УДК 332.1:004.9:004.808.9

Институциональные изменения в государственном финансовом контроле в эпоху цифровых трансформаций и киберугроз

Медик Ирина Николаевна

Кандидат экономических наук, доцент,
кафедра мировой экономики и экономической безопасности,
Байкальский государственный университет,
664003, Российская Федерация, Иркутск, ул. Ленина, 11;
e-mail: m.irina.n@list.ru

Аннотация

Цель исследования заключается в анализе институциональных изменений в системе государственного финансового контроля в условиях цифровой трансформации и растущих киберугроз. Описаны современные вызовы, связанные с ускоренной интеграцией цифровых технологий и изменениями в глобальной экономической среде, что требует пересмотра существующих механизмов контроля и надзора за финансовыми потоками. Выявлены основные проблемы, такие как устаревание традиционных методов контроля, неадекватная подготовка кадров и отсутствие координации между различными государственными структурами, отвечающими за безопасность финансовой системы. Методы исследования основаны на междисциплинарном подходе, включающем сравнительный анализ, системный подход и моделирование сценариев развития финансового контроля в цифровой среде. Проведен анализ национальных и международных практик, изучены законодательные инициативы, направленные на усиление защиты информационных систем и адаптацию контрольных механизмов к новым реалиям. Особое внимание уделено анализу угроз, связанных с кибербезопасностью, и оценке их влияния на эффективность работы контрольных органов. Результаты исследования демонстрируют, что модернизация государственного финансового контроля требует интеграции информационных технологий, разработки новых нормативно-правовых актов и формирования институциональных механизмов, способных оперативно реагировать на вызовы цифровой эпохи. Практическая значимость результатов заключается в возможности использования разработанных рекомендаций для совершенствования финансового контроля, повышения прозрачности бюджетных процессов и усиления противодействия киберугрозам. В работе также предложена структура взаимодействия между государственными органами, научным сообществом и частным сектором, что позволит повысить надежность и устойчивость финансовой системы. Выявлена необходимость постоянного мониторинга технологических и кибернетических изменений, а также развития профессиональной подготовки специалистов в области информационной безопасности. Авторы приходят к выводу, что успех реформ в данной сфере во многом зависит от оперативной адаптации институциональных практик и внедрения инновационных технологий, способствующих защите финансовых интересов государства и общества. Таким образом, представленные результаты способствуют развитию теоретических основ и практических аспектов

институциональных преобразований в государственном финансовом контроле в эпоху цифровых трансформаций и киберугроз.

Для цитирования в научных исследованиях

Медик И.Н. Институциональные изменения в государственном финансовом контроле в эпоху цифровых трансформаций и киберугроз // Экономика: вчера, сегодня, завтра. 2025. Том 15. № 3А. С. 468-482.

Ключевые слова

Институциональные изменения, государственный контроль, финансовый контроль, цифровые трансформации, киберугрозы.

Введение

Государственный финансовый контроль переживает существенные институциональные изменения, когда цифровые технологии становятся краеугольным камнем практически всех экономических процессов. Постоянное проникновение инновационных решений в инфраструктуру органов публичного управления порождает как новые возможности повышения прозрачности и эффективности, так и значительные риски в форме киберугроз. Эти риски связаны не только с угрозой внешнего вмешательства, но и со сложностями в обеспечении надежной защиты информации при высоком уровне распределенности цифровых платформ. Ситуация усложняется тем, что государственный финансовый контроль традиционно ориентировался на соблюдение регламентированных процедур, тогда как в цифровую эпоху такие процедуры подвергаются пересмотру ввиду появляющихся технологий. Трансформация касается не только технического оснащения, но и методологических основ, которые должны постоянно адаптироваться к динамичной среде [Матафонова, 2021]. В то же время усиливается роль международного сотрудничества, поскольку киберпространство не имеет четких государственных границ, и финансовые потоки становятся объектом пристального внимания со стороны международных институтов. Постепенно формируется новая архитектура регулирования, включающая в себя не только законодательные акты на национальном уровне, но и транснациональные соглашения и стандарты, в том числе в сфере кибербезопасности государственных финансовых систем [Зарицкая, Куликова, 2018]. Эти изменения структурируют и само понимание прозрачности: сейчас под ней подразумевают не только учетные показатели, но и степень защищенности информации в реальном времени. Таким образом, государственный финансовый контроль претерпевает комплексный сдвиг, предполагающий модернизацию всех составляющих – от нормативно-правовой базы до технических средств анализа и аудита данных. В условиях, когда цифровые платформы стали неотъемлемой частью взаимодействия между государственными органами и гражданами, возникает необходимость в выработке более гибких форм контроля, учитывающих особенности цифровой среды и готовых масштабироваться по мере усложнения киберугроз. Технологическая составляющая всего этого процесса создает предпосылки для повышения эффективности, однако одновременно повышает уязвимость важнейших данных, поэтому становится очевидной потребность в институциональных изменениях, охватывающих как законодательную сферу, так и практику контроля.

Все более широкое внедрение автоматизированных систем учета и мониторинга денежных

потоков привело к тому, что государственные структуры вынуждены пересматривать методы и роли отдельных институтов надзора. Характерные для прошлого века формы контроля, основанные преимущественно на проверке документации и физическом присутствии ревизоров, уже не могут в полной мере отражать уровень непрерывных цифровых взаимодействий. На смену приходят аналитические платформы, которые опираются на технологии больших данных и машинного обучения [Пумбрасова, Бессчетнова, 2020]. Такие платформы позволяют обрабатывать огромные объемы информации за короткий промежуток времени, выявляя закономерности и потенциальные отклонения, неочевидные при ручной проверке. Этот переход к автоматизированному анализу способствует тому, что государственный финансовый контроль становится более проактивным и сконцентрированным на прогнозировании рисков. Меняется и компетентностный профиль сотрудников контрольных органов: от них уже не требуется исключительно умение работать с бумажными носителями и составлять отчеты, гораздо более важными становятся навыки анализа цифровых данных и понимание специфики киберугроз [Васянина, 2022]. Вместе с тем остается открытым вопрос о том, как обеспечить надлежащую кибербезопасность самих этих аналитических систем, поскольку их функционирование формирует новые точки уязвимости. Кроме того, стремительное внедрение оцифрованных процессов может порождать проблемы хранения и аутентификации данных, особенно если учет ведется на распределенных платформах. Государственный финансовый контроль, чтобы сохранять свою актуальность, должен учитывать эти вызовы на этапе формирования как стратегии, так и тактики надзорной деятельности. Наконец, необходимо подчеркнуть, что традиционные механизмы согласования полномочий между различными государственными органами часто не успевают за технологическими изменениями, в результате чего возрастает риск пробелов и дублирований в контрольных процедурах.

