МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ПОДГОТОВКИ ПРЕТЕНДЕНТОВ К СДАЧЕ КВАЛИФИКАЦИОННОГО ЭКЗАМЕНА

Использование информационных технологий в процессе сбора аудиторских доказательств

Москва - 2020

ОГЛАВЛЕНИЕ

1. Понятие информационных технологий

1.1. Нормативное регулирование

В мае 2017 года Указом Президента Российской Федерации № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» [1] 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») [2], 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.

1.2. 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.

Примеры тестов по теме:

Тест 1

Адрес сайта в сети Интернет в целях обеспечения доступа к информации, размещенной в сети Интернет, для удобства пользователей обозначенный символами, например zakaz.ru, это… (выберите ОДИН правильный ответ):

A. страница сайта
B. доменное имя
C. сетевой адрес

Правильный ответ: B.

Тест 2

ООО «Поставка» продает изделия из металлопроката. Вся информация о ценах и ассортименте представлена на сайте www.postavka.ru. Для участия в электронных торгах ООО «Поставка» использует компьютерное устройство, по данным производителя, серийный номер этого устройства **00-16-E5-E1-E1-02.** ***Выход в сеть Интернет осуществляется через*** **IP 82.134.200.83.**

Укажите соответствие между описанием элемента информационных технологий и его названием (правильное соответствие укажите графически – линиями или стрелками):

IP 82.134.200.83.	*MAC-адрес устройства*
00-16-E5-E1-E1-02	*Доменное имя*
www.postavka.ru	*Сетевой адрес*

Правильный ответ:
IP 82.134.200.83. – Сетевой адрес.
00-16-E5-E1-E1-02 – MAC-адрес устройства.
www.postavka.ru – Доменное имя.

Тест 3

Аудиторская фирма для создания своего сайта обратилась к разработчику сайтов – компании «Вэблогистика». Для размещения сайта в сети Интернет аудиторская фирма заключила договор с компанией «Бэст.Рунет». Теперь вся информация о деятельности аудиторской организации доступна в сети Интернет на сайте **www.audit2020.ru.** ***Выход в сеть Интернет осуществляется через*** **IP 80.155.200.83.**

Укажите соответствие между описанием элемента информационных технологий и его названием (правильное соответствие укажите графически – линиями или стрелками):

www.audit2020.ru	*Провайдер хостинга*
IP 80.155.200.83.	*Доменное имя*
«Бэст.Рунет»	*Сетевой адрес*

Правильный ответ:
www.audit2020.ru – Доменное имя.
IP 80.155.200.83. – Сетевой адрес.
«Бэст.Рунет» – Провайдер хостинга.

1.3. 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 1).

Таблица 1

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.

