МРНТИ 06.39.27; 06.39.31 DOI:https://doi.org/10.55871/2072-9847-2025-69-4-116-128

Шакирова Н.А.*
Магистр IT
АО «Центр электронных финансов»
Астана, Республика Казахстан
E-mail: dyomindom@gmail.com

Сыздыкова А.С.
АО «Центр электронных финансов»
Астана, Республика Казахстан
E-mail: anelya2391@gmail.com

Рахметов Н.Ж.
ТОО «Центр исследований, анализа и оценки эффективности»
Астана, Республика Казахстан
E-mail: nurlybek.r@gmail.com

Бокаев Б.Н.
PhD, исследователь
Сиракузский Университет
Школа гражданства и связей с общественностью Максвелла, США
e-mail: b.bokayev@syr.edu
ORCID: 0000-0002-1037-7085

МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ПРОВЕДЕНИЯ IT АУДИТА И ОЦЕНКИ ЭФФЕКТИВНОСТИ ДЕЯТЕЛЬНОСТИ ГОСУДАРСТВЕННЫХ ОРГАНОВ ПО ПРИМЕНЕНИЮ ИКТ В РЕСПУБЛИКЕ КАЗАХСТАН

Аннотация. В статье представлены результаты комплексной исследовательской работы, направленной на изучение методологических, нормативных и практических аспектов внедрения ИТ-аудита в системе государственного управления Республики Казахстан. Исследование охватывает анализ существующих подходов к оценке эффективности применения информационно-коммуникационных технологий (ИКТ) в государственных органах и их соотношение с актуальными международными стандартами аудита ISSAI 5300, COBIT 2019 и ISO/IEC 27001. На основе проведенного сравнительного анализа национальной практики государственного аудита и зарубежных подходов, применяемых в Высших органах аудита (ВОА) других стран, разработана обновленная комплексная методика проведения ИТ-аудита. Предложенная методика включает инструменты оценки цифровой зрелости государственных учреждений, анализ результативности и эффективности ИТ-процессов, а также интеграцию мер по управлению информационными рисками. Методологической основой совершенствования методики является трехуровневая интеграция: объединение международных стандартов ISSAI 5300, COBIT 2019 и ISO/IEC 27001 с национальными нормативными требованиями; внедрение комбинированной модели оценки цифровой зрелости, адаптированной к казахстанским реалиям; применение системы количественных показателей и качественных индикаторов результативности ИТ-процессов. Усовершенствованная методика обеспечивает интеграцию количественных показателей эффективности, риск-ориентированного анализа инфраструктуры ИКТ и принципов управляемости информационных технологий в государственных органах.
Реализация предложенных методологических подходов и инструментов позволит государственным органам Республики Казахстан и аудиторским органам: повысить прозрачность и объективность оценки состояния цифровой трансформации; улучшить качество и обоснованность аудиторских заключений и рекомендаций; обеспечить эффективность процессов внедрения ИКТ и рациональное использование ИТ-ресурсов; снизить информационные риски и повысить уровень информационной безопасности.
Ключевые слова: IT-аудит, информационная безопасность, ISSAI 5300, COBIT 2019, ISO 27001, государственный аудит, эффективность ИКТ

ВВЕДЕНИЕ

В условиях четвертой промышленной революции государственный сектор зарубежных стран активно внедряет инновационные информационные технологии и цифровые сервисы. По данным Организации экономического сотрудничества и развития (ОЭСР) и Организации Объединенных Наций, доля государственных расходов на ИКТ достигает 3-5% от общего бюджета развитых стран [1]. Однако исследования, проведенные консалтинговой

компанией McKinsey, свидетельствуют о том, что 40-60% крупных ИТ-проектов в государственном секторе либо превышают первоначальную смету, либо не достигают запланированных целей [2].

Провал государственных ИТ-проектов обусловлен комплексом взаимосвязанных факторов: недостаточной проработкой планов и размыванием масштаба проектов, приводящими к неконтролируемому расширению объема работ; слабым взаимодействием с заинтересованными сторонами; неадекватным управлением рисками и дефицитом квалифицированных кадров; технологическим устареванием решений вследствие недостаточной адаптивности к изменяющимся условиям. Это обуславливает необходимость внедрения системных методик ИТ-аудита, которые позволили бы выявлять подобные риски на ранних этапах реализации проектов и разрабатывать адекватные корректирующие меры.

Традиционный государственный аудит, исторически ориентированный на проверку финансовых и хозяйственных операций, должен эволюционировать в направлении включения ИТ-аудита как отдельного и равноправного направления контрольной деятельности. Это требование отражено в документах Международной организации Высших органов аудита (ИНТОСАИ) и рекомендациях ОЭСР по развитию государственного аудита в цифровую эпоху [3]. Ведущие аудиторские организации мира уже применяют консультативный подход в ИТ-аудите, включающий разработку рекомендаций по оптимизации ИТ-процессов.

Разработка и внедрение научно обоснованной методики ИТ-аудита в Республике Казахстан является актуальной задачей, продиктованной глобальной цифровизацией государственного управления, необходимостью повысить эффективность инвестиций в ИТ и усилить защиту информации в госсекторе. На фоне исполнения Указа Президента №954 [4] и выявленных Высшей аудиторской палатой проблем цифровой политики [5] требуется единая методика оценки эффективности применения ИКТ в государственных органах, интегрированная с международными требованиями информационной безопасности (ISO/IEC 27001:2022) [6] для обеспечения прозрачности, сопоставимости и устойчивости цифровых преобразований.

Решение этой задачи будет способствовать повышению качества государственных услуг, укреплению доверия граждан к государственным учреждениям и ускорению процесса цифровой трансформации Казахстана на пути к становлению эффективного цифрового государства.

В 2025 году «Центром исследований, анализа и оценки эффективности» была проведена комплексная исследовательская работа по теме осуществления ИТ-аудита и оценки эффективности применения ИКТ в государственных органах Республики Казахстан [7]. В ходе этого исследования был проведен детальный анализ национальной практики государственного аудита, изучены международные подходы, применяемые в Высших органах аудита развитых стран, и исследовано соответствие казахстанских норм требованиям международных стандартов ISSAI 5300, COBIT 2019 и ISO/IEC 27001. Результаты этой работы послужили основой для разработки обновленной, комплексной методики ИТ-аудита, которая органически интегрирует лучшие международные практики с требованиями и спецификой казахстанской системы государственного аудита.

