МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ
ДЛЯ ПОДГОТОВКИ ПРЕТЕНДЕНТОВ
К СДАЧЕ КВАЛИФИКАЦИОННОГО ЭКЗАМЕНА
НА II ЭТАПЕ

Информационные технологии в аудиторской деятельности: источники для подготовки и примеры заданий

Москва – 2021

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Настоящие методические материалы предназначены для подготовки претендентов к сдаче модулей второго этапа квалификационного экзамена, вступившего в действие 31 марта 2020 года.

Рассмотрены примеры использования информационных технологий в аудите, включая подходы к их решению, связанные:

- с получением аудиторских доказательств;
- коммуникациями в ходе аудита;
- проверкой данных бухгалтерской (финансовой) отчетности;
- аудиторскими рисками, возникающими при использовании информационных технологий, в том числе касающимися соблюдения законодательства в сфере ПОД/ФТ.

Экзаменационные задания (вопросы) на оценку ИТ-компетенций соответствуют действующей нормативно-правовой базе. Критерием их актуальности является применимость в аудиторских процедурах, что позволяет оценить уровень владения компетенциями, необходимыми при осуществлении (участии) в аудиторской деятельности в современных экономических условиях.

Для решения экзаменационных заданий (вопросов) потребуется знание рекомендованных источников для подготовки к сдаче экзамена, а также навыки участия в аудиторской деятельности.

Кроме того, понимая отсутствие публичных источников для подготовки, Единая аттестационная комиссия разработала и разместила на своем сайте примерные экзаменационные билеты и методические материалы, рассматривающие подходы к их решению и оцениванию.

1. НАИБОЛЕЕ ЗНАЧИМЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В АУДИТЕ

1.1. Востребованность IT-компетенций аудитора в современной экономике

Цифровая экономика начала активно развиваться в XX веке с развитием компьютерных технологий, позволивших более эффективно осуществлять финансово-хозяйственные операции в режиме «онлайн». Национальный проект «Цифровая экономика» со сроком реализации до 31 декабря 2024 года рассчитан на прорывное развитие цифровой экономики в России в интересах повышения конкурентоспособности страны и национальной безопасности. Цель России в перспективе 15–20 лет – войти в группу лидирующих экономик мира за счет цифровых преобразований традиционных отраслей и развития самостоятельной и конкурентоспособной цифровой индустрии.

Благодаря реализации Национального проекта «Цифровая экономика» доля бизнес-процессов в интернет-среде и цифровых транзакций растет с каждым годом. Успешность компании оценивается по способности генерировать инновации, а перспективы развития цифровых технологий в ближайшем будущем связаны с цифровыми активами. Все это меняет систему ценностных показателей хозяйствующих субъектов, подлежащих обязательному аудиту и пользователей сопутствующих аудиту услуг. Сегодня цифровая среда аудиторской деятельности неразрывно связана с бизнес-процессами, компьютерными технологиями, базами данных, позволяющими в интернет-среде взаимодействовать с компаниями, государственными структурами и правительственными органами, проводить цифровые транзакции между контрагентами.

Таким образом, IT- технологии в аудите и консалтинге и цифровизация бизнес-процессов сегодня относятся к обязательным профессиональным компетенциям аудитора, связаны с этикой и деловой репутацией аудиторов. Это подтверждают результаты анализа деятельности аудиторско-консалтинговых компаний, а также мнение экспертов и партнеров этих компаний.

Тенденции повышения уровня информационной технологичности аудита и изменения структуры консалтинговых услуг позволяют прогнозировать дальнейшую востребованность IT-компетенций аудиторов, что и нашло отражение в новом компетентностном, уровневом, модульном квалификационном экзамене на получение квалификационного аттестата

аудитора в Российской Федерации, разработанном на основе международных стандартов образования аудиторов в соответствии с Поручением Правительства Российской Федерации, под руководством Министерства финансов Российской Федерации и Совета по аудиторской деятельности.

1.2. Включение в экзамен наиболее значимых аспектов использования информационных технологий в аудите

Вопросы применения информационных технологий в аудиторской деятельности включены в профессиональный экзамен уже на первом этапе (базовом уровне экзамена). Для подготовки к сдаче первого этапа квалификационного экзамена Единой аттестационной комиссией разработаны и размещены на ее сайте Методические материалы «Использование информационных технологий в процессе сбора аудиторских доказательств. В них рассмотрены вопросы содержания тестов, нацеленных на оценку знания претендентами основных положений, связанных с нормативно-правовой базой, определяющей понятийным аппарат и основы регулирования использования информационных технологий в Российской Федерации. В отличие от базового уровня экзамена, следующий – второй этап (основной уровень), предполагает не только знание и понимание претендентом основ информационных технологий, но в большей степени ориентирован на оценку компетенций владения информационными технологиями на уровне «применение». Таким образом, одним из факторов успешной сдачи экзамена является наличие у претендента опыта работы в аудиторской деятельности, навыков работы с применением информационных технологий в ходе проверок бухгалтерской (финансовой) отчетности.

Для разработки экзаменационных заданий второго этапа экзамена привлекаются специалисты-практики, имеющие значительный опыт проведения аудиторских проверок. Специалисты разрабатывают сценарии задач, основываясь на актуальных аспектах аудиторских проверок. Затем разработанные задачи проходят несколько этапов экспертизы, в ходе которых оценивается сложность, адекватность и понятность описания ситуации, ее типичность, соответствие предлагаемого решения задачи собственной практике экспертов и т.д. Такая объемная по содержанию работа способствует формированию экзаменационных заданий практической направленности, ориентированных на реальную экономическую ситуацию, практику проведения аудиторских проверок и оказания иных видов аудиторских услуг.

Ситуации, разработанные для экзамена, могут быть крайне разнообразными, но в любом случае проверяются экспертами на наличие, если можно так сказать «типичности» решения в аудиторской практике. Так, например, в задания не включаются вопросы, подразумевающие спорность или неоднозначность решения, или требующих знания процесса обработки информации в какой-то конкретной специальной компьютерной программе, к которой у претендента может и не быть доступа и т.д. Однако, обычно эксперты соглашаются с заданиями, связанными с использованием баз данных и открытых информационных источников (сайты ФНС, картотека арбитражных дел и т.д.), а также общими вопросами обработки информации в программе Excel и т.д. Таким образом, уровень оцениваемых знаний претендента в области информационных технологий определяется потребностями профессиональной деятельности.

Например, уровень владения навыками тестирования надежности общих и прикладных средств контроля устанавливается исходя из требований Международного стандарта аудита 315 (пересмотренный) «Выявление и оценка рисков существенного искажения посредством изучения организации и ее окружения» (МСА 315). Следует отметить, что достаточно детально данные вопросы, а также риски, связанные с использованием информационных технологий, рассматриваются в модуле «Управленческий учет, управление рисками, внутренний контроль» также на 2 этапе экзамена. Задания экзаменационного билета по данному модулю составлены таким образом, чтобы оценить наличие, в том числе, ИТ-компетенций с учетом специфики данного модуля:

- применять стандарты и методы риск-менеджмента для идентификации, оценки, управления рисками и бизнес-процессами в организации, включая ИТ-риски и риски мошенничества;
- анализировать компоненты и элементы системы внутреннего контроля, применять процедуры и риск-ориентированные методы внутреннего контроля, в том числе в области ИТ;
- оценивать эффективность контрольных процедур, в том числе ИТ-контроль в бизнес-процессах, связанных с подготовкой финансовой отчетности.

В соответствии с Порядком проведения квалификационного экзамена лица, претендующего на получение квалификационного аттестата аудитора (п.22), претендент самостоятельно выбирает последовательность сдачи модулей каждого этапа квалификационного экзамена. Однако логично было бы модуль «Управленческий учет, управление рисками, внутренний контроль» сдавать перед модулем «Аудиторская деятельность и

профессиональные ценности», так как часть вопросов модуля по аудиторской деятельности уже достаточно подробно будет изучена претендентом.

Задания на применение информационных технологий в аудите могут быть крайне разнообразны, но вместе с тем, представляют собой эпизоды реальных аудиторских проверок, являющихся достаточно типичными для аудиторской практики.