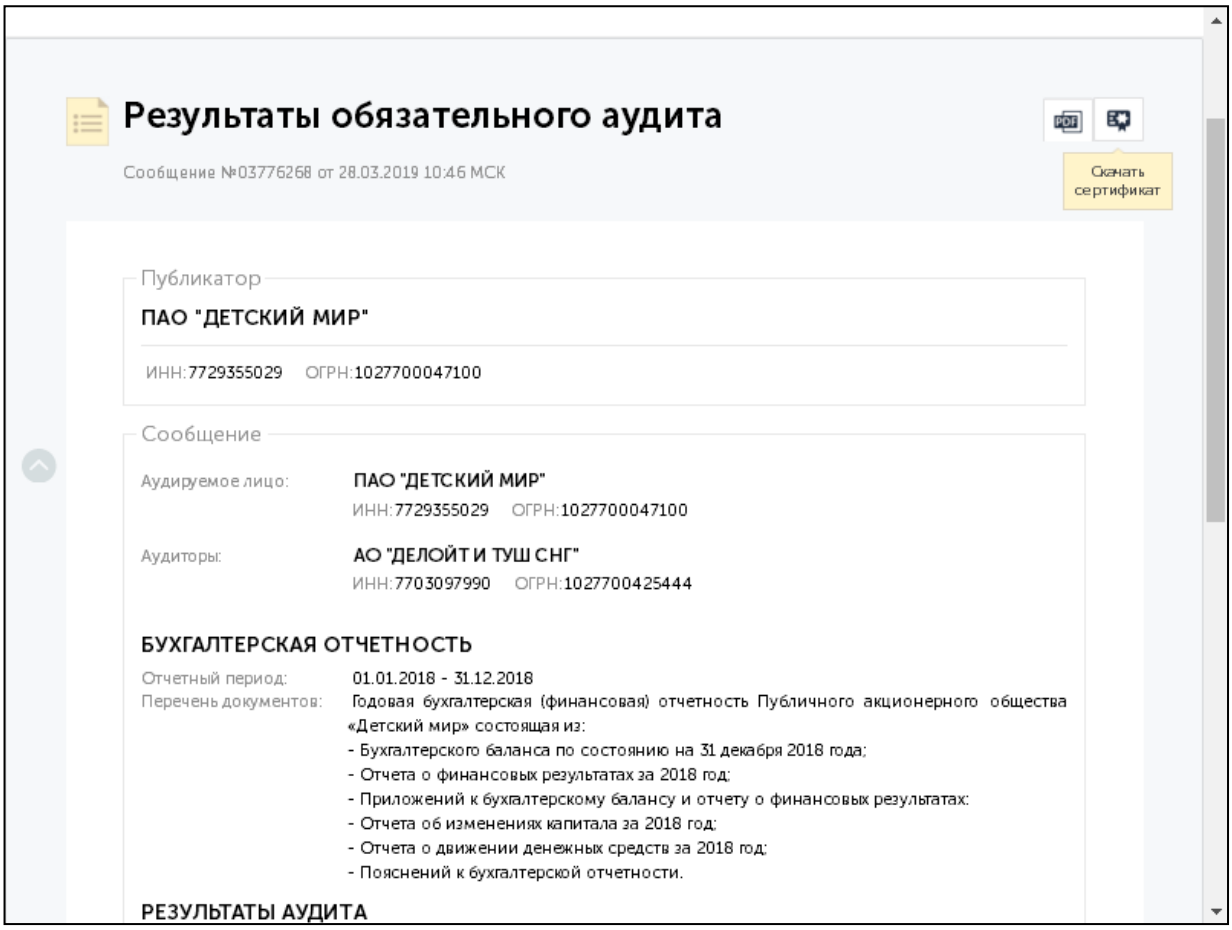

Рис.1. Пример размещения на сайте документа с отсоединенной электронной подписью

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.

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.

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

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. Также в соответствии со статьей 13 этого закона 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, на территории Российской Федерации, в том числе размещать базы данных информации, 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, на территории Российской Федерации.

Пример тестов по теме:

Тест 1

Постройте указанные виды электронной подписи в порядке ВОЗРАСТАНИЯ НАДЕЖНОСТИ идентификации (правильную последовательность укажите цифрами рядом с соответствующими позициями):

- ☐ *1. Усиленная неквалифицированная электронная подпись*
- ☐ *2. Усиленная квалифицированная электронная подпись*
- ☐ *3. Простая электронная подпись*

Правильный ответ: 3; 1; 2.

Тест 2

Укажите, верны или неверны утверждения в области использования электронной подписи:

	Верно	*Не верно*
Использование квалифицированной электронной подписи сводит риск подписания документа неуполномоченным лицом к нулю	☐	☐
Электронная подпись всегда размещается в том же файле, где содержится подписываемый документ	☐	☐
Для проверки электронной подписи можно использовать сайт госуслуг	☐	☐

Правильный ответ:
Первое утверждение – не верно.
Второе утверждение – не верно.
Третье утверждение – верно.

Тест 3.

Аудитор готовит отчет клиенту по результатам аудита. В связи с нехваткой времени он решил сохранить данные на Google Диск и доделать отчет дома в выходные. Оцените его действия (выберите ОДИН правильный ответ):

- ☐ *A. Это запрещено, так как не может быть обеспечена конфиденциальность данных аудируемого лица.*
- ☐ *B. Такие действия являются обычной практикой.*
- ☐ *C. Так можно делать, если доступ на Google Диск защищен паролем с высоким уровнем безопасности.*

Правильный ответ: A.

2. Использование информационных технологий в аудите

Перевод бизнес-процессов в электронную форму оказывает на аудиторскую деятельность влияние одновременно по двум направлениям:

1) изменение бизнес-процессов аудируемых лиц, неуклонное увеличение доли операций в цифровом пространстве; в связи с чем возрастает влияние рисков, связанных с использованием информационных технологий аудируемым лицом;

2) изменение бизнес-процессов самой аудиторской организации, замещение традиционных контрольных процедур, осуществляемых аудитором, автоматизированными системами поиска, обработки и анализа информации.

2.1. Использование в ходе аудита данных информационных систем

Значительное количество информации, связанной с деятельностью аудируемого лица, 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 2).

Таблица 2

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 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.

