

|  |  |
| --- | --- |
| ИССАИ 5300 | Международные стандарты высших органов аудита (ИССАИ) издаются Международной организацией высших органов аудита (ИНТОСАИ). Для получения дополнительной информации см. веб-сайт *www.issai.org* |

ИНТОСАИ

***Руководство по аудиту ИТ***

***Июнь 2016***

**ИССАИ 5300: Руководство по аудиту ИТ**

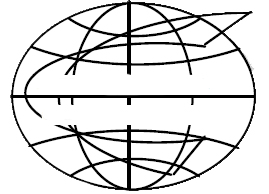
|  |
| --- |
| **Комитет по профессиональным стандартам ИНТОСАИ** |

**Секретариат Комитета по профессиональным стандартам**

Rigsrevisionen • Landgreven 4 • Абонентский почтовый ящик 9009 • 1022 Копенгаген K • Дания (P.O. Box 9009 • 1022 Copenhagen K • Denmark)

Тел.: +45 3392 8400 • Факс: +45 3311 0415 • E mail: info@rigsrevisionen.dk

ИНТОСАИ



ОПЫТ ВЗАИМОДЕЙСТВИЯ

ДЛЯ ВСЕОБЩЕГО БЛАГА

Генеральный секретариат ИНТОСАИ – RECHNUNGSHOF

(Счетная палата Австрийской Республики)

DAMPFSCHIFFSTRASSE 2

А-1033 ВЕНА

АВСТРИЯ

Тел. ++43 (1) 711 71 • Факс: ++43 (1) 718 09 69

АДРЕС ЭЛЕКТРОННОЙ ПОЧТЫ: intosai@rechnungshof.gv.at;

САЙТ ВО ВСЕМИРНОЙ СЕТИ: http://www.intosai.org

Содержание

[ПРЕДИСЛОВИЕ 6](#_Toc468720132)

[A. СТРУКТУРА ПРОВЕДЕНИЯ АУДИТА ИТ 7](#_Toc468720133)

[1. Полномочия и сфера применения стандарта ИССАИ 5300 7](#_Toc468720134)

[2. Введение в процедуру проведения Аудита ИТ 7](#_Toc468720135)

[3. Определение Аудита ИТ 7](#_Toc468720136)

[4. Мандат на проведение Аудитов ИТ 8](#_Toc468720137)

[B. ОБЩИЕ ТРЕБОВАНИЯ, ОТНОСЯЩИЕСЯ ТОЛЬКО К АУДИТАМ ИТ 8](#_Toc468720138)

[5. Риск-ориентированный подход к проведению Аудита ИТ 8](#_Toc468720139)

[6. Существенность 10](#_Toc468720140)

[7. Документация 10](#_Toc468720141)

[8. Компетентность 12](#_Toc468720142)

[C. ТРЕБОВАНИЯ К ПРОЦЕССУ АУДИТА ИТ 12](#_Toc468720143)

[9. Планирование Аудита ИТ 12](#_Toc468720144)

[10. Стратегическое планирование аудита ИТ I 13](#_Toc468720145)

[11. Годовое планирование аудита ИТ 14](#_Toc468720146)

[12. Групповой уровень планирования Аудита ИТ по выбранному аудиту 14](#_Toc468720147)

[13. Проведение надлежащей выборки для Аудита ИТ 16](#_Toc468720148)

[14. Цели аудита ИТ 16](#_Toc468720149)

[15. Область Аудита ИТ 19](#_Toc468720150)

[16. Возможности ВОА по проведению аудитов ИТ 20](#_Toc468720151)

[17. Распределение ресурсов 21](#_Toc468720152)

[18. Привлечение сторонних ресурсов 21](#_Toc468720153)

[19. Взаимодействие с организацией, подлежащей проверке 22](#_Toc468720154)

[20. Аудиторское доказательство 22](#_Toc468720155)

[21. Проведение аудита - Сбор аудиторских доказательств 23](#_Toc468720156)

[22. Надзор и анализ 24](#_Toc468720157)

[23. Случаи мошенничества, коррупции и прочих нарушений 25](#_Toc468720158)

[24. Ограничения 25](#_Toc468720159)

[25. Мониторинг исполнения аудиторских рекомендаций 25](#_Toc468720160)

[D. ТЕХНИЧЕСКИЕ ПРИЕМЫ И ИНСТРУМЕНТЫ АУДИТА ИТ 26](#_Toc468720161)

[26. Определение специализированных методов для проведения Аудита ИТ 26](#_Toc468720162)

[27. Методы планирования 26](#_Toc468720163)

[28. Методы проведения аудита 26](#_Toc468720164)

[29. Выбор надлежащей системы для хранения информации 28](#_Toc468720165)

[30. Требование к Инструментам Аудита ИТ: 28](#_Toc468720166)

[E. ОТЧЕТНОСТЬ 30](#_Toc468720167)

[31. Требования к отчетности по Аудиту ИТ 31](#_Toc468720168)

[32. Содержание и форма Отчета по Аудиту ИТ 31](#_Toc468720169)

[Приложение А - Методы анализа данных 33](#_Toc468720170)

ПРЕДИСЛОВИЕ

Стандарты ИССАИ серий 5300-5399 относятся к Руководству по аудиту информационных технологий в рамках деятельности ИССАИ. Стандарт ИССАИ 5300, первый из серии ИССАИ 5300, содержит всеобъемлющие общие принципы ИССАИ по основополагающим вопросам аудита ИТ. В нем указываются общие принципы, подход и методология проведения Аудитов ИТ.

Стандарт ИССАИ 5300 также разработан для ВОА в качестве руководства по проведению Аудитов ИТ, разработке новых возможностей проведения Аудита ИТ и использования ограниченных ресурсов Аудита ИТ для предоставления проходящим аудит организациям, государственным органам и физическим лицам страны гарантии добросовестности, надежности и эффективности использования ресурсов при реализации ИТ.

Стандарт ИССАИ 5300 разработан ИССАИ путем проведения анализа действующих стандартов, связанных с Аудитами ИТ/Аудитами информационных систем, стандартов по информационным системам, национальных и международных стандартов проведения аудита, в частности, существующих стандартов ИССАИ. Еще одной особенностью ИССАИ 5300 является обеспечение надлежащей связи/соотношения основы Аудита ИТ с различными формами аудита, установленными на уровне 3 ИССАИ.

Кроме того, являясь рекомендацией уровня 4, материалы настоящего стандарта ИССАИ разделены на две категории: **Требования,** имеющие основное значение для проведения качественного Аудита ИТ, и **Пояснения**, дающие общие разъяснения требований. Это сделано для того, чтобы обеспечить основную функцию ИССАИ по предоставлению общего вспомогательного руководства, как предусмотрено в рамках деятельности ИССАИ.

Стандарт ИССАИ 5300 также учитывает уровни развития Информационных систем в государственном секторе и уровни разработки процедур Аудита ИТ в различных ВОА.

Стандарт ИССАИ основан на следующих подтемах:

1. Структура проведения Аудита ИТ
2. Общие требования, относящиеся только к Аудиту ИТ
3. Требования, относящиеся к Процедуре Аудита ИТ
4. Технические приемы и инструменты Аудита ИТ
5. Требования к отчетности по Аудиту ИТ.

Стандарт включает отдельное приложение по Анализу данных.

Стандарт ИССАИ является основой для разработки последующих стандартов серии 5300-5399 и/или специальных рекомендаций по отдельным вопросам, так как в нем излагаются темы, имеющие особую актуальность для сообщества ИТОСАИ в области Аудита ИТ.

Стандарт ИССАИ составлен проектной группой, в которую входили представители Бразилии, Индии (руководитель проектной группы), Индонезии, Японии, Польши и США.

1. СТРУКТУРА ПРОВЕДЕНИЯ АУДИТА ИТ
2. Полномочия и сфера применения стандарта ИССАИ 5300
   1. Стандарт ИССАИ 5300 предусматривает комплексную структуру для проведения Аудита ИТ в рамках деятельности ИССАИ.
   2. Структура, изложенная в настоящем стандарте ИССАИ, соответствует Основополагающим принципам аудита государственного сектора (ISSAI 100), Основополагающим принципам финансового аудита (ISSAI 200), Основополагающим принципам аудита эффективности (ISSAI 300), Основополагающим принципам аудита соответствия (ISSAI 400).
   3. Стандарт ИССАИ содержит требования к осуществлению профессиональной практики при проведении Аудита ИТ, сопровождающиеся пояснениями для обеспечения большей ясности и облегчения понимания стандарта.
   4. Требования содержат информацию, необходимую для обеспечения высокого качества проведения Аудита ИТ. Они поясняют аудиторам их обязанности, а заинтересованным лицам - содержание процесса Аудита ИТ, проводимого ВОА.
   5. В сопровождающих требования объяснениях дается более подробное описание того, что означает то или иное требование и на какие сферы оно распространяется.
   6. Стандарт ИССАИ подготовлен Проектной группой, в которую вошли представители Японии, Польши, Индонезии, Индии, США и Бразилии.
3. Введение в процедуру проведения Аудита ИТ
   1. Государственные организации с возрастающей активностью переходят на Информационно-коммуникационные технологии (ИКТ) в осуществлении своих функций и предоставлении различных услуг. Такие системы ИКТ часто называют также «Информационные системы» (ИС) или «Системы информационных технологий» (ИТ).
   2. Высшие органы аудита (ВОА) имеют полномочия проводить аудиторские проверки Правительства и правительственных органов на основании соответствующих аудиторских мандатов.[[1]](#footnote-1)
   3. Это позволяет ВОА обеспечивать эффективность, подотчетность, результативность и прозрачность сферы государственного управления.[[2]](#footnote-2)
   4. Непрерывное развитие Информационно-коммуникационных технологий предоставляет возможность получать, хранить, обрабатывать и предоставлять информацию в электронной форме. Такой переход к электронной обработке информации вызвал принципиальные изменения в условиях работы ВОА. Наряду с этим увеличиваются государственные расходы в сфере ИТ. Таким образом, ВОА не могут обойтись без развития надлежащих возможностей проведения Аудитов ИТ.
4. Определение Аудита ИТ
   1. Аудит ИТ определяется следующим образом:

«Проверка и анализ систем ИТ и сопутствующих средств контроля для подтверждения соблюдения или выявления нарушений принципов законности, эффективности, экономичности и результативности систем ИТ и сопутствующих средств контроля».

* 1. Таким образом, Аудит ИТ[[3]](#footnote-3) является широким понятием, которое тесно связано с Финансовым аудитом[[4]](#footnote-4) (оценкой правильности и соответствия другим предпосылкам подготовки финансовой отчетности организации), Аудитом соответствия[[5]](#footnote-5) (оценкой системы внутреннего контроля) и Аудитом эффективности [[6]](#footnote-6)(оценкой соответствия Систем ИТ потребностям пользователей и отсутствия возникновения в связи с ними ненужных рисков). Однако в некоторых обстоятельствах аудиторская проверка может быть направлена только на ИТ-компонент системы.

1. Мандат на проведение Аудитов ИТ
   1. Мандат ВОА на проведение Аудитов ИТ основан на общем мандате ВОА на проведение аудитов.[[7]](#footnote-7) Некоторые ВОА могут получать отдельные мандаты на проведение Аудитов ИТ или Аудитов ИТ систем.
   2. Для многих ВОА полномочия на проведение Финансовых аудитов, Аудитов эффективности и Аудитов соответствия являются достаточными для проведения Аудитов ИТ. Это связано с тем, что ИТ системы обеспечивают основную деятельность организации и могут включать финансовые системы. Таким образом, для проведения Аудитов ИТ не обязательно требуется получение специальных полномочий.
   3. При предоставлении отдельный мандат должен учитывать юрисдикцию проведения аудита ИТ систем, которые используются организацией для решения функциональных задач. Также он должен предусматривать предоставление организацией своевременного, беспрепятственного, прямого и свободного доступа ко всем необходимым документам и информации[[8]](#footnote-8), хранящимся на бумаге или в электронной форме, независимо от того, насколько указанная функция или ее часть выполняется собственными силами или с привлечением сторонних исполнителей.
   4. Мандат ВОА на проведение Аудита ИТ должен соответствовать принципам ИССАИ уровней 1 и 2.
2. ОБЩИЕ ТРЕБОВАНИЯ, ОТНОСЯЩИЕСЯ ТОЛЬКО К АУДИТАМ ИТ
3. Риск-ориентированный подход к проведению Аудита ИТ

**Требование:**

**При применении риск-ориентированного подхода ИТ Аудитор должен учитывать риски Аудита ИТ**.

**Аудит ИТ должен проводиться на основе риск-ориентированного подхода**

**Пояснение:**

* 1. Риск-ориентированный подход предусматривает выявление элементов риска[[9]](#footnote-9) в проверяемой организации, а также их потенциальных последствий, определяя таким образом приоритетные области проведения проверки.
  2. Рисками при проведении аудита организации являются Неотъемлемый риск, Риск контроля и Риск необнаружения. Элементы риска выявляются на основе трех указанных рисков. В совокупности три риска составляют так называемый Аудиторский риск.
  3. Неотъемлемые риски - это риски, присущие системе, которые могут отразиться на исполнении функции, порученной организации в рамках ее компетенции. Анонимность пользователей является неотъемлемым риском Системы ИТ, особенно в сетевой среде. Чтобы реагировать на неотъемлемые риски, организации должны применять меры контроля. В некоторых случаях организация может даже принять риски как таковые без проведения мероприятий по их контролю, если последствия таких рисков оцениваются как несущественные и находящиеся на допустимом уровне риска.
  4. Риски контроля - это риски возможной неэффективности мер контроля. В таких случаях могут возникать существенные ошибки, которые должны выявляться максимально оперативно. ИТ системы неизменно реагируют на них с применением Средств контроля приложений[[10]](#footnote-10) и Общих средств контроля[[11]](#footnote-11). Именно от надежности таких средств контроля зависит выполнение функции организации/ Системы ИТ. Отказ или неэффективность средств контроля создает ситуацию возникновения Рисков контроля.
  5. Риск необнаружения при проведении Аудита ИТ - это риск не обнаружить отсутствия или сбоя в работе средств контроля ИТ и сопутствующих средств контроля, что может привести к нарушению нормального функционирования Системы ИТ.
  6. На выбор ВОА предлагается множество способов и методик оценки рисков. Они варьируются от простой классификации профиля рисков Систем ИТ на высокие, средние и низкие, по заключению аудиторов ИТ ВОА, до сложных, имеющих научный характер расчетов для определения количественного показателя риска систем ИТ.[[12]](#footnote-12)

1. Существенность

**Требование:**

**ВОА должны учитывать существенность на всех этапах процесса аудита ИТ.**

**Пояснение:**

* 1. Аудиторы ИТ должны учитывать существенность на протяжении всего процесса аудита (ИТ). Соображения существенности влияют на решения, относящиеся к характеру, сроку и рамкам процедур проверки, а также оценке результатов аудита. Соображения могут включать в себя беспокоящие заинтересованные стороны вопросы, общественные интересы, нормативные требования и последствия для общества.[[13]](#footnote-13)
  2. Существенность относится ко всем аспектам аудитов эффективности, таким как выбор темы, определение критериев, оценка доказательств и документации, а также управление рисками в случае получения несоответствующих или малозначительных результатов аудиторских исследований или отчетов.
  3. Вопрос существенности Аудита ИТ должен решаться в общих рамках определения существенности для ВОА. Перспектива существенности может варьироваться в зависимости от характера аудита ИТ. Материальность аудитов государственного сектора, эффективности и соответствия, частью которых является Аудит ИТ, рассматривается в стандартах ИССАИ 200, 300 и 400[[14]](#footnote-14).
  4. Существенность и риск

Оценка риска при проведении аудита ИТ неразрывно связана с требованиями к существенности соответствующих аудитов. Существенность несоответствия требованиям оценивается на основе способности соответствующих пользователей влиять на решения. При высоком уровне неотъемлемых рисков неисполнение может иметь существенное значение по причине возможности накопления последствий такого несоответствия. При высоком уровне риска контроля (что означает отсутствие/нарушение функционирования необходимых средств контроля выявленных рисков) даже незначительное несоблюдение требований может иметь существенное значение также по причине возможности накопления последствий такого несоответствия.

* 1. Аудиторы ИТ не всегда имеют возможность проверки всех случаев/модулей или систем с учетом ограничений и себестоимости проведения проверки. В такой ситуации Аудиторы ИТ могут оценить существенность и провести аудиторскую выборку для более подробной проверки с целью составления обоснованного аудиторского заключения. Также можно использовать инструменты ИТ при проведении различных видов выборки. Размер выборки определяется уровнями Неотъемлемых рисков и Рисков контроля. Чем выше уровень Неотъемлемого риска или Риска контроля, тем больше размер выборки.

1. Документация

**Требование:**

**ВОА обеспечивает ведение достаточного объема документации по процессу Аудита ИТ и его результатам, для того чтобы любой опытный Аудитор ИТ, не имеющий отношение к данному Аудиту, мог воспроизвести весь процесс.**

**Аудитор подготавливает аудиторскую документацию, которая по полноте и детализации дает общее представление о процессе проведения данного аудита.**

**Анализ документации должен обеспечивать любому аудитору ИТ возможность сделать такие же выводы по его результатам.**

**Пояснение:**

* 1. Общие требования к документации по Аудиту ИТ определяются на Уровне 3 ИССАИ - Стандарты ИССАИ 100, 200, 300 и 400. Эти положения в той же мере относятся и к Аудиту ИТ. Однако характер Аудита ИТ может предусматривать внесение определенных корректировок в порядок составления документов.
  2. Функция оформления документов в процессе Аудита ИТ состоит в том, чтобы обеспечивать понимание планирования и исполнения аудиторской проверки, выбор мер, которые должны приниматься по результатам и выводам Аудита и составление рекомендаций по результатам проверки. Документация должна иметь достаточную степень детализации, чтобы дать возможность опытному аудитору ИТ, не имеющему предварительных сведений о проверке, понять характер, сроки, предмет и результаты процедур, выполненных в соответствии со стандартами ИССАИ, национальными стандартами, а также действующими законодательными и нормативными требованиями. Подтверждения аудиторских заключений и рекомендаций, обоснование всех существенных вопросов, требующих вынесения профессионального суждения и связанные с ними выводы, должны быть оформлены документально в понятной для опытного аудитора форме. Документация должна быть достоверной и не вызывать разногласий по содержанию с проходящей проверку организацией.
  3. Документация в процессе Аудита ИТ имеет существенное значение для отображения каждого этапа аудита и каждого результата или их соотнесения с исполнением или неисполнением конкретных требований действующих стандартов или нормативных положений.
  4. Как и при проведении любого аудита, если результат Аудита ИТ не соответствует общему аудиторскому заключению по существенному вопросу или имеются разногласия с проходящей проверку организацией по аудиторскому заключению, Аудитор ИТ должен документально оформить порядок устранения такого несоответствия и/или урегулирования противоречия.
  5. Формат документации по Аудиту ИТ

Документация по Аудиту ИТ предусматривает оформление бумажных документов и создание электронных шаблонов для записи информации по аудируемой Системе ИТ, внесения сведений о встречах с Руководством и совещаниях группы аудита, результатов аудиторской проверки, подтверждений аудиторских выводов. ИССАИ не предусматривает стандарта оформления документации по Аудиту ИТ. Кроме того, форматы документов могут быть различными в зависимости от конкретного ВОА. Отдельные ВОА могут устанавливать определенный уровень стандартизации по составлению контрольных перечней, образцов писем, организации документооборота и пр.

* 1. Хранение документации по Аудиту ИТ

Документация по Аудиту ИТ может сохраняться и быть защищенной от внесения изменений и несанкционированного удаления. ВОА могут разрабатывать новые стандарты хранения документации по аудиту ИТ или адаптировать действующие стандарты с учетом выполнения требований по хранению документации по Аудиту ИТ. Период обеспеченного таким образом хранения составляет часть мандата отдельных ВОА и нормативного положения, регулирующего их деятельность.

Особое внимание следует уделять носителям, формату, сроку действия и требованиям к хранению таких данных для обеспечения их считываемости в течение срока, установленного ВОА в отношении хранения соответствующих данных и правил архивирования. Это может предусматривать конвертацию данных из одного формата в другой, чтобы соответствовать техническому прогрессу и предотвращать старение данных.

1. Компетентность

**Требование:**

**ВОА должны обеспечивать, чтобы в состав группы аудита входили участники, которые в совокупности обладают компетентностью для проведения Аудита ИТ в соответствии с установленными стандартами**.

**Пояснение:**

* 1. Необходимые знания, профессиональные навыки и компетентность могут приобретаться в процессе профессионального обучения, путем привлечения сторонних ресурсов в соответствии со стратегическим планом ВОА.