Наиболее значимые аспекты использования информационных технологий в аудите, рассматриваемые в экзаменационных заданиях 2 этапа можно сгруппировать в четыре направления:

1) конфиденциальность работы в интернет-среде;
2) использование информационных систем для получения аудиторских доказательств;
3) использование информационных технологий для коммуникаций в ходе аудита;
4) использование информационных технологий для проверки данных бухгалтерской (финансовой) отчетности.

Одной из ключевых тем является оценка рисков, возникающих при использовании информационных технологий аудитором. В данной статье рассмотрим вопросы, связанные с конфиденциальностью работы аудитора в интернет-среде.

1.3. Конфиденциальность работы аудитора в интернет-среде

Конфиденциальность аудита закреплена в статье 9 Закона 307-ФЗ «Об аудиторской деятельности». Однако сегодня аудиторы отмечают, что одной из основных проблем работы молодых специалистов является их привычка обсуждать все вопросы в социальных сетях, на форумах и чатах. Незаметно эта модель поведения переносится и на профессиональную деятельность. Не случайно использованию информационных технологий при сборе аудиторских доказательств уделяется внимание на компьютерном тестировании на первом этапе экзамена по модулю «Основы аудиторской деятельности», чтобы у тех, кто приходит в профессию, формировалось правильное представление о соблюдении принципов аудиторской деятельности.

На втором этапе экзамена, определенном в модели экзамена как основной уровень аттестации аудитора, эта тема находит свое продолжение уже в более развернутом виде, ориентированном на понимание и практическое применение компетенций и профессиональных навыков. Так, эти вопросы могут касаться организации передачи документов по

электронным каналам связи, использования личных адресов электронной почты слабозащищенных почтовых сервисов, размещения копий документов клиента в «облачных хранилищах» и так далее.

При этом ситуация может быть сформулирована по-разному, например: «в ходе обсуждения начала аудиторской проверки, главный бухгалтер аудируемого лица попросил для оперативности присылать ему текущую информацию на его личный адрес электронной почты…», «для удобства работы с большим объемом документов клиента аудитор разместил их в облачном хранилище…», «включенный в состав аудиторской группы практикант разместил видеоотчет о своей работе по проекту на своей странице в социальной сети…».

От претендента требуется понимание рисков, связанных с разглашением информации клиента по вине аудитора. От претендента требуется идентификация такого риска, то есть четкое описание ситуации, последствий, к которым могут привести подобные риски, а также меры предосторожности, которые могут снизить идентифицированные угрозы. Такие меры принимаются во многих аудиторских организациях, они могут включать различные действия, в том числе: явный запрет, прописанный в локальных актах аудиторской организации, на использование личных адресов электронной почты, запрет на выкладку документов в облачные хранилища, специальная регламентация порядка передачи, обработки и хранения электронных документов и электронных копий бумажных носителей в аудиторской организации, разработка шаблонов протоколов обмена информации с аудируемым лицом, четкое определение в договоре рисков, связанных с конфиденциальностью передаваемой информации и ее нарушениями сторонами. При этом вопросы конфиденциальности в аудиторской деятельности рассматриваются не только на уровне действий младшего персонала аудиторской группы.

В последнее время все чаще появляются нормативно-правовые документы, связанные с защитой информации на уровне организации, отрасли или национальных интересов Российской Федерации, например, Постановление Правительства РФ от 4 апреля 2019 г. N 400 «Об особенностях раскрытия и предоставления информации, подлежащей раскрытию и предоставлению в соответствии с требованиями Федерального закона «Об акционерных обществах» и Федерального закона «О рынке ценных бумаг». Закон «Об аудиторской деятельности» также содержит требования к размещению информации в базах данных, в которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение сведений и документов

(копий документов), полученных и (или) составленных в ходе оказания аудиторских услуг.

Данный аспект может также входить в сценарии экзаменационных заданий. Например, «Аудиторская организация «Сигма» проводит аудит финансовой отчетности ПАО «АВС», материнская компания которого находится в Великобритании. Аудитор материнской компании, проверяющий консолидированную отчетность, просит подготовленные аудиторской фирмой «Сигма» рабочие документы разместить на своем сервере».

Хотелось бы обратить внимание, что вопросы применения информационных технологий еще недостаточно проработаны в практической деятельности аудиторских компаний, и профессиональный опыт постоянно накапливается. На практике зачастую подобные вопросы требуют консультирования у ИТ-специалистов или переговоров с аудируемым лицом. Поэтому в некоторых случаях, что обязательно указывается в задании, сценарий может предусматривать не единственно верный ответ, а у претендента есть возможность предлагать свои варианты, исходя из собственной аудиторской практики. При решении подобных вопросов от претендента ожидается, прежде всего, понимание рисков, связанных с описанной ситуацией, а также ссылок на этические и (или) нормативные требования, которые могут быть нарушены, предложений по разрешению этой ситуации, которые в том числе могут содержать и обращение за дополнительной юридической консультацией или консультацией в СРО аудиторов. Подобные элементы ответа используются для оценки профнавыков претендента и являются неотъемлемой частью маркировки задания.

2. АУДИТОРСКИЕ IT-РИСКИ

2.1. Нормативно-правовые аспекты управления рисками аудита в цифровой среде

Стратегия развития информационных технологий в качестве одной из основных задач включает защиту национальных интересов Российской Федерации. Так, технические средства информационных систем, используемых государственными субъектами, должны размещаться на территории Российской Федерации. Операторы государственных и муниципальных информационных систем, а также информационных систем юридических лиц, осуществляющих закупки в соответствии с Федеральным законом от 18 июля 2011 года № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц», не должны допускать при эксплуатации информационных систем использования размещенных за пределами территории Российской Федерации баз данных и технических средств, не входящих в состав таких информационных систем.

Федеральный закон «Об информации, информационных технологиях и о защите информации» также определяет порядок организации интернет-пространства. В настоящее время для сбора информации активно начитают использоваться роботы, например, широкое распространение получили боты – специальные роботизированные программы, построенные по определенному алгоритму, способные самостоятельно искать информацию по запросу и отличающиеся высоким быстродействием. Наиболее популярными информационными технологиями для передачи регуляторной, финансовой и другой отчетности, являются XBRL и блокчейн. Банком России утверждены Правила формирования и представления отчетности организаций в формате XBRL. Кроме того, быстро развиваются технологии блокчейн как распределенная, децентрализованная публичная система данных, содержащая транзакции (например, дата, время и сумма покупки), цифровую подпись покупателя и продавца транзакции, уникальный идентификатор, который позволяет отличить его от любого другого блока. Примеров использования блокчейна является умный контракт (смарт-контракт) –компьютерная программа, которая отслеживает и обеспечивает исполнение оцифрованных договорных обязательств, которые находятся на блокчейне. Стороны прописывают в таком контракте условия сделки и санкции за их невыполнение, ставят цифровые подписи, а умный контракт самостоятельно определяет, все ли исполнено, и принимает решение:

завершить сделку и выдать требуемое (деньги, акции, недвижимость), наложить на участников штраф или пеню, закрыть доступ к активам и т. п. Если аудируемая организация использует умные контракты, необходимо рассмотреть вопрос о привлечении эксперта по информационным технологиям.

Блокчейн можно использовать и в процессе аудита. Аудиторские организации «большой четверки» – PWC, Deloitte, Ernst & Young и KPMG – в 2018 г. начали пилотный проект с 20 тайваньскими банками, чтобы протестировать технологию блокчейна для целей аудита финансовой отчетности клиентов банка. Целью этого пилотного проекта является оптимизация процессов внешнего подтверждения, которые в настоящее время требуют от аудитора вручную, путем направления письменных запросов и анализа полученных ответов, получать и проверять аудиторские доказательства операций компаний с третьими сторонами. Чаще всего эти подтверждения требуют, чтобы аудиторы проверяли, что остатки на счетах в банках компаний соответствуют внутренним записям о сумме денежных средств.

Ряд громких мошенничеств в истории, в том числе таких печально известных, как Peregrine Financial Group, были совершены путем подделки писем с подтверждением банка. Поэтому защита данных очень важна. При использовании новой схемы на Тайване данные о транзакциях будут перенесены банками в блокчейн, который будет доступен аудиторским фирмам.

