

В. А. Астафьева (v_astaf@mail.ru),
канд. экон. наук, доцент

Т. М. Моисеева (moiseevl@mail.ru),
канд. техн. наук, доцент

Е. В. Ковальчук (kovalchuk@open.by),
ст. преподаватель

Белорусский торгово-экономический
университет потребительской кооперации
г. Гомель, Республика Беларусь

ОБЛАЧНЫЕ ТЕХНОЛОГИИ В БУХГАЛТЕРСКОМ УЧЕТЕ: ПРОБЛЕМЫ, РИСКИ, РАЗВИТИЕ

В статье рассмотрены вопросы, связанные с рисками, возникающими при использовании облачных технологий при автоматизации бухгалтерского учета.

The questions related risks involved in using the cloud technologies in the automation of accounting.

Бурное развитие современных информационных технологий предопределяет новые формы использования программных продуктов по автоматизации бухгалтерского учета. Среди основных тенденций развития информационных технологий следует выделить одну из главных – использование интернет-технологий. Реализация данного направления предполагает применение облачных технологий.

Облачные технологии в настоящий момент развиваются стремительно и охватывают все больше сфер (например, происходит повсеместное внедрение электронного документооборота организаций с соответствующими субъектами налоговой и банковской систем, системы пенсионного обеспечения и социального страхования). На рост роли облачных технологий нацелена государственная политика Республики Беларусь. В 2014 г. принят Указ Президента Республики Беларусь № 46 «Об использовании государственными органами и иными государственными организациями телекоммуникационных технологий», который регламентирует создание G-Cloud (государственного облака). В соответствии с этим документом первый инфраструктурный оператор beCloud определен оператором республиканской платформы, действующей на основе технологий облачных вычислений. В настоящее время beCloud уже реализует пилотный проект по миграции в облако информационных систем Министерства по налогам и сборам Республики Беларусь. А к концу 2018 г. все органы государственного управления и государственные организации будут использовать в своей работе облачные технологии за счет подключения их к республиканской платформе.

По информации, опубликованной в авторитетном журнале Byte, в течение периода 2014–2018 гг. объем вычислений, выполняемых в публичных облаках, будет расти со скоростью 44% в год [1].

В специальной литературе различают несколько видов сервисов для использования облачных технологий, среди которых выделяют 3 основных:

- Платформа как услуга (platform as a service – PaaS). При таком использовании облачных технологий потребителю предоставляются средства для развертывания на облачной инфраструктуре создаваемых или приобретаемых им приложений, разрабатываемых с использованием поддерживаемых провайдером инструментов и языков программирования.

- Инфраструктура как услуга (infrastructure as a service – IaaS). Пользователю предлагаются для использования средства обработки данных, их хранения и другие возможности, на основании которых можно выполнять произвольное программное обеспечение.

- Программное обеспечение как услуга (software as a service – SaaS). Пользователю доступно программное обеспечение, развернутое на удаленных серверах, доступ к которым обеспечивается через сеть «Интернет». Такой вид услуги исключает оплату за лицензирование и обновление программного обеспечения [2].

На рисунке 1 представлены 3 вышерассмотренных сервиса с точки зрения конечных пользователей.

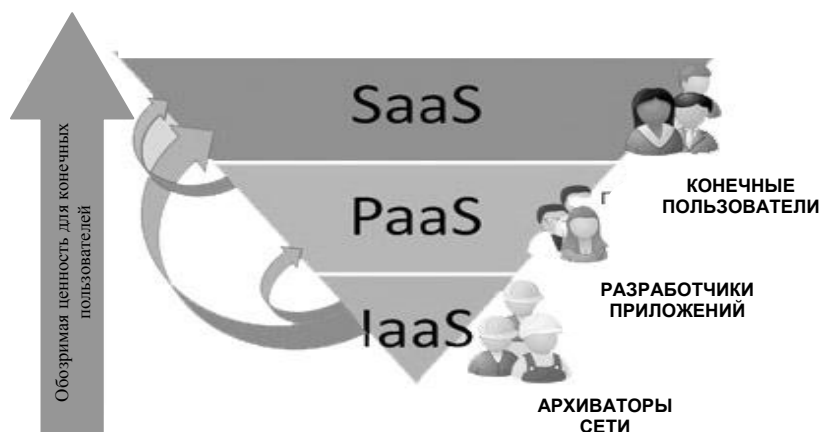


Рисунок 1 – Модели работы с облаком для разных групп пользователей

При автоматизации бухгалтерского учета наибольшее развитие получила облачная технология *программного обеспечения как услуги*. С точки зрения информационных технологий в бухгалтерском учете под облаком понимают сеть компьютеров, обеспечивающих работу определенного прикладного программного обеспечения и предоставляющих пользователю возможность работы с этими программными продуктами за определенную плату либо бесплатно, а также хранения собственной информации [2].

Ключевыми преимуществами данного сервиса являются радикальное сокращение затрат на развертывание программного обеспечения в организации и быстрота внедрения прикладных разработок, доступ к которым осуществляется через обычный браузер. В отличие от традиционных решений SaaS-сервисами можно начать пользоваться сразу после оплаты, что бывает крайне выгодно в условиях быстро растущего малого и среднего бизнеса. К тому же организации могут легко прогнозировать и оптимизировать расходы, периодически оплачивая только то количество лицензий, которое реально задействовано в работе.

Началом распространения облачных технологий в бухгалтерском учете послужило развитие платформы 1С и выпуск платформы «1С: Предприятие 8.2». Вариация 8.2 в отличие от предыдущих версий позволила организовать работу в тонком и даже web-клиенте. Дальнейшее развитие данная технология получила в семействе программ «1С: Предприятие 8.3». Аренда продуктов 1С в облаке по системе SaaS позволяет работать с программным обеспечением как с услугой с ежемесячной абонентской платой. Данный тип услуги обеспечивает полную мобильность. Неважно, где находятся сотрудники, – везде, где есть Интернет, они смогут работать с программами 1С удаленно.

Реализация способа работы с программами 1С в облаке в Республике Беларусь распространена не так широко, как в Российской Федерации и Украине. Прежде всего это обусловлено тем обстоятельством, что платформа «1С: Предприятие 8.3» и прикладные решения по бухгалтерскому учету на ее основе в Республике Беларусь были разработаны лишь в 2014 г. и, как следствие, наблюдается низкое использование данного сервиса.

Развитие облачных технологий в бухгалтерском учете зависит и от уровня компьютерной грамотности специалистов по бухгалтерскому учету. Как показывает практика, большинство руководителей и специалистов по бухгалтерскому учету в Беларуси не владеют содержанием облачных сервисов и настроены весьма отрицательно по перспективам их использования. Основная составляющая опасений – проблемы безопасности, причем, в широком значении этого слова. Под подозрением несанкционированного доступа находятся как располагаемые в «невесомости» данные, доступ к ним, так и сама технология в целом.

Более того, мало кто из провайдеров облачных услуг может в доступной форме изложить заказчику эти риски, определить используемые механизмы защиты своих сервисов и инфраструктуры.

Безусловно, данные риски существуют при любой форме использования сети «Интернет». Вместе с тем развитие электронного документооборота в Республике Беларусь и в рамках этого принятие в 2014 г. ряда нормативно-правовых актов, регламентирующих использование товарно-транспортных и товарных накладных в виде электронных документов, предопределяют расширение использования Интернета в бухгалтерском учете и предполагают проведение работ по минимизации данных рисков. Следовательно, вопросы информационной безопасности и управления рисками будут одними из ключевых при условии перехода в облака.

На наш взгляд, использование облачных технологий в прикладном программном обеспечении по бухгалтерскому учету будет все более расширяться, и задача менеджера – обеспечить минимизацию всех видов рисков. Повышение безопасности облачных сервисов возможно при активном участии двух сторон – заказчиков и провайдеров. Бухгалтера, оценив риски, начнут применять прикладные решения, предназначенные для защиты данных и сервисов в облачной среде, что позволит снизить эти риски до приемлемого уровня. Провайдеры облачных услуг будут планомерно выполнять рекомендации и лучшие

практики экспертов по защите облачных вычислений, а не просто декларировать защищенность своих сервисов. Без осознания специалистами по бухгалтерскому учету возможности защиты данных и сервисов в облаке никакие экономические выгоды от внедрения не смогут привести к значительному росту использования облачных сервисов.

Для того чтобы проводить работу по снижению рисков, следует их идентифицировать. Большинство менеджеров по бухгалтерскому учету и ведущих специалистов в области информационных технологий выделяют лишь риски, связанные с безопасностью информации и ее несанкционированным использованием. На наш взгляд, здесь имеет место гораздо более широкий спектр рисков: технических, юридических, операционных и информационных. Изучив опыт использования облачных технологий в бухгалтерском учете (программа «1С: Бухгалтерия 8.2»), были выделены виды рисков, представленные на рисунке 2.

Виды рисков и направления их минимизации зависят от видов облачных сервисов (IaaS, PaaS, SaaS) и форм использования облачных технологий (частное, публичное или комбинированное облако). Если частное облако находится в собственности организации и физически существует внутри ее юрисдикции, то возможно абстрагироваться от идеи облака и полагать, что организация его не использует. При использовании частного облака можно считать клиентами работников организации, а ее саму – провайдером услуг. Данная форма использования облачных сервисов в основном применяется крупными организациями.



Рисунок 2 – Виды рисков использования облачных технологий в бухгалтерском учете

На рисунке 3 представлена информация о реализации защиты данных при различных видах использования облачных сервисов.

IaaS	PaaS	SaaS
<ul style="list-style-type: none"> Заказчик облачных услуг может использовать любые средства защиты, устанавливаемые на предоставляемую аппаратную платформу 	<ul style="list-style-type: none"> Заказчик облачных услуг привязан к предоставляемой платформе. Выбор средств защиты информации платформы (особенно сертифицированных) ограничен и, как правило, лежит на облачном провайдере. Заказчик может настраивать функции защиты приложений. Компромисс между средствами защиты и облачными услугами 	<ul style="list-style-type: none"> Заказчик облачных услуг не имеет возможности по выбору средств и механизмов защиты облака. Выбор лежит на облачном провайдере

Рисунок 3 – Виды облачных сервисов и реализация защиты данных

Как видно из рисунка 3, в зависимости от выбора облачных технологий вопросы по обеспечению информационной безопасности частично может решать потребитель облачных услуг. Но в нашем случае облако по модели SaaS, обеспечение информационной и технической безопасности предоставлено провайдеру облачных услуг.

Перед использованием облачных технологий в бухгалтерском учете после идентификации рисков должна проводиться работа по их минимизации и мониторингу. Основной проблемой в оценке рисков является неопределенность, выраженная в терминах вероятности. Некоторыми учеными предлагается количественно оценивать риски применения облачных ИТ-сервисов на основе аддитивной модели анализа. Для построения аддитивной модели предлагается использовать 6 показателей: сохранность хранимых данных, защита данных при передаче, аутентификация, изоляция пользователей, нормативно-правовые вопросы, реакция на происшествие [3].

Данный подход в оценке рисков использования облачных технологий представляется оправданным, однако в случае функционирