УДК 04.056

ПРОВЕРКА И ОЦЕНКА ИНФОРМАЦИОННЫХ СИСТЕМ: СОВРЕМЕННЫЕ ПОДХОДЫ К АУДИТУ В КОНТЕКСТЕ НОРМАТИВНОЙ БАЗЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Останина Д.Е., студент гр. ИБс-211, 5 курс

Научный руководитель: Прокопенко Е.В., к.ф-м.н., доцент

Кузбасский государственный технический университет им. Т.Ф, Горбачёва,

г. Кемерово

Аннотация

В статье рассматривается современное состояние методологии аудита информационных систем в условиях сформировавшейся и динамично развивающейся российской нормативной базы. Актуальность исследования обусловлена необходимостью систематизации многоуровневой системы обязательных требований – от федеральных законов до отраслевых приказов регуляторов, – которые формируют уникальный ландшафт аудита ИС в Российской Федерации. Автором проведен компаративный анализ четырех групп нормативных документов: стандартов аудиторской деятельности (МСА), технических регламентов ФСТЭК и ФСБ России, национальных стандартов серии ГОСТ Р ИСО/МЭК 27000, а также специализированных стандартов Счетной палаты РФ. Особое внимание уделено документационной архитектуре аудита: определен перечень документов аудируемого лица, подлежащих инспектированию, и их привязка к конкретным нормативным требованиям. Предложена авторская уровневая модель нормативно-правового регулирования аудита ИС в РФ.

Ключевые слова: аудит информационных систем, нормативная база РФ, МСА 315, Приказ ФСТЭК №117, ГОСТ Р 56939-2024, СГА 305, документационное обеспечение, ISO/IEC 27006, сертификация СМИБ, оценка соответствия.

1. Введение

Парадигма аудита информационных систем в Российской Федерации претерпевает фундаментальную трансформацию. Если в 2010-е годы методологическая база формировалась преимущественно заимствованием международных фреймворков (COBIT, ITIL, ISO/IEC 27000), то к 2025–2026 гг. сложилась целостная, иерархически организованная национальная система нормативных требований, прямо регулирующая порядок проверки и оценки информационных систем.

Данная система характеризуется следующими особенностями:

1. **Императивность** – значительная часть требований имеет статус федеральных законов, указов Президента, приказов регуляторов

(ФСТЭК, ФСБ, Роскомнадзор), обязательных к исполнению в установленных категориях ИС (ГИС, КИИ, ИСПДн);

2. **Дифференциация по субъектам** – принципиально различаются требования к аудиту государственных информационных систем (Счетная палата, Казначейство), коммерческих организаций (аудиторские организации, действующие по МСА) и сертификационному аудиту (органы по сертификации СМИБ);

3. **Актуализация** – 2024–2025 гг. ознаменовались введением в действие новых редакций ключевых ГОСТов (ГОСТ Р 56939-2024 «Разработка безопасного программного обеспечения»), разработкой идентичного ISO/IEC 27006-1:2024 проекта национального стандарта ПНС 1.0.079-1.120.25, а также принятием Приказа ФСТЭК №117 от 11.04.2025, формирующего требования к ГИС.

Цель настоящего исследования – систематизация действующей нормативной базы РФ в области аудита информационных систем, определение перечня документов аудируемого лица, подлежащих проверке в соответствии с каждым из нормативных блоков, и построение архитектуры документационного обеспечения аудиторских процедур.

2. Иерархическая модель нормативно-правового регулирования аудита ИС в РФ

Проведенный анализ источников позволяет выделить четыре уровня нормативного регулирования, формирующих целостную систему требований к проверке и оценке информационных систем в Российской Федерации.

2.1. Уровень I. Законодательный базис

Фундамент составляют федеральные законы, определяющие правовой режим информации и информационных систем. В соответствии со стандартом СГА 305 «Аудит федеральных информационных систем и проектов» (утв. постановлением Коллегии Счетной палаты РФ от 23.12.2016 № 11ПК, ред. от 28.12.2018) базовыми актами выступают:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» – определяет понятийный аппарат, правовой статус ГИС, требования к операторам;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» – формирует требования к защите ИСПДн, включая обязанность оператора по проведению мероприятий по обеспечению безопасности (ст. 19);
- Федеральный закон от 05.04.2013 № 44-ФЗ – регламентирует закупки ИС для государственных нужд, включая экспертизу результатов выполненных работ.

Указанные законы не содержат прямых предписаний о порядке аудита, но формируют **объект проверки**: аудитор обязан установить соответствие ИС требованиям данных законов.

2.2. Уровень II. Подзаконные нормативные акты и требования регуляторов

Второй уровень образуют приказы федеральных органов исполнительной власти, устанавливающие конкретизированные требования к ИС различных категорий.

Ключевой документ 2025 года – **Приказ ФСТЭК России № 117 от 11.04.2025** «Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений».

Данный приказ вводит обязательные для применения требования к: **порядку разработки безопасного программного обеспечения** в случае самостоятельной разработки оператором (п. 14). Нормативная ссылка: ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» (утв. приказом Госстандарта от 24.10.2024 № 1504-ст); **порядку мониторинга информационной безопасности** информационных систем (п. 14). Нормативная ссылка: ГОСТ Р 59547-2021 «Защита информации. Мониторинг информационной безопасности. Общие положения».

Документация, подлежащая аудиту по требованиям ФСТЭК:

- Документация на разработку ПО (спецификации, техническое задание, тест-планы);
- Регламенты мониторинга ИБ;
- Журналы регистрации событий (логи);
- Акты испытаний (в том числе приемочных).

2.3. Уровень III. Национальные стандарты (ГОСТ Р), идентичные международным

Третий уровень представлен национальными стандартами, принятыми в развитие федерального закона «О стандартизации» и идентичными международным документам ИСО/МЭК.

Центральное место занимает **ГОСТ Р ИСО/МЭК 27006-2020** «Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности» (утв. приказом Росстандарта от 08.09.2020 № 628-ст, введен в действие 01.07.2021).

Данный стандарт: идентичен ISO/IEC 27006:2015; устанавливает требования к органам по сертификации СМИБ; дополняет требования ISO/IEC 17021-1 и ISO/IEC 27001; служит критериальной базой для аккредитации органов по сертификации.

Важнейшее событие 2025 года – публичное обсуждение проекта **ПНС 1.0.079-1.120.25**, разработанного ФАУ «Национальный институт аккредитации». Документ идентичен ISO/IEC 27006-1:2024 и придет на смену ГОСТ Р ИСО/МЭК 27006-2020. Его утверждение ожидается в 2026 году.

Документация, подлежащая аудиту при сертификации СМИБ:

- Заявление о применимости (Statement of Applicability);
- Политики и процедуры СМИБ;
- Документированная информация о компетентности персонала;
- Протоколы внутренних аудитов;
- Документы о сертификации (certification documents).

2.4. Уровень IV. Специализированные стандарты аудита (Счетная палата, Минфин)

Четвертый уровень – стандарты, непосредственно регламентирующие процесс проведения аудита как вида деятельности.

СГА 305 «Аудит федеральных информационных систем и проектов» (Стандарт внешнего государственного аудита) – разработан Счетной палатой РФ в соответствии с Федеральным законом № 41-ФЗ, с учетом международных стандартов ИНТОСАИ.

Область применения: контрольные и экспертно-аналитические мероприятия в отношении федеральных информационных систем на всех этапах жизненного цикла.

Международные стандарты аудита (МСА) – признаны для применения на территории РФ Приказом Минфина России от 09.01.2019 № 2н.

Ключевой стандарт для аудита ИС: МСА 315 (пересмотренный, 2019 г.) «Выявление и оценка рисков существенного искажения посредством изучения организации и ее окружения» (введен в действие на территории РФ Приказом Минфина России от 27.10.2021 № 163н).

МСА 315 обязывает аудитора: понимать ИТ-среду организации; выявлять средства контроля, связанные с обработкой информации; оценивать риски существенного искажения на уровне предпосылок; инспектировать документацию (наблюдение, запросы, аналитические процедуры).

Приложение А165 к МСА 315 прямо указывает на необходимость оценки средств контроля, связанных со сверкой детализированных записей с основным регистром, а также дополнительных средств контроля организаций-пользователей обслуживающих организаций (отсылка к МСА 402)

3. Компаративный анализ подходов

Существенной особенностью российской системы является дифференциация целей и процедур аудита в зависимости от субъекта проверки и назначения ИС.

3.1. Внешний аудит финансовой отчетности (аудиторские организации)

Нормативный базис: МСА, признанные Минфином РФ.

Цель аудита ИС: получение уверенности в том, что ИТ-средства контроля обеспечивают достоверность бухгалтерской (финансовой) отчетности.

Объект проверки: общие средства ИТ-контроля (управление доступом, управление изменениями, ИТ-операции), прикладные средства контроля (логика расчетов, проводки).

Документация: ограничивается документацией, непосредственно влияющей на учетный процесс.

3.2. Сертификационный аудит СМИБ (органы по сертификации)

Нормативный базис: ГОСТ Р ИСО/МЭК 27006-2020 (перспектива – ПНС 1.0.079-1.120.25).

Цель: подтверждение соответствия системы менеджмента информационной безопасности требованиям ГОСТ Р ИСО/МЭК 27001.

Объект проверки: документированная информация СМИБ (политики, процедуры, записи).

Документация: полный пакет документов СМИБ, включая внутренние аудиты, анализ со стороны руководства, корректирующие действия.

3.3. Государственный аудит федеральных ИС (Счетная палата РФ)

Нормативный базис: СГА 305, Федеральный закон № 41-ФЗ.

Цель: оценка эффективности использования бюджетных средств, создание и развитие ГИС, соответствие целям государственных программ.

Объект проверки: контракты на создание ИС, техническая документация, фактически достигнутые показатели, соблюдение запретов (Постановление № 1236 – импортозамещение ПО).

Документация: документация о закупках, проектная документация, отчеты о ходе выполнения работ.

4. Практическая реализация аудиторских процедур: документационный срез

На основе систематизированной нормативной базы возможно построение типового чек-листа аудитора для проверки документационного обеспечения ИС.

Блок 1. Проверка наличия правоустанавливающих документов на ИС

Наличие приказа о создании/вводе в эксплуатацию ИС; наличие утвержденного технического задания; соответствие реализованной ИС утвержденному ТЗ (акты приемки, протоколы испытаний); регистрация ИС в реестре (для ГИС – ФГИС УИС, ФГИС КИ).

Блок 2. Проверка документации по защите информации

Наличие утвержденной модели угроз и нарушителя; наличие акта классификации ИС; наличие политики информационной безопасности, утвержденной руководителем; наличие приказа о разграничении прав доступа и матрицы доступа; наличие эксплуатационной документации на средства защиты информации (СКЗИ, МЭ, СОВ).

Блок 3. Проверка документации по управлению инцидентами и непрерывностью

Наличие регламента регистрации и рассмотрения инцидентов ИБ; наличие журнала инцидентов ИБ; наличие регламента резервного копирования; наличие актов тестового восстановления данных.

Блок 4. Проверка документации по аудиту и совершенствованию

Наличие планов внутренних аудитов (для СМИБ); наличие отчетов о внутренних аудитах; наличие протоколов анализа СМИБ со стороны руководства; наличие документов по корректирующим действиям.

5. Проблемы и перспективы развития нормативной базы РФ в сфере аудита ИС

Проведенный анализ позволяет идентифицировать ряд системных проблем и перспективных направлений развития.

Проблема 1. В ФЗ-149, МСА 315 и ГОСТ Р 27006 используются различные определения средств контроля, рисков, аудиторских доказательств. Отсутствие унифицированного понятийного аппарата создает риски неоднозначной трактовки результатов аудита.

Проблема 2. Наличие сертификата соответствия СМИБ (ISO 27001) не освобождает аудиторскую организацию от выполнения процедур по МСА 315, но может быть использовано как фактор снижения объема тестирования (МСА 610). Методика такой интеграции в российской практике не формализована.

Проблема 3. ГОСТ Р ИСО/МЭК 27001-2006 устарел (актуальная международная версия – ISO/IEC 27001:2022). Разработка новой редакции национального стандарта, идентичного ISO/IEC 27001:2022, является критически важной задачей на 2025–2026 гг..