В то же время, цифровые транзакции несут в себе высокие риски, связанные с преступной деятельностью. При глобальности процесса обращения криптовалюты, отсутствии регулятора и единого информационного центра виртуальные валюты могут способствовать финансированию преступной деятельности и способствовать отмыванию денег, являющихся ее результатом.

Далее рассмотрим актуальные вопросы экзаменационных заданий, связанные с оценкой компетенций и профессиональных навыков аудитора в цифровой среде такие, как получение аудиторских доказательств, коммуникации в ходе аудита, проверка данных бухгалтерской (финансовой) отчетности, оценка аудиторских рисков, возникающих при использовании информационных технологий.

2.2. Использование информационных систем для получения аудиторских доказательств

В практике аудиторской деятельности распространено обращение за информацией об аудируемом лице на официальные сайты ФНС, картотеки арбитражных дел, надзорных органов. На втором этапе экзамена могут быть задания, связанные с построением программы аудита, когда требуется описать последовательность действий аудитора, например, по проверке полноты раскрытия информации о ведущихся судебных делах и полноты и точности созданных оценочных обязательств на их урегулирование. Ожидается, что претендент опишет последовательность необходимых аудиторских процедур и укажет информационные ресурсы, которые следует использовать в этой ситуации (дополнительно к описанию действий, предусмотренных соответствующим стандартом аудиторской деятельности).

Аналогичные задания могут быть связаны с необходимостью построения программы аудита по полноте раскрытия информации о связанных сторонах. В этом случае претенденту необходим опыт работы с электронными сервисами, чтобы он мог достаточно детально изложить порядок действий (в дополнение к описанию требования соответствующего стандарта аудиторской деятельности). Решение задания не предусматривает использование какого-либо специального платного программного обеспечения, но предполагается, что претендент способен продемонстрировать знание им применения функционала общедоступных сервисов. Задания могут быть связаны с использованием государственного информационного ресурса, публичных кадастровых карт, информации о залоге недвижимости и автомобилей, иных аналогичных сервисов.

При решении таких заданий от претендента не требуется большого опыта работы со всеми без исключения открытыми информационными системами, но знание их учитывается при оценке количества баллов за выполнение задания. Таким образом, задание формируется для того, чтобы оценить способность претендента использовать информационные системы в аудите. Обычно это реализуется через набор из 3-5 небольших вопросов по разным аспектам проверки. При этом, эксперты при проведении экспертизы разработанного задания проверяют его на «реальность», поэтому появление в задании «нетипичной» информационной системы, неизвестной широкому кругу претендентов, имеющих практический опыт аудиторской деятельности, отсутствует.

Ожидается, что претендент также продемонстрирует понимание рисков, связанных с оценкой надежности и уместности информации из

конкретного источника. На указанные факторы может повлиять соответствие цели аудиторской процедуры и используемого источника, периодичность обновления данных в источнике и т.д. Также ожидается, что претендент понимает и способен применить принцип профессионального скептицизма при оценке информации, полученной из разных источников, если это уместно исходя из условия задания.

Данные информационных систем могут использоваться аудитором и в «обычном» режиме, например, путем направления стандартного бумажного запроса и получения официального ответа на бумажном носителе. Этот режим не предусматривает использование информационных технологий аудитором.

2.3. Использование информационных технологий для коммуникаций в ходе аудита

Значительную роль в развитии коммуникаций в ходе аудита с использованием электронных технологий сыграла пандемия коронавируса 2020 года. Если раньше это направление было более теоретическим, чем практическим, то сегодня это «передний фронт» работы аудитора. Спектр крайне широк: это и обмен документами по цифровым каналам связи, это использование электронной подписи при организации документооборота, это видеоконференции и использование вэб-камер для наблюдения за работой аудируемой организации.

Экзаменационные задания могут быть различного типа, и сочетать в себе знание как теории, например, правил использования электронной подписи, так и практики организации документооборота в электронной среде. От претендента ожидается идентификация рисков, возникающих в подобной ситуации:

- конфиденциальность информации;
- риски сбоя работы информационных систем (потери или искажения информации при передаче);
- риск выбора ненадлежащего адресата;
- ненадлежащее использование электронной подписи и т.д.

Задание может включать оценку компетенций претендента, связанных с проверкой электронной подписи, а именно, каким образом это можно сделать.

2.4. Использование информационных технологий для проверки данных бухгалтерской (финансовой) отчетности

Определение информационных технологий достаточно широкое: «информационные технологии – это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов». Сегодня использование информационных технологий для проверки данных бухгалтерской (финансовой) отчетности является одним из наиболее популярных направлений в ИТ-аудите. В таблице 1 представлена схема сочетания информационных технологий клиента и аудитора (автоматизации операций учета и аудита).

Таблица 1

Возможные варианты сочетания автоматизации операций учета и аудита

Операция в учете	**Аудиторская процедура**	**Характеристика и пример**
Ручная	Ручная	Широко использовалась в XX веке. Накладная написана от руки, реестры заполнены вручную, аудитор проверяет выборочно самостоятельно лично.
Автоматизированная	Ручная	Начало XXI века. Учет начинает стремительно автоматизироваться. Аудитор проверяет выборочно самостоятельно лично.
Автоматизированная	Автоматизированная	Наши дни. Начинается развитие автоматизированных/ роботизированных программ аудита. Проверка проводится программой, как правило, сплошным образом.
Ручная	Автоматизированная	Наши дни. Неоцифрованные документы клиента (накладные, договоры и т.д.) загружаются в программу, которая выполняет функции по их обработке и сверке итоговых данных с учетом и отчетностью.

Несмотря на тотальную цифровизацию процессов, одной из проблем аудита является продолжение использования ручных процедур проверки. Включение вопросов информационных технологий в программу квалификационного экзамена является признанием того, что на сегодняшний день переход на использование электронных технологий является одним из приоритетов развития аудиторской профессии.

Несомненным лидеров в развитии этого направления являются крупные аудиторские организации, которые достаточно много ресурсов направляют на создание программ «робоаудита».

Аудит представляет собой стандартный процесс, состоящий в преобразовании документов и иной информации клиента в аудиторское заключение. Используя технологии роботизированной автоматизации процессов (Robotic Process Automation -RPA) в настоящее время активно ведутся разработки по алгоритмизации процесса аудита. При этом одной из первых тестируемых областей является этап планирования аудита, на котором собирается информация об аудируемом лице. Данные для оценки рисков собираются аудитором как из информации, предоставленной самим аудируемом лицом, так и из внешних источников (базы данных, государственные информационные ресурсы, открытые средства массовой информации и т.д.). Для преобразования исходных данных клиента в стандартизированный и машиночитаемый формат использовалась система Python, поисковые боты, в результате генерируется сводная электронная таблица, соответствующая рабочему документу этапа планирования.

На следующем этапе исследований уже разработана модель роботизации процесса аудита доходов. Технология RPA использовалась для проведения детальных тестов, сначала собирая аудиторские доказательства из нескольких файлов (включая договоры, спецификации, накладные и другие документы в формате pdf и реестры отгрузок из бухгалтерских программ), компилируя эти доказательства в стандартизированный формат, импортируя их в программное обеспечение для анализа данных, а затем выполняя аудиторские тесты, которые предварительно запрограммированы для соответствия сумме продаж от детали счета до детали отгрузки и заказа на продажу.

Также, уже реализован пилотный проект по роботизации аудита пенсионных планов с установленными выплатами. Обычно это чрезвычайно трудоемкий и длительный процесс, особенно на этапе основных процедур, когда аудиторы вручную импортируют данные аудита в рабочие книги Excel и выполняют различные аспекты тестирования, включая написание и выполнение функций Excel, а также копирование и вставку данных из и в разные таблицы.

Разработчики роботизированной модели столкнулись с рядом трудностей. Например, при аудите операций с пенсионными планами, выяснилось, что разные организации могут представлять фамилии сотрудников, используя разные метки, такие как «Фамилия сотрудника», «Фамилия» или «Фамилия получателя», что создает препятствия в автоматизации. Используя стандартную метку (например, «Last_Name»),

формат этого поля может быть стандартизирован как текст с максимальной длиной 100 символов[1].