1. ТРЕБОВАНИЯ К ПРОЦЕССУ АУДИТА ИТ
2. Планирование Аудита ИТ

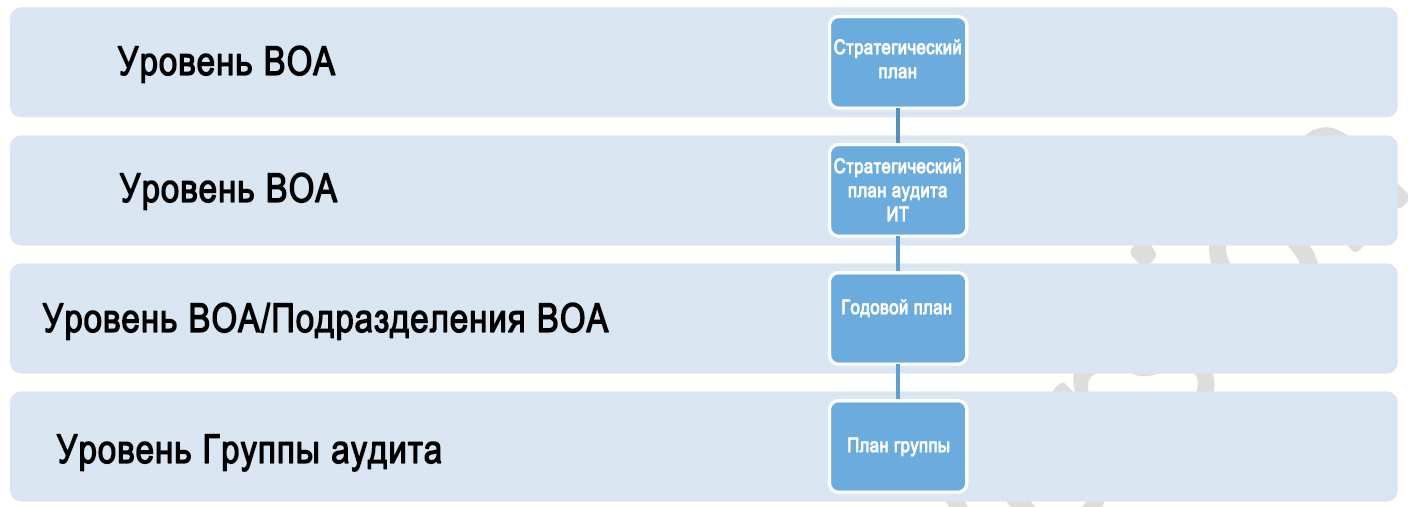
**Требование:**

**Планирование Аудита ИТ осуществляется ВОА на основе оценки рисков.**

**Пояснение:**

* 1. Планирование ВОА процесса Аудита ИТ может осуществляться в соответствии с законодательными мандатами, законодательными/исполнительными заявками или по собственной инициативе.
  2. Планирование аудита в рамках ВОА на основе Оценки рисков

ВОА могут планировать проведение аудита на основе выборки по результатам оценки риска. В данном процессе ВОА определяют приоритетность и проводят отбор аудиторских проверок, которые должны проводиться на основе оценки рисков. Планирование риск-ориентированного Аудита ИТ может осуществляться на трех уровнях: Стратегическом, Ежегодном и Групповом в рамках общего Стратегического плана ВОА. Однако ВОА могут выбрать использование одного или сочетание большего числа уровней с учетом доступных ресурсов и требований к аудиту на основе анализа рисков.



**Рисунок 1: СТАНДАРТНАЯ ИЕРАРХИЯ ПЛАНИРОВАНИЯ АУДИТА ДЛЯ ВОА**

1. Стратегическое планирование аудита ИТ

**Требование:**

**Стратегический план ВОА должен включать элементы, относящиеся к Аудиту ИТ и соответствующим потребностям.**

**ВОА разрабатывает Стратегический план Аудита ИТ в соответствии с общим Стратегическим планом аудита.**

**Пояснение:**

* 1. Стратегический план Аудита ИТ включает цели и задачи проведения аудита систем ИТ в государственных организациях в рамках юрисдикции ВОА. План разрабатывается на период 3-5 лет и отражает последние достижения в сфере ИТ и их внедрении в деятельность государственных организаций. Стратегический план проведения аудита Систем ИТ должен быть согласован с общим Стратегическим планом ВОА.
  2. ВОА формулируют цели по обеспечению прозрачности, отчетности и надлежащего управления в рамках разработки политики общего видения, миссии и декларации ценностных ориентиров. Стратегический план или цели могут включать вопросы Институционального развития, Развития организационной системы, Развития профессионального потенциала по мере необходимости в качестве мер достижения стратегических целей. В целях Аудита ИТ ВОА могут проводить оценку своей среды путем опросов, взаимодействия с проходящими проверку организациями, оценку направлений и развития технологических решений и их внедрения в проверяемых организациях, а также любых иных законодательных или обязательных требований.
  3. На данном этапе актуальным является определение среды аудиторской проверки. ВОА могут определить приоритеты аудита по результатам оценки среды и всей совокупности аудита и выделить свои собственные Стратегические цели и задачи. Для достижения общих целей при наличии ограниченных средств и ресурсов ВОА должны включить в стратегический план реализации выявление потребностей, связанных с организационным развитием, что предусматривает наличие у ВОА действующих полномочий и правовых оснований ВОА для проведения Аудита ИТ, развитие организационной системы для создания систем и процедур ВОА для проведения Аудита ИТ, а также развитие профессионального потенциала для приобретения необходимых навыков и возможностей в целях проведения Аудита ИТ.
  4. Планирование аудита на основе оценки рисков

Планирование аудита на основе оценки рисков предусматривает оценку элементов рисков, которые могут оказать воздействие на актуальность аудита и достоверность аудиторских выводов по результатам проверки. Оценка рисков на уровне Стратегического планирования Аудита ИТ касается вопросов релевантности Аудитов ИТ к общей стратегической цели ВОА по обеспечению надлежащего управления, прозрачности и подотчетности в процессе управления.

* 1. ВОА проводят периодический анализ и пересмотр Стратегического плана в отношении целей обеспечения прозрачности, подотчетности и участия в надлежащем управлении.
  2. При решении вопросов, связанных со Стратегическим планированием, ВОА могут ссылаться на стандарты ИССАИ, в частности, на стандарт ИССАИ 100 «Основополагающие принципы аудита государственного сектора».

1. Годовое планирование аудита ИТ

**Требование:**

**Годовой план Аудита ИТ должен быть согласован со Стратегическим планом Аудита ИТ**.

**В Годовой план Аудита ИТ включаются важные вопросы, предусмотренные в Стратегическом плате Аудита ИТ в порядке из значимости, определенном путем оценки рисков.**

**Пояснение:**

* 1. ВОА должны обеспечивать согласование Годового плана Аудита ИТ со стратегическим планом Аудита ИТ. На стадии планирования производится выбор Системы ИТ или организации для проведения аудита.
  2. В рамках Стратегического плана Аудита ИТ ВОА может использовать риск-ориентированный подход для определения приоритетов и актуальных тем. Это предусматривает создание и использование перечня подлежащих проверке организаций/систем ИТ по ключевым критериям выполнения оценки рисков. В перечне может также быть указана вся совокупность аудита, определенная на Стадии стратегического планирования, но с указанием конкретных сведений и характеристик по типам Систем ИТ/организаций, которые используются в оценке их профиля риска. Разработанная ВОА структура оценки рисков может впоследствии быть использована при завершении аудиторской выборки.
  3. Наряду с риск-ориентированным подходом к выбору объектов аудита ВОА должны проводить аудиты в соответствии с требованиями закона или по запросу надзорных органов (Конгресса, Парламента и пр.) или руководящих лиц.

1. Групповой уровень планирования Аудита ИТ по выбранному аудиту

**Требование:**

**Групповой план Аудита ИТ должен быть согласован с Оценкой риска в рамках Годового плана ИТ**.

**Групповой уровень плана Аудита ИТ предусматривает вопросы, связанные с основными областями риска, выявленными в Годовом плане Аудита ИТ, и включает подробную программу проведения аудита.**

**Пояснение:**

* 1. Данный уровень предусматривает разработку детальной программы аудита, начиная с постановки задач проведения выбранного Аудита ИТ.
  2. Обязательным условием разработки программы аудита является четкое понимание проверяемой организации, ее Информационных систем и деятельности, связанной с ИТ.
  3. Объем знаний об организации и ее процессах, необходимый Аудиторам ИТ, определяется характером организации и степенью детализации выполняемых аудиторских работ. Необходимо определить задачи или цели реализации системы ИТ. Знания об организации должны учитывать коммерческие, финансовые и неотъемлемые риски, присущие организации и ее Системам ИТ. Кроме того, это предусматривает объем привлечения организацией сторонних исполнителей для выполнения своих задач, а также, в целом, отражение бизнес-процессов в среде ИТ[[15]](#footnote-15). Аудитор должен использовать такую информацию для выявления потенциальных проблем, формулирования задач и объема работ, выполнения работ и учета действий руководства, которые аудиторы ИТ должны предусмотреть.
  4. В рамках риск-ориентированного подхода Риски контроля будут соотноситься с такими элементами Общих средств контроля ИТ и Средств контроля приложений. Чем выше Риски контроля, тем актуальнее потребность в проведении дополнительных тестов на существенность.
  5. Как правило, аудиторов ИТ привлекают для тестирования технологических средств контроля, а аудиторы, не связанные с ИТ, проводят тестирование финансовых и регулятивных средств контроля и контроля за соответствием. Роль аудитора заключается в том, чтобы определить потенциальные коммерческие и ИТ риски проверяемой организации и оценить адекватность используемых средств целям контроля. При проверке общих средств контроля ИТ аудитору важно учитывать различные категории и варианты применения таких средств, оценить степень надзора руководства и информированности сотрудников о таких средствах и выяснить, насколько эффективными являются средства контроля для выполнения предусмотренной функции. Даже в небольших организациях, не использующих сложных информационных систем и бизнес-процессов для составления финансовой отчетности, эти элементы играют значительную роль[[16]](#footnote-16). Неэффективность средств контроля существенно снижает надежность средств контроля, связанных с отдельными приложениями ИТ[[17]](#footnote-17). Аудиторам ИТ важно понимать соотношение функции приложения и соответствующих рабочих процессов. Аудиторы ИТ должны выявлять все операции входа, обработки, совершаемые приложением, и операции на создаваемом им выходе. Точное представление о воздействии мастер-данных на операции входа, обработки и выхода и обеспечение их безопасности может помочь Аудиторам ИТ при оценке соответствия системы ИТ требованиям точности, полноты, целостности, конфиденциальности, доступности, надежности, релевантности и соответствия данных на всех этапах обработки информации: накопления данных, их обработки и представления/вывода информации.
  6. На основе понимания Информационной системы и проверяемой организации Аудиторы ИТ могут выбирать метод проведения Аудита ИТ. Аудит ИТ, в результате, предусматривает проверку Управления ИТ, Общих средств контроля ИТ и Средств контроля приложений ИТ или сочетания этих составляющих.

1. Проведение надлежащей выборки для Аудита ИТ

Аудиторская выборка[[18]](#footnote-18) определяется как применение процедур проверки к менее чем 100% элементам в рамках совокупности релевантности аудита таким образом, что все элементы выборки можно было бы выбрать для обеспечения аудитора разумной основой для составления выводов о совокупности в целом. Это также относится к выборке в рамках Аудита ИТ. Кроме того, при планировании аудиторской выборки аудитор учитывает цель процедуры проверки и характеристики совокупности, из которой осуществляется выборка, а также методики и инструменты, используемые для проведения выборки, и их анализ.