Перспективное направление: разработка и утверждение **федерального стандарта аудиторской деятельности (ФСАД) «Аудит информационных систем»** либо специализированного **Приказа Минфина России**, детализирующего применение МСА 315 в части оценки ИТ-контролей при аудите бухгалтерской отчетности. Данный документ мог бы унифицировать требования к документации, объему тестирования и квалификации аудиторов.

6. Заключение

Проведенное исследование позволяет сделать вывод о том, что в Российской Федерации к 2026 году сформирована **целостная, многоуровневая система нормативных требований** к проверке и оценке информационных систем.

Ключевыми элементами данной системы выступают: Законодательная база (ФЗ-149, ФЗ-152); Требования регуляторов (Приказ ФСТЭК №117, Постановление №1119); Национальные стандарты (ГОСТ Р 56939-2024, ГОСТ Р 59547-2021, ГОСТ Р ИСО/МЭК 27006-2020); Специализированные стандарты аудита (МСА 315, СГА 305).

Документационная архитектура аудита ИС включает четыре категории источников доказательств: организационно-распорядительную документацию, техническую документацию, эксплуатационные журналы и регистры, а также отчетные документы предыдущих аудитов.

Дальнейшее развитие методологии аудита информационных систем в РФ должно быть направлено на:

- гармонизацию национальных стандартов с актуальными версиями ISO/IEC 27001:2022 и ISO/IEC 27006-1:2024;
- разработку отраслевых методик аудита (здравоохранение, финансы, транспорт);
- внедрение риск-ориентированного подхода к определению объема документационного тестирования.

Список литературы

1. Приказ ФСТЭК России от 11.04.2025 № 117 «Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» // ФСТЭК России: официальный сайт. – 2025. – П. 14. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-utverzhdeny-prikazom-fstek-rossii-ot-11-aprelya-2025-g-n-117 (дата обращения: 21.02.2026).

2. ПНС 1.0.079-1.120.25 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. Часть 1. Общие положения» (проект) // ГАРАНТ.РУ: информационно-правовой портал. – 2025. – URL: https://www.garant.ru/ (дата обращения: 21.02.2026)

3. Приказ Минфина России от 09.01.2019 № 2н «О введении в действие международных стандартов аудита на территории Российской Федерации и о признании утратившими силу некоторых приказов Министерства финансов Российской Федерации» (ред. от 16.10.2023) // КонсультантПлюс: некоммерческая интернет-версия. – URL: https://www.consultant.ru/document/cons_doc_LAW_317185/ (дата обращения: 21.02.2026).

4. ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»: дата введения 2022-06-01 // Электронный фонд правовых и нормативно-технических документов. – URL: https://docs.cntd.ru/document/1200181890 (дата обращения: 21.02.2026).

5. СГА 305 «Аудит федеральных информационных систем и проектов»: утв. постановлением Коллегии Счетной палаты РФ от 23.12.2016 № 11ПК: ред. от 28.12.2018. Приложение № 1. Перечень законодательных и иных нормативных правовых актов Российской Федерации в сфере информационных технологий и защиты информации // СудАкт: интернет-ресурс «Судебные и нормативные акты РФ». – URL: https://sudact.ru/law/sga-305-standart-vneshnego-gosudarstvennogo-audita-kontrolia/sga-305/1/ (дата обращения: 21.02.2026).

6. Международный стандарт аудита 315 (пересмотренный, 2019) «Выявление и оценка рисков существенного искажения»: введен в действие на территории РФ приказом Минфина России от 27.10.2021 № 163н // КонсультантПлюс: некоммерческая интернет-версия. – 2023. – П. 13–14. – URL: https://www.consultant.ru/document/cons_doc_LAW_404880/ (дата обращения: 21.02.2026).

7. ГОСТ Р ИСО/МЭК 27006-2020 «Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности»: утв. приказом Росстандарта от 08.09.2020 № 628-ст: дата введения 2021-07-01 // Электронный фонд правовых и нормативно-технических документов – 2020. – URL: https://docs.cntd.ru/document/1200175373 (дата обращения: 21.02.2026).