В этих проектах роботизируются только те задачи, которые повторяются, просты, основаны на правилах и требуют много времени. Задачи, требующие профессионального суждения, сложно автоматизировать, и аудиторы должны уделять больше времени таким задачам. Понятно, что технология может помочь улучшить аудит, но аудиторское суждение не может быть легко заменено машинами. Профессиональный скептицизм, например, может быть описан как образ мыслей, который помогает аудиторам определить, является ли учетный режим или поведение клиента разумным. Разработчики отмечают, чтобы добиться большей масштабируемости и гибкости автоматизации процессов, нужна не только роботизация, а новый уровень: интеллектуальная автоматизация процессов (Intelligent Process Automation - IPA).

Сегодняшний квалификационный экзамен, бесспорно, является значительным шагом в оценке ИТ-компетенций будущих аудиторов, но задания, подготовленные к экзамену достаточно просты. Кроме того, понимая отсутствие публичных источников для подготовки к подобным заданиям, Единая аттестационная комиссия разработала и разместила на своем сайте методические материалы для подготовки претендентов к модулям 2 этапа, где приведены примеры подобных заданий в разных модулях.

Например, рассмотрено задание на проверку выручки интернет-магазина. Действительно, сегодня практика не только аудита, но и личный опыт каждого из нас наполнен примерами использования цифровой среды: заказали яндекс.такси и оплатили электронными деньгами; выбрали платный просмотр фильма и оплатили, нажав на кнопку мобильного телефона; и многое другое. А как теперь проводить аудит отчетности этих компаний?

Для решения этих заданий нет необходимости иметь опыт аудита всех возможных организаций, работающих в электронной среде. От претендента требуется понимание, что тезис «запросить договор, накладную и счет-фактуру и сверить с данными бухгалтерского учета» не всегда подходит, нужно тестировать бизнес-процесс и его трансляцию на уровне бухгалтерского учета.

[1] see *Audit Data Standards,* AICPA Assurance Services Executive Committee Emerging Assurance Technologies Task Force, August 2013, http://bit.ly/2VVwtbU

В модуле «Управленческий учет, управление рисками, внутренний контроль» проверяются компетенции по управлению бизнес-процессами и их контролю.

Понимание аудитором бизнес-процесса аудируемого лица описано в международных стандартах аудиторской деятельности МСА 315 и МСА 330. Для лучшего понимания схемы работы можно использовать графическое описание, например, нарисовать схему получения заказа, выполнение заказа, получения оплаты и т.д. Затем для каждого элемента описать риски, которые могут привести к искажению одной или нескольких предпосылок составления отчетности, и указать ответное действие аудитора, которое будет уместно в отношении идентифицированных рисков.

Сама описанная выше модель не имеет специфики при выполнении ручных или автоматизированных процедур контроля, вопрос в масштабе и сроках. Например, аудитор ставит цель – проверить, все ли заказы услуг такси (заявки) зафиксированы в используемой программе. Аналогично – заказы в интернет-магазине, заявки на просмотр фильма и т.д. Если не использовать информационные технологии, то как может быть организована проверка? Возможно, по просьбе аудитора откроют данные системы и покажут - вот оплата, вот заявка, вот маршрут. Однако, соответствует ли эта процедура поставленной цели – нет, мы получим ответ только на вопрос – по всем ли оплаченным поездкам в программе есть заявки. И даже, если по некоторым услугам заявки нет, то означает ли это, что признанные суммы дохода фиктивны (не соблюдена предпосылка «наличие»)?

От претендента ожидается, что за время, отведенное на решение, он способен поставить некоторые задачи. Как правило, ответы на задания такого рода предусматривают возможные альтернативные варианты, и предложенные разными претендентами варианты могут отличаться, например:

- проанализировать зафиксированное количество заказов услуг такси по дням в разрезе (утро/день/вечер) за три последних года, до текущей даты; проанализировать динамику;
- сопоставить зафиксированное количество заказов услуг такси по дням в разрезе (утро/день/вечер) с количеством отраженных в учете платежей (выручки);
- сопоставить зафиксированное количество заказов услуг такси, по дням в разрезе (утро/день/вечер) с количеством машин на маршруте в этот период;

- сопоставить зафиксированное количество заказов услуг такси, по дням в разрезе (утро/день/вечер) с количеством операторов в колл-центре в этот период;
- сопоставить зафиксированное количество заказов услуг такси, по дням в разрезе (утро/день/вечер) с количеством звонком и смс-сообщений (по данным оператора связи - при наличии таких данных).

Некоторые претенденты, обладающие достаточным опытом, могут предложить иные, возможно, более эффективные процедуры, например, синхронизировать данные GPS передвижения машины и учтенные перемещения автомашин по маршрутам. Кто-то вспомнит пандемию и проверку таксистом пропуска – значит, можно синхронизировать случаи проверки пропусков и фиксацию выручки. Кто-то может предположить, что весь автотранспорт принадлежит иным лицам, и аудируемая организация выступает только в роли посредника при получении и распределении заказов и т.д., поэтому предложит другие процедуры. Задания подобного типа могут быть увязаны с оценкой эффективности систем внутреннего контроля, с построением тестов средств контроля и другими аспектами аудита. Также задания могут быть связаны с проведением аналитических процедур для оценки рисков и для получения аудиторских доказательств.

Аналогичные задания могут касаться различных отдельных участков учета, например, амортизации основных средств, расходов на оплату труда, расходов на уплату процентов по заемным средствам и т.д.

2.5. Оценка рисков в сфере ПОД/ФТ

В модулях 2 этапа экзамена могут быть вопросы, связанные с рисками соблюдения законодательства в сфере ПОД/ФТ (противодействия легализации (отмыванию) доходов, полученных преступным путем). Например, в модуле «Правовое регулирование экономической деятельности» могут быть вопросы на умение анализировать хозяйственную операцию и оценивать правомерность ее осуществления лицом, которому оказываются аудиторские и прочие услуги, связанные с аудиторской деятельностью. Решение подобных заданий основывается на применении Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» в части определения организаций, относящихся к «обслуживающим организациям, осуществляющим обязательный контроль» (их права и обязанности), а также критериев отнесения сделок к числу подлежащих обязательному контролю. При подготовке ответов на подобные

задания могут использоваться публичные источники Федеральной службы Российской Федерации по финансовому мониторингу, рекомендованные для использования в квалификационном экзамене Минфином России и размещенные на официальном сайте Федеральной службы Российской Федерации по финансовому мониторингу: отчет «Национальная оценка рисков легализации (отмывания) преступных доходов»; отчет о секторальной оценке рисков легализации (отмывания) преступных доходов и финансирования терроризма с участием аудиторов; памятка для субъектов статьи 7.1 Федерального закона № 115-ФЗ от 05.03.2020.

Баллы за ответ на подобные задания присваиваются за демонстрацию компетенций Программы, за правильные рассуждения, в частности, например, за указание на то, что организации в соответствии с Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» отнесены к обслуживающим организациям, осуществляющим обязательный контроль; за указание на то, что сделка отвечает установленным в законе критериям и подлежит обязательному контролю; за указание на право обслуживающих организаций запрашивать документы и т.п.

ПРИЛОЖЕНИЕ 1.

Понятия информационных технологий

1. Нормативное регулирование

В мае 2017 года Указом Президента Российской Федерации № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» были определены цели, задачи и меры по реализации внутренней и внешней политики России в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов.

Основные понятия, связанные с использованием информационных технологий, даны в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Федеральный закон «Об информации, информационных технологиях и о защите информации»), в котором имеется следующее определение:

информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Также введены определения наиболее общих терминов, связанных с использованием информационных технологий.

- **информация** – сведения (сообщения, данные) независимо от формы их представления;
- **информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. Различают государственные, муниципальные и иные системы. Наиболее известной среди федеральных государственных информационных систем является ЕСИА – «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»;
- **информационно-телекоммуникационная сеть** – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;
- **оператор информационной системы** – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Стратегия развития информационных технологий в качестве одной из основных задач включает защиту национальных интересов Российской Федерации. Так, технические средства информационных систем, используемых государственными органами, органами местного самоуправления, государственными и муниципальными унитарными предприятиями или государственными и муниципальными учреждениями, **должны размещаться на территории Российской Федерации**.
Операторы государственных информационных систем, муниципальных информационных систем, информационных систем юридических лиц, осуществляющих закупки в соответствии с Федеральным законом от 18 июля 2011 года № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц», не должны допускать при эксплуатации информационных систем использования размещенных за пределами территории Российской Федерации баз данных и технических средств, не входящих в состав таких информационных систем.