Аудитор определяет размер выборки, достаточный для снижения риска выборки до приемлемо низкого уровня. Аудитор выбирает элементы для выборки таким образом, чтобы можно выбрать любой элемент выборки из всей их совокупности. Проведение аудитов в среде ИКТ может потребовать анализа 100% совокупности, особенно на этапе предварительной оценки (см. Раздел 21 ниже). Но при этом выборка может потребоваться для проведения теста на существенность (Раздел 21 ниже) или детальной проверки. Аудиторы ИТ могут использовать рекомендации ИССАИ 1530 или иные разработанные процедуры, применяемые ВОА для проведения выборки.[[19]](#footnote-19)

1. Цели аудита ИТ

**Требование:**

**Цели Аудита ИТ должны быть согласованы с Областями рисков, выявленными на Групповом уровне планирования Аудита ИТ, в зависимости от типа подхода к проведению аудита - Финансового аудита, Аудита эффективности или соответствия.**

**Пояснение:**

* 1. Целями Аудита ИТ является проверка сочетаемости процессов ИТ и ресурсов ИТ для выполнения поставленных задач организации в целях обеспечения Эффективности, Результативности и Экономичности операций в соответствии с существующими правилами и требованиями сбалансированности рисков.
  2. Таким образом, Аудит ИТ может проводиться в отношении комплексной Системы ИТ или по отдельным направлениям, таким как Безопасность ИТ, Приобретение бизнес-решения, Общие средства контроля ИТ, Средства контроля приложений или иным направлениям, указанным в Руководствах для РГАИТ.
  3. Область Аудита ИТ пересекается с Финансовым аудитом, Аудитом соответствия или Аудитом эффективности. Аудит ИТ может сопровождать три указанных вида проверок, выполняться в рамках любой из них или в сочетании с ними, т.е. Финансовый аудит, Аудит соответствия и Аудит эффективности.[[20]](#footnote-20)
  4. Цели Финансового аудита

Определение Финансового аудита [[21]](#footnote-21) включает вопросы конфиденциальности, подготовки финансовой отчетности в соответствии с требованиями структуры финансовой отчетности и ее представления в соответствии с целесообразными требованиями существенности. Это предполагает целый ряд задач по обеспечению гарантии соответствия финансовой системы структуре учета при подготовке финансовой отчетности и представлению финансовых результатов без существенных ошибок. Таким образом, Система ИТ должна отражать все требования к подготовке финансовой отчетности, т.е. сбору финансовой информации, применению основных требований, обработке информации, соблюдению установленного формата. В целом, указанные вопросы относятся к Средствам контроля приложений операций на Входе, Выходе и при Обработке. Тем не менее, Средства контроля приложений зависят от наличия надлежащей поддержки со стороны Общих средств контроля ИТ и Управления ИТ. Таким образом, для завершения аудиторской проверки Финансовые аудиторы должны подтвердить гарантию адекватности Системы ИТ и соответствующих средств контроля. Факты подтверждения гарантии системы ИТ должны выявляться в процессе Аудита ИТ системы при рассмотрении всех аспектов Управления ИТ, Общих средств контроля ИТ и Средств контроля приложений ИТ.

Если гарантия подтверждается в рамках полноценного Аудита ИТ, проведение Аудита ИТ в процессе каждого финансового аудита по той же системе может не потребоваться при наличии гарантий отсутствия изменений и нарушений функционирования системы в течение периода с момента проведения последнего Аудита ИТ.

* 1. Цели Аудита соответствия

Аудит соответствия является независимой оценкой того, соответствует ли конкретный предмет рассмотрения действующим требованиям властей, определенным в качестве критериев. Аудит соответствия выполняется посредством получения оценки соответствия деятельности, финансовых сделок и информации во всех материальных отношениях требованиям властей, регулирующих деятельность проверяемой организации.

Целью аудита соответствия в государственном секторе, таким образом, является предоставление ВОА возможности оценки соответствия деятельности учреждений государственного сектора требованиям авторитетных источников, регулирующих деятельность этих учреждений. Это подразумевает предоставление отчетности о степени соответствия учреждения установленным критериям. Аудит ИТ позволяет проводить такие оценки по автоматизированным системам. Аудит соответствия может быть связан с правильностью (соблюдение формальных критериев, таких как соответствующие законы, положения и соглашения) или с правильным поведением (соблюдением общих правил по эффективному финансовому управлению и правил поведения государственных служащих). «Правильность» - это то, на что нацелен аудит соответствия, а «правильное поведение» рассматривается в контексте государственного сектора, где существуют определенные ожидания относительно управления финансами и поведения организаций и должностных лиц государственного сектора. В силу вышеизложенного, в зависимости от мандата ВОА, охват аудита может включать аспекты проверки правильного поведения[[22]](#footnote-22).

Цели и особенности аудита соответствия определяют необходимость соответствия надлежащим процессам, требованиям единообразия и правильности. Система ИТ в государственном секторе также должна соответствовать действующим требованиям законов и нормативно-правовых актов, стандартов и рекомендаций, принятых организацией. Для составления аудиторского заключения аудиторы ИТ должны проверить соответствие Системы ИТ таким нормативным требованиям, стандартам, рекомендациям и различным параметрам эффективности организации. Все такие оценки проводятся по установленным критериям, составленным на основе правил, законов, стандартов, критериев эффективности или даже собственных требований. Оценка соответствия в отношении Управления ИТ предусматривает проверку гарантий на механизмы для обеспечения выполнения и периодического мониторинга функций управления, а также проверку эффективности работы механизма внутреннего контроля и надлежащей реализации всех установленных правил ИС. Оценка соответствия в отношении Общих средств контроля ИТ предусматривает оценку наличия средств контроля с проведением надлежащего мониторинга и принятием мер по снижению рисков, а также соблюдения установленных стандартов и параметров эффективности организации. Оценка Средств контроля приложений ИТ предусматривает проверку наличия отражения бизнес-процессов и правил в системе ИТ, а также средств контроля операций входа, обработки и выхода, связанных с проверкой достоверности, полноты, точности данных и надежности процессов.

Аудит соответствия неизбежно потребует применения Компьютеризированных методов аудита (CAAT) для анализа информации и определения исключений.

* 1. Цели Аудита эффективности

Аудит эффективности является независимым, объективным и надежным изучением того, работают ли правительственные предприятия, системы, процессы, программы, мероприятия или организации в соответствии с принципами экономичности, эффективности и результативности, и есть ли резервы для улучшения.

Аудиторы ИТ проводят проверку реализуемых систем ИТ по критериям экономичности, результативности, эффективности и ценности для граждан.

Проверка экономичности реализации ИТ систем предусматривает минимизацию ресурсных затрат в течение срока действия Системы ИТ, т.е. с момента приобретения системы в течение периода ее эксплуатации. При привлечении сторонних ресурсов для выполнения каких-либо функций расходы на такое привлечение должны быть минимизированы. Лучшим способом минимизировать такие затраты является изучение и освоение рынка. Однако неточное определение требований пользователей по причине отсутствия достоверного представления о них в самой организации может помешать применению таких мер и увеличить затраты. Оценка возможности выполнения функций, переданных на исполнение, собственными силами и средствами может стать показателем неэкономичного использования ресурсов. При проведении Аудита эффективности приобретений ИТ Аудиторы ИТ должны обращать особое внимание на ограничения организации или процесса приобретения, в зависимости от обстоятельств.

Проверка эффективности реализации ИТ систем предусматривает оценку максимально возможного использования ресурсов или минимизации неэффективного использования ресурсов при обеспечении количества (полноты), качества (точности и надежности) и своевременности (доступности) результатов. Аудиторы ИТ могут выявить признаки неэффективности при наличии дублирования процессов, ненадлежащих простоев процессов и лишних процедур проверки, встроенных в систему.

Проверка результативности реализации Систем ИТ предусматривает установление факта соответствия установленным задачам, что, помимо прочего, должно соответствовать общим целям и задачам организации. Отсутствие достижения целей организации с использованием Системы ИТ может быть признаком неэффективного использования Системы ИТ.

Аудит эффективности также способствует обеспечению подотчетности и прозрачности. Аудит эффективности фокусируется на областях, которые могут дать еще большую отдачу для граждан и которые имеют наибольший потенциал для улучшения. Он предоставляет конструктивные стимулы, побуждающие ответственные стороны совершать соответствующие действия. Внедрение ИТ - новая инициатива для большинства государственных и правительственных органов. По своей сути аудит эффективности в рамках Аудита ИТ для конструктивного продвижения системы управления на основе Систем ИТ должен стать основой методов, применяемых Аудиторами ИТ. Замеченные недостатки должны быть выявлены таким образом, чтобы не уничтожать инициативу, а стимулировать усовершенствование системы.

* 1. Аудиторы ИТ могут быть привлечены к проведению аудита для применения инструментов СААТ. Условия привлечения в таком случае могут помочь в определении того, насколько оно может считаться Аудитом ИТ. Использование инструментов СААТ только для анализа данных не является Аудитом ИТ, поскольку в данном случае не проводится оценка Системы ИТ.

1. Область Аудита ИТ

**Требование:**

**Аудиторы ИТ определяют область аудита на стадии планирования для обеспечения реализации целей и задач аудита.**

**Пояснение:**

* 1. После определения целей Аудита ИТ Аудиторы должны также определить область аудита. Как правило для этого одновременно совершаются два действия. Определение области Аудита ИТ предусматривает определение объема проведения аудиторского исследования в отношении систем ИТ и их функциональности, подлежащих проверке Процессов ИТ, мест размещения Систем ИТ, подлежащих проверке, сроков проверки и видов аудита (Финансовый аудит/Аудит соответствия/Аудит эффективности). Фактически, это процесс обозначения или установления границ проведения аудита.
  2. Системы ИТ обеспечивают бизнес-функции организации и, как правило, используют определенные процессы ИТ, включая ввод данных в систему, запрос информации, создание отчетов. Большинство Систем ИТ и сопутствующее сетевое оборудование размещены в отдельных помещениях. Безопасность физического помещения и находящегося в нем оборудования может стать объектом аудита ИТ.
  3. Аудитор должен установить период проведения аудиторского анализа (т.е. проверка информации за один год, 3 года и т.д.), чтобы составить достоверное заключение по проведенной проверке. При проведении аудита Системы ИТ стандартный период проверки может устанавливаться в соответствии с требованиями конкретного аудита.
  4. Область аудита также может включать определенные области ИТ системы, которые являются актуальными для достижения Цели аудита ИТ. Типичными областями ИТ являются Управление ИТ, Разработки и приобретения, Операции ИТ, Аутсорсинг, Безопасность ИТ, План непрерывности деятельности и План работ в аварийной ситуации, Средства контроля приложений[[23]](#footnote-23). Данные элементы являются достаточными для любой Системы ИТ. Но поскольку сфера ИТ изменяется постоянно, Аудиторы ИТ не должны исключать возможности появления новых областей для проведения проверок, если это будет считаться целесообразным.[[24]](#footnote-24) Комплексный Аудит ИТ должен предусматривать проверку всех областей ИТ.
  5. Область аудита зависит от профиля риска проверяемой системы ИТ, а также от доступных ресурсов. При повышенных рисках область аудита может быть ограничена, но включать широкий спектр вопросов в рамках Аудита ИТ.