Пример теста по теме

В ходе аудита отчетности ООО «Аметист» выяснилось, что Общество два года назад получило в банке крупный кредит под залог принадлежащего ему здания, однако уже полгода не выплачивает платежи в погашение кредита. Укажите соответствие необходимой аудитору информации и информационных ресурсов, на которых он может получить такую информацию (правильное соответствие укажите графически – линиями или стрелками):

Информация о ведущихся судебных разбирательствах	*Сайт Единого государственного реестра недвижимости*
Информация о ведущемся исполнительном производстве	*Сайт Арбитражного суда*
Информация о факте залога недвижимого имущества	*Сайт Службы судебных приставов*

Правильный ответ:

Информация о ведущихся судебных разбирательствах – Сайт Арбитражного суда.

Информация о ведущемся исполнительном производстве – Сайт Службы судебных приставов.

Информация о факте залога недвижимого имущества – Сайт Единого государственного реестра недвижимости.

2.2. 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 [3]. 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 [4].

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.

Пример теста по теме:

Укажите соответствие между описанием информационной технологии и ее применением (правильное соответствие укажите графически – линиями или стрелками):

Формат передачи регуляторной, финансовой и другой отчетности, основанный на расширяемом языке таксономии	*Умный контракт*
Цифровой контроль за соблюдением условий сделки	*XBRL*
Децентрализованная публичная система информации, представляющая собой связанные в цепочку ячейки	*Блокчейн*

Правильный ответ:

Формат передачи регуляторной, финансовой и другой отчетности, основанный на расширяемом языке таксономии – XBRL.

Цифровой контроль за соблюдением условий сделки – Умный контракт.

Децентрализованная публичная система информации, представляющая собой связанные в цепочку ячейки – Блокчейн.

2.3. Оценка значимости риска использования информационных технологий 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 3).

Таблица 3

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.

Пример теста по теме:

Постройте виды бизнеса аудируемых лиц по степени ВОЗРАСТАНИЯ ВЛИЯНИЯ информационных технологий (правильную последовательность укажите цифрами рядом с соответствующими позициями):

☐ *1. Продажа мебели по интернет-заказам с оплатой банковскими картами*
☐ *2. Обучение слушателей на семинарах с оплатой на счет в банке*
☐ *3. Выращивание овощей на полях с последующей продажей за наличные*
☐ *4. Предоставление микрозаймов онлайн с подтверждением через СМС*

Правильный ответ: 3; 2; 1; 4.

2.4. 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 [5]. Авторизация открывает доступ пользователю после успешного прохождения ими аутентификации.

Способы аутентификации [6]:

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[1].

Пример теста по теме:

Постройте перечисленные способы аутентификации по степени ВОЗРАСТАНИЯ НАДЕЖНОСТИ (правильную последовательность укажите цифрами рядом с соответствующими позициями):

- ☐ *1. Одноразовый пароль*
- ☐ *2. Подтверждение через СМС-сообщение*
- ☐ *3. Подтверждение через отпечаток пальца*
- ☐ *4. Многоразовый пароль*

Правильный ответ: 4; 1; 2; 3.

2.5. Роботизация аудита

Хотя практика аудита за последние 30 лет улучшилась благодаря включению офисного программного обеспечения, такого как Microsoft Excel и Word, программного обеспечения для рабочих документов, такого как CaseWare Working Paper, и таких инструментов аудита, как Audit Command Language (ACL) и CaseWare IDEA, количество ручных, повторяющихся, простых и основанных на правилах задач всё еще отнимает

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

бóльшую часть времени аудиторов [7]. Примерами таких задач являются подготовка данных аудита, организация файлов, интеграция данных из нескольких файлов, выполнение базовых тестов аудита в Excel, копирование и вставка данных и ручные аннотации. Эти задачи не только трудоемки и основаны на правилах; они также подвержены ошибкам. Для дальнейшего повышения эффективности и результативности практики аудита аудиторам необходимо переосмыслить методы и использовать более современные технологии.

Роботизированная автоматизация процессов (RPA – Robotic process automation) – это программное обеспечение, которое взаимодействует с другим прикладным программным обеспечением на уровне пользовательского интерфейса (то есть таким же образом, как и человек) и используется для автоматизации процессов, которые структурированы, основаны на правилах и повторяются, а также с машиночитаемыми данными. RPA может автоматизировать задачи, выполняемые в разных программных приложениях. Кевин Моффит (Kevin Moffit) предложила, чтобы RPA могла способствовать автоматизации процессов аудита [8].