2. Организация интернет-пространства

Федеральный закон «Об информации, информационных технологиях и о защите информации» также определяет ряд терминов, связанных с организацией интернет-пространства.

Поисковая система – информационная система, осуществляющая по запросу пользователя поиск в сети Интернет информации определенного содержания и предоставляющая пользователю сведения об указателе страницы сайта в сети Интернет для доступа к запрашиваемой информации, расположенной на сайтах в сети Интернет, принадлежащих иным лицам, за исключением информационных систем, используемых для осуществления государственных и муниципальных функций, оказания государственных и муниципальных услуг, а также для осуществления иных публичных полномочий, установленных федеральными законами. Среди наиболее известных поисковых систем можно назвать Google и Яндекс.

Доменное имя – обозначение символами, предназначенное для адресации сайтов в сети Интернет в целях обеспечения доступа к информации, размещенной в сети Интернет. Доменные имена обычно формируются с расширением: по странам (Россия – .ru, Украина – .ua, США – .us) или по видам организаций. Например, Единая аттестационная комиссия в сети Интернет имеет доменное имя eak-rus.ru.

Сайт в сети Интернет – совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети Интернет по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети Интернет. Сайт – это одна веб-страница или совокупность веб-страниц,

доступных в сети Интернет через протоколы HTTP/HTTPS. Например, сайт Единой аттестационной комиссии https://eak-rus.ru/.

Страница сайта в сети Интернет (также интернет-страница) – часть сайта в сети Интернет, доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети Интернет. Например, результаты экзаменов Единая аттестационная комиссия размещает на странице https://eak-rus.ru/rezultaty_ekzamenov.

Сетевой адрес – идентификатор в сети передачи данных, определяющий при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему. Обычно сетевой адрес называют еще IP-адресом (от IP – Internet Protocol), который состоит из четырех групп цифр, разделенных точками, например: 132.134.1.102. Сетевой адрес зависит от количества выходов в сеть, у компьютера их может быть несколько: например, сетевое подключение по проводной сети и подключение по сети Wi-Fi. При смене сети данный адрес может изменяться.

От IP-адреса следует отличать MAC-адрес (Media Access Control address) – индивидуальный 12-значный код, который присваивается электронному устройству производителем и обычно записывается в виде 12 символов, например: 00-18-E3-16-8D-4E. MAC-адрес еще называют физическим адресом устройства. Он уникален для каждого устройства, поэтому еще называется Hardware Address (адрес устройства). Данный адрес может изменяться при замене комплектующих устройства, которым присвоен данный адрес.

Владелец сайта в сети Интернет – лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети Интернет, в том числе порядок размещения информации на таком сайте.

Провайдер хостинга – лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети Интернет.

3. Работа с документами в интернет-среде и безопасность

В соответствии со статьей 11 «Документирование информации» Федерального закона «Об электронной подписи» законодательством Российской Федерации или соглашением сторон могут быть установлены требования к документированию информации.

Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

В настоящее время в практике возник еще один термин – **электронный образ документа**.

В приказе Судебного департамента при Верховном Суде Российской Федерации от 28 декабря 2016 г. № 252 (в редакции от 20 февраля 2018 г.) «Об утверждении Порядка подачи в арбитражные суды Российской Федерации документов в электронном виде, в том числе в форме электронного документа» (вместе с «Порядком подачи в арбитражные суды Российской Федерации документов в электронном виде, в том числе в форме электронного документа») разделены два понятия:

электронный документ – документ, созданный в электронной форме без предварительного документирования на бумажном носителе, подписанный электронной подписью в соответствии с законодательством Российской Федерации;

электронный образ документа (электронная копия документа, изготовленного на бумажном носителе) – переведенная в электронную форму с помощью средств сканирования копия документа, изготовленного на бумажном носителе, заверенная простой электронной подписью или усиленной квалифицированной электронной подписью.

Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

В соответствии с п. 4 указанной выше статьи в целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.

Порядок использования электронной подписи определяется Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон «Об электронной подписи»).

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

В соответствии со статьей 5 Федерального закона «Об электронной подписи» существуют следующие виды электронных подписей (ЭП, ранее использовался термин ЭЦП – электронно-цифровая подпись) (таблица 2).

Таблица 2

Вид электронной подписи и их характеристика

Вид электронной подписи	Характеристики
Простая электронная подпись	Электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом Самым распространенным вариантом использования простой электронной подписи является письмо по электронной почте, автор которого идентифицируется через вход на почтовый сервис по паролю и логину. В соответствии со статьей 9 Федерального закона «Об электронной подписи» использование простой электронной подписи для подписания электронных документов, содержащих сведения, составляющие государственную тайну, или в информационной системе, содержащей сведения, составляющие государственную тайну, не допускается.
Усиленная неквалифицированная электронная подпись	Электронная подпись, которая: 1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи; 2) позволяет определить лицо, подписавшее электронный документ; 3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания; 4) создается с использованием средств электронной подписи.
Усиленная квалифицированная электронная подпись	Электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам: 1) ключ проверки электронной подписи указан в квалифицированном сертификате; 2) для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным Федеральным законом «Об электронной подписи».

В соответствии с пунктом 3 статьи 12 Федерального закона «Об электронной подписи» при проверке электронной подписи средства электронной подписи должны:

1) показывать самостоятельно или с использованием программных, программно-аппаратных и технических средств, необходимых для отображения информации, подписанной с использованием указанных средств, содержание электронного документа, подписанного электронной подписью;

2) показывать информацию о внесении изменений в подписанный электронной подписью электронный документ;

3) указывать на лицо, с использованием ключа электронной подписи которого подписаны электронные документы.

Для создания ключа электронной подписи и создания ключа проверки электронной подписи используются средства электронной подписи – шифровальные (криптографические) средства.

Ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, ***выданные удостоверяющим центром*** либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Квалифицированный сертификат ключа проверки электронной подписи – сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным нормативными правовыми актами, и ***созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти***, уполномоченным в сфере использования электронной подписи.

Усиленная электронная подпись может быть в формате отсоединенной и присоединенной.

- При создании присоединенной подписи формируется один файл, который содержит и саму подпись, и документ, для которого она была создана.
- Отсоединенная подпись формируется в отдельном от подписываемого документа файле с расширением .sig или .sgn.

На рис. 1 представлен пример размещения на сайте документа с отсоединенной электронной подписью.

Для проверки электронной подписи лицами, не являющимися участниками электронного документооборота, существует ряд сервисов, например:

- портал госуслуг https://www.gosuslugi.ru/pgu/eds;
- https://ca.kontur.ru/articles/proverka-elektronnoi-podpisi;
- https://iecp.ru/ep/ep-verification.