Материалы и методы исследования

В условиях нарастающей взаимозависимости между государственными информационными системами все сильнее проявляются проблемы межведомственной координации. Цифровые платформы, предназначенные для контроля над бюджетными расходами и поступлениями, нередко пересекаются с другими информационными ресурсами, включая базы данных правоохранительных органов и налоговых служб. Такая конвергенция информации способствует повышению эффективности работы надзорных структур, поскольку данные можно сопоставлять из различных источников и оперативно вскрывать возможные несоответствия [Шичанин, 2021]. Однако это же усиливает уровень уязвимости, ведь компрометация одного узла может повлечь неконтролируемый доступ к обширным массивам конфиденциальных сведений. В результате органы государственного финансового контроля становятся не только потребителями данных, но и держателями критической инфраструктуры, требующей постоянной защиты. Здесь проявляется вся сложность современных киберугроз: хакерские атаки могут быть направлены не только на кражу финансовой информации, но и на нарушение целостности данных, что способно приводить к искажению показателей бюджетной отчетности и финансовых прогнозов [Никифорова, 2019]. Для противодействия таким сценариям недостаточно только технических мер: возникает необходимость совершенствовать нормативно-правовые механизмы, которые могли бы устанавливать четкие правила взаимодействия между ведомствами и задавать критерии кибербезопасности для всех участников процесса. Но для этого требуются институциональные изменения, способные

обеспечить интенсивное сотрудничество между различными ветвями государственного аппарата, а также с экспертным сообществом и частным сектором.

Одновременно растет потребность в ясных определениях и правовом закреплении ключевых понятий, связанных с цифровым контролем и защитой бюджетных данных. Государственные структуры не всегда успевают адаптироваться к стремительному развитию технологий, что порождает пробелы и коллизии в законодательстве. Проблема усугубляется тем, что международное информационное взаимодействие требует унификации терминологии и подходов. Создание общей нормативной базы, регулирующей вопросы кибербезопасности в области государственного финансового контроля, может значительно упростить обмен передовыми практиками между странами и обеспечить более высокую степень предсказуемости действий надзорных органов [Горохова, 2023]. Вместе с тем, поскольку каждая страна имеет свою правовую систему и уникальные особенности политико-административной структуры, полная унификация представляется затруднительной. В рамках отдельных объединений государств уже формируются инициативы по стандартизации принципов кибербезопасности и цифрового надзора, однако окончательная гармонизация требует длительного времени и учета множества факторов. В итоге национальные органы государственного финансового контроля вынуждены формировать собственные внутренние регламенты, опираясь на международные рекомендации и при этом адаптируя их под местные условия. Такой процесс вновь подчеркивает необходимость комплексного подхода к модернизации институтов: законодательно-ориентированные реформы должны идти бок о бок с технологическим развитием и обновлением компетенций персонала. Трансформация правовой базы будет эффективна только тогда, когда одновременно изменятся и методы, и инструменты контроля. В противном случае создается несбалансированная система, в которой формальные требования существуют, но их исполнение затруднено из-за отсутствия нужных ресурсов или несогласованности различных государственных структур.

Результаты и обсуждение

Среди наиболее актуальных технологий, способных повлиять на будущее государственного финансового контроля, выделяются блокчейн-платформы и смарт-контракты. Их использование потенциально упростит ведение бюджетного учета и сократит риск манипуляций с финансовыми данными, поскольку записи в распределенном реестре сложно подделать [Саркисян, Мамий, 2023]. Однако сам факт интеграции блокчейн-технологий в государственные системы вызывает множество вопросов, связанных как с техническими ограничениями, так и с правовыми аспектами. Необходим подробный анализ того, насколько оправдано применение распределенных реестров для сложных финансовых операций, обычно сопровождающихся многочисленными проверками и согласованиями. Кроме того, есть проблема масштабируемости, ведь блокчейн-платформы могут становиться менее эффективными при росте объема транзакций. При этом институциональные изменения, связанные с официальным признанием юридической силы смарт-контрактов, требуют существенной законодательной подготовки, особенно в области регулирования споров, возникающих при сбоях в смарт-контрактах. Государственный финансовый контроль, внедряющий подобные инновации, должен учитывать также и репутационные риски: одна крупная уязвимость или ошибка в распределенном реестре может поставить под сомнение всю концепцию прозрачности цифровых финансовых процессов. Для смягчения этих угроз может потребоваться создание

специализированных органов или подразделений, наделенных компетенциями по аудиту и мониторингу блокчейн-систем [Морозова, 2022]. Такой подход должен сочетаться с механизмами ответственности и страхования на случай непредвиденных технических или организационных сбоев. Таким образом, внедрение новых технологий становится катализатором институциональных изменений, затрагивающих не только технологическую, но и правовую, организационную и этическую плоскости.

Важнейшим направлением адаптации традиционных институтов к условиям цифровизации становится расширение международного сотрудничества, в том числе в сфере обмена информацией о методах и средствах контроля. Активное участие в глобальных сетях по кибербезопасности, а также в профильных экономических организациях дает государственным органам возможность учиться на опыте других стран и своевременно внедрять проверенные практики в свою деятельность [Кашина, Демидов , 2023]. Однако это сотрудничество может наталкиваться на проблемы политических разногласий и различий в уровнях экономического развития. Для того чтобы преодолеть эти препятствия, требуются многосторонние дипломатические усилия и заключение двусторонних и многосторонних соглашений, предполагающих унификацию технических протоколов и механизмов аудита. Институциональная структура государств должна включать в себя подразделения, специализирующиеся на координации международных проектов, поскольку в условиях глобальной цифровой среды устойчивость государственной финансовой системы немыслима без тесного взаимодействия с зарубежными партнерами. Нельзя исключить и активной роли частных компаний, которые могут предоставлять экспертные услуги и технологические решения по выявлению и пресечению киберугроз. При этом важно, чтобы государственные структуры обладали достаточным уровнем автономной компетенции и не становились полностью зависимыми от внешних подрядчиков, поскольку это может создать дополнительные риски утечки конфиденциальной информации. Стратегическое планирование, ориентированное на долгосрочные цели, выходит на первый план, когда речь заходит о распределении ролей и обязанностей между различными акторами в сфере государственного финансового контроля. Без четких институтов, способных обеспечивать взаимодействие на международном уровне, сами технологии не дадут устойчивых результатов и не смогут защитить общество от финансовых потерь или искаженных бюджетных решений.