1. Возможности ВОА по проведению аудитов ИТ

**Требование:**

**ВОА должны иметь надлежащие возможности для проведения Аудита ИТ.**

**ВОА должны создать надлежащие возможности, если они не доступны, до начала проведения Аудита ИТ.**

**Пояснение:**

* 1. Проведение аудита является основной функцией ВОА, при этом в их распоряжении уже могут иметься возможности и средства для выполнения этой работы. Однако проведение аудита ИТ требует наличия особых возможностей и ресурсов. В совокупности группа по проведению Аудита ИТ должна обладать следующими возможностями:

1. Персонал, имеющий профессиональные навыки и подготовку в сфере ИТ
2. Понимание существующих правил и положений, а также среды, в которой действует система ИТ
3. Знание стандартов/рекомендаций, относящихся к Аудиту ИТ, применяемых ВОА
4. Знание методов ИТ по сбору аудиторских доказательств в автоматизированных системах
5. Знание актуальных Инструментов аудита ИТ для проведения сбора, анализа, предоставления результатов проверки и повторного выполнения проверяемых функций
6. Наличие надлежащей Инфраструктуры ИТ для сбора аудиторских доказательств и их сохранения
7. Наличие надлежащих Инструментов аудита ИТ для анализа собранных доказательств
8. Распределение ресурсов

**Требование:**

**ВОА должны определять и распределять надлежащие и компетентные ресурсы для проведения Аудита ИТ.**

**Пояснение:**

* 1. ВОА могут использовать различные варианты распределения ресурсов для проведения Аудита ИТ.
  2. Самым распространенным методом является наличие централизованной группы, включающей специалистов или экспертов в сфере ИТ, которые оказывают содействие другим сотрудникам при проведении Аудитов ИТ. ВОА имеют возможность эффективно использовать профессиональную квалификацию нескольких сотрудников для проведения Аудитов ИТ, если они только начинают заниматься этой деятельностью.
  3. Другим вариантом является комплектация штата специалистов ИТ в каждой соответствующей группе ВОА. Но если каждая группа проводит небольшое количество аудитов, то это может рассматриваться как неэффективное использование Специалистов ИТ. По мере увеличения количества Аудитов ИТ ВОА могут организовать специализированную группу или отдел Аудита ИТ. Такая группа полностью обеспечивает проведение Аудитов ИТ по инициативе ВОА.
  4. Группа ИТ может взаимодействовать с другими группами в составе ВОА, которые уже имеют сведения о проверяемой организации, что позволяет ей оперативно получать информацию о целях организации и соотносить бизнес-процессы с обеспечивающей их Системой ИТ для более эффективного проведения Аудита ИТ.

1. Привлечение сторонних ресурсов

**Требование:**

**ВОА могут рассматривать возможность привлечения сторонних ресурсов для проведения Аудита ИТ при отсутствии достаточных внутренних возможностей**.

**Пояснение:**

* 1. При недостаточности собственных ресурсов ВОА вправе использовать сторонние ресурсы при проведении Аудита ИТ или поручать проведение ИТ группе исполнителей. Такими ресурсами являются, в основном, внешние консультанты или подрядчики, имеющие навыки работы с методами и инструментами Аудита ИТ, включая базы данных, программное обеспечение и прочие аспекты Аудита ИТ. Ресурсы также включают наличие инфраструктуры ИТ, необходимой ВОА для проведения аудитов. В основном, это те же ресурсы, которые используются при проведении любого другого аудита, однако, Аудит ИТ может предусматривать необходимость специального анализа, конвертации данных и наличие инструментов хранения.
  2. В отношении работы сторонних исполнителей по поручению ВОА должен проводиться надлежащий контроль на основании документально оформленного контракта или договора о предоставлении услуг, заключенного ВОА. Проведение работ и предоставление ее результатов ВОА должно осуществляться в соответствии с действующими процедурами и стандартами, принятыми ВОА. Это означает, что ВОА, в любом случае, потребуется наличие квалифицированного штатного персонала для контроля выполнения работ при привлечении ВОА внешних исполнителей.

1. Взаимодействие с организацией, подлежащей проверке

**Требование:**

**ВОА осуществляют взаимодействие с проверяемой организацией до начала аудита.**

**Пояснение:**

* 1. Как и при проведении любого аудита, проверяемая организация должна быть ознакомлена с объемом и целями проверки, при этом критерии оценки должны быть согласованы с ней по мере необходимости. В случае необходимости ВОА вправе направить проверяемой организации письмо о намерениях с указанием условий взаимодействия сторон.
  2. Особенность проведения Аудита ИТ заключается в том, что ВОА должна обеспечить надлежащее содействие со стороны проверяемой организации для выполнения аудита, включая получение доступа к учетным записям и информации, а также согласование получения электронных данных в формате, необходимом для проведения анализа.

1. Аудиторское доказательство

**Требование:**

**ВОА обеспечивает достаточность, надежность и точность аудиторских доказательств, подтверждающих аудиторское заключение.**

**Аудиторские доказательства предоставляются для воссоздания и анализа процесса аудита после его завершения.**

**Пояснение:**

* 1. Аудиторское доказательство - это сбор данных, записей, документов и информации, полученных Аудиторами ИТ для обоснования своих выводов, представленных соответствующим заинтересованным лицам в соответствующие сроки (в момент проведения аудита или впоследствии), которые должны быть достаточными, надежными и точными.
  2. Как таковое, доказательство должно соответствовать критериям достаточности, надежности и точности/достоверности в соответствии с внутренними стандартами обеспечения качества ВОА.
  3. Доказательство в рамках аудита ИТ должно быть надлежащим образом получено и сохранено, чтобы обеспечить его доступность в будущем без изменения данных. Аудиторы ИТ должны обеспечить наличие в доказательствах временных отметок [[25]](#footnote-25)изменений в каждом случае, когда возникает риск изменения доказательства.
  4. Аудиты ИТ предусматривают различные возможности для идентификации, сбора, хранения и архивации доказательств. Доказательства могут быть получены при проведении специальных тестов на выборке, по которой проводится проверка. Аудиторы ИТ могут выполнять тесты по всем транзакциям или выборкам по мере необходимости, но электронные данные могут всегда тестироваться по определенному критерию в полном объеме. Однако обоснование исключений может выполняться выборочно по образцам при большом количестве исключений. Выборка для аудита может осуществляться произвольно или на систематической основе. Может использоваться монетарная выборка или выборка на основе решения Аудиторов ИТ.
  5. Специальные методы и инструменты для сбора аудиторских доказательств в рамках Аудитов ИТ рассматриваются ниже в Разделе D.

1. Проведение аудита - Сбор аудиторских доказательств

**Требование:**

**Аудитор ИТ обеспечивает сбор надлежащих и достаточных доказательств, их анализ для обеспечения выполнения задач и целей аудита.**

**Пояснение:**

* 1. Предварительная оценка средств контроля ИТ

Аудиторы ИТ должны провести предварительную оценку Средств контроля ИТ в проверяемой системе для подтверждения гарантии, что существующие средства контроля ИТ (Общие средства контроля и Средства контроля приложений) являются надежными и эксплуатируются в рамках надлежащей системы Управления ИТ. Оценка средств контроля на данном уровне предусматривает:

1. Оценку наличия и эффективности соответствующих механизмов Управления ИТ.
2. Оценку соответствия целей ИТ и Целей бизнеса.
3. Оценку наличия надлежащих механизмов для:
4. Эффективного управления проектом ИТ
5. Приобретения и разработки решения ИТ (включая приложение ИТ, аппаратное и программное обеспечение, кадровые ресурсы, сеть, сервисные решения и пр.)
6. Эксплуатации систем ИТ
7. Обеспечения информационной безопасности
8. Обеспечения непрерывности деятельности и реагирования на аварийные ситуации
9. Обеспечения надлежащего управления изменениями
10. Обеспечения предоставления услуг и обратной связи
11. Обеспечения соответствия установленным правилам, нормативным актам, процедурам путем мониторинга и контроля.

Указанное выше, за исключением п. (vii), составляет Общие средства контроля ИТ, не настроенные на отдельные потоки операций или приложений, а обслуживающие общую инфраструктуру ИТ, включая связанные с ИТ политики, процедуры и практику, а также контроль операций центра данных (политика и стандарты ИТ), приобретение и обслуживание системного ПО, безопасность доступа (физическая и логическая), распределение обязанностей, обеспечение непрерывности деятельности и контроль действий в аварийных ситуациях, разработку и техническое обслуживание системы приложений.

Дополнением к оценке Общих средств контроля ИТ является знание бизнес-процессов и их отражение в системе ИТ и сопутствующих средствах контроля ИТ приложений.

Исключения, определенные после предварительной оценки, являются основанием для принятия решений о проведении теста на существенность системы ИТ и средств контроля.

* 1. Тест на существенность

Проведение тестов на существенность предусматривает детальное тестирование Средств контроля ИТ аналогично процессу предварительной оценки с использованием различных методик и инструментов для запроса, извлечения и анализа данных. При тестировании на существенность тесты разрабатываются для обоснования допущений в соответствии с целями аудита. Тесты должны быть разработаны с использованием методов[[26]](#footnote-26), указанных в Разделе D.

1. Надзор и анализ

**Требование:**

**ВОА обеспечивают регулярный надзор и анализ аудитов ИТ.**

**Пояснение:**

* 1. При проведении аудита Руководитель группы должен осуществлять надлежащий надзор за работой группы, а также анализ документально оформленной работы, выполненной Группой аудита ИТ (Элемент 5 - «Выполнение аудита и прочих работ», ИССАИ 40). Руководитель группы аудиторов должен обладать надлежащей компетентностью для осуществления функций руководства, наставничества и управления при проведении аудитов.

1. Случаи мошенничества, коррупции и прочих нарушений

**Требование:**

**ВОА и Аудиторы ИТ должны выявлять и оценивать риски мошенничества, актуальные для целей аудита ИТ**.

**ВОА совершает надлежащие действия по мере необходимости и в рамках требований действующего законодательства для реагирования в случаях мошенничества, коррупции и прочих нарушений.**

**Пояснение:**

* 1. При проведении Аудита ИТ аудиторы могут столкнуться со случаями мошенничества, коррупции и связанных с ними нарушений. Требования по отчетности о мошенничестве могут стать предметом особых положений аудиторского мандата или соответствующих законов или нормативных актов, и от аудитора может потребоваться информировать о таких вопросах стороны за пределами объекта аудита, такие как регулирующие и правоохранительные органы. В такой ситуации ВОА должны принимать надлежащие меры, установленные в мандатах и действующем законодательстве.
  2. Они должны сохранять отношение профессионального скептицизма и быть бдительными в случае вероятного мошенничества в ходе проведения аудита.

1. Ограничения

**Требование:**

**ВОА должны определять, указывать ограничения и уведомлять о них на каждой стадии проведения аудита на соответствующем уровне.**

**Пояснение:**

* 1. Ограничения в рамках Аудита ИТ указываются на каждом этапе проведения проверки на соответствующих уровнях путем направления документально оформленных сообщений.
  2. Ограничения по Аудиту ИТ также должны быть указаны в отчете.
  3. Стандартными ограничениями являются отсутствие надлежащего доступа к данным и информации, отсутствие необходимой документации по процессу компьютеризации, использование Аудиторами ИТ собственных методов расследования и анализа для составления заключения. В отчете также должны быть точно указаны любые иные ограничения, возникающие в работе Аудиторов ИТ.