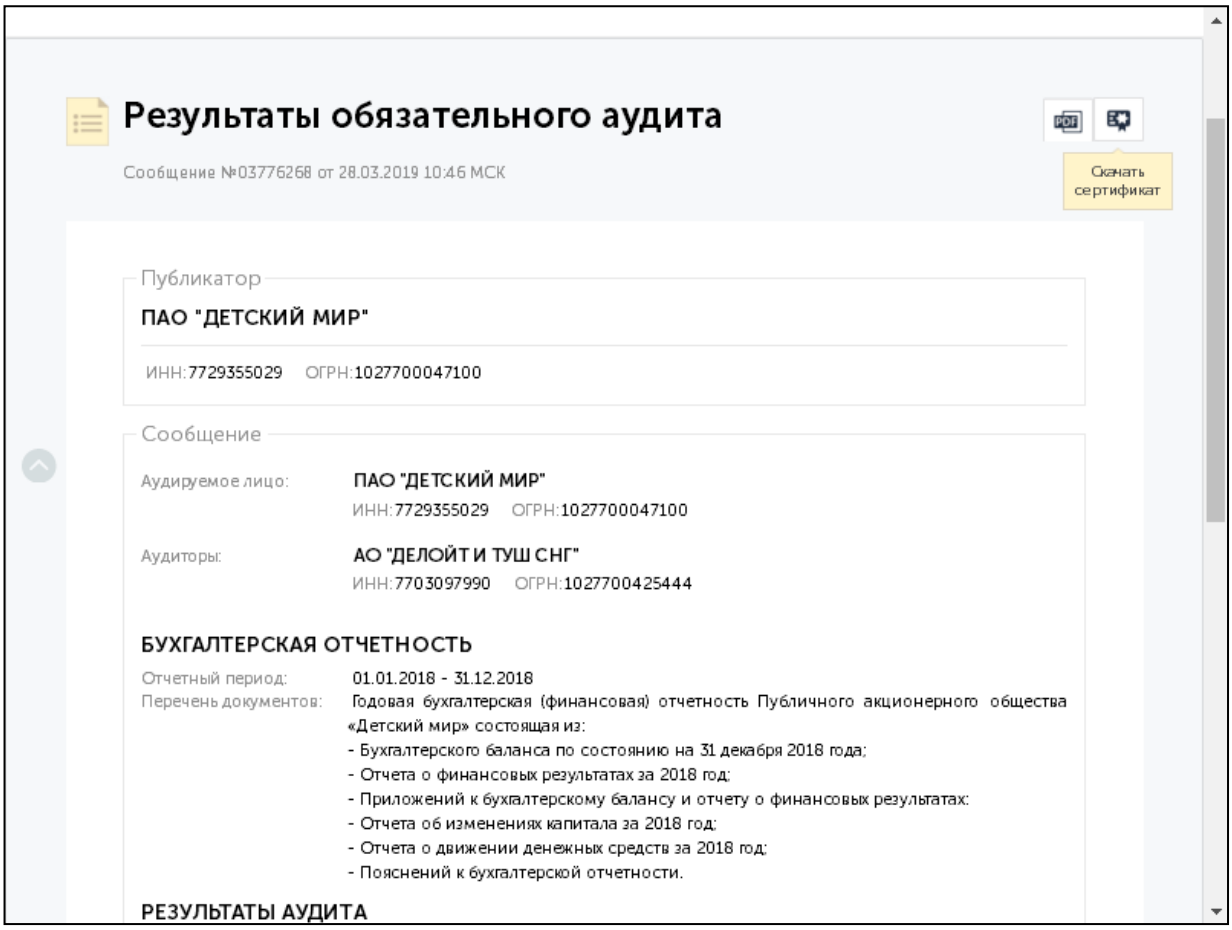

Рис.1. Пример размещения на сайте документа с отсоединенной электронной подписью

На рис. 2 представлен скриншот страницы сайта госуслуг для проверки электронной подписи. Однако следует учитывать, что использование электронной подписи при современном уровне развития ИТ может быть связано с риском мошенничества, а это, в свою очередь, требует организации эффективных систем контроля, включая множественную проверку с использованием надежных электронных сервисов.

Кроме того, в процессе аудита аудитор получает от клиента и создает сам разнообразные документы. Основной проблемой является ограничение доступа третьих лиц к этой информации, которая в большинстве случаев носит конфиденциальный характер. Требование обеспечения конфиденциальности информации закреплено в статье 9 Федерального закона «Об аудиторской деятельности» № 307-ФЗ от 30 декабря 2008 г.

Рис. 2. Скриншот страницы сайта госуслуг для проверки электронной подписи

В соответствии со статьей 13 Федерального закона «Об аудиторской деятельности» № 307-ФЗ от 30 декабря 2008 г. аудиторские организации и аудиторы обязаны обеспечивать хранение документов (копий документов), полученных и (или) составленных в ходе оказания аудиторских услуг, в течение не менее пяти лет после года, в котором они были получены и (или) составлены.

Необходимо также указывать сведения о базах данных информации, в которых осуществляется сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение сведений и документов (копий документов), полученных и (или) составленных в ходе оказания аудиторских услуг, на территории Российской Федерации.

ПРИЛОЖЕНИЕ 2.

Использование информационных технологий в аудите

1. Использование в ходе аудита данных информационных систем

Перевод бизнес-процессов в электронную форму оказывает значительное влияние на аудиторскую деятельность, что связано с изменением бизнес-процессов аудиторской организации, прежде всего, замещением традиционных контрольных процедур, осуществляемых аудитором, автоматизированными системами поиска, обработки и анализа информации.

Сегодня информацию о деятельности аудируемого лиц, аудиторы могут получить из государственных и муниципальных информационных систем таких, как сервисы Федеральной налоговой службы, картотеки арбитражных дел, публичных кадастровых карт и т.д., а также коммерческих ресурсов, например, СПАРК (таблица 3).

Таблица 3

Примеры использования информационных систем для сбора аудиторских доказательств

Вид аудиторского доказательства	**Используемая информационная система**
Размещение бухгалтерской отчетности (до 2020 года)	Сайт Росстата
Размещение бухгалтерской отчетности и аудиторского заключения (с марта 2020 года)	Единый информационный ресурс ФНС
Факт государственной регистрации аудируемого лица, юридический адрес, зарегистрированная величина уставного капитала	Сайт Федеральной налоговой службы/Проверь себя и контрагента
Наличие судебных исков (предъявленные самим аудируемым лицом, к аудируемому лицу и т.д.), история рассмотрения дела	Сайт Арбитражного суда/Картотека арбитражных дел
Наличие исполнительного производства	Сайт Службы судебных приставов
Существование земельного участка с указанным кадастровым номером, информация о его собственнике, кадастровой стоимости и обременениях	Единый государственный реестр недвижимости, Публичная кадастровая карта

В настоящее время для сбора информации активно начитают использоваться роботы, например, широкое распространение получили боты – специальные роботизированные программы, построенные по определенному алгоритму, способные самостоятельно искать информацию по запросу и отличающиеся высоким быстродействием.

2. Блокчейн и XBRL

Наиболее популярными информационными технологиями являются XBRL и блокчейн. **XBRL** – это формат передачи регуляторной, финансовой и другой отчетности, который основан на расширяемом языке разметки XML.

Организации всё чаще применяют XBRL или Inline XBRL в качестве инструмента для составления своей отчетности. Например, Банком России утверждены Правила формирования отчетности в формате XBRL и ее представления в Банк России. Файл в формате xml или xbrl, представляемый в Банк России отчитывающейся организацией, содержит факты о деятельности организации, соответствующие концептам, определенным в таксономии XBRL, на основе которой формируется файл.

Очень быстро развивается и **блокчейн** (blockchain). Обычно он описывается как распределенная, децентрализованная публичная система данных. Блоки в блокчейне содержат записи информации:

1) транзакции (например, дата, время и сумма покупки),

2) цифровая подпись покупателя и продавца транзакции,

3) уникальный идентификатор, называемый «хеш», который позволяет отличить его от любого другого блока.

Цепочка в блокчейне – это связь между всеми блоками. Каждый раз, когда происходит новая транзакция, она добавляется в цепочку как постоянный блок.

Одним из примеров использования блокчейна является умный контракт (также смарт-контракт от smart contract) – это компьютерная программа, которая отслеживает и обеспечивает исполнение оцифрованных договорных обязательств, которые находятся на блокчейне. Стороны прописывают в таком контракте условия сделки и санкции за их невыполнение, ставят цифровые подписи, а умный контракт самостоятельно определяет, все ли исполнено, и принимает решение: завершить сделку и выдать требуемое (деньги, акции, недвижимость), наложить на участников штраф или пеню, закрыть доступ к активам и т. п.

«Прочитать» умный контракт сможет только IT-специалист, поскольку он написан на языке программирования. Поэтому, если аудируемая организация использует умные контракты, необходимо рассмотреть вопрос о привлечении специалиста по информационным технологиям (эксперта).

Блокчейн можно использовать и в процессе аудита. Например, аудиторские организации «большой четверки» – PWC, Deloitte, Ernst &

Young и KPMG – в 2018 г. начали пилотный проект с 20 тайваньскими банками, чтобы протестировать технологию блокчейна для целей аудита финансовой отчетности клиентов банка.