Настоящая статья посвящена представлению и научному обоснованию этой разработанной методики, а также демонстрации ее практического применения.

Целью статьи является представление и научное обоснование комплексной методики проведения ИТ-аудита, разработанной на основе интеграции международных стандартов (ISSAI 5300, COBIT 2019, ISO/IEC 27001) с национальными нормативными требованиями и спецификой государственного управления Республики Казахстан. В статье изложены теоретические основы, методологические подходы и практические инструменты, позволяющие трансформировать ИТ-аудит из традиционной функции контроля в механизм совер-

шенствования государственного управления и оптимизации использования информационно-технологических ресурсов.

Научная новизна работы заключается в том, что предложен комплексный подход к оценке эффективности ИКТ, включающий синтез риск-ориентированного анализа, принципов управляемости ИТ и мониторинга корректирующих мер, который превращает IT-аудит из инструмента контроля в механизм совершенствования государственного управления. Разработан набор количественных и качественных индикаторов, отражающих специфику применения ИКТ в казахстанской системе государственного управления и обеспечивающих сопоставимость результатов аудита между государственными органами.

Практическая значимость проведенного исследования и изложенных в статье результатов определяется следующим. Во-первых, непосредственное внедрение предложенной методики в деятельность Высшей аудиторской палаты РК позволит провести качественно новый уровень оценки эффективности ИТ-процессов в государственных органах и оптимизировать использование ИТ-ресурсов. Во-вторых, методика обеспечивает повышение прозрачности цифровой трансформации в государственном секторе благодаря систематическому мониторингу цифровой зрелости и результативности ИТ-инвестиций. В-третьих, внедрение риск-ориентированной приоритизации при проведении аудита позволит снизить ИТ-риски и повысить информационную безопасность государственных учреждений. В-четвертых, методика обеспечивает рациональное использование государственных ресурсов посредством выявления неэффективных ИТ-процессов и разработки обоснованных рекомендаций по их совершенствованию.

ОСНОВНАЯ ЧАСТЬ

Обзор литературы

Muhammad Fauzan Hanif и др. (2025) рассматривают риск-ориентированный подход к приоритезации ресурсов с широким применением признанных фреймворков и стандартов – COBIT, ISO/IEC 27001, NIST Cybersecurity Framework, SOC и ISSAI 5300 для госсектора [8]. Аудит рассматривается как охватывающий профилактические, корректирующие элементы контроля по уровням управления, контроля приложений, инфраструктуры и данных. Современные тренды включают аудит облачных сервисов, автоматизацию и аналитическую обработку данных, непрерывный мониторинг и усиление кибербезопасности.

Также в работе Merhout J.W и Havelka D. (2008) IT-аудит трактуется как независимое исследование управленческих утверждений организации, которое следует набору руководящих принципов и стандартов, устанавливаемых внешними надзорными органами [9]. Авторы подчеркивают, что IT-аудит является неотъемлемой частью корпоративного управления. В рамках комплексной методики они выделяют восемь факторов, которые охватывают все заинтересованные стороны процесса: факторы аудиторской команды и факторы процесса и методики аудита, включая методологию, временные рамки и риск-ориентированный подход; факторы, контролируемые клиентом, такие как поддержка, кооперация и качество отношений; факторы, контролируемые самим IT-аудитом – опыт, управление и лидерство; факторы технической компетенции персонала; факторы социальных и межличностных навыков, в частности коммуникацию, независимость и мотивацию; факторы окружающей среды и организации; а также факторы целевого процесса или системы. Исследование также выявляет, что шесть из перечисленных факторов признаются критическими всеми участниками процесса: аудиторская методология, достаточное время, поддержка со стороны клиента и руководства, качество отношений, организационные изменения и четкое определение объема и целей аудита.

Далее исследование Ситнова А.А. и Бареевой Б.Р. (2020) представлено в контексте Казахстана через концепцию IT-аудита как проверки соответствия информационной системы бизнес-задачам компании [10]. Авторы определяют аудит как комплексное изучение, оценку и анализ текущего состояния IT-инфраструктуры предприятия с целью установления

соответствия средств и процессов поставленным бизнес-задачам. Предлагаемая четырехэтапная модель оптимизации IT включает сбор качественных и количественных показателей, выявление проблемных зон, разработку плана реорганизации и создание технического задания для развития инфраструктуры. По мнению авторов, IT-аудит целесообразен при нерегламентированных бизнес-процессах, слабой внутренней коммуникации, отсутствии стратегии развития информационных систем или при внедрении новых информационных систем для оценки их эффективности.

В работе Ситнова А.А. (2019) рассматривается риск-ориентированный подход к IT-аудиту, опирающийся на COBIT как базовый регулятор методологии [11]. Автор описывает модель анализа рисков, где критерии аудита формируются на основе оценки рисков: сначала оцениваются IT-ресурсы, необходимые для достижения бизнес-целей, затем анализируются уязвимости и угрозы, определяется степень риска по совокупности вероятности, уязвимости и потенциального ущерба, выбираются и оцениваются контрмеры, затем определяется остаточный риск и разрабатывается план внедрения адекватных механизмов управления. Особый акцент делается на управлении ожиданиями стейкхолдеров: важно точно определить участников и их требования, создать единое информационное поле, разбить проект на итерации и обеспечить регулярную обратную связь – ежедневные отчеты и недельные демонстрации. В условиях Казахстана ключевые риски чаще связаны не с техническими аспектами, а с расхождением ожиданий между бизнесом и IT-командами, пользователями и бизнес-партнерами.

