Информационная система поддержки аудиторской деятельности

Г.П. Акимова, А.Ю. Даниленко, Е.В. Пашкина, М.А. Пашкин,
А.А. Подрабинович, И.В. Туманова

Федеральное государственное учреждение «Федеральный исследовательский центр «Информатика и управление» Российской академии наук», г. Москва, Россия

Аннотация. В статье рассмотрены особенности создания и внедрения автоматизированных информационных систем для аудиторских организаций. Приведено описание деловой логики таких организаций. Описаны особенности реализации систем, связанные с автоматизируемыми деловыми процессами. Сделан вывод о возможности замещения программного обеспечения в рассматриваемой сфере деятельности отечественными аналогами. Учтен опыт разработки АИС для ряда аудиторских организаций.

Ключевые слова: *автоматизированные информационные системы, информационная безопасность, аудиторская деятельность, аудиторские организации, цифровизация; импортозамещение.*
DOI: 10.14357/20790279230306

Введение

Широкое внедрение информационных технологий во все сферы жизни общества, именуемое в последнее время цифровизацией, требует создания все большего числа автоматизированных информационных систем (АИС) различного назначения [1]. Эти системы, предназначенные для автоматизации деловых процессов организаций всех форм собственности, существенно ускоряют работу и предоставляют возможность гибкого управления организациями их руководителям. Одной из сфер, в которых внедрение АИС приносит существенные преимущества, является аудиторская деятельность.

Правовые основы регулирования аудиторской деятельности определены Законом [2]. Согласно этому закону «Аудиторская деятельность (аудиторские услуги) – деятельность по проведению аудита и оказанию сопутствующих аудиту услуг, осуществляемая аудиторскими организациями, индивидуальными аудиторами». Закон устанавливает, что аудиторская деятельность осуществляется в соответствии со стандартами и иными требованиями, установленными Банком России, саморегулируемой организацией аудиторов. И далее «Аудит – независимая проверка бухгалтерской (финансовой) отчетности аудируемого лица в целях выражения мнения о достоверности такой отчетности».

Поскольку упомянутым законом установлено требование обязательного ежегодного аудита для широкого круга организаций (участники рынка ценных бумаг, различные фонды, акционерные общества, акции которых находятся в собственности Российской Федерации или муниципальных образований и т.д.), спрос на услуги по проведению аудиторских проверок большой. Организаций, оказывающих такие услуги, более 3000, в каждой из них трудится не менее 5 аудиторов [3]. Ряд российских фирм входит в международные сети аудиторских организаций. При этом все аудиторские организации России должны работать в соответствии с международными стандартами аудита (часть 2 статьи 1 Закона [2]).

Следствием такого широкого международного сотрудничества неизбежно стало внедрение программного обеспечения иностранного производства для автоматизации деловых процессов российских аудиторских организаций. В последнее время международные связи в сфере аудиторской деятельности стали разрушаться. Это привело, в частности, к сложностям использования информационных систем зарубежного производства, многие из которых хранят и обрабатывают информацию на серверах, размещенных в иностранных государствах. Следствием этих процессов неизбежно становится потребность в импортозамещении программного обеспечения и технических средств.

1. Деловая логика аудиторских организаций

Аудит выполняется по запросу организации-клиента и включает в себя изучение полученных документов с подготовкой мотивированного заключения. При взаимодействии аудиторской организации и организации-клиента используются различные каналы связи. Помимо обычной пересылки бумажных документов почтой в последнее время все шире применяются современные технологии. Для обмена небольшими объемами данных используется электронная почта, а полноценное взаимодействие выполняется с помощью специально разработанных автоматизированных информационных систем.

Важной особенностью аудиторской деятельности является необходимость сохранения аудиторской тайны. Согласно статья 9 Закона [2] «Аудиторскую тайну составляют любые сведения и документы, полученные и (или) составленные аудиторской организацией и ее работниками, а также индивидуальным аудитором и работниками, с которыми им заключены трудовые договоры, при оказании услуг, предусмотренных настоящим Федеральным законом». И далее «Аудиторская организация и ее работники, индивидуальный аудитор и работники, с которыми им заключены трудовые договоры, обязаны соблюдать требование об обеспечении конфиденциальности информации, составляющей аудиторскую тайну».

Отметим, что в [2] не предусмотрены меры по сохранению конфиденциальности аудиторской тайны, как это оговаривается, например, в случае персональных данных [4, 5] (сертификация информационных систем, применение специально разработанных средств защиты информации, жесткие требования к этим средствам и т.д.). Единственное требование [2] в этой части гласит: «Аудиторская организация, индивидуальный аудитор не вправе передавать сведения и документы, составляющие аудиторскую тайну, третьим лицам либо разглашать эти сведения и содержание документов» и далее «В случае разглашения аудиторской тайны аудиторской организацией, индивидуальным аудитором,… Банком России… лицо, которому оказывались услуги, предусмотренные настоящим Федеральным законом, вправе потребовать от виновного лица возмещения причиненных убытков».

Это означает, что для данных, обрабатываемых и передаваемых в ходе аудиторской деятельности не предусмотрены никакие меры по обеспечению информационной безопасности (которая включает обеспечение конфиденциальности, целостности и доступности информации), в случае нарушения конфиденциальности возможна только финансовая ответственность, а доступность и целостность не рассматриваются. Безусловно, данные, циркулирующие в ходе аудиторской проверки, могут содержать коммерческую тайну [6], персональные данные и другую информацию, защита которой предусмотрена законодательством России, поэтому в большинстве случаев АИС, обрабатывающие такие данные, должны быть надежно защищены.

Внутренними регламентами некоторых аудиторских организаций предусматривается уничтожение всей информации, связанной с завершенными проверками, в базах данных (БД) АИС. Это требование не содержится в Законе, но такая логика работы позволяет существенно уменьшить возможность утечки конфиденциальной информации.

Деловой процесс аудиторской проверки, подлежащий автоматизации с помощью АИС, можно представить следующим образом:

1. Заключение договора на оказание услуг. Отношения аудиторской организации с организацией-клиентом, как правило, долгосрочные. Договор может заключаться на несколько лет.
2. Организация-клиент отправляет запрос в аудиторскую организацию на выполнение работ по аудиту.
3. Назначаются сотрудники, которые будут работать по данному запросу.
4. В организацию-клиент направляется запрос с перечислением документов, которые должны быть предоставлены.
5. Происходит обмен данными между организацией-клиентом и аудиторской организацией, в ходе которого формируется набор документов, устраивающий аудиторов.
6. Выполняется экспертиза полученных материалов сотрудниками аудиторской организации.
7. Готовится заключение по результатам экспертизы.

Таким образом, автоматизированная система должна обеспечивать выполнение обмена документами между обеими организациями, участвующими в процессе. При этом количество документов и их объем могут быть весьма значительными, общий объем данных может составлять сотни гигабайт.

2. Учет особенностей деловой логики при реализации АИС

2.1. База данных пользователей

Если аудиторская организация работает много лет, имеет хорошую репутацию, то у нее, как правило, широкий круг заказчиков, с которыми идет постоянное сотрудничество. Тем самым у корпора-

тивной АИС будет большое количество пользователей, что может оказать существенное влияние на ее архитектуру и реализацию.

Большое количество учетных записей в БД пользователей (свыше 5000) предъявляет повышенные требования к АИС в части реализации алгоритмов авторизации пользователей в системе и управления доступом. Одним из решений, позволяющих упростить работу в этой части, может служить уничтожение учетных записей неактивных пользователей, а именно уволенных сотрудников организации и сотрудников организаций-клиентов, работа с которыми завершена. С другой стороны, последний вариант может оказаться нецелесообразным, поскольку отношения аудиторской организации с организациями-клиентами часто бывают долгосрочными в виду того, что аудиторские проверки выполняются регулярно, а для многих организаций ежегодно.

2.2. Авторизация в АИС

При создании АИС аудиторской организации, как и в случае любой АИС, требуется выбрать алгоритмы идентификации и аутентификации, позволяющие идентифицировать пользователя и проверить его полномочия с целью дальнейшей авторизации пользователя, т.е. предоставления ему полномочий для работы в системе. Применение аппаратных средств или биометрии для внешних пользователей и сотрудников организации-клиента, практически нереально, поэтому используется традиционная схема с вводом логина (системного имени) и пароля. Поскольку для внешних пользователей личное получение этих атрибутов невозможно, то требуется разработка схемы их получения в удаленном режиме. При этом само создание учетной записи для внешнего пользователя выполняет сотрудник аудиторской организации, основные данные сотрудников организации-клиента передаются в аудиторскую организацию по электронной почте. В состав этих данных входят фамилия, имя, отчество, почтовый адрес на сервере корпоративной электронной почты, предпочтительный вариант написания системного имени. При создании учетной записи для нее задаются системное имя (оно может отличаться от предложенного, поскольку именно такое написание может уже использоваться для другого пользователя АИС) и временный (или одноразовый) пароль. Эта информация отправляется внешнему пользователю на предоставленный электронный адрес, далее он средствами АИС при первом соединении с сервером должен установить для себя постоянный пароль. С этой целью возможна реализация отдельной страницы для первого входа, на которой не будет возможности никаких действий, кроме смены пароля.

Для внутренних пользователей, сотрудников аудиторской организации возможно использование парольной аутентификации, при этом создание учетных записей существенно проще, чем в случае внешних пользователей. Если все сотрудники аудиторской организации зарегистрированы в домене корпоративной вычислительной сети, то возможно использование доменной идентификации и аутентификации. В этом случае вся информация о пользователе извлекается из БД домена.

2.3. Применение облачных технологий

Существенным вопросом при заказе, разработке и внедрении АИС в любой организации является выбор вычислительных мощностей для сервера АИС. Возможные варианты: самостоятельная закупка оборудования и аренда вычислительных ресурсов у сторонней организации. В последнее время появилась новая возможность, точнее модификация второго варианта, использование облачных сервисов. Этот вариант отличается от традиционной аренды вычислительных ресурсов тем, что арендодатель предоставляет достаточно широкий набор дополнительных услуг.

Самое главное достоинство применения облачных сервисов для решения своих бизнес-задач состоит в существенном сокращении расходов на вычислительные ресурсы. При этом необходимо учесть, что помимо прямых расходов на закупку оборудования затраты на собственные хранилища данных включают расходы, связанные с обслуживанием всего программно-аппаратного комплекса, в частности на его квалифицированное администрирование. Следует также учесть, что в случае применения облачных технологий потребитель получает готовые решения, которые прошли апробацию большим числом пользователей. При этом основное отличие от покупаемых отдельно программных продуктов состоит в том, что провайдер облака обеспечивает совместимость различных компонент, наличие необходимых драйверов, а также своевременное и качественное обновление версий всех используемых программных продуктов. То же самое относится и к антивирусной защите, обеспечиваемой централизованно во всем облаке, что позволяет наиболее эффективно использовать все возможности антивирусных программных продуктов с регулярным обновлением их собственных баз данных и программных модулей.

2.4. Архитектура информационной системы

С точки зрения архитектуры АИС для аудиторской организации предпочтителен вариант тонкого клиента, когда в качестве клиентского приложения

используется стандартный интернет-браузер в отличие от архитектуры с использованием толстого клиента, при котором на клиентское место устанавливается отдельное специально разработанное приложение. Фактически вариант тонкого клиента оказывается безальтернативным вследствие большого числа пользователей, не являющихся сотрудниками аудиторской организации, поскольку установка своих программ в организациях-клиентах сложна технически и организационно.

2.5. Информационные объекты и права доступа

При проведении конкретной аудиторской проверки обычно занято несколько человек со стороны организации-клиента и несколько сотрудников аудиторской организации. Работа ведется в рамках проекта, соответственно имеется возможность образовать команду проекта, в которую входят сотрудники обеих организаций. С точки зрения АИС проект описывается отдельным информационным объектом, реквизитами которого должны быть название, краткое описание, даты открытия и завершения работ, состав команды проекта. При этом для команды проекта целесообразно создать группу в БД пользователей АИС для задания прав доступа на информационные объекты в проекте, назначить руководителя проекта и менеджера из числа сотрудников аудиторской организации.

Все передаваемые между организацией-клиентом и аудиторской организацией данные циркулируют в виде файлов, в БД АИС для каждого из них создается отдельный информационный объект, связываемый с объектом, описывающим проект. Создание объектов для файлов позволяет выполнять все действия стандартным для АИС образом: выполнять поиск, открывать файл для просмотра, задавать права доступа, экспортировать информацию из БД в виде файла.

Права доступа к информационным объектам должны задаваться с учетом деловой логики, реализуемой в рамках АИС и определяемой Законом. Вся информация доступна только членам команды проекта, это требование прямо следует из Закона. Права могут задаваться следующим образом:

– создание файлов в проекте доступно только членам команды проекта;
– чтение доступно всем членам команды. Это право может быть ограничено создателем объекта, менеджером или руководителем проекта. Ограничение может касаться запрета чтения для всех сотрудников организации-клиента, кроме создателя файла. Такой запрет обычно связан с финансовыми документами, в первую очередь с данными о зарплатах, премиях и других выплатах;
– права на редактирование определяются деловой логикой конкретной аудиторской организации: оно может быть полностью запрещено для файлов, уже находящихся в БД АИС или разрешено создателю этого информационного объекта. Разрешено редактирование реквизитов информационного объекта создателю в части описания файла, сотрудникам аудиторской организации для служебных пометок и системным учетным записям для ведения протокола работы, т.е. записей о чтении файла, редактировании реквизитов и других подобных действиях;
– уничтожение информационных объектов членам проектной команды обычно запрещено, в случае обнаружения ошибок в представленных данных создатель файла может подготовить его новую версию или объекта (возможен вариант включения новой версии в существующий объект). Регламентом работы аудиторской организации может быть предусмотрено уничтожение всей информации по завершенной проверке. Это действие подразумевает уничтожение файлов и должно выполняться автоматически по отдельной команде руководителя или менеджера проекта, но описывающие файл информационные объекты, могут сохраняться для формирования различных отчетов (необходимость их уничтожения определяется логикой работы аудиторской организации);
– изменение прав доступа к информационным объектам для АИС, работающих в аудиторских организациях, в большинстве случаев не требуется. Исключением может быть установка запрета на чтение, описанного ранее. Тем не менее, само наличие такой возможности требует предусмотреть при разработке АИС возможность изменения прав доступа для создателей информационных объектов, менеджеров и руководителей проектов.

2.6. Особенности проектов как информационных объектов

Отдельно следует рассмотреть процедуры создания, редактирования и уничтожения проектов. При работе с проектами неминуемо приходится вносить изменения в БД пользователей АИС, а именно создавать новые учетные записи и включать их в группу, соответствующую команде проекта. В норме такие действия должны выполняться администратором безопасности АИС, однако в случае аудиторских организаций количество проектов и членов их команд столь велико, что один или два человека просто физически не могут выполнять такой объем работ. В связи с этим в АИС может быть создана отдельная группа пользовате-

лей, члены которой будут исполнять обязанности руководителей и менеджеров проектов (группа руководителей). Члены этой группы наделяются правом создавать учетные записи пользователей (это право может быть ограничено требованием создавать учетные записи только для внешних пользователей, не сотрудников аудиторской организации) и создавать новые проекты, причем в момент создания проекта необходимо указать свою роль в проекте – руководитель или менеджер.

Руководитель или менеджер может назначить сотрудника организации на роль менеджера или руководителя, включить сотрудников своей и внешней организаций в команду проекта. В ряде случаев выдвигается требование реализовать в АИС возможность назначения менеджером или руководителем проекта сотрудника аудиторской организации, не входящего в группу руководителей. В таком случае требуется исключить возможность включения этого пользователя в группу руководителей, т.е. исполнять обязанности руководителя или менеджера он может только для своего проекта.

2.7. Другие особенности АИС для аудиторской организации

В некоторых случаях для повышения уровня конфиденциальности аудиторской информации выдвигается требование запрета получения файлов на рабочих местах пользователей. Этот режим подразумевает просмотр данных на экране без получения исходного файла. Для реализации этой технологии требуется преобразовать файл на сервере АИС в формат, который может быть просмотрен средствами интернет-браузера, например, jpeg или pdf.

Как и в любой АИС, существенной частью функциональных возможностей системы в рассматриваемом случае является формирование различных уведомлений пользователям. Уведомления могут быть связаны как с какими-либо запланированными событиями (приближение срока сдачи документов или завершения работ), так и с событиями в АИС (получение заказанных данных и т.д.).

Применение средств формирования различных отчетов при автоматизации деловых процессов аудиторской организации позволяет отслеживать загрузку сотрудников, сроки выполнения работ, получение и отправку документов. Все перечисленные действия существенно облегчают работу сотрудников и руководителей.

Заключение

Приведенные в статье особенности деловой логики аудиторских организаций (большой объем БД пользователей системы, особенности администрирования и своеобразные алгоритмы назначения прав доступа к информационным объектам) не препятствуют разработке АИС для автоматизации их работы. Отказ от ПО иностранного производства в данной сфере деятельности не должен приводить к критическим последствиям для отрасли в целом, создание российских аналогов зарубежных АИС для поддержки аудиторской деятельности не только возможно, но и не является сложной технически и затратной по ресурсам задачей.

Литература

1. Программа «Цифровая экономика Российской Федерации» http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf.
2. Федеральный закон «Об аудиторской деятельности» от 30.12.2008 № 307-ФЗ с изменениями и дополнениями. https://www.consultant.ru/document/cons_doc_LAW_83311/
3. *Архипова Т.О., Зверев А.А.* Современные тенденции развития аудиторских услуг в России // Молодой ученый. 2021. № 24 (366). С. 212–215. https://moluch.ru/archive/366/82317/ (дата обращения: 10.04.2023).
4. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ http://www.consultant.ru/document/cons_doc_LAW_61801
5. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119.
6. Федеральный закон о коммерческой тайне №98-ФЗ от 29 июля 2004 г.

Акимова Галина Павловна. Федеральный исследовательский центр «Информатика и управление» РАН, г. Москва. Ведущий научный сотрудник, кандидат технических наук. Область научных интересов: системное программирование, системный анализ, информационные технологии, влияние человеческого фактора, информационно-аналитические системы, электронный документооборот, электронный архив. E-mail: akimova@isa.ru

Даниленко Андрей Юрьевич. Федеральный исследовательский центр «Информатика и управление» РАН, г. Москва. Старший научный сотрудник, кандидат физико-матиматических наук. Область научных интересов: системное программирование, системный анализ, информационные технологии, электронный документооборот, информационная безопасность, защита данных. E-mail: danilenko@isa.ru (ответственный за переписку).

Пашкина Елена Владимировна. Федеральный исследовательский центр «Информатика и управление» РАН, г. Москва. Ведущий программист. Область научных интересов: системное программирование, информационные технологии, электронный документооборот, электронный архив. E-mail: pashkina@isa.ru

Пашкин Матвей Александрович. Федеральный исследовательский центр «Информатика и управление» РАН, г. Москва. Ведущий программист. Область научных интересов: системное программирование, информационные технологии, информационно-аналитические системы, электронный архив. E-mail: pashkin@isa.ru

Подрабинович Андрей Александрович. Федеральный исследовательский центр «Информатика и управление» РАН, г. Москва. Ведущий программист. Область научных интересов: системное программирование, проектирование и создание методов и программных средств управления электронными документами, защита информации в документооборотных системах. E-mail: podrabinovich@isa.ru

Туманова Ирина Владимировна. Федеральный исследовательский центр «Информатика и управление» РАН, г. Москва. Ведущий программист. Область научных интересов: системное программирование, информационные технологии, электронный документооборот, электронный архив. E-mail: tumanova-irin@mail.ru

Audit Support Information System

Akimova G.P., Danilenko A.Yu., Pashkina E.V., Pashkin M.A., Podrabinovich A.A., Tumanova I.V.
Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, Moscow, Russia

Abstract. The article discusses the features of the creation and implementation of automated information systems for audit organizations. The description of the business logic of such organizations is given. The features of the implementation of systems associated with automated business processes are described. The conclusion is made about the possibility of replacing software in the considered field of activity with domestic analogues. In preparing the article, the experience of developing AIS for a number of audit organizations was taken into account.

Keywords: *automated information systems; information security; audit activity; audit organizations; digitalization; import substitution*.
DOI: 10.14357/20790279230306

References

1. Programma “Tsifrovaya ekonomika Rossiyskoy Federatsii” [Program “Digital Economy of the Russian Federation”]. http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf.
2. Federal’nyy zakon «Ob auditorskoy deyatel’nosti» ot 30.12.2008 № 307-FZ. [Federal Law “On Auditing” dated December 30, 2008 No 307-FZ]. https://www.consultant.ru/document/cons_doc_LAW_83311/.
3. *Arkhipova T.O., Zverev A.A.* Sovremennyye tendentsii razvitiya auditorskikh uslug v Rossii // Molodoy uchenyy. 2021. № 24 (366). S. 212–215. [Arkhipova T. O., Zverev A. A. Modern trends in the development of audit services in Russia // Young scientist. 2021. No. 24 (366). pp. 212–215]. https://moluch.ru/archive/366/82317.
4. Federal’nyy zakon “O personal’nykh dannykh” ot 27.07.2006 № 152-FZ. [Federal Law “On Personal Data” of July 27, 2006 No 152-FZ]. http://www.consultant.ru/document/cons_doc_LAW_61801.
5. Ob utverzhdenii trebovaniy k zashchite personal’nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal’nykh dannykh. Postanovleniye Pravitel’stva Rossiyskoy Federatsii ot 1 noyabrya 2012 g. № 1119. [On the approval of requirements for the protection of personal data during their processing in personal data information systems. Resolution of the Government of the Russian Federation of November 1, 2012 No 1119].

6. Federal'nyy zakon o kommercheskoy tayne № 98-FZ ot 29 iyulya 2004 g. [Federal Law on Trade Secrets No. 98-FZ of July 29, 2004].

Akimova G.P. Ph.D.(Eng.), Leading Research Scientist, Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia, author of more than 50 printed works, research interests: system programming, system analysis, information technology, the influence of the human factor, information and analytical systems, electronic document management, electronic archive. E-mail: akimova@isa.ru

Danilenko A.Yu. Ph.D.(Phys.-Math.), Senior Research Scientist, Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia, author more than 40 publications (1 monograph), research interests: system programming, system analysis, information technology, electronic document management, information security, data protection. E-mail: danilenko@isa.ru

Pashkina E.V. Leading Programmer, Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia, author of more than 15 publications, research interests: system programming, information technology, electronic document management, electronic archive. E-mail: pashkina@isa.ru

Pashkin M.A. Research Scientist, Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia, author of more than 15 publications, research interests: system programming, information technology, information and analytical systems, electronic archive. E-mail: pashkin@isa.ru

Podrabinovich A.A. Leading Programmer, Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia, author of more than 15 publications, research interests: system programming, design and creation of methods and software for managing electronic documents, protection of information in document circulation systems. E-mail: podrabinovich@isa.ru

Tumanova I.V. Leading Programmer, Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia, author of more than 5 publications, research interests: system programming, information technology, electronic document management, electronic archive. E-mail: tumanova-irin@mail.ru