Целью этого пилотного проекта является оптимизация процессов внешнего подтверждения, которые в настоящее время требуют от аудитора вручную (путем направления письменных запросов и анализа полученных ответов) получать и проверять аудиторские доказательства операций компаний с третьими сторонами. Чаще всего эти подтверждения требуют, чтобы аудиторы проверяли, что остатки на счетах в банках компаний соответствуют внутренним записям о величине денежных средств. Ряд громких мошенничеств в истории, в том числе таких печально известных, как Peregrine Financial Group, были совершены путем подделки писем с подтверждением банка. Поэтому защита данных очень важна. При использовании новой схемы на Тайване данные о транзакциях будут перенесены банками в блокчейн, который будет доступен аудиторским фирмам.

Платформа, основанная на блокчейне, была разработана тайваньской фирмой FISC (Financial Information Service Co) и предназначалась для использования при проведении финансовой разведки (IT intelligence). Крупнейшие банки Тайваня будут участвовать в тестировании платформы блокчейна, благодаря которой аудиторы, в свою очередь, смогут получать данные об операциях клиента и оценить, способствует ли такой метод обеспечению безопасности и автоматизации процесса подтверждения и значительному сокращению времени на осуществление процесса аудита.

3. Оценка значимости риска использования информационных технологий аудируемым лицом

Другим источником ИТ-рисков для аудиторов является перевод бизнес-процессов аудируемых организаций в электронную форму, что вызывает изменение их бизнес-процессов, прежде всего увеличение количества операций в цифровой среде, что влечет возрастание аудиторских рисков, связанных с использованием информационных технологий самим аудируемым лицом.

В соответствии с требованиями МСА 315 «Выявление и оценка рисков существенного искажения посредством изучения организации и ее окружения» (введен в действие на территории Российской Федерации приказом Министерства финансов России от 9 января 2019 г. № 2н) при изучении контрольных действий в организации аудитор должен получить понимание того, каким образом организация отвечает на риски, возникающие вследствие использования информационных технологий (пункт 21). В этой связи, для оценки значимости риска использования информационных технологий аудируемого лица можно воспользоваться

группировкой организаций, имеющих общую специфику бизнес-процессов, включая составление финансовой отчетности (таблица 4).

Таблица 4

Группировка аудируемых организаций по степени риска использования информационных технологий (по видам бизнес-процессов, отраслевым особенностям)

Группировка аудируемых организаций по видам бизнес-процессов и отраслевым особенностям по использованию информационных технологий	Оценка значимости риска использования информационных технологий
Майнинг криптовалюты, совершение операций с цифровыми активами (например, биткоинами или иными криптовалютами)	Очень высокая
Совершение основных операций в интернет-среде (электронные платежи, услуги телекоммуникаций, интернет-торговля услугами), иные операции в интернет-среде, не имеющие материальной формы	Высокая
В интернет-среде осуществляется только часть бизнес-процессов (например, получение заказов: Яндекс-такси, интернет-торговля одеждой и т. д.)	Средняя
Промышленность, строительство, традиционная торговля, сельское хозяйство	Низкая

В соответствии с МСА 220 «Контроль качества при проведении аудита финансовой отчетности», утвержденным приказом Министерства финансов Российской Федерации от 9 января 2019 г. № 2н, при назначении аудиторской группы в ходе рассмотрения компетентности и необходимых возможностей, которыми должны обладать члены всей рабочей группы, руководитель задания может учесть такие критерии, как:

- понимание специфики аудиторских заданий подобного характера и сложности, наличие практического опыта в этой области, достигаемые соответствующей профессиональной подготовкой и участием;
- понимание профессиональных стандартов и применимых законодательных и нормативных требований;
- технические знания, включая знание соответствующих информационных технологий и специализированных областей бухгалтерского учета или аудита (пункт А11).

Поэтому, приступая к выполнению задания, необходимо, прежде всего, оценить степень влияния ИТ на бизнес аудируемого лица, риски, связанные с их применением.

В зависимости от результатов оценки руководитель задания оценивает компетентность состава аудиторской группы. Если руководитель сочтет компетентность членов группы недостаточной, необходимо рассмотреть вопрос о привлечении консультанта или эксперта.

Аудиторская группа включает лицо, применяющее знания специализированной области бухгалтерского учета или аудита, будь то специально нанятое или состоящее в штате аудиторской организации, если такая имеется, которое выполняет аудиторские процедуры в интересах данного задания. Однако лицо такой компетентности не входит в число членов аудиторской группы. Если единственной формой участия привлеченного специалиста в выполнении аудиторского задания является консультирование, он не является членом рабочей группы (МСА 220, пункт А10).

Если принято решение о привлечении эксперта в области информационных технологий, необходимо определить специализацию эксперта и уровень его квалификации, с учетом тех задач, которые должны быть решены в ходе аудита.

Система сертификации специалистов в области аудита ИТ-систем разработана CobiT (Control Objectives for Information and Related Technologies). CobiT является системой стандартов и руководств в области управления IT-аудитом и безопасностью, а также руководством по управлению IT-процессами.

В качестве экспертов в области информационных технологий могут привлекаться, например, специалисты в области аудита ИТ, информационной безопасности и рисков ИТ:

- Аудитор информационных систем (Certified Information Systems Auditor™ – CISA®);
- Менеджер информационной безопасности (Certified Information Security Manager™ – CISM®);
- Менеджер по управлению корпоративными ИТ (Certified in the Governance of Enterprise IT™ – CGEIT®);
- Менеджер по управлению рисками использования информационных систем (Certified in Risk and Information Systems Control™ – CRISC®).

Если, по мнению руководителя задания, аудиторская группа не обладает достаточной компетентностью в сфере информационных технологий, он должен отказаться от выполнения задания.

4. Системы идентификации и аутентификации

В пункте А107 МСА 315 указано, что, с точки зрения аудитора, средства контроля за ИТ-системами эффективны, если они обеспечивают целостность информации и безопасность данных, обрабатываемых такими системами, и включают эффективные общие и прикладные средства контроля за ИТ-системами.

Прикладные средства контроля – это автоматизированные или осуществляемые вручную процедуры, которые обычно выполняются на уровне бизнес-процессов и применяются для обработки операций отдельными приложениями.

Прикладные средства контроля могут быть по своему характеру предотвращающими или обнаруживающими и предназначены для обеспечения целостности данных бухгалтерского учета. Следовательно, прикладные средства контроля относятся к процедурам, используемым для инициирования, регистрации, обработки и обобщения операций или другой финансовой информации. Эти средства контроля помогают убедиться в том, что операция действительно имела место, санкционирована, записана и обработана точно и в полном объеме. Примеры включают отслеживание изменений введенных данных и проверку сквозной нумерации с принимаемыми вручную мерами по отчетам об отклонениях или с исправлением данных на этапе ввода.

Общие средства контроля за ИТ-системами – это политика и процедуры, которые связаны со многими приложениями и поддерживают эффективное функционирование прикладных средств контроля. Они применяются в отношении главного сервера, иных серверов, а также аппаратно-программных комплексов конечных пользователей. Общие средства контроля за ИТ-системами, которые обеспечивают целостность информации и безопасность данных, как правило, включают средства контроля:

- за центром обработки данных и работой сети;
- приобретением, изменением и обслуживанием системного программного обеспечения;
- изменением программ;
- обеспечением безопасного доступа;
- приобретением, разработкой и обслуживанием прикладных программ.

Общие средства контроля за ИТ-системами применяются для снижения рисков, связанных с применением информационных технологий, например:

- зависимость от систем или программ, которые неточно обрабатывают данные, обрабатывают неточные данные либо делают то и другое одновременно;
- несанкционированный доступ к данным, что может вызвать уничтожение данных или ненадлежащие изменения в данных, включая отражение несанкционированных или несуществующих операций или неточное отражение операций. Такие риски могут возникать, если к общей базе данных имеет доступ большое количество пользователей;
- возможность получения персоналом ИТ-отдела прав доступа, превышающих необходимые права доступа для выполнения их обязанностей, что нарушает порядок разделения обязанностей;
- несанкционированные изменения данных в основных файлах;
- несанкционированные изменения систем или программ;

- неспособность внесения необходимых изменений в системы или программы;

- ненадлежащее ручное вмешательство;

- возможная потеря данных или неспособность получить необходимый доступ к данным.

Аудитор может изучить применяемые аудируемой организацией средства идентификации и аутентификации лиц, обладающих правом доступа к определенным информационным системам, в том числе к программам бухгалтерского учета.

Авторизация – предоставление определенному лицу или группе лиц прав на выполнение определенных действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий. Авторизация подразумевает:

1) процесс включения нового пользователя в список лиц, имеющих право доступа к информации; в том числе создания идентификатора нового пользователя (например, в самом простом варианте: логин, пароль);

2) запрос аутентификации при попытке входа в систему (например: ввод пароля, логина);

3) при успешном прохождении аутентификации предоставление доступа к данным.

Аутентификация – процедура проверки пользователя, выполняющего авторизацию. Авторизация открывает доступ пользователю после успешного прохождения ими аутентификации.

Способы аутентификации:

Пароли. Пользователь вводит пароль в систему, система сравнивает введенный пароль с хранящимся в системе эталонным паролем, при совпадении открывается доступ к информации. По срокам действия различают:

- многоразовые пароли;
- одноразовые пароли.

Использование многоразовых паролей имеет ряд существенных недостатков. Во-первых, сам эталонный пароль хранится на сервере аутентификации, который может быть взломан. Во-вторых, пользователь вынужден запоминать (или записывать) свой многоразовый пароль. Злоумышленник может заполучить его, просто применив навыки социальной инженерии, без всяких технических средств (например, мошенники выманивают данные банковских карт у пенсионеров). Кроме того, сильно снижается защищенность системы в случае, когда субъект сам выбирает себе пароль. По сравнению с использованием многоразовых паролей одноразовые пароли предоставляют более высокую степень защиты.

Поэтому в ходе выполнения процедур, предусмотренных пунктом 21 МСА 315, следует рассмотреть такие вопросы, как:

- процесс авторизации персонала, имеющего доступ к формированию информации, имеющей значение для отчетности;

- порядок создания и обновления паролей;
- порядок прекращения доступа к системе, например, в случае перемещения сотрудника на другую должность или увольнения.

Электронная подпись. В этом случае используются все виды электронной подписи, установленные статьей 5 Федерального закона «Об электронной подписи». Наиболее надежной является усиленная квалифицированная подпись. Закрытый ключ хранится на материальном носителе, обычно это ключ-брелок eToken.

В ходе выполнения процедур, предусмотренных пунктом 21 МСА 315, следует:

- выяснить, какая информация, значимая для формирования отчетности, вводится в систему с подтверждением электронной подписью;
- провести анализ значимости информации и вида электронной подписи;
- выяснить, как обеспечивается хранение ключей электронной подписи (токенов);
- провести выборочную проверку электронной подписи.

Подтверждение по СМС. Привлекательность данного метода заключается в том, что ключ получается не по тому каналу, по которому производится аутентификация, что практически исключает атаку типа «человек посередине» (Man in the middle (MITM)). Дополнительный уровень безопасности может дать требование ввода PIN-кода мобильного средства. Данный метод получил широкое распространение в банковских операциях через сеть Интернет.

Биометрические системы. Примерами внедрения указанных методов являются системы идентификации пользователя по рисунку радужной оболочки глаза, отпечаткам ладони, форме ушей, инфракрасной картине капиллярных сосудов, по почерку, по запаху, по тембру голоса и даже по ДНК.

Аутентификация посредством GPS. Новейшим направлением аутентификации является доказательство подлинности удаленного пользователя путем определения его местонахождения. Данный защитный механизм основан на использовании системы космической навигации типа GPS (Global Positioning System).

Многофакторная аутентификация. Она построена на совместном использовании нескольких факторов аутентификации. Это значительно повышает защищенность системы.

В государственных информационных системах процедура аутентификации установлена нормативными документами[2].

[2] См., например: https://esia.gosuslugi.ru/registration/policiesTerms.xhtml.

Источники

1. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы». Электронный ресурс. (дата обращения 30 октября 2020 года).
2. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 01.05.2019) «Об информации, информационных технологиях и о защите информации».- Электронный ресурс – Консультант плюс. (дата обращения 30 октября 2020 года).
3. Big Four to Pilot Blockchain-based Auditing in Taiwan, By Emma Zhou, Regulation Asia Published on 24th July 2018. Источник: https://www.regulationasia.com/big-four-to-pilot-blockchain-based-auditing-in-taiwan/. (дата обращения 30 октября 2020 года).
4. Международный стандарт аудита 315 (пересмотренный) «Выявление и оценка рисков существенного искажения посредством изучения организации и ее окружения» (введен в действие на территории Российской Федерации Приказом Минфина России от 09.01.2019 № 2н).
5. Международный стандарт аудита 330 «Аудиторские процедуры в ответ на оцененные риски» (введен в действие на территории Российской Федерации Приказом Минфина России от 09.01.2019 № 2н)
6. Отчет Росфинмониторинга «Национальная оценка рисков легализации (отмывания) преступных доходов» (Основные выводы). http://www.fedsfm.ru. (дата обращения 30 октября 2020 года).
7. Отчет о секторальной оценке рисков легализации (отмывания) преступных доходов и финансирования терроризма с участием аудиторов. http://www.fedsfm.ru. (дата обращения 30 октября 2020 года).
8. Памятка для субъектов статьи 7.1 Федерального закона № 115-ФЗ от 05.03.2020 - http://www.fedsfm.ru. (дата обращения 30 октября 2020 года).
9. Guru Raj Singh //Blockchain, XBRL and the Future of Reporting// December 20, 2018. Источник: https://www.datatracks.com/blog/blockchain-xbrl-and-the-future-of-reporting/.
10. «Big Four to Pilot Blockchain-based Auditing in Taiwan», By Emma Zhou, Regulation Asia Published on 24th July 2018. Источник: https://www.regulationasia.com/big-four-to-pilot-blockchain-based-auditing-in-taiwan/.
11. «ГОСТ Р ИСО/МЭК 9594-8-98. Государственный стандарт Российской Федерации. Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации» (принят и введен в действие Постановлением Госстандарта России от 19.05.1998 № 215) (Электронный ресурс – Консультант плюс, дата обращения 30 октября 2020 года).

12. By Michael Cohen, CPA (retired), Andrea M. Rozario, CPA and Chanyuan (Abigail) Zhang//Exploring the Use of Robotic Process Automation (RPA) in Substantive Audit Procedures. A Case Study. (дата обращения 30 октября 2020 года).

13. «Robotic Process Automation for Auditing», Journal of Emerging Technologies in Accounting, Spring 2018, http://bit.ly/2JKLCee. (дата обращения 30 октября 2020 года).

14. By Deniz Appelbaum, PhD and Robert Nehmer, PhD// The Coming Disruption of Drones, Robots, and Bots. How Will It Affect CPAs and Accounting Practice? June 2017 (дата обращения 30 октября 2020 года).

15. «Drones and Bridge Inspections – Changing the Process», RDO Integrated Controls blog, Oct. 10, 2016, http://bit.ly/2rUVfKs. (дата обращения 30 октября 2020 года).

16. Examining Automation in Audit// Andrea M. Rozario, CPA, Abigail Zhang, Dr. Miklos A. Vasarhelyi / April 1, 2019- Электронный ресурс. Дата обращения: 28 сентября 2020 года// https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/examining-automation-audit (дата обращения 30 октября 2020 года).

17. Audit Data Standards, AICPA Assurance Services Executive Committee Emerging Assurance Technologies Task Force, August 2013, http://bit.ly/2VVwtbU(дата обращения 30 октября 2020 года).

18. Использование информационных технологий в процессе сбора аудиторских доказательств. Методические материалы для подготовки претендентов. https://eak-rus.ru/files/2020/audit-1et-mm.pdf.

19. Методические материалы для подготовки претендентов. Сайт АНО «ЕАК» http://www.eak-rus.ru/

Консультационные статьи АНО «ЕАК» в журнале «Аудитор»:

20. Информационные технологии в аудиторской деятельности //Аудитор. 2020. Т. 6. № 4. С. 24-29.

21. Оценка компетенций и профессиональных навыков аудитора в цифровой среде: наиболее значимые аспекты использования информационных технологий в аудите //Аудитор. 2020. Т. 6. № 8. С. 20-24.

22. Оценка компетенций и профессиональных навыков аудитора в цифровой среде: аудиторские IT-риски //Аудитор. 2020. Т. 6. № 10. С. 11-16.