикации «06» июля 2026 года

Режим доступа: <https://izd-mn.com/PDF/45MNNPK26.pdf> свободный – Загл. с экрана –  
Яз. рус., англ.

ООО «Издательство «Мир науки»  
«Publishing company «World of science», LLC

Адрес:

Юридический адрес – 127055, г. Москва, пер. Порядковый, д. 21, офис 401.

Почтовый адрес – 127055, г. Москва, пер. Порядковый, д. 21, офис 401.

<https://izd-mn.com/>

**ДАННОЕ ИЗДАНИЕ ПРЕДНАЗНАЧЕНО ИСКЛЮЧИТЕЛЬНО ДЛЯ ПУБЛИКАЦИИ НА  
ЭЛЕКТРОННЫХ НОСИТЕЛЯХ**