1. Мониторинг исполнения аудиторских рекомендаций

**Требование:**

**ВОА должны проводить мониторинг исполнения аудиторских рекомендаций по вопросам, указанным в отчете как актуальные для сферы ИТ.**

**Пояснение:**

* 1. ВОА участвуют в последующем контроле действий, предпринятых ответственной стороной в ответ на вопросы, поставленные в отчете о результате проверки. Такой мониторинг должен быть направлен на эффективное решение организацией указанных в отчете вопросов, включая более широкий контекст, например, при использовании одной системы ИТ несколькими государственными организациями; недостаточные или неудовлетворительные действия объекта аудита могут стать основанием для составления нового отчета ВОА.

1. ТЕХНИЧЕСКИЕ ПРИЕМЫ И ИНСТРУМЕНТЫ АУДИТА ИТ

**Требование:**

**ВОА должны использовать надлежащие методы проведения Аудита ИТ, соответствующие характеру участия в аудите и требованиям целей аудита.**

**Пояснение:**

1. Определение специализированных методов для проведения Аудита ИТ
   1. Методы проведения аудита ИТ относятся к использованию методик и процедур для исследования контрольной среды системы ИТ, сбора и анализа доказательств для получения гарантии адекватности средств контроля.
2. Методы планирования
   1. При планировании аудита системы ИТ аудитор должен, прежде всего, знать порядок взаимодействия конкретного приложения и бизнес-процессов объекта аудита. В этих целях необходимо получить базовую информацию об использовании системы для осуществлении основной деятельности. Традиционные методы проведения аудита, включая изучение документов, опросы ключевых сотрудников (ответственных за бизнес-процессы и сотрудников организации ИТ) и наблюдение процедур, являются полезными для общего понимания принципов взаимодействия системы и деятельности организации. Изучение правил и процедур ИТ, пользовательских руководств в сфере ИТ, документации по договорам ИТ аутсорсинга, документов по функциональной структуре, технических инструкций поставщика, перечня отчетов (стандартных и специализированных) помогает лучше узнать среду, в которой работает система, и выявить коммерческие риски, возникающие вследствие сбоя средств контроля.
   2. На этапах годового и группового планирования аудита ИТ проводятся оценки рисков систем ИТ, разработанных или используемых различными объектами аудита. Этот процесс можно объективно провести с использованием методов, представленных в разделе «Планирование» настоящего Стандарта.
3. Методы проведения аудита
   1. Выбор методов имеет принципиальное значение при проведении тестирования на соответствие и существенность. При тестировании на существенность тесты разрабатываются для обоснования допущений в соответствии с целями аудита. Тесты должны разрабатываться на основе применения одного метода или большего их числа[[27]](#footnote-27), например, Опросы, Анкетирование, Наблюдение, Сквозные проверки, составление Технологических схем, Сбор и анализ данных, Проверка достоверности, Повторные вычисления, Повторная обработка, Подтверждение со стороны третьих лиц и пр.
   2. Для оценки адекватности общих компьютерных средств контроля, которые применяются в сфере управления ИТ, разработки и приобретения систем, операций ИТ, Информационной безопасности, планирования непрерывности деятельности, применяются те же методы, что и для других видов аудита.
   3. Методы, специально разработанные для Аудита ИТ, в основном используются для оценки средств контроля приложений ИТ. При тестировании средств контроля приложений аудитор должен:
4. Определить важные компоненты приложения и объем потока информации через систему, получить правильное представление о приложении путем анализа доступной документации и опроса соответствующих сотрудников.
5. Определить риски средств контроля приложения и их последствия путем анализа критичности бизнес-процессов, с которыми взаимодействует сегмент приложения.
6. Разработать стратегию тестирования для выявления сильных и слабых сторон средств контроля и оценки воздействия последних.
   1. Для лучшего понимания проверяемой системы, включая ее ключевые контрольные точки, и разработки применяемой стратегии тестирования важно ознакомиться с сопутствующей документацией, включая функциональные спецификации, документы по управлению изменениями с момента первого запуска или последнего аудита, руководствами для пользователей, техническими инструкциями поставщиков и пр.
   2. Стратегия тестирования также зависит от таких факторов, как подвергающиеся риску активы, срок эксплуатации приложения, обеспечивающего деятельность, качество внутренней системы контроля, чувствительность операций, основные изменения бизнес-процессов, вызывающие изменения приложения, результаты предыдущих аудитов, если они проводились.
   3. Для оценки Разделения обязанностей и входной авторизации необходимо ознакомиться с должностными инструкциями, сопоставить их с привилегиями, предоставляемыми системой, рассмотреть процедуры авторизации, подтвердить наличие журналов регистрации операций по аккаунтам пользователей, имеющих привилегии администратора. Общий отчет об операциях должен быть проверен на наличие доказательств его анализа руководством.
   4. В каждой проверяемой организации используется индивидуальное сочетание аппаратного и программного обеспечения, операционных систем, систем управления базами данных, ПО приложений, сетевого ПО и пр. Для проведения необходимого анализа приложения ИТ Аудиторы ИТ должны иметь возможность сбора информации по всем этим источникам. Важным условием для извлечения данных является знание Системы ИТ и базы данных организации, включая действующие бизнес-процессы, их значение для организации, используемые протоколы и пр. Тестирование на существенность в отношении адекватности средств контроля приложений предусматривает:
7. Извлечение соответствующих бизнес-данных организации
8. Трансформацию и загрузку данных в инструмент
9. Проведение анализа данных
10. Проверку достоверности результатов тестирования
11. Составление аудиторских заключений

Указанные процедуры могут выполняться аудиторами ИТ с использованием методов, указанных в Приложении А.

1. Выбор надлежащей системы для хранения информации
   1. Аудитор ИТ должен обеспечивать сохранение результатов и доказательств аудита для выполнения требований надежности, полноты, достаточности и достоверности. Также Аудитор ИТ должен обеспечить хранение информации по процедурам аудита, чтобы иметь возможность впоследствии провести проверку их достоверности. Это предусматривает использование надлежащих методов документального оформления, которые будут рассмотрены ниже.
   2. Использование вывода данных по мере возможности должно осуществляться при наличии сопроводительного письма. Если это невозможно, следует создать внутренние документы с указанием важных сведений, например, даты передачи информации, имени файла, из которого произведен сброс данных,[[28]](#footnote-28) а также сведений о происхождении данных из производственной или иной среды. Электронные доказательства, созданные и используемые для составления аудиторского отчета, должны быть связаны с такими документами.
   3. Аудитор ИТ должен определить целесообразность использования указанных выше методов и обеспечить их целостность и эффективность. Применение любого из указанных методов не должно отражаться на целостности системы приложения и данных в проверяемой организации.
2. Требование к Инструментам Аудита ИТ:

ВОА предоставляет целесообразные инструменты Аудита ИТ с учетом оценки рисков при проведении аудита, а также возможностей и ресурсов, имеющихся в распоряжении ВОА.

Пояснение:

* 1. Проведение аудита ИТ требует наличия знаний процессов и методов, а также профессиональных навыков использования инструментов Аудита ИТ для проведения таких проверок, умения работать с информацией, которая хранится и обрабатывается в электронной форме, при отсутствии внешне различимого аудиторского следа.
  2. Компьютерные методы проведения аудита (СААТ) - это инструменты ИТ, которые помогают Аудитору при проведении различных автоматизированных тестов для оценки системы ИТ или данных, и являются исключительно эффективными для работы с большими объемами данных в электронном формате. Методы СААТ используются также для тестирования средств контроля и проведения тестов на существенность в Финансовом аудите, Аудите соответствия и Аудите эффективности. Использование СААТ и сфера их применения определяются различными факторами на стадиях планирования и проведения аудита.
  3. Практическая ценность инструментов СААТ:

Инструменты СААТ очень эффективны для осуществления таких действий в рамках Аудита ИТ, как Анализ журнала пользователей, составление Отчетов об исключениях, Подведение итогов, Сравнение файлов, Стратификация, Выборка, Проверка дубликатов, Выявление просчетов, Старение, Расчет виртуальных полей и пр. (более подробная информация об этих элементах указана в разделе о методах Аудита ИТ). Использование инструментов СААТ предоставляет множество преимуществ по сравнению с ручной проверкой. Вот лишь некоторые из них:

1. Тестирование на существенность, анализ больших объемов данных проводятся за короткие сроки со значительно меньшими затратами труда
2. Тесты могут проводиться повторно по различным файлам/данным
3. Могут создаваться гибкие и комплексные тесты путем изменения параметров
4. Предоставляется возможность автоматизации документального оформления тестов и результатов аудита
5. Более эффективное применение ресурсов аудита
   1. Выбор инструментов СААТ при проведении Аудита ИТ: Применение СААТ связано с определенными расходами на лицензионное ПО, совместимое компьютерное оборудование, привлечение квалифицированного персонала. Таким образом, при решении вопроса об использовании инструментов СААТ для Аудита ИТ необходимо учесть следующие важные факторы:
6. Насколько инструменты СААТ увеличивают ценность аудита?
7. Насколько вероятно повторное использование тестов при проведении других/будущих аудитов по тем же или другим организациям, имеющим сходный характер деятельности или операций?
8. Насколько обработка операций производится в режиме онлайн/реального времени?
9. Насколько дороже по затратам средств и времени может обойтись использование других методов аудита?
   1. Ниже представлены некоторые самые известные примеры инструментов СААТ:

* Аудиторские программные продукты общего назначения разработаны для удовлетворения специальных требований аудиторов и содержат стандартные тесты, выполняемые аудиторами в рамках аудита ИТ, включая общие функции: извлечение данных, подведение итогов, старение, стратификация, проверка дублирующих элементов и пр.
* Язык структурированных запросов (SQL) - это язык, не ориентированный на процедуры и используемый для определения и манипулирования данными в Системах управления реляционными базами данных (СУБД).
* Крупноформатные таблицы также являются полезными инструментами СААТ и могут использоваться для проведения простых запросов, включая извлечение данных в соответствии с заранее заданными критериями, сортировку, подведение итогов и пр.
* Инструменты для проведения интеллектуального анализа данных помогают в определении закономерностей в больших объемах данных и извлечении информации из таких комплектов данных, их трансформации в понятные структуры для последующего использования путем визуализации данных.
* Отраслевые аудиторские программы разрабатываются с целью обеспечения функциональных возможностей общего характера, относящихся к определенным отраслям, т.е. они предусматривают специфическую логику для создания аудиторских запросов и пр. Они часто применяются в отраслях с наличием развитой структуры документирования и установленными бизнес-процессами, включая банковскую отрасль, производство, нефтегазовую индустрию, транспортные перевозки и пр.
* Сервисные программы выполняют функции анализа, конфигурирования, оптимизации или технического обслуживания инфраструктуры ИКТ. Основными примерами сервисного ПО в сфере Аудита ИТ являются программы контроля и ревизии, программы отладки, программы для анализа дискового пространства, файл-менеджеры, сетевые сервисные программы, программы оптимизации профиля сети.
* Хорошо развитые системы имеют встроенные аудиторские модули (Специализированное аудиторское ПО) для создания стандартных и индивидуальных отчетов. Такие программы предоставляются в составе встроенных функциональных возможностей приложений по планированию ресурсов предприятия (ERP). Кроме того, существуют готовые программы, предоставляющие аудиторам ИТ доступ к данным ERP только для чтения через приложения в интерфейсе.
  1. Чтобы использовать инструменты СААТ в определенной области, аудитор должен провести тщательное планирование. Для проведения аудита с применением инструментов СААТ важно получить информацию/сведения о взаимодействии таблиц/файлов, триггерах/словарях баз данных, структуре записей, контрольных суммах, размере/формате данных, документации системы.