Повышение уровня прозрачности и подотчетности в государственном финансовом контроле невозможно без системной антикоррупционной политики, особенно когда речь идет о внедрении высокотехнологичных решений. Дело в том, что цифровые платформы способны усиливать неравномерность доступа к информации, если при их разработке и внедрении не закладываются принципы открытости. При этом новые формы контроля предполагают не только усиление автоматического надзора, но и возможность общественного мониторинга в режиме реального времени [Кузнецов, 2020]. Однако реализация таких шагов требует четкого понимания того, какие именно данные могут и должны быть доступны широкой публике, а какие необходимо ограничивать в интересах национальной безопасности. Помимо технических аспектов, проблема антикоррупционной защиты связана с тем, что в цифровую эпоху схемы злоупотреблений часто становятся более изощренными, используя анонимные сети, поддельные цифровые идентификаторы и умелое маскирование транзакций в сложных структурах. Чтобы противостоять этому, государственные органы стремятся выработать комплекс мер, сочетающих в себе уголовно-правовое преследование, административное регулирование и организационные реформы в сфере контроля. Подобная многоуровневая

система может эффективно работать только при условии, что у нее есть институты, способные быстро реагировать на изменения в тактике злоумышленников [Норец, 2021]. Таким образом, антикоррупционная политика перестает быть уделом отдельных подразделений и становится частью глобальной стратегии цифровой трансформации государственного финансового контроля.

Задача обеспечения безопасности государственных финансовых операций усложняется тем, что в дело все активнее вступают внедренные алгоритмы искусственного интеллекта. Эти алгоритмы могут генерировать рекомендации по распределению бюджетных средств либо выявлять подозрительные транзакции, что резко повышает скорость и точность контроля. Но одновременное использование таких инструментов порождает вопросы о том, каковы потенциальные риски ошибочных решений, принимаемых алгоритмом, и каким образом можно проверить корректность его работы [Малышева, 2022]. При этом доступность огромных объемов данных делает методы машинного обучения более совершенными, но и открывает дорогу к новым киберугрозам, направленным на искажение данных, на которых обучаются модели. Институциональные реформы должны предусматривать механизмы прозрачности в отношении использования искусственного интеллекта, а также отчетность за последствия, вызванные решениями, которые алгоритм может инициировать. Еще один сложный момент – это защита персональных данных сотрудников и аудиторов, участвующих в контроле, ведь цифровые системы обычно собирают и обрабатывают информацию о том, кто, когда и какие действия выполнял. Если такие сведения попадут в руки злоумышленников, может возникнуть серьезный риск для личной безопасности людей и для целостности контрольных процедур. Государственные структуры, стремящиеся к эффективному применению искусственного интеллекта, сталкиваются с острым дефицитом высококвалифицированных IT-специалистов, которые способны не просто управлять новыми системами, но и обеспечивать их надежность. Институциональные изменения, таким образом, должны включать в себя и кадровую реформу, направленную на привлечение и удержание таких специалистов, а также на постоянное обновление компетенций уже работающих сотрудников. В конечном счете только комплексный подход позволит органам государственного финансового контроля сохранять актуальность и надежность в эпоху стремительной цифровизации.

Ключевым аспектом сохранения устойчивости государственного финансового контроля остается интеграция моделей риск-менеджмента во все стадии бюджетного цикла и аудиторских процедур. Традиционно риск-ориентированный подход применялся в коммерческом секторе и заключался в оценке вероятных финансовых потерь, связанных с конкретными операциями. В контексте государственных финансов добавляется необходимость учета политических факторов, социального эффекта и стратегических задач развития [Норец, 2021]. Концепция риск-менеджмента становится особенно востребованной, когда речь идет о киберугрозах, которые могут появляться внезапно и менять свою конфигурацию под влиянием внешних обстоятельств. Переход от обычной реактивной системы контроля к проактивному управлению рисками требует реформирования методологических основ и расширения технических возможностей по мониторингу. Органы контроля начинают разрабатывать сценарные режимы, в которых оценивают разные варианты кибератак и коррупционных схем, чтобы заранее выработать меры реагирования. Такой подход, по сути, меняет институциональную культуру: вместо ожидания проверок и штрафов возникает постоянная готовность к обновлению регламентов и инструкций, основанная на анализе актуальных угроз. Направленность на прогнозирование киберрисков помогает не только снижать финансовые потери, но и укреплять