В рамках анализа Казахстана важную роль играют исследования, посвященные внедрению и совершенствованию IT-аудита в стране. Туребекова В,О. и соавторы (2023) предлагают всесторонний обзор типов практического IT-аудита в государственном и коммерческом секторах Казахстана: экспресс-обследование, аудит бизнес-процессов, критерийальный аудит, комплексный многоцелевой аудит, операционный аудит, аудит размещения IT-ресурсов, аудит информационной безопасности, аудит управления IT, аудит IT-процессов и аудит законности использования IT [12]. При этом подчеркивается взаимодополнение COBIT и ITIL: COBIT – управленческий уровень, ITIL – операционные практики.

Рамазанова К.М. и Нургалиева А.М. (2023) продолжают тему влияния информационных технологий на эффективность внутреннего аудита и подчеркивают, что внедрение IT положительно коррелирует с уровнем эффективности, но практическая реализация часто отстает [13]. Они проводят SWOT-анализ дистанционного аудита, выявляя сильные стороны (доступ к данным, снижение командировочных расходов, увеличение скорости процедур), слабые стороны (зависимость от качества связи, коммуникационные проблемы, риски безопасности, вопросы доверия, затраты на внедрение), возможности (стандартизация процедур, цифровые базы данных, онлайн-сервисы, обработка данных в реальном времени) и угрозы (быстрое обновление технологий, зависимость от третьих лиц и киберриски, правовое регулирование). Выводы авторов сводятся к тому, что дистанционный аудит дополняет очный формат, но не может полностью заменить его, и его успешное внедрение требует инвестиций в кадровый потенциал. Также в данной работе отмечается роль государственной программы «Цифровой Казахстан» в контексте государственной цифровизации как стратегической основы развития IT-аудита. Авторы подчеркивают, что программа формирует предпосылки для трансформации аудита в государственном управлении. В то же время отмечается низкая зрелость бизнес-процессов и дефицит квалифицированных экспертов, что требует инвестиций в человеческий капитал, адаптации международных стандартов и разработки мер по развитию компетенций для успешной реализации цифровых инициатив и интеграции IT-аудита в государственные процессы.

В работе «Core Concepts Information Technology Auditing» (2025) формулируются фундаментальные принципы и современные тренды IT-аудита [14]. В рамках этого источника подчеркивается систематический характер изучения информационных систем для обеспе-

чения их целостности, конфиденциальности и доступности, соответствия регуляциям и выявления уязвимостей с последующим предоставлением рекомендаций.

Стандарты серии ISSAI 5100, 5300 устанавливают требования к проведению ИТ-аудита в государственном секторе, включая принципы оценки управления информационными технологиями, анализ информационной безопасности и оценку эффективности ИТ-инвестиций [15,16].

В итоге обзор консолидирует ключевые направления: закрепление риск-ориентированного подхода и применения COBIT 2019 в государственном управлении Казахстана, интеграцию ITIL и ISO/ISMS в локальные методические решения, развитие кадрового потенциала и инфраструктуры для дистанционного аудита, а также учет стратегических рамок государственной программы «Цифровой Казахстан» как драйвера цифровой трансформации аудита.

Анализ современной литературы выявляет ряд важных пробелов, которые обосновывают актуальность настоящего исследования. Во-первых, несмотря на развитую практику ИТ-аудита в развитых странах, литература содержит ограниченное количество работ, посвященных специфике адаптации международных стандартов ИТ-аудита к условиям государственного управления в странах с переходной экономикой. Во-вторых, в международной и казахстанской литературе недостаточно исследован вопрос комплексной интеграции ISSAI 5300, COBIT 2019 и ISO/IEC 27001 в единую методику ИТ-аудита, учитывающую оценку цифровой зрелости и мониторинг корректирующих мер. В-третьих, в существующих подходах к ИТ-аудиту слабо разработаны механизмы трансформации ИТ-аудита из инструмента контроля в механизм совершенствования управления ИТ-ресурсами через консультативный подход. В-четвертых, отсутствуют специализированные исследования, посвященные разработке системы количественных и качественных индикаторов, отражающих специфику применения ИКТ в казахстанской системе государственного управления и обеспечивающих сопоставимость результатов аудита между государственными органами.

Указанные пробелы в научной и методической литературе обусловили необходимость проведения комплексного исследования, результаты которого позволили бы разработать адаптированную, практически применимую методику ИТ-аудита, соответствующую международным стандартам и специфике казахстанской системы государственного управления. Настоящая статья направлена на заполнение этих пробелов и представление комплексного решения для развития ИТ-аудита как отдельного и равноправного направления деятельности государственного аудита в Республике Казахстан.

МЕТОДОЛОГИЯ И МЕТОДЫ

В основе проведенного исследования лежит интегративный методологический подход, сочетающий нормативно-правовой анализ, сравнительный анализ международных стандартов и эмпирическую оценку практик ИТ-аудита в государственных органах Республики Казахстан. Методологическая рамка опирается на принципы ISSAI 5300 (этапность и доказательная база ИТ-аудита), на риск-ориентированную модель управления и зрелости процессов, предложенную в COBIT 2019, а также на требования к системе менеджмента информационной безопасности ISO/IEC 27001. Такое сочетание позволило сформировать трехуровневую методику оценки: соответствие нормативным требованиям, оценка цифровой зрелости процессов и анализ управления информационными рисками.

Эмпирическая часть исследования выполнена с использованием смешанных методов. Для выявления текущей практики и проблем внедрены методы документального анализа (регламенты, внутренние политики, отчеты аудита), экспертные интервью с представителями Высшей аудиторской палаты и ИТ-подразделений, а также сравнительный анализ зарубежных практик (кейсы Турции, США, Финляндии и др.). Для количественной оценки разработана шкала цифровой зрелости (0–5) с набором унифицированных показателей – наличия стратегии ИТ-управления, формализации процессов, уровня автоматизации, измеримости показателей и уровня информационной безопасности. Итоговые

выводы и рекомендации сформированы на основе синтеза качественных наблюдений и количественных индикаторов с учетом применимости в условиях национальной практики государственного управления.

РЕЗУЛЬТАТЫ И ДИСКУССИЯ

ИТ-аудит представляет собой независимую оценку эффективности, безопасности и зрелости управления информационными технологиями в государственных органах. В отличие от классического финансового аудита, ИТ-аудит фокусируется на анализе процессов управления ИТ, инфраструктуры, информационных систем, цифровых проектов и политики информационной безопасности.

Основные задачи ИТ-аудита включают:

- оценку эффективности использования ИТ-ресурсов;
- проверку уровня безопасности и устойчивости ИТ-инфраструктуры;
- анализ соответствия нормативным требованиям и международным стандартам;
- выявление рисков и уязвимостей в ИТ-среде;
- формирование рекомендаций по оптимизации ИТ-процессов и управлению ИТ-ресурсами.

Проведение ИТ-аудита обеспечивает три ключевых эффекта:

1. Управленческий – повышение обоснованности решений и качества цифрового управления;
2. Финансово-экономический – оптимизация расходов и повышение ROI от цифровизации;
3. Организационный – формирование системного подхода к управлению ИТ и распределению ответственности.

Анализ международного опыта показывает, что подходы к организации ИТ-аудита в различных странах различаются по степени институционализации, методологической базе и уровню интеграции с системами кибербезопасности, однако объединены общей тенденцией – усилением роли ИТ-аудита в обеспечении прозрачности и эффективности государственного управления.

В **Турции** ИТ-аудит выделен в самостоятельное направление в структуре Высшего органа аудита (Sayıştay) [17]. Здесь функционирует специализированный отдел, в котором работают сертифицированные аудиторы (в том числе CISA). Этот отдел отвечает за разработку методологий, проведение аудитов и поддержку других подразделений. Турция активно внедряет стандарты ISO 27001 и NIST, ориентируясь на международные практики и развивая национальную систему защиты данных и кибербезопасности.

В **США** ИТ-аудит осуществляет Департамент информационных технологий и кибербезопасности, а ключевую роль в обеспечении контроля играет Счетная палата США (GAO) [18]. Применяются стандарты и методологии NIST, FISMA, FITARA и SOC 2. Американская практика отличается системностью и комплексным охватом – от управления ИТ-инвестициями до оценки зрелости программ и обеспечения информационной безопасности. Аудиты GAO в последние годы выявили проблемы с применением Agile-метрик, недостаточной реализацией стратегий кибербезопасности, слабым контролем ИТ-портфелей и неэффективным использованием лицензий программного обеспечения.

В **Литве** отсутствует отдельный департамент ИТ-аудита; соответствующие функции интегрированы в работу других подразделений Национального аудиторского офиса [19]. Основное внимание уделяется соответствию стандартам ЕС, таким как ISO/IEC 27001 и NIST, а также взаимодействию с Европейским агентством по кибербезопасности (ENISA). Литва активно развивает инициативы по цифровизации государственного сектора и повышению доверия к цифровым технологиям.

Финляндия демонстрирует высокий уровень зрелости в области информационной безопасности, опираясь на стандарты ISO 27001 и NIST Cybersecurity Framework [20]. Зна-

чительное внимание уделяется защите персональных данных и соблюдению требований GDPR. В стране последовательно развиваются программы по обучению специалистов в области ИТ-аудита и внедрению современных инструментов для оценки и мониторинга киберустойчивости.

В **Швеции** отдельного подразделения, отвечающего исключительно за ИТ-аудит, не создано [21]. Его функции интегрированы в общие департаменты аудита эффективности. Страна применяет стандарты ISO/IEC 27001, COBIT, а также подходы NIST и положения EU Cybersecurity Act. Особое внимание уделяется интеграции кибербезопасности и аудита, внедрению инструментов анализа рисков и повышению прозрачности ИТ-услуг.

В **Великобритании** также отсутствует отдельный департамент ИТ-аудита, однако внимание сосредоточено на независимости и прозрачности аудиторского процесса [22]. Применяются признанные в мировой практике стандарты ISACA, CISA и методология ITIL, а также программа Cyber Essentials и национальный Cyber Assessment Framework (HMG). Существенное значение придается соблюдению требований GDPR и укреплению системы защиты данных в государственном секторе.

Международная практика свидетельствует о нескольких устойчивых тенденциях. Во-первых, наблюдается процесс централизации функций ИТ-аудита и их институционального укрепления, что характерно для Турции, США и Финляндии. Во-вторых, происходит унификация методологической базы. В-третьих, ИТ-аудит все чаще рассматривается не только как инструмент контроля, но и как элемент системы управления рисками и цифровой безопасности. Во многих странах (особенно США и Великобритании) аудит тесно интегрирован с практиками киберустойчивости и оценкой эффективности ИТ-инвестиций. Наконец, важное направление развития – подготовка и сертификация ИТ-аудиторов, а также внедрение аналитических инструментов для мониторинга угроз и оценки эффективности государственных ИТ-систем.

Таким образом в международной практике наибольшее распространение получили три стандарта:

– ISSAI 5300 (INTOSAI) – определяет принципы и этапность проведения ИТ-аудита (планирование, сбор доказательств, формирование выводов);

– COBIT 2019 (ISACA) – представляет рамочную модель управления ИТ, включая оценку зрелости процессов и управляемости цифровой инфраструктуры;

– ISO/IEC 27001 – задает требования к системам управления информационной безопасностью.

На текущий момент действующая практика ИТ-аудита в Казахстане пока остается недостаточно развитой. Элементы указанных стандартов были адаптированы в казахстанскую практику, что позволило создать комплексную методику, включающую оценку цифровой зрелости, эффективность управления ИТ и уровень информационной безопасности.

Анализ практики IT-аудита в Казахстане выявил системные ограничения, снижающие его эффективность и тормозящие развитие цифрового управления в госсекторе. Основные проблемы – отсутствие нормативно закрепленной методологической базы и единых стандартов: в действующем законодательстве нет четкого определения ITаудита, его целей, задач и порядка проведения, что создает правовую неопределенность и затрудняет сопоставимость результатов. Частые изменения стратегических и нормативных документов подрывают преемственность и стабильность цифровых инициатив, усложняя долгосрочное планирование.