Технология «машинного взгляда». Чтобы RPA можно было масштабировать и использовать во многих средах, данные должны содержать согласованные метки и иметь одинаковый формат. Например, разные организации могут представлять фамилии сотрудников, используя разные метки, такие как «Фамилия сотрудника», «Фамилия» или «Фамилия получателя», что создает препятствия в автоматизации. С использованием стандартной метки (например, «Last_Name») формат этого поля может быть стандартизирован как текст с максимальной длиной 100 символов.

Аналогично при проверке доходов от аренды большого количества объектов недвижимости программа может распознать различные вариации указания объекта в договоре и затем проанализировать данные на предмет соотношения ставки аренды, срока, местоположения объекта, стоимости аренды и т. д.

Часто для анализа больших массивов используют технологии **Big Data** – методы, позволяющие обрабатывать большие массивы данных по многочисленным параметрам за короткий срок.

Использование дронов при инвентаризации активов. Широкое использование беспилотников (дронов) привело к возникновению новой категории технологий – Dronnovation, включающей использование дронов, механических роботов и роботизированных процессов (или ботов) [9]. Дроны лучше проверяют, наблюдают и контролируют, чем люди, а роботы лучше поднимают тяжелые предметы и работают круглосуточно. Снижение затрат делает такие устройства, как дроны и роботы, более

привлекательными для автоматизированных приложений. Дроны позволяют собирать ту информацию, которую раньше в принципе невозможно было собрать.

Беспилотники часто используются для фотографирования, наблюдения и видеозаписи во многих отраслях, таких как сельское хозяйство и добыча полезных ископаемых. С подключенными камерами и датчиками беспилотники могут записывать видео, данные о составе воздуха или веществ, наносить на карту данные. Эти показания и видеоролики затем могут быть переданы в программные приложения для расшифровки и анализа. Такое использование беспилотной техники может быть легко применено для инвентаризации [10]. Новейшие технологии позволяют беспилотникам «видеть» сквозь препятствия, например через коробки и ящики, во всех направлениях, выше или ниже своего местоположения (технология SmartX), что делает их применение эффективным.

Пример теста по теме:

Укажите соответствие между описанием информационной технологии и ее применением в процессе аудита (правильное соответствие укажите графически – линиями или стрелками):

Беспилотники (технология сбора информации дронами)	*Получение внешнего подтверждения от контрагентов*
Распознавание содержания контрактов и анализ данных («машинный взгляд»)	*Информация о количестве засеянных площадей*
Децентрализованная публичная система информации, представляющая собой связанные в цепочку ячейки (блокчейн)	*Анализ содержания накладной*

Правильный ответ:

Беспилотники (технология сбора информации дронами) – Информация о количестве засеянных площадей.

Распознавание содержания контрактов и анализ данных («машинный взгляд») – Анализ содержания накладной.

Децентрализованная публичная система информации, представляющая собой связанные в цепочку ячейки (блокчейн) – Получение внешнего подтверждения от контрагентов.

3. Рекомендации по подготовке к компьютерному тестированию ИТ- компетенций в модуле «Основы аудиторской деятельности»

При подготовке к экзамену следует ориентироваться на темы и вопросы Программы модуля, размещенной на сайте АНО «ЕАК» [11].

В экзаменационный билет по модулю «Основы аудиторской деятельности» входят тесты трех видов:

на знание теоретических основ: применяются для проверки основополагающих знаний, на которых в дальнейшем будет базироваться работа аудитора. Тестами на знание проверяется точная информация, основные определения, принципы, обязательные требования законодательства

на понимание теоретических основ: применяются для проверки понимания основ, принципов или иных базовых знаний. Тесты на понимание могут содержать задание выбрать правильный пример (примеры) в подтверждение принципа или утверждения; обобщить или классифицировать информацию по определенному признаку; интерпретировать ситуацию в соответствии с требованиями стандартов и т.д.

на применение базовых знаний: могут быть представлены в виде схематичного описания практической ситуации, требующей применения основополагающих знаний. Тесты на применение также могут представлять собой вопрос без описания практической ситуации, однако, требующий логических рассуждений и выводов для нахождения правильного ответа.

Тесты по модулю «Основы аудиторской деятельности» в большей степени направлены на понимание нормативно-правовых актов, регулирующих аудиторскую деятельность в РФ. Тесты на знание теоретических основ (базовых принципов и понятий), а также применение базовых знаний используются при проверке соответствующих компетенций, однако их объем в общем количестве тестов меньше, чем тестов на понимание.

По структуре тесты представляют собой вопросы с многовариантным ответом, то есть имеются альтернативы выбора. Однако правильным ответом будет являться только один, который может быть в зависимости от вида теста простым (один вариант, в том числе расчетное значение), или комбинированным (комбинация правильных ответов в виде простой совокупности, или правильно выбранной последовательности, или правильно указанного соответствия).

Тесты по информационным технологиям обязательно включаются в экзаменационный билет в соответствии с Программой модуля по модулю «Основы аудиторской деятельности» по теме 12. «Требования в отношении получения доказательств в отдельных случаях» (п.4.1.Использование информационных технологий в процессе сбора аудиторских доказательств).

В экзаменационном билете для оценки компетенций в области информационных технологий претенденту могут быть предложены следующие типы тестов:

1. **простой тест**: вопрос и только один правильный ответ из 3-5 представленных; либо тест с вариативным количеством правильных ответов: вопрос и несколько правильных ответов из 3-5 представленных;
2. **тест-последовательность**: вопрос и ответ к нему в виде последовательности предлагаемых вариантов ответов;
3. **составной тест**: вопрос и 2-3 мини-вопроса, относящиеся к одной ситуации, в каждом мини-вопросе даны несколько вариантов ответа, например: «верно»/«неверно»;
4. **тест на соответствие**: 2-3 понятия (ключевые слова) должны быть сопоставлены претендентами как логически связанные с соответствующими им 2-3 другими понятиями (ключевыми словами).

Для лучшего понимания данных типов тестов приведем примеры тестов, оценивающих знание и применение информационных технологий на этапе сбора аудиторских доказательств, в соответствии с указанной выше классификацией тестов по типам.

Простой тест:

Адрес сайта в сети "Интернет" в целях обеспечения доступа к информации, размещенной в сети "Интернет, обозначенный символами для удобства пользователей, например, «zakaz.ru» это:

A. Страница сайта
B. Доменное имя
C. Сетевой адрес

Правильный ответ:
B. доменное имя

Тест-последовательность:

Постройте указанные виды электронной подписи в порядке ВОЗРАСТАНИЯ НАДЕЖНОСТИ идентификации (правильную последовательность укажите цифрами рядом с соответствующими позициями):

☐ *1. усиленная неквалифицированная электронная подпись*

☐ *2. усиленная квалифицированная электронная подпись*

☐ *3. простая электронная подпись*

Правильный ответ: 3,1,2

Составной тест:

Укажите, верны или неверны утверждения в области использования электронной подписи:

	Верно	*Не верно*
Использование квалифицированной электронной подписи сводит риск подписания документа неуполномоченным лицом к нулю	☐	☐
Электронная подпись всегда размещается в том же файле, где содержится подписываемый документ	☐	☐
Для проверки электронной подписи можно использовать сайт госуслуг	☐	☐

Правильный ответ:
Первое утверждение – неверно
Второе утверждение – неверно
Третье утверждение –верно.

Тест на соответствие:

В ходе аудита отчетности ООО «Аметист» выяснилось, что Общество два года назад получило в банке крупный кредит под залог принадлежащего ему здания, однако уже полгода не выплачивает платежи в погашение кредита. Укажите соответствие необходимой аудитору информации и информационных ресурсов, на которых он может получить такую информацию:

Информация о ведущихся судебных разбирательствах	*Сайт Единого государственного реестра недвижимости*
Информация о ведущемся исполнительном производстве	*Сайт Арбитражного суда РФ*
Информация о факте залога недвижимого имущества	*Сайт службы судебных приставов*

Правильный ответ:
Информация о ведущихся судебных разбирательствах - Сайт Арбитражного суда РФ
Информация о ведущемся исполнительном производстве- Сайт службы судебных приставов
Информация о факте залога недвижимого имущества - Сайт Единого государственного реестра недвижимости

Использованные 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 – Консультант плюс, дата обращения 30 ноября 2019 года).

2. Ст. 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 ноября 2019 года).

3. 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/.

4. «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/.

5. «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 ноября 2019 года).

6. Цитируется по источнику: https://ru.wikipedia.org › wiki › TLS.

7. 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.

8. «Robotic Process Automation for Auditing», Journal of Emerging Technologies in Accounting, Spring 2018, http://bit.ly/2JKLCee.

9. 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

10. «Drones and Bridge Inspections – Changing the Process», RDO Integrated Controls blog, Oct. 10, 2016, http://bit.ly/2rUVfKs.

11. Сайт АНО «ЕАК» http://www.eak-rus.ru/