доверие общественности к государственным структурам, поскольку реагирование на потенциальные проблемы демонстрирует ответственность и дальновидность. При этом внедрение систем риск-менеджмента не может быть простым копированием коммерческих практик: оно требует детализации с учетом специфики государственных функций, особого правового статуса и многообразия бюджетных программ. В итоге формируется новая ветвь внутри государственного финансового контроля, специализирующаяся на анализе и управлении рисками, которая должна быть наделена особыми полномочиями и тесно взаимодействовать с другими структурными элементами системы контроляПереключаясь к экономической составляющей цифровой трансформации, следует подчеркнуть растущую роль прослеживаемости финансовых транзакций как одного из критериев эффективности контроля. В условиях, когда платежи становятся моментальными и проходят через множество цифровых платформ, органы, ответственные за государственный финансовый контроль, фокусируются на создании систем, позволяющих в режиме реального времени отслеживать путь бюджетных средств от момента их выделения до конечного получателя [Решетникова, Глушенко, 2020]. Такая прослеживаемость помогает выявлять случаи нецелевого использования, мошенничества и коррупции на самых ранних этапах, повышая шансы на возврат утраченных средств и привлечения виновных к ответственности. Однако, чтобы подобная система функционировала, необходимы институциональные условия, включающие правовые и технические стандарты обмена данными между разными ведомствами и финансовыми институтами. Возникает потребность в надежной цифровой инфраструктуре, способной обрабатывать огромные потоки транзакций и предотвращать несанкционированный доступ к банковским и бюджетным базам. Важно также учитывать, что чрезмерная прозрачность может вступать в конфликт с нормами о конфиденциальности и защите персональных данных. Государственные структуры на фоне цифровой трансформации оказываются на перекрестке требований публичной отчетности и приватности, пытаясь найти баланс, приемлемый для всех заинтересованных сторон. В результате в рамках государственного финансового контроля формируются специальные подразделения или группы, которые занимаются анализом транзакций, обеспечением соответствия сложившимся нормам защиты данных и применением технологий шифрования. Все это приводит к существенным изменениям в институциональной архитектуре, которая должна быть динамичной и гибкой, чтобы успевать за развитием цифровой экономики и киберугроз.

Основная проблема, с которой сталкиваются ведомства, заключается в том, что цифровая трансформация идет намного быстрее, чем процесс внесения изменений в законодательство и организационные правила. Органы государственного финансового контроля вынуждены действовать на грани устаревших регламентов, которые не всегда адаптированы к новым технологическим реалиям [Васянина, 2022]. Эта диспозиция порождает риски правовой неопределенности, злоупотреблений и торможения инноваций. Институциональные изменения должны исходить из понимания того, что власть в цифровую эпоху не столько контролирует технологии, сколько вынуждена к ним приспосабливаться. При этом успешная адаптация невозможна без опоры на ясную концепцию цифрового развития, в которой четко определено место и роль финансового контроля. Стратегические документы национального уровня, посвященные цифровизации, обычно содержат пункты о необходимости создания комплексной системы безопасности, однако они требуют конкретизации и воплощения в решениях разных уровней управления [Матафонова, 2021]. Институциональная перестройка может начинаться с формирования специальных комитетов или групп, которые бы координировали действия по

цифровизации, киберзащите и реформам в сфере бюджетного контроля. В их задачи входит не только техническое переоснащение, но и налаживание схем взаимодействия, согласование нормативных актов и проведение обучающих программ для сотрудников. Общий успех этих мер определяется тем, насколько они скоординированы между собой и поддерживаются политическим руководством. Если аналитические центры и профильные ведомства работают разрозненно, то часть инициатив может остаться на бумаге, а цифровая трансформация продолжится по стихийному сценарию, уязвимому для внешних атак и внутренних злоупотреблений.

С другой стороны, нельзя переоценивать исключительно технологическую компоненту. Иногда реформы, связанные с цифровизацией, также поднимают вопросы организационных структур: исчезают одни должности, появляются другие, а у некоторых служб существенно меняются функциональные обязанности [Зарицкая М.И., Куликова, 2018]. Эта эволюция кадров отметилась уже сейчас, когда повышается роль специалистов по кибербезопасности и анализу больших данных, тогда как традиционные ревизоры смещаются к более узким функциям ручной проверки редких специфических случаев. Кроме того, растет актуальность гибридной специализации, при которой сотрудник обладает знаниями не только в сфере государственного финансового контроля, но и в IT-сфере. Такой подход снижает риск неправильной интерпретации данных, а также облегчает передачу информации и ответственности внутри государственного аппарата. Естественно, что столь серьезные организационно-кадровые реформы наталкиваются на сопротивление, ведь любая бюрократическая система инертна и не любит перемен. Следовательно, институциональные изменения должны сопровождаться стимулирующими мерами, в том числе обновленной системой мотивации труда, карьерными лифтами и программами переподготовки. Отдельный блок вопросов касается этических норм и прозрачности приема на работу: в условиях, когда государство заботится о кибербезопасности, повышается риск чрезмерного контроля над персоналом. Все эти моменты еще раз иллюстрируют сложность цифровой трансформации, которая не ограничивается лишь новыми технологиями, но требует переосмысления всей системы ценностей и процедур в пространстве государственного контроля.

Современные средства аналитики, такие как инструменты бизнес-разведки, все активнее интегрируются в практику государственного контроля, предоставляя новые возможности для глубинного анализа, визуализации и прогнозирования финансовых потоков [Никифорова В.Д., Никифоров, 2019]. Эти инструменты прикладываются не только к большим массивам данных, но и к различным цифровым документам, отчетам, официальным письмам, создавая единое непрерывное поле для расследования потенциальных нарушений. В определенной мере механизм умной аналитики помогает приоритизировать проверки, концентрируясь на областях, где риск отклонений наиболее велик. Вместе с тем любая автоматизация процесса принятия решений влечет за собой вопросы о человеческом факторе и конечной ответственности. Государственные структуры должны сохранять компетентность и в ручном анализе, чтобы при необходимости проверять корректность результатов, которые выдают алгоритмы машинного обучения. Следовательно, вместо упрощения система становится более комплексной, ведь требует сочетания высокотехнологичных и традиционных методов [Горохова, 2023]. Рост компьютерной грамотности сотрудников контрольных органов становится обязательным условием, и эти компетенции должны закрепляться не только на уровне персональных навыков, но и институционально, через программы подготовки и сертификации. Такая двойственность – автоматизация и сохранение ручных экспертиз – формирует новую парадигму, где решения

принимаются коллективно человеком и машиной. Этот этап эволюции неизбежно отразится на правовом регулировании, ведь появятся новые требования к сохранению и проверке цифровых документов, а также к контролю над деятельностью алгоритмов искусственного интеллекта. Институциональные изменения в результате коснутся почти каждого уровня управления и приведут к необходимости дополнительного финансирования в долгосрочной перспективе.