1. ОТЧЕТНОСТЬ

**Требование:**

**Отчеты Аудитора ИТ должны отражать результаты процесса Аудита ИТ в зависимости от их существенности для целей аудита.**

**Отчет по Аудиту ИТ должен быть комплексным, сбалансированным, убедительным, своевременным и удобным для чтения.**

**Пояснение:**

1. Требования к отчетности по Аудиту ИТ
   1. Поскольку Аудит ИТ может проводиться в рамках финансового аудита, аудита эффективности, аудита соответствия или сочетания указанных проверок, требования к отчетности по Аудиту ИТ должны, соответственно, учитывать требования Стандартов ИССАИ 100 - 400 и, в зависимости от характера проводимого аудита, ИССАИ 1700, 1705 и 1706 в случае Финансового аудита и, соответственно, уровня 4 ИССАИ по Аудиту соответствия и Аудиту эффективности.
   2. Аудиторы ИТ, в любом случае, должны принимать во внимание требования об ограниченном использовании технического жаргона, учитывать конфиденциальный характер представленной информации, например, паролей, имен пользователя, идентификационных данных, личной информации.
2. Содержание и форма Отчета по Аудиту ИТ
   1. Общий план отчета по Аудиту ИТ содержит следующие пункты:
3. Цели аудита
4. Объем аудита
5. Сроки проведения аудита
6. Критерии аудита
7. Методология аудита
8. Краткий обзор
9. Результаты аудиторских исследований
10. Аудиторские заключения
11. Рекомендации аудита
12. Любые сопутствующие пункты и риски, ограничения, оговорки, запреты, проблемы, которые возникают у Аудитора при проведении проверки.
    1. Несмотря на технический характер Аудита ИТ, Аудиторы должны обеспечивать, чтобы текст отчета был понятен руководству, сотрудникам проверяемой организации, заинтересованным лицам, широкому кругу лиц.
    2. Аудиторы ИТ могут обсудить проект отчета с руководством системы ИТ до его оформления и представления и указать свое мнение в отношении результатов, выводов и рекомендаций в окончательном отчете, если это применимо.
    3. Объект аудита может пойти на риск и не вносить корректировок в состояние, указанное в отчете, в связи с высокой стоимостью, сложностью действий по внесению таких корректив или по иным причинам. Такое положение должно быть отражено в отчете, направляемом ответственным руководителям в соответствии с внутренней структурой управления.
    4. Если между аудитором ИТ и объектом аудита возникают разногласия по конкретной рекомендации или комментарию аудитора, в приложении к отчету могут быть указаны позиции обеих сторон и причины разногласий. Позиция проверяемой организации может быть также изложена в основном тексте отчета или в сопроводительном письме.
    5. Аудиторы ИТ могут учитывать возможные негативные последствия отчета после публикации аудиторских отчетов ВОА. Так, если аудитор ИТ выявляет проблемы безопасности в системе ИТ и указывает их в отчете до устранения таких проблем, уязвимость системы ИТ становится общеизвестным фактом до проведения ремонтных работ. В таком случае ВОА может рассматривать возможность публикации отчета после устранения неисправности системы ИТ или указания уязвимости без каких-либо подробностей во избежание негативных последствий отчета.
    6. Завершением всего процесса Аудита ИТ является мониторинг принятия мер по результатам проверки. Он проводится для контроля успешного устранения всех недостатков, выявленных в ходе Аудита ИТ. Как правило, это результат выполнения ВОА непрерывной оценки риска. В рамках мониторинга принятия мер по указанным в отчете результатам Аудита ИТ Аудитор ИТ возобновляет аудит по истечении разумного периода времени для проверки надлежащего выполнения всех рекомендаций.

Приложение А - Методы анализа данных

* 1. **Извлечение соответствующих бизнес-данных организации:**

Понимание структуры данных на основе получения от проверяемой организации и изучения документов, определяющих данные. Если проверяемая организация предоставляет доступ только для чтения, данные, хранящиеся в таблицах, актуальных для проведения аудита, могут быть извлечены путем направления запроса в базу данных при наличии соответствующих навыков. В противном случае, организации может быть направлен запрос на предоставление копии соответствующих исходных данных. Данные могут быть получены в форме сброса базы данных, содержащей записи структуры таблицы и/или данных из БД, который проводится в форме списка установок SQL. Для импорта/анализа данных из копии извлеченных выведенных данных Аудиторам ИТ может понадобиться создание среды, аналогичной среде проверяемой организации (совместимые версии приложений БД, операционных систем, компьютерного оборудования и пр.). Во многих случаях это составляет самый важный аспект контрольной проверки приложения, поскольку правильное извлечение данных определяет эффективность всех последующих процессов. Для обеспечения удобства чтения и анализа Аудитору ИТ может также потребоваться конвертация данных из одного формата в другой.

* 1. **Трансформация и загрузка данных:**

Использование аудиторских программ и инструментов для извлечения, трансформации и загрузки данных (ETL) для импорта данных из различных платформ БД. Самые распространенные инструменты анализа данных (более подробную информацию о них см. в Разделе об инструментах) позволяют импортировать данные из различных БД в базовый формат крупноформатных таблиц инструмента. Такие инструменты используют мастер по импорту данных, который облегчает процесс импорта (интерпретации, конвертации, форматирования) данных для последующего анализа. Аудитор должен провести предварительное форматирование исходных данных для упрощения процесса анализа. Общее аудиторское программное обеспечение или специализированные сервисные программы также могут использоваться для оценки функционирования различных сервисных программ систем ИТ. Применение любых таких программ по отдельности или в сочетании зависит от целей аудита и объема предусмотренных работ.

* 1. **Проведение анализа данных**

Основные этапы анализа данных проверяемой организации для получения гарантии качества средств контроля приложений являются общими для любых форм анализа данных. Основными задачами анализа данных являются:

* определение цели анализа или проекта;
* знание изучаемого(ых) образца(ов);
* знание инструментов, используемых для сбора данных;
* понимание структуры и форматов данных[[29]](#footnote-29); и
* создание уникального идентификатора при необходимости совмещения или слияния.
* Аудиторы ИТ должны разработать:
* Перечень вопросов/Задачи исследования
* Методы ответов на вопросы исследования
* Критерии оценки
* Доказательства
* Анализ
* Заключение
* Процедуры реструктурирования файлов (создание синтаксиса и новых переменных по мере необходимости)
* Процедуры очистки данных (например, удаление резко отклоняющихся значений)

Основная часть анализа может проводиться в файле рабочих данных. В некоторых случаях может потребоваться трансформация комплектов первичных данных или особые вводные данные для соблюдения требований статистических программ или инструментов, которые использует аудитор.

* 1. **Знание видов данных и представление**

Анализ данных может проводиться в копии данных, полученных от проверяемой организации, чтобы сохранить оригинал для последующих подтверждений и анализа по мере необходимости.

Для проведения анализа информации может использоваться ПО общего назначения или Специализированное аудиторское ПО. Такие инструменты дают возможность не только импортировать, но и анализировать данные. При анализе данных также может использоваться Язык структурированных запросов. Информация по комплексным системам, включая ERP, указана в специализированных отчетах. Для проведения надлежащего анализа аудиторы должны ознакомиться с такими отчетами. Аудиторы ИТ должны проверить надежность, компетентность, целесообразность и достаточность полученных данных. По мере возможности, они должны иметь временные метки и быть надлежащим образом утвержденными проверяемой организацией. В частности, переменные в различных областях данных могут потребовать особого кодирования для представления различных данных.

* цифрового
* последовательного
* по дате и времени
* денежного

Отдельные методы анализа данных для проверки целостности приложений также зависят от целей аудита. Такими методами являются:

1. **Использование данных тестов:** Анализ на основе данных тестов проводится при тестировании качества программы. Исходным допущением является то, что надежность программы при прохождении серии специализированных тестов позволяет сделать общий вывод о ее надежности. Использование данных теста предусматривает Разработку данных теста и Создание данных теста для подключения программы на основе данных теста. Часто сам разработчик применяет этот метод на этапе тестирования приложения до ввода приложения или изменений к нему в эксплуатацию (т.е. живая транзакционная операция). При проверке недавно установленной системы ИТ или изменений в процессе управления аудитор может ознакомиться с проведенными процедурами на этапе тестирования.
2. **Сравнение кодов:** Разработчики используют методы сравнения кодов, которые предполагают проведение сравнения Исходного кода программы или изменений со стандартными методологиями разработки конкретного языка программирования с целью выявления программных ошибок, нарушений безопасности или соглашений по программированию. В основном, это инструменты для разработчиков, которые редко используются аудиторами ИТ. В отношении кодовых образцов, отобранных независимыми группами по тестированию безопасности, аудиторы устанавливают факт проверки кода на безопасность и документального оформления результатов, а также надлежащего устранения выявленных нарушений и слабых мест. Однако аудиторы, обладающие необходимыми навыками, могут использовать метод сравнения кодов в отношении управления изменениями или при первоначальном вводе в эксплуатацию программы приложения, если это предусмотрено объемом работ.
3. **Проверка целостности данных:** Проверка целостности данных предусматривает проведение серии тестов на существенность, проверяющих точность, полноту, последовательность и авторизацию данных, находящихся в системе. Такие тесты выявляют слабые места в средствах контроля операций ввода или обработки. Тестирование целостности данных помогает определить устойчивость реляционной целостности путем проверки программ валидации, встроенных в приложение при разработке требований входных условий и характеристик данных на этапе определения таблиц при разработке базы данных.

Такие тесты предусматривают использование определенных методов анализа данных, которые могут применяться Аудиторами ИТ при помощи инструментов общего анализа или общих аудиторских программ.

1. **Выборка:** Методы выборки помогают при составлении адекватных заключений на основе статистически достаточных проверок ограниченных данных. Аудиторы ИТ используют два основных метода выборки. Это Атрибутивная выборка и Изменяемая выборка. Атрибутивная выборка применяется для проведения тестирования на соответствие, составляется на основе наличия или отсутствия атрибута и обеспечивает выводы, выраженные показателем частоты возникновения. Изменяемая выборка применяется в тестировании на существенность, составляется на основе изменяемых характеристик совокупности и обеспечивает выводы по отклонениям от нормы.

При проверке валидации и иных средств контроля входных операций в системе, использующей большие объемы данных, аудитору может быть полезным составить случайную выборку записей операций, хранящихся в БД системы.