Существенным ограничением является дефицит квалифицированных специалистов в областях IT-аудита и кибербезопасности. Нехватка кадров, знакомых с международными стандартами (ISO/IEC 27001, NIST, COBIT, CISA и др.), уменьшает качество проверок и препятствует внедрению современных практик. Низкая цифровая зрелость организаций, устаревшие системы, слабая интеграция ИТ с бизнес-процессами и зависимость от импорт-

ных технологий затрудняют комплексную оценку инфраструктуры и повышают риски для национальной цифровой безопасности. Задержки реализации крупных ИКТ-проектов приводят к неэффективному использованию бюджетных средств и срыву сроков достижения стратегических целей.

Недостатки управления архитектурой «электронного правительства» также ограничивают прозрачность и эффективность: отсутствует системный учет объектов информатизации, не всегда ведется актуальная документация и четко не регламентирован жизненный цикл систем, что провоцирует дублирование функций. Особую проблему представляет недостаточное соблюдение требований по информационной безопасности и защите персональных данных – в процессе аудита возникают риски несанкционированного доступа и утечек, требующие усиления нормативных и организационных мер. Наблюдается и недооценка руководством стратегической роли IT-аудита, что формализует процедуры и снижает внимание к управлению ИТ-рисками.

Внутренний фокус на проверке целевого использования бюджетных средств ограничивает содержательное поле аудита: международная практика охватывает более широкий спектр задач – оценку цифровой зрелости, эффективности процессов, соответствия международным стандартам, уровня информационной безопасности и возврата инвестиций (ROI). Для повышения эффективности IT-аудита в Казахстане необходим комплекс мер институционального, методологического и кадрового характера, включая адаптацию международных стандартов и создание единой методики, обеспечивающей объективность и сопоставимость оценок.

В предлагаемом доработанном варианте методики показан расширенный подход: IT-аудит трактуется как управленческая оценка цифровых процессов и зрелости, а не только как техническая проверка. Такой комплексный взгляд позволяет выявлять системные риски, дублирование функций, пробелы в интеграции и управлении ИТ-ресурсами, повышая прозрачность и качество управления. Новая модель смещает акцент с формального контроля к аналитической и рискориентированной оценке, рассматривая информационные системы как элементы единой экосистемы цифрового управления.

Ключевые элементы методики включают оценку всей системы ИТ управления – процессы, кадры, архитектуру, безопасность и использование данных – и внедрение шкалы зрелости (0–5) с количественными показателями для сравнительного анализа между органами и мониторинга динамики цифрового развития. Оценка проводится по критериям: наличие стратегии ИТ управления, формализация процессов, уровень автоматизации, измеримость показателей, управление данными и наличие обратной связи. Такой подход позволяет не только фиксировать текущее состояние, но и формулировать приоритетные направления совершенствования, повышая результативность ИТ проектов и оптимизируя расходы.

Ниже приведены практические примеры применения вышеупомянутой методики:

Пример 1. Неэффективное использование лицензий. В результате аудита было выявлено, что фактически используется лишь 40% оплаченных лицензий. После внедрения системы мониторинга расходы на сопровождение были сокращены на 40%.

Пример 2. Отсутствие резервного копирования. На основе критериев ISO 27001 внедрена система резервного копирования, что позволило сократить время восстановления после сбоев с нескольких дней до нескольких часов.

Пример 3. Дублирование функций систем. Объединение схожих информационных систем позволило устранить дублирование функций и сэкономить ежегодные бюджетные средства.

Новая методика преобразует ИТ-аудит из инструмента контроля в механизм управления качеством цифровой трансформации: помимо выявления нарушений, она выявляет резервы повышения эффективности, оптимизации расходов и совершенствования ИТ-управления в государственном секторе. В результате формируется единый подход к оценке

цифрового управления, основанный на международных стандартах и ориентированный на непрерывное улучшение процессов.

Согласно международной практике, для проведения ИТ-аудита аудитор должен знать национальное законодательство и международные стандарты, обладать техническими компетенциями для анализа архитектуры ИС, оценки уровня информационной безопасности и зрелости процессов, понимать жизненный цикл разработки и уметь формулировать обоснованные рекомендации. ИТ-аудит требует сочетания навыков финансового контроля, технологического анализа и управления рисками: аудитор выполняет контрольную, аналитическую и консультативную функции, оценивая вклад ИТ в достижение целей госоргана.

Планирование аудита начинается с анализа объекта, постановки целей, определения критериев оценки и состава доказательной базы. Необходимо определить, какие ИС подлежат проверке, их роль в реализации задач органа и связанные с ними риски. В процессе аудита собираются данные, анализируется архитектура и процессы, проверяется соответствие требованиям безопасности и оценивается цифровая зрелость. Результаты оформляются в аналитический отчет с выводами и управленческими рекомендациями; методика предполагает применение унифицированных шаблонов, профилей рисков и форм фиксации данных для обеспечения объективности и воспроизводимости.

Завершающий этап – мониторинг выполнения рекомендаций, позволяющий отслеживать реализацию корректирующих мер и оценивать достигнутый эффект.

ЗАКЛЮЧЕНИЕ

Внедрение обновленной методики ИТ-аудита – важный шаг к модернизации государственного контроля в Казахстане. Методология смещает акцент с формального контроля на рискориентированную и аналитическую оценку, нацеленную не только на обнаружение нарушений, но и на повышение эффективности цифрового управления. Интеграция международных стандартов (ISSAI, COBIT, ISO) обеспечивает сопоставимость практик с мировыми подходами и формирует единый механизм оценки цифровой зрелости государственных органов. В долгосрочной перспективе развитие ИТ-аудита в системе ВАП создает предпосылки для повышения прозрачности, эффективности и устойчивости цифровой трансформации государственного сектора.

Основные векторы дальнейшего развития:

– Углубление рискориентированного подхода. Аудит будет все больше фокусироваться на критичности цифровых процессов, приоритетной оценке объектов повышенного риска и применении аналитических средств для раннего выявления угроз, что позволит оперативно снижать риски, связанные с эффективностью и безопасностью государственных ИС.

– Развитие методологии аудита кибербезопасности. Учитывая рост киберугроз и расширение цифровой инфраструктуры, требуется комплексная оценка защищенности, механизмов реагирования на инциденты, управления уязвимостями и устойчивости критически важных систем.

– Аудит алгоритмов и систем ИИ. Появляется необходимость проверки корректности алгоритмов, прозрачности логики принятия решений, отсутствия дискриминации, соблюдения этических норм и требований безопасности при использовании ИИ в госсекторе.

– Кадровое развитие и стандартизация компетенций. Для реализации новой методики нужны специалисты, совмещающие ИТ, аналитические и аудиторские компетенции. Создание специализированной подготовки, единых профилей компетенций и систем непрерывного повышения квалификации повысит качество аудита и укрепит доверие к государственным институтам.

В итоге совершенствование методологии, усиление кибер и алгоритмической составляющих, а также инвестирование в кадровый потенциал создадут условия для перехода от реактивного контроля к проактивному управлению цифровыми рисками и повышению результативности государственного управления в цифровой экономике.

Список использованных источников

1. OECD (2023). «Government at a Glance 2023: Towards Better-Working Public Services». OECD Publishing. https://doi.org/10.1787/3d5c5d31-en

2. McKinsey & Company (2023). «Why Government IT Projects Still Fail» // McKinsey on Government. – № 8. – С. 45-52. https://icmsol.com/resources/why-government-it-projects-fail

3. OECD (2021). «Digital Government in Chile: Policy Recommendations». OECD Public Governance Reviews. – Paris: OECD Publishing. https://www.oecd.org/en/publications/digital-government-in-chile_d1b72d93-en/full-report.html

4. Указ Президента Республики Казахстан «О Системе ежегодной оценки эффективности деятельности центральных государственных и местных исполнительных органов областей, городов республиканского значения, столицы» от 19 марта 2010 года № 954. [Электронный ресурс.] – URL: https://adilet.zan.kz/rus/docs/U100000954_ (дата обращения – 12.04.2025)

5. Сайт Высшей аудиторской палаты Республики Казахстан. Итоги государственного аудита эффективности политики цифрового развития подвели в Высшей аудиторской палате РК. [Электронный ресурс.] – URL: https://www.gov.kz/memleket/entities/esep/press/news/details/932553?lang=ru (дата обращения – 10.05.2025)

6. Информационная безопасность, кибербезопасность и защита персональных данных – Системы менеджмента информационной безопасности – Требования. ISO/IEC 27001:2022 (E). Пер. А. Горбунов. [Электронный ресурс.] – URL: https://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27001-2022.pdf (дата обращения: 05.03.2025)

7. Исследование в части осуществления ITаудита в сфере информационных технологий и проведения оценки эффективности деятельности государственных органов по применению ИКТ в Казахстане. Международный опыт по внедрению ITаудита в ВОА. ВАП РК, ЦИАОЭ, 2025 г.

8. Muhammad Fauzan Hanif, Ahmad Rofik Harahap, Ade Fakhrudin, Dimas Febriawan Integrating COBIT and ISO Frameworks in IT Audits: A Literature Review. September 2025. International Journal of Emerging Research in Engineering Science and Management 4(3):8-14. DOI:10.58482/ijeresm. v4i3.2

9. Merhout J.W., Havelka D. Information Technology Auditing: A Value-Added IT Governance Partnership between IT Management and Audit // Communications of the Association for Information Systems. 2008. Vol. 23. Article 26. P. 463-482.

10. Sitnov A.A., Bareeva B.R. IT audit as a check of compliance with the requirements of the company's business objectives system // Economic problems and legal practice. 2020. Vol. XVI. No. 2. P. 98-101. URL: https://cyberleninka.ru/article/n/it-audit-kak-proverka-sootvetstviya-informatsionnoy-sistemy-biznes-zadacham-kompanii

11. Sitnov A.A. Information Systems Audit – Risk-oriented Approach // Economic problems and legal practice. 2019. Vol. XV. No. 5. P. 94-97.

12. Turebekova B.O., Saparbayeva S.S., Barysheva S.K., Orazalinova M.S. Introduction and improvement of IT audit in Kazakhstan // Bulletin of Turan University. 2023. No. 1(97). P. 11-23.

13. Ramazanova K.M., Nurgaliyeva A.M. Information technologies as one of the important factors in the development of the effectiveness of internal audit // Bulletin of the Karaganda University, Series "Economics". 2023. No. 1(109). P. 123-131.

14. Core Concepts Information Technology Auditing. Comprehensive Educational Resource. 2025.

15. Стандарт GUID 5310 (ISSAI 5310) – Методика проверки безопасности информационных систем. [Электронный ресурс.] – URL: https://www.eurosai.org/handle404?exporturi=/export/sites/eurosai/.content/documents/others/ISSAI/ISSAI-5310-RU.pdf (дата обращения: 08.03.2025)

16. ISSAI – 5300 – Руководство по ИТ-аудиту https://www.issai.org/pronouncements/guidelines-on-it-audit/.

17. Веб-сайт высшего органа аудита Турции – Sayistay Baskanligi [Электронный ресурс.] – URL: http://www.sayistay.gov.tr (дата обращения – 07.05.2025)

18. Веб-сайт высшего органа аудита США – Government Accountability Office. [Электронный ресурс.] – URL: http://www.gao.gov (дата обращения – 03.05.2025)

19. Веб-сайт высшего органа аудита Литвы – Valstybės kontrolė (National Audit Office). [Электронный ресурс.] – URL: https://www.valstybeskontrole.lt (дата обращения – 20.04.2025)

20. Веб-сайт высшего органа аудита Финляндии – National Audit Office of Finland. [Электронный ресурс.] – URL: http://www.vtv.fi (дата обращения – 20.04.2025)

21. Веб-сайт высшего органа аудита Швеции – Riksrevisionen. [Электронный ресурс.] – URL: http://www.riksrevisionen.se (дата обращения – 28.04.2025)

22. Веб-сайт высшего органа аудита Великобритании – National Audit Office, NAO. [Электронный ресурс.] – URL: http://www.nao.org.uk (дата обращения – 16.04.2025)

References

1. OECD (2023). «Government at a Glance 2023: Towards Better-Working Public Services». OECD Publishing. https://doi.org/10.1787/3d5c5d31-en

2. McKinsey & Company (2023). «Why Government IT Projects Still Fail» // McKinsey on Government. – № 8. – S. 45-52. https://icmsol.com/resources/why-government-it-projects-fail

3. OECD (2021). «Digital Government in Chile: Policy Recommendations». OECD Public Governance Reviews. – Paris: OECD Publishing. https://www.oecd.org/en/publications/digital-government-in-chile_d1b72d93-en/full-report.html

5.Ukaz Prezidenta Respubliki Kazahstan «O Sisteme ezhegodnoj ocenki effektivnosti deyatel'nosti central'nyh gosudarstvennyh i mestnyh ispolnitel'nyh organov oblastej, gorodov respublikanskogo znacheniya, stolicy» ot 19 marta 2010 goda № 954. [Elektronnyj resurs.] – URL: https://adilet.zan.kz/rus/docs/U100000954_ (data obrashcheniya – 12.04.2025)

4. Sajt Vysshej auditorskoj palaty Respubliki Kazahstan. Itogi gosudarstvennogo audita effektivnosti politiki cifrovogo razvitiya podveli v Vysshej auditorskoj palate RK. [Elektronnyj resurs.] – URL: https://www.gov.kz/memleket/entities/esep/press/news/details/932553?lang=ru (data obrashcheniya – 10.05.2025)

5. Informacionnaya bezopasnost', kiberbezopasnost' i zashchita personal'nyh dannyh – Sistemy menedzhmenta informacionnoj bezopasnosti – Trebovaniya. ISO/IEC 27001:2022 (E). Per. A. Gorbunov. [Elektronnyj resurs.] – URL: https://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27001-2022.pdf (data obrashcheniya: 05.03.2025)

6. Issledovanie v chasti osushchestvleniya IT audita v sfere informacionnyh tekhnologij i provedeniya ocenki effektivnosti deyatel'nosti gosudarstvennyh organov po primeneniyu IKT v Kazahstane. Mezhdunarodnyj opyt po vnedreniyu IT audita v VOA. VAP RK, CIAOE, 2025 g.

7. Muhammad Fauzan Hanif, Ahmad Rofik Harahap, Ade Fakhrudin, Dimas Febriawan 8. Integrating COBIT and ISO Frameworks in IT Audits: A Literature Review. September 2025. International Journal of Emerging Research in Engineering Science and Management 4(3):8-14. DOI:10.58482/ijeresm.v4i3.2

9. Merhout J.W., Havelka D. Information Technology Auditing: A Value-Added IT Governance Partnership between IT Management and Audit // Communications of the Association for Information Systems. 2008. Vol. 23. Article 26. P. 463-482.

10.Sitnov A.A., Bareeva B.R. IT audit as a check of compliance with the requirements of the company's business objectives system // Economic problems and legal practice. 2020. Vol. XVI. No. 2. P. 98-101. URL: https://cyberleninka.ru/article/n/it-audit-kak-proverka-sootvetstviya-informatsionnoy-sistemy-biznes-zadacham-kompanii

11.Sitnov A.A. Information Systems Audit – Risk-oriented Approach // Economic problems and legal practice. 2019. Vol. XV. No. 5. P. 94-97.

12.Turebekova B.O., Saparbayeva S.S., Barysheva S.K., Orazalinova M.S. Introduction and improvement of IT audit in Kazakhstan // Bulletin of Turan University. 2023. No. 1(97). P. 11-23.

13.Ramazanova K.M., Nurgaliyeva A.M. Information technologies as one of the important factors in the development of the effectiveness of internal audit // Bulletin of the Karaganda University, Series "Economics". 2023. No. 1(109). P. 123-131.

14.Core Concepts Information Technology Auditing. Comprehensive Educational Resource. 2025.

15.Standart GUID 5310 (ISSAI 5310) – Metodika proverki bezopasnosti informacionnyh sistem. [Elektronnyj resurs.] – URL: https://www.eurosai.org/handle404?exporturi=/export/sites/eurosai/.content/documents/others/ISSAI/ISSAI-5310-RU.pdf (data obrashcheniya: 08.03.2025)

16.ISSAI – 5300 – Rukovodstvo po IT-auditu https://www.issai.org/pronouncements/guidelines-on-it-audit/.

17.Veb-sajt vysshego organa audita Turcii – Sayistay Baskanligi [Elektronnyj resurs.] – URL: http://www.sayistay.gov.tr (data obrashcheniya – 07.05.2025)

18.Veb-sajt vysshego organa audita SSHA – Government Accountability Office. [Elektronnyj resurs.] – URL: http://www.gao.gov (data obrashcheniya – 03.05.2025)

19.Veb-sajt vysshego organa audita Litvy – Valstybės kontrolė (National Audit Office). [Elektronnyj resurs.] – URL: https://www.valstybeskontrole.lt (data obrashcheniya – 20.04.2025)

20.Veb-sajt vysshego organa audita Finlyandii – National Audit Office of Finland. [Elektronnyj resurs.] – URL: http://www.vtv.fi (data obrashcheniya – 20.04.2025)

21.Veb-sajt vysshego organa audita SHvecii – Riksrevisionen. [Elektronnyj resurs.] – URL: http://www.riksrevisionen.se (data obrashcheniya – 28.04.2025)

22.Veb-sajt vysshego organa audita Velikobritanii – National Audit Office, NAO. [Elektronnyj resurs.] – URL: http://www.nao.org.uk (data obrashcheniya – 16.04.2025)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНДА АКТ ҚОЛДАНУ БОЙЫНША МЕМЛЕКЕТТІК ОРГАНДАР ҚЫЗМЕТІНІҢ ТИІМДІЛІГІН БАҒАЛАУ ЖӘНЕ IT АУДИТ ЖҮРГІЗУДІҢ ӘДІСНАМАЛЫҚ НЕГІЗДЕРІ

Шакирова Н. А.*
ақпараттық технологиялар магистрі
Электрондық қаржы орталығы
Астана, Қазақстан
e-mail: dyomindom@gmail.com

Рахметов Н. Ж.
Зерттеулер, талдау және тиімділікті бағалау орталығы
Астана, Қазақстан
e-mail: nurlybek.r@gmail.com

Сыздыкова А. С.
Электрондық қаржы орталығы
Астана, Қазақстан
e-mail: anelya2391@gmail.com

Бокаев Б. Н.
PhD, зерттеуші
Сиракуз университеті
Максвелл азаматтық және мемлекеттік басқару мектебі,АҚШ
e-mail: b.bokayev@syr.edu
ORCID: 0000-0002-1037-7085

Аңдатпа. Мақалада Қазақстан Республикасының Мемлекеттік басқару жүйесінде IT-аудитті енгізудің әдіснамалық, нормативтік және практикалық аспектілерін зерделеуге бағытталған кешенді зерттеу жұмысының нәтижелері келтірілген. Зерттеу мемлекеттік органдарда ақпараттық-коммуникациялық технологияларды (АКТ) қолдану тиімділігін бағалаудың қолданыстағы тәсілдерін талдауды және олардың ISSAI 5300, COBIT 2019 және ISO/IEC 27001 өзекті халықаралық аудит стандарттарымен арақатынасын қамтиды. Мемлекеттік аудиттің ұлттық практикасын және басқа елдердің жоғары аудит органдарында қолданылатын шетелдік тәсілдерді салыстырмалы талдау негізінде IT-аудит жүргізудің жаңартылған кешенді әдістемесі әзірленді. Ұсынылған әдістеме Мемлекеттік мекемелердің цифрлық жетілуін бағалау құралдарын, IT-процестердің тиімділігі мен тиімділігін талдауды, сондай-ақ ақпараттық тәуекелдерді басқару жөніндегі шараларды интеграциялауды қамтиды. Әдістемені жетілдірудің әдіснамалық негізі үш деңгейлі интеграция болып табылады: ISSAI 5300, COBIT 2019 және ISO/IEC 27001 халықаралық стандарттарын ұлттық нормативтік талаптармен біріктіру; қазақстандық шындыққа бейімделген цифрлық жетілуді бағалаудың аралас моделін енгізу; IT-процестердің нәтижелілігінің сандық көрсеткіштері мен сапалық индикаторлары жүйесін қолдану. Жетілдірілген әдістеме тиімділіктің сандық көрсеткіштерін, АКТ инфрақұрылымын тәуекелге бағдарланған талдауды және мемлекеттік органдарда ақпараттық технологияларды басқару қағидаттарын интеграциялауды қамтамасыз етеді. Ұсынылған әдіснамалық тәсілдер мен құралдарды іске асыру Қазақстан Республикасының мемлекеттік органдары мен аудиторлық органдарға: цифрлық трансформацияның жай-күйін бағалаудың ашықтығы мен объективтілігін арттыруға; аудиторлық қорытындылар мен ұсынымдардың сапасы мен негізділігін жақсартуға; АКТ енгізу процестерінің тиімділігін және IT-ресурстарды ұтымды пайдалануды қамтамасыз етуге; ақпараттық тәуекелдерді азайтуға және ақпараттық қауіпсіздік деңгейін арттыруға мүмкіндік береді.

Түйін сөздер: IT-аудит, ақпараттық қауіпсіздік, ISSAI 5300, COBIT 2019, ISO 27001, мемлекеттік аудит, АКТ тиімділігі.

METHODOLOGICAL FOUNDATIONS OF IT AUDIT AND EVALUATION OF THE EFFECTIVENESS OF GOVERNMENT AGENCIES IN THE USE OF ICT IN THE REPUBLIC OF KAZAKHSTAN

Шакирова Н.А.*
Master's Degree in Information Technology
E-finance Center
Astana, Republic of Kazakhstan
e-mail: dyomindom@gmail.com

Сыздыкова А.С.
E-finance Center
Center for Research, Analysis and Evaluation of Effectiveness
Astana, Republic of Kazakhstan
e-mail: anelya2391@gmail.com

Рахметов Н.Ж.
Center for Research, Analysis and Evaluation of Effectiveness
Astana, Republic of Kazakhstan
e-mail: nurlybek.r@gmail.com

Bokayev B. N.
PhD, Syracuse University
Maxwell School of Citizenship and Public Affairs, USA
PhD researcher
e-mail: b.bokayev@syr.edu
ORCID: 0000-0002-1037-7085

Abstract. The article presents the results of a comprehensive research work aimed at studying the methodological, regulatory and practical aspects of the implementation of IT audit in the public administration system of the Republic of Kazakhstan. The study covers the analysis of existing approaches to assessing the effectiveness of information and communication technologies (ICT) in government agencies and their relationship to the current international auditing standards ISSAI 5300, COBIT 2019 and ISO/IEC 27001. Based on a comparative analysis of the national practice of state audit and foreign approaches used in the Supreme Audit Institutions of other countries, an updated comprehensive methodology for conducting IT audit has been developed. The proposed methodology includes tools for assessing the digital maturity of government agencies, analyzing the effectiveness and efficiency of IT processes, as well as integrating information risk management measures. The methodological basis for improving the methodology is a three-level integration: combining international standards ISSAI 5300, COBIT 2019 and ISO/IEC 27001 with national regulatory requirements; the introduction of a combined model for assessing digital maturity adapted to the realities of Kazakhstan; the use of a system of quantitative indicators and qualitative indicators of the effectiveness of IT processes. The improved methodology ensures the integration of quantitative performance indicators, risk-based analysis of the ICT infrastructure and principles of information technology manageability in government agencies. The implementation of the proposed methodological approaches and tools will allow the state bodies of the Republic of Kazakhstan and audit bodies to: increase transparency and objectivity in assessing the state of digital transformation; improve the quality and validity of audit reports and recommendations; ensure the effectiveness of ICT implementation processes and the rational use of IT resources; reduce information risks and increase information security.

Keywords: IT audit, information security, ISSAI 5300, COBIT 2019, ISO 27001, state audit, ICT efficiency.