Эффективность государственного финансового контроля в эпоху цифровых трансформаций выступает не только фактором экономической стабильности, но и условием социальной справедливости. Население, сталкиваясь с цифровыми услугами государственных органов, ожидает, что средства бюджета распределяются грамотно и без злоупотреблений. Если контроль оказывается неэффективным, у граждан формируется недоверие к государственным институтам, которое усиливается при каждом скандале, связанном с потерей данных или хищением средств [Морозова, 2022]. Поэтому обеспечение кибербезопасности и прозрачности — это не просто техническая задача; это элемент укрепления общественного договора. Институциональные реформы призваны обеспечить такой уровень взаимодействия и согласованности между ведомствами, чтобы цифровая трансформация сопровождалась минимизацией рисков. Важно, что в этот процесс могут активно вовлекаться и общественные организации, которые традиционно выполняют функцию контроля уличной движущей силой, сигнализируя о проблемах и инициируя публичную дискуссию. Наступает момент, когда подобная активность трансформируется благодаря цифровым платформам: граждане могут в реальном времени указывать на недостатки в использовании бюджетных денег, опираясь на открытые данные. Государственные институты, понимая это, должны настроиться на более прозрачное взаимодействие и быстроту реакции. Новый формат коммуникации неизбежно ведет к принципиально иной системе отчетности, где ключевую роль играет не столько формальная отчетность по стандартам, сколько качество взаимодействия в цифровом пространстве.

Вне всяких сомнений, инструменты кибербезопасности должны развиваться вместе с ростом систем анализа. Ведь чем более изощренными становятся инструменты контроля, тем большую ценность представляет их взлом для злоумышленников. Тенденция к усложнению кибератак требует постоянного обновления средств защиты: от межсетевых экранов до криптографических протоколов, от систем обнаружения вторжений до комплексных программ по обучению персонала [Кузнецов, 2020]. Меры информационной безопасности уже невозможно воспринимать как второстепенный процесс, который можно передать на аутсорсинг. Институциональные сдвиги предполагают, что каждая структура государственного финансового контроля будет иметь собственные подразделения или ответственных лиц за информационную безопасность, владеющих актуальными технологиями и контактами с компетентными органами. В этой плоскости становится востребованным комплексный аудит информационной инфраструктуры, включающий в себя оценку не только технических средств, но и организационных практик, связанных с обработкой и хранением данных. При этом процесс аудита нужно внедрять на постоянной основе, чтобы не допускать накопления уязвимостей и вовремя их устранять. Как итог, формируется новый формат надзорной деятельности, который считает кибербезопасность органичным элементом всего финансового контроля. Отдельные функции по защите информации уже не могут существовать в изоляции, поскольку цифровая среда объединяет все направления финансовых потоков и аудиторских процедур.

Следует подчеркнуть, что для современной системы государственного финансового контроля недостаточно концентрироваться только на внутренних ресурсах. Необходим широкий охват взаимодействия с частным сектором, который зачастую обладает более

продвинутыми технологическими решениями и экспертизой. Это касается и предприятий, специализирующихся в разработке систем кибербезопасности, и консалтинговых организаций, предлагающих решения по автоматизации контроля, и провайдеров ИТ-инфраструктуры [Кашина, Демидов , 2023]. Однако такое сотрудничество должно быть встроено в жесткие рамки защиты государственной тайны и бюджетной информации, поскольку утечки могут иметь катастрофические последствия. Интерес частных компаний в подобных взаимодействиях тоже понятен: государственный сектор является весьма крупным заказчиком, и успешная работа над его проектами гарантирует не только экономические выгоды, но и международную репутацию. Институциональные изменения в этом контексте предполагают четкое определение прав и обязанностей участников: как распределяется ответственность за возможные сбои или утечки, каким образом регулируются конфликты интересов, и на каких условиях привлекаются внешние специалисты. С одной стороны, гибкая модель партнерства позволит государству быстро внедрять инновации, дополнительное финансирование и разработки. С другой стороны, без четкой регламентации повышается вероятность коррупционных сделок, связанных с госзакупками и тендерами на поставку программного обеспечения. Поэтому государственным органам важно сохранять прозрачность и конкурентность в этой сфере, публикуя документы о расходах и результатах контрольных мероприятий там, где это не нарушает вопросы национальной безопасности [Шичанин, 2021]. Если удастся выстроить сбалансированную схему взаимодействия, то синергия госорганов и частного сектора окажется одним из главных драйверов цифровой трансформации финансового контроля.

Нельзя забывать и об уровне муниципального управления, где также происходят важные процессы распределения и использования бюджетных средств. Часто именно на местном уровне цифровизация отстает сильнее всего, что создает диспропорцию в общей системе контроля. Такая неоднородность затрудняет комплексный анализ, так как данные с мест могут быть представлены в несовместимых форматах или с большими задержками. Государственные финансовые органы должны разрабатывать стратегии, которые обеспечат единый стандарт цифровой инфраструктуры по всей вертикали управления, либо же создать механизмы интеграции разнородных систем [Малышева, 2022]. Институциональные изменения, нацеленные на преодоление разброса в технологическом оснащении, предполагают изменение финансирования, оптимизацию процедур закупок ИТ-решений и подготовку персонала на местах. При этом необходимо учитывать, что муниципальные бюджеты зачастую ограничены, поэтому государственный центр может предлагать субсидии или специальные гранты на модернизацию контрольных функций в регионах. Особого внимания требует формирование компетенций: без обученных кадров, способных использовать цифровые инструменты, любая приобретенная техника или программное обеспечение не принесут желаемого эффекта. В конечном счете все элементы системы — от местного уровня до федеральных органов – должны быть связаны в единую архитектуру, обеспечивающую непрерывную и безопасную обработку данных о финансовых потоках.