Большинство приложений для анализа данных, включая приложения крупноформатных таблиц и Аудиторское ПО общего применения, предусматривают использование простых функций для выбора определенных элементов данных (поле/колонка/строка) и сопутствующих ячеек данных для создания подмножеств объемов выбранных данных с использованием алгоритмов, основанных на случайных последовательностях номеров или простых формулах.

1. **Суммирование и стратификация:** Эти два метода позволяют профилировать данные до проведения тестирования средств контроля. Суммирование данных помогает при подсчете транзакций по определенным атрибутам, позволяя аудитору получить общее представление о совершенных операциях. Например, суммирование дебиторской задолженности по типам клиентов дает полезную информацию о высоком уровне невыплаты задолженностей. Очень полезной функцией, предусмотренной в крупноформатной таблице и аудиторских инструментах общего назначения, является сводная таблица. Она позволяет очень быстро обобщать информацию из больших таблиц.

Стратификация данных определяет плотность распределения данных по определенным корзинам или интервалам. Она дает важную информацию о характере данных и помогает определить области проведения детального тестирования.

1. **Условные запросы:** Метод извлечения данных на основе условных запросов полезен для проведения ряда проверок качества средств контроля приложений, предусматривающих тестирование полноты, целостности и правильности отражения бизнес-правил.
   1. Тестирование средств контроля входных операций: Например, в системе ИТ, обеспечивающей конкретные государственные программы образования/социальной помощи, необходимо создать записи о постоянных выгодоприобретателях в форме таблиц мастер-данных БД. В данном случае при тестировании средств контроля входных операций проводится извлечение образца мастер-записей, хранящихся в мастер-таблице, и проверка наличия в выбранных на основе связанных атрибутов данных (уникальные идентификаторы, имена, адреса, идентификаторы места положения) пропусков, бессмысленных значений, повторов и пр. Подтверждение таких ошибок означает наличие дефектов в описании данных при составлении таблицы.
   2. Тест средств контроля обработки: Для тестирования средств контроля обработки проводится специальный тест на существенность для определения надлежащего отражения определенного бизнес-правила в системе ИТ, которая используется для обработки. Например, в системе налогового департамента такой тест может проводиться для проверки надлежащего отражения в системе условий предоставления налоговой скидки. В данном случае извлечение записей может проводиться из выборки налоговых данных, составленной на условии моделирования правила в соответствии с законом. Результат такого извлечения, не соответствующий условию операции, может являться признаком ошибки средства контроля или ненадлежащего отражения бизнес-правила в системе. Такое ненадлежащее отражение приводит к постоянному возникновению ошибок, которые могут иметь существенные негативные последствия для финансов организации.

Аудиторы ИТ должны обладать глубокими знаниями соответствующих бизнес-правил организации для разработки эффективных условных запросов при проверке надлежащего отражения бизнес-правил в приложении.

* + 1. **Выявление повторов:** Общий тест на реляционную целостность данных в БД проводится для проверки наличия повторов, которые не должны существовать по логике определенных правил организации. Например, в базе данных по налогам или социальному страхованию соответствующая идентификация должна быть уникальной по закону. Подтверждение наличия дубликатов в этом поле данных является признаком ненадлежащей валидации входных данных и имеющихся данных, что приводит к возникновению операционных или финансовых рисков в проверяемой организации. Инструменты анализа предоставляют простые функции для выявления дублируемых ключей. Они могут появляться даже в таблицах операций, что повышает риск двойных платежей.

Аудиторы ИТ должны оценить необходимость проведения таких тестов в зависимости от наличия тестирования средств контроля приложения в рамках данного процесса. Например, если аудитор проверяет средства финансового контроля в приложениях в связи с обработкой дебиторской задолженности, возможность дублирования созданного системой номера заказа на покупку практически равна нулю. Однако, такой тест может использоваться, если аудитор проводит проверку средств контроля при подаче дублированных счетов поставщика (внешний ввод), который не является вводом, созданным системой.

* + 1. **Анализ просчета:** Цель использования данного метода заключается в проверке полноты и тестировании просчетов в цифровых данных, которые должны иметь последовательную нумерацию. В таблицах MS Excel это определяется путем серийной сортировки значений в соответствующем поле данных с добавлением расчетного поля на основе логики последовательности и фильтрации рядов, где возникают исключения. В аудиторских программах общего назначения используются простые опции выявления просчетов, если возникает необходимость выявления ошибок. Для использования функций поиска дубликатов или просчетов аудитору не обязательно обладать большим опытом запросов.
    2. **Работа с множественными файлами:** Исходные БД часто содержат большое количество операций и мастер-таблиц, чтобы провести необходимую нормализацию данных. При работе с импортированными данными полезно соединять определенные поля в одну таблицу при использовании согласованного ключа. Аудиторское ПО общего назначения позволяет объединять множественные файлы при помощи функции соединения. Применение в сводных таблицах функций согласования или условных запросов помогают аудитору оценить референциальную целостность между таблицами данных или даже между отдельными связанными приложениями, используемыми организацией.

Например, если организация регистрирует на своем портале потенциальных поставщиков и использует отдельное приложение по закупкам для привлечения заказов на покупку, бизнес-правила должны предусматривать наличие связи между базой данных поставщиков и базой данных закупок. Объединение таблиц из этих отдельных баз данных путем совмещения названий или идентификации поставщиков поможет определить эффективность взаимодействия между двумя связанными приложениями.

Для получения гарантий средств контроля приложений Аудиторы ИТ должны применять комбинированные методы.

1. ИССАИ 1, Лимская декларация [↑](#footnote-ref-1)
2. Резолюция Генеральной Ассамблеи Организации Объединенных Наций A/66/209 [↑](#footnote-ref-2)
3. Аудит ИТ также называется Аудит ИС, Аудит системы, Информационный аудит, Аудит информационной безопасности, анализ компьютерной гарантии, гарантия ИТ и пр. [↑](#footnote-ref-3)
4. ИССАИ 200 «Основополагающие принципы финансового аудита» [↑](#footnote-ref-4)
5. ИССАИ 400 «Основополагающие принципы аудита соответствия» [↑](#footnote-ref-5)
6. ИССАИ 300 «Основополагающие принципы аудита эффективности» [↑](#footnote-ref-6)
7. Принцип 3, ИССАИ 10 - Мексиканская декларация независимости ВОА и ИССАИ 100 - Основополагающие принципы аудита государственного сектора [↑](#footnote-ref-7)
8. Неограниченный доступ к учетным записям; Принцип 4, ИССАИ 10 - Мексиканская декларация о независимости ВОА [↑](#footnote-ref-8)
9. Элементы риска относятся к таким областям, как Управление ИТ, проектирование и разработка Системы, Использование собственных ресурсов или привлечение сторонних исполнителей, Операции, Безопасность ИТ, Мониторинг и Контроль. [↑](#footnote-ref-9)
10. Средства контроля приложений - это средства, встроенные в отдельное приложение и группу связанных приложений, составляющих систему приложений ИТ. К ним относятся средства контроля входных данных, обработки, выходных данных и основных данных, применяемые на этапах ввода, обработки и вывода данных системы ИТ. [↑](#footnote-ref-10)
11. Общие средства контроля - это средства контроля сопутствующих систем и процессов, поддерживающих систему приложений ИТ. Они относятся к обоснованию аудита эффективности системы ИТ, проектированию и разработке системы, слияниям, использованию собственных ресурсов/привлечению сторонних исполнителей, операциям (кроме средств контроля приложений), управлению кадрами, безопасности ИТ, мониторингу и пр. Общие средства контроля и средства контроля приложений являются неразрывно связанными, обеспечивая эффективное применение системы ИТ. Неэффективность средств контроля существенно снижает надежность средств контроля, связанных с отдельными приложениями ИТ. [↑](#footnote-ref-11)
12. Руководство по коммуникациям для высших органов аудита, составленное Рабочей группой по аудиту ИТ (РГАИТ) [↑](#footnote-ref-12)
13. ИССАИ 100 «Основополагающие принципы аудита государственного сектора» - п. 41 [↑](#footnote-ref-13)
14. ИССАИ 200 - «Основополагающие принципы финансового аудита», ИССАИ 300 - «Основополагающие принципы аудита эффективности», ИССАИ 400 - «Основополагающие принципы аудита соответствия» [↑](#footnote-ref-14)
15. Организации, переходящие с ручной среды на компьютерную, обычно проводят процедуры модернизации бизнес-процессов (МБП). Может возникать ситуация, когда некоторые бизнес-процессы по-прежнему выполняются вручную параллельно с использованием Систем ИТ. Такие ситуации представляют особый интерес для Аудиторов ИТ. [↑](#footnote-ref-15)
16. ИССАИ 1315 - «Выявление и оценка рисков существенного искажения на основе сведений об организации и ее среде» [↑](#footnote-ref-16)
17. Руководство по коммуникациям для высших органов аудита, составленное РГАИТ [↑](#footnote-ref-17)
18. ИССАИ 1530 «Финансовый аудит, аудиторская выборка» [↑](#footnote-ref-18)
19. ИССАИ 1530 «Финансовый аудит, аудиторская выборка», стр. 15. [↑](#footnote-ref-19)
20. ИССАИ 100 - «ВОА могут также проводить совмещенные проверки, включающие аспекты финансового аудита, аудита эффективности и/или соответствия». [↑](#footnote-ref-20)
21. ИССАИ 200 «Основополагающие принципы финансового аудита». [↑](#footnote-ref-21)
22. ИССАИ 400 «Основополагающие принципы аудита соответствия» [↑](#footnote-ref-22)
23. Руководство по коммуникациям для высших органов аудита, составленное Рабочей группой по аудиту ИТ (РГАИТ) [↑](#footnote-ref-23)
24. Глава 9 «Дополнительные актуальные темы», Руководство РГАИТ по аудиту информационных технологий для Высших органов аудита [↑](#footnote-ref-24)
25. Временная отметка - это данные, добавленные к информации (электронной, бумажной, видео и пр.) для отметки времени создания, получения или редактирования информации. Во временных отметках могут указываться различные параметры и сведения по мере необходимости (день, дата, часы, минуты, секунды, миллисекунды и пр.). [↑](#footnote-ref-25)
26. Методы могут использоваться для проведения тестирования на соответствие и на существенность. Для проведения двух оценок Аудитор ИТ может выбрать один из указанных методов или несколько. [↑](#footnote-ref-26)
27. Указанные методы могут использоваться для проведения предварительного тестирования и тестирования на существенность. Применение многих методов описано в Руководстве по коммуникациям для Высших органов аудита, составленное РГАИТ. [↑](#footnote-ref-27)
28. Сброс данных определяется как передача большого объема данных из одной системы или места размещения в другую систему или место [↑](#footnote-ref-28)
29. Это самый важный этап перед проведением анализа данных. Структура означает знание различных баз данных и хранящихся в них таблиц, используемых алгоритмов кодирования и взаимодействия между таблицами и БД. В этой связи знание различных моделей баз данных может оказаться очень полезным. [↑](#footnote-ref-29)