Существенной новацией последнего времени можно считать разработку электронных систем отчетности, которые автоматически формируют аналитические материалы на основе поступающей информация [Пумбрасова Н.В., Бессчетнова, 2020]. Такие системы позволяют существенно разгрузить аудиторов от рутинной работы, одновременно повышая скорость выявления нарушений. Однако их эффективность во многом зависит от корректности исходных данных, а также от алгоритмов, заложенных в систему. Если базовые правила и нормы, прописанные в программном коде, будут некорректными или устаревшими, результат может вводить в заблуждение и формировать иллюзию контроля. Поэтому новая институциональная

парадигма государственного финансового контроля став во главу угла постоянную валидацию внедренных решений, возможность их обновления и интеграцию с другими системами. Интересно, что столь плотное взаимодействие между технологиями и нормативной базой вынуждает разработчиков тесно сотрудничать с юристами, экспертами по аудиту и представителями высших органов финансового надзора, чтобы программный продукт отражал изменения законодательства и практики. Киберугрозы, в свою очередь, тоже фокусируются на этих новейших системах, анализируя возможность введения в программу ложных данных, манипулирования правами доступа или дестабилизации работы всей сети [Никифорова Никифоров, 2019]. Перед лицом таких рисков государственные структуры приходят к идее многоступенчатой защиты, где проверка информации осуществляется на нескольких уровнях, включая в том числе ручные методы сверки. Это может казаться шагом назад в сторону бюрократии, но на деле обеспечивает более высокую надежность на случай, если один из сегментов будет скомпрометирован.

На пересечении госуправления, технологий и финансов все более востребованными становятся новые формы публичных слушаний, когда результаты контроля и планы по цифровой трансформации обсуждаются с заинтересованными сторонами. Цель подобных обсуждений – выявить болевые точки и получить предложения о том, какие меры могут усилить кибербезопасность и прозрачность финансовых операций [Саркисян, Мамий, 2023]. В условиях, когда граждане становятся активными в цифровом пространстве, подобная обратная связь может поступать как через официальные каналы, так и через публичные платформы, социальные сети и краудсорсинг-проекты. Институциональная настройка на участие граждан и организаций гражданского общества означает, что государство не просто внедряет технологии “сверху”, но и учитывает, как они влияют на общество и какие корректировки требуются. Для этого могут создаваться экспертно-консультационные советы, куда приглашаются представители различных социальных групп, бизнеса, академического сообщества [Шичанин, 2021]. Результаты таких открытых дискуссий зачастую склоняют к изменению планов внедрения, перераспределению приоритетов и уточнению нормативных актов. В то же время сам факт публичного обсуждения повышает общий уровень прозрачности и доверия, что крайне важно для институтов государственного контроля. Ведь если граждане не понимают или не принимают логику цифровых реформ, они могут саботировать их внедрение, создавая дополнительную напряженность и препятствия на пути модернизации.

Заключение

Для полноценного функционирования системы государственного финансового контроля в условиях цифровизации важно также наличие эффективной судебной ветви, способной быстро и качественно разбирать споры, возникающие при подозрениях на нарушения или кибератаки. Судебные органы должны располагать необходимыми компетенциями в области информационных технологий, чтобы объективно оценивать представленные доказательства и формулировать решения, основанные на технических аспектах [Матафонова, 2021]. В ряде стран уже создаются специальные судебные палаты или суды, специализирующиеся на цифровых спорах, однако в масштабном смысле практика еще не устоялась. Это порождает правовую неопределенность и необходимость частых консультаций с техническими экспертами, что может затягивать процесс рассмотрения дел. Институциональные изменения, призванные укрепить судебную поддержку для цифрового финансового контроля, включают дополнительные программы обучения судей и создание форматов взаимодействия судов с

аудиторскими и надзорными органами. Если государственная система правосудия не будет успевать за темпами цифровизации, тогда даже самые совершенные методы контроля окажутся недостаточно эффективными, поскольку не будут подкреплены правовыми решениями.

Наконец, переход к комплексной цифровой модели государственного финансового контроля не обходится без ресурсов, необходимых для финансирования этого мира инноваций. В эпоху, когда бюджеты многих стран испытывают ограничения, важно расставлять приоритеты и обеспечивать, чтобы цифровизация не проводилась за счет сокращения важнейших общественных программ. Ответственным шагом будет разработка детализированных финансовых планов, где отражена стоимость внедрения конкретных технологий, обучения персонала, обеспечения кибербезопасности и поддержания систем в актуальном состоянии. Также необходимо учитывать траты на постоянное обновление инфраструктуры, поскольку любая технологическая система имеет ограниченный жизненный цикл. При ограниченных ресурсах государственные органы могут обращаться к механизмам государственно-частного партнерства, грантам, международной технической помощи. Но во всех случаях требуется четкая отчетность и прозрачность распределения этих средств, чтобы не возникало новых поводов для коррупции. В итоге вопрос финансирования становится частью широкой стратегической дискуссии о том, какую роль играет цифровая трансформация в долгосрочном развитии страны, и как государственный финансовый контроль может способствовать устойчивому экономическому росту и социальной стабильности.

Таким образом, институциональное обновление в сфере государственного финансового контроля должно охватывать все ключевые элементы управления: правовые нормы, организационную структуру, профессиональную подготовку кадров, взаимодействие с бизнесом и гражданским обществом, а также механизмы финансирования технологических инноваций [Васянина, 2022]. Без согласованного развития всех этих направлений риск фрагментарности и неэффективности будет только возрастать, учитывая всю растущую сложность современного киберпространства. Государствам необходимо не только следовать лучшим мировым практикам, но и создавать собственные уникальные решения, учитывающие специфику политических, экономических и социальных условий. В эпоху, когда мобильность и распределенность финансовых потоков становятся нормой, а киберугрозы появляются в самых неожиданных формах, институты контроля не могут оставаться статичными. И хотя процесс реформ часто сталкивается с бюрократическими барьерами и сопротивлением, ставка на цифровые решения и системные изменения уже показывает свою эффективность в отдельных проектах и инициативных группах ведомств. Постепенно формируется понимание, что цифровая трансформация государственного финансового контроля – это не одномоментное явление, а постоянный процесс, требующий регулярной корректировки и пересмотра приоритетов. Эту динамику нужно воспринимать как естественную составляющую развития государственных институтов, если они хотят оставаться релевантными и обеспечивать полноценную защиту финансовых интересов общества и государства.

Библиография

1. Васянина Е.Л. Цифровая трансформация государственного финансового контроля: проблемы, перспективы развития // Актуальные проблемы административного и административно-процессуального права (Сорокинские чтения): сборник статей. СПб., 2022. С. 46-52.
2. Горохова Д.В. Цифровизация государственного финансового контроля // Государственный контроль в финансово-бюджетной сфере: Коллективная монография. Москва, 2023. С. 490-496.
3. Зарицкая М.И., Куликова А.Э. Государственный финансовый контроль в цифровой экономике: вызовы и риски

// Перспективы финансовой деятельности современных компаний в цифре: коллективная монография молодых исследователей Финансового университета при Правительстве РФ. М., 2018. С. 50-61.
4. Кашина М.А., Демидов М.О. Реформа государственного институционального контроля в условиях цифровизации: китайский способ повышения доверия в обществе // Реформа как инструмент государственного управления: Коллективная монография. Санкт-Петербург, 2023. С. 269-288.
5. Кузнецов Н.В. Исследование влияния современных цифровых технологий на институциональное развитие финансового рынка и системный анализ последствий цифровизации финансового рынка // НИР: грант № 20-010-00346. Российский фонд фундаментальных исследований. 2020.
6. Малышева В.А. Государственный финансовый контроль в условиях цифровой экономики // Наука Юга России: достижения и перспективы: Тезисы докладов. Ростов-на-Дону, 2022. С. 136.
7. Матафонова И.В. Роль финансового контроля в развитии экономики // Россия и регионы мира: воплощение идей и экономика возможностей: Материалы XI Евразийского экономического форума молодежи. Екатеринбург, 2021. С. 260.
8. Морозова С.С. Электронное правительство в условиях цифровых трансформаций: проблемы функционирования и перспективы развития // Политическое в условиях цифровых трансформаций: Материалы конференции. М., 2022. С. 329-337.
9. Никифорова В.Д., Никифоров А.А. Институциональная трансформация социально-экономической системы под влиянием процессов цифровизации // Технологическая перспектива в рамках Евразийского пространства: новые рынки и точки экономического роста: труды 5-ой Международной научной конференции. 2019. С. 22-27.
10. Норец Н.К. Обеспечение безопасности цифровой трансформации финансовых продуктов // Региональные аспекты экономической безопасности: Сборник материалов. Уфа, 2021. С. 13-16.
11. Норец Н.К. Риски и безопасность цифровой трансформации финансовых услуг // Возможности и угрозы цифрового общества: Материалы Всероссийской научно-практической конференции. Ярославль, 2021. С. 206-209.
12. Пумбрасова Н.В., Бессчетнова Ю.Д. Государственный финансовый контроль в условиях цифровизации экономики // Учетно-аналитические инструменты развития цифровой экономики: Сборник статей. 2020. С. 87-90.
13. Решетникова Н.Н., Глушенко С.А. Влияние цифровых финансовых технологий на глобальную и национальную финансовую безопасность // Финансово-экономическая безопасность Российской Федерации и ее регионов: Сборник материалов конференции. 2020. С. 52-54.
14. Саркисян М.А., Мамий Е.А. Развитие цифровизации финансовых институтов России в современных условиях // Галактика науки 2023: Сборник статей. Краснодар, 2023. С. 86-93.
15. Шичанин М.А. Трансформация публичных финансов в эпоху цифровизации (на примере публичного финансового контроля) // Традиции и новации в системе современного российского права: Материалы XX Международной конференции молодых ученых. М., 2021. С. 363-365.

Institutional changes in state financial control in the era of digital transformations and cyber threats

Irina N. Medik

PhD in Economic,
Associate Professor,
Department of world economy and economic security,
664003, 11 Lenina str., Irkutsk, Russian Federation;
e-mail: m.irina.n@list.ru

Abstract

The aim of the research is to analyze the institutional changes in the system of state financial control in the context of digital transformation and growing cyber threats. The paper describes the modern challenges associated with the accelerated integration of digital technologies and changes in the global economic environment, which require a revision of existing mechanisms of control and

oversight of financial flows. Key issues identified include the obsolescence of traditional control methods, inadequate personnel training, and the lack of coordination among various state structures responsible for the security of the financial system. The research methods are based on an interdisciplinary approach that includes comparative analysis, a systematic approach, and the modeling of scenarios for the development of financial control in the digital environment. The work analyzes both national and international practices, and examines legislative initiatives aimed at strengthening the protection of information systems and adapting monitoring mechanisms to new realities. Special attention is given to the analysis of threats related to cybersecurity and the assessment of their impact on the effectiveness of control bodies. The study's results demonstrate that the modernization of state financial control requires the integration of information technologies, the development of new regulatory legal acts, and the formation of institutional mechanisms capable of providing rapid response to the challenges of the digital era. The practical significance of the findings lies in the possibility of using the developed recommendations to improve financial control, enhance the transparency of budgetary processes, and strengthen the counteraction to cyber threats. The work also proposes a structure for interaction between state authorities, the scientific community, and the private sector, which will help to increase the reliability and resilience of the financial system. The discussion of the obtained data revealed the necessity for continuous monitoring of technological and cybernetic changes, as well as for the development of professional training for specialists in the field of information security. The authors conclude that the success of reforms in this area largely depends on the prompt adaptation of institutional practices and the implementation of innovative technologies that contribute to protecting the financial interests of the state and society. Thus, the presented results contribute to the development of both the theoretical foundations and the practical aspects of institutional transformations in state financial control in the era of digital transformations and cyber threats.

For citation

Medik I.N. (2025) Institutsional'nye izmeneniya v gosudarstvennom finansovom kontrole v epokhu tsifrovykh transformatsii i kiberugroz [Institutional changes in state financial control in the era of digital transformations and cyber threats]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 15 (3A), pp. 468-482.

Keywords

Institutional changes, state control, financial control, digital transformations, cyber threats.

References

1. Gorokhova D.V. (2023) Tsifrovizatsiya gosudarstvennogo finansovogo kontrolya [Digitalization of state financial control]. Gosudarstvennyi kontrol' v finansovo-byudzhetnoi sfere: Kollektivnaya monografiya [State control in the financial and budgetary sphere: Collective monograph]. Moscow, pp. 490-496.
2. Kashina M.A., Demidov M.O. (2023) Reforma gosudarstvennogo institutsional'nogo kontrolya v usloviyakh tsifrovizatsii: kitaiskii sposob povysheniya doveriya v obshchestve [Reform of state institutional control in the context of digitalization: the Chinese way to increase trust in society]. Reforma kak instrument gosudarstvennogo upravleniya: Kollektivnaya monografiya [Reform as a tool of public administration: Collective monograph]. Saint Petersburg, pp. 269-288.
3. Kuznetsov N.V. (2020) *Issledovanie vliyaniya sovremennykh tsifrovykh tekhnologii na institutsional'noe razvitie finansovogo rynka i sistemnyi analiz posledstvii tsifrovizatsii finansovogo rynka: NIR: grant № 20-010-00346* [Study of the impact of modern digital technologies on the institutional development of the financial market and system analysis of the consequences of financial market digitalization: research work: grant No. 20-010-00346]. *Rossiiskii fond fundamental'nykh issledovanii* [Russian Foundation for Basic Research].

4. Malysheva V.A. (2022) Gosudarstvennyi finansovyi kontrol' v usloviyakh tsifrovoi ekonomiki [State financial control in the digital economy]. Nauka Yuga Rossii: dostizheniya i perspektivy: Tezisy dokladov [Science of the South of Russia: achievements and prospects: Abstracts of reports]. Rostov-on-Don, p. 136.
5. Matafonova I.V. (2021) Rol' finansovogo kontrolya v razvitii ekonomiki [The role of financial control in economic development]. Rossiya i regiony mira: voploshchenie idei i ekonomika vozmozhnostei: Materialy XI Evraziiskogo ekonomicheskogo foruma molodezhi [Russia and regions of the world: implementation of ideas and economy of opportunities: Proceedings of the XI Eurasian Economic Youth Forum]. Ekaterinburg.
6. Morets N.K. (2021) Obespechenie bezopasnosti tsifrovoi transformatsii finansovykh produktov [Ensuring the security of digital transformation of financial products]. Regional'nye aspekty ekonomicheskoi bezopasnosti: Sbornik materialov [Regional aspects of economic security: Collection of materials]. Ufa, pp. 13-16.
7. Morets N.K. (2021) Risk i bezopasnost' tsifrovoi transformatsii finansovykh uslug [Risks and security of digital transformation of financial services]. Vozmozhnosti i ugrozy tsifrovogo obshchestva: Materialy Vserossiiskoi nauchno-prakticheskoi konferentsii [Opportunities and threats of the digital society: Proceedings of the All-Russian scientific-practical conference]. Yaroslavl, pp. 206-209.
8. Morozova S.S. (2022) Elektronnoe pravitel'stvo v usloviyakh tsifrovykh transformatsii: problemy funktsionirovaniya i perspektivy razvitiya [E-government in the context of digital transformations: problems of functioning and development prospects]. Politicheskoe v usloviyakh tsifrovykh transformatsii: Materialy konferentsii [Political in the context of digital transformations: Conference proceedings]. Moscow, pp. 329-337.
9. Nikiforova V.D., Nikiforov A.A. (2019) Institutsional'naya transformatsiya sotsial'no-ekonomicheskoi sistemy pod vliyaniem protsessov tsifrovizatsii [Institutional transformation of the socio-economic system under the influence of digitalization processes]. *Tekhnologicheskaya perspektiva v ramkakh Evraziiskogo prostranstva: novye rynki i tochki ekonomicheskogo rosta: trudy 5-oi Mezhdunarodnoi nauchnoi konferentsii* [Technological perspective in the Eurasian space: new markets and points of economic growth: proceedings of the 5th International scientific conference], pp. 22-27.
10. Pumbrasova N.V., Besschetnova Yu.D. (2020) Gosudarstvennyi finansovyi kontrol' v usloviyakh tsifrovizatsii ekonomiki [State financial control in the context of digitalization of the economy]. Uchetno-analiticheskie instrumenty razvitiya tsifrovoi ekonomiki: Sbornik statei [Accounting and analytical tools for the development of the digital economy: Collection of articles], pp. 87-90.
11. Reshetnikova N.N., Glushenko S.A. (2020) Vliyanie tsifrovykh finansovykh tekhnologii na global'nuyu i natsional'nuyu finansovuyu bezopasnost' [Impact of digital financial technologies on global and national financial security]. Finansovo-ekonomicheskaya bezopasnost' Rossiiskoi Federatsii i ee regionov: Sbornik materialov konferentsii [Financial and economic security of the Russian Federation and its regions: Conference proceedings], pp. 52-54.
12. Sarkisyan M.A., Mamiy E.A. (2023) Razvitie tsifrovizatsii finansovykh institutov Rossii v sovremennykh usloviyakh [Development of digitalization of Russian financial institutions in modern conditions]. Galaktika nauki 2023: Sbornik statei [Galaxy of Science 2023: Collection of articles]. Krasnodar, pp. 86-93.
13. Shichanin M.A. (2021) Transformatsiya publichnykh finansov v epokhu tsifrovizatsii (na primere publichnogo finansovogo kontrolya) [Transformation of public finance in the era of digitalization (on the example of public financial control)]. Traditsii i novatsii v sisteme sovremennogo rossiiskogo prava: Materialy XX Mezhdunarodnoi konferentsii molodykh uchenykh [Traditions and innovations in the system of modern Russian law: Proceedings of the XX International conference of young scientists]. Moscow, pp. 363-365.
14. Vasianina E.L. (2022) Tsifrovaya transformatsiya gosudarstvennogo finansovogo kontrolya: problemy, perspektivy razvitiya [Digital transformation of state financial control: problems, development prospects]. Aktual'nye problemy administrativnogo i administrativno-protsessual'nogo prava (Sorokinskie chteniya): sbornik statei [Topical issues of administrative and administrative procedural law (Sorokin readings): collection of articles]. Saint Petersburg, pp. 46-52.
15. Zaritskaya M.I., Kulikova A.E. (2018) Gosudarstvennyi finansovyi kontrol' v tsifrovoi ekonomike: vyzovy i riski [State financial control in the digital economy: challenges and risks]. Perspektivy finansovoi deyatel'nosti sovremennykh kompanii v tsifre: kollektivnaya monografiya molodykh issledovatelei Finansovogo universiteta pri Pravitel'stve RF [Prospects for financial activities of modern companies in the digital sphere: collective monograph by young researchers of the Financial University under the Government of the Russian Federation]. Moscow, pp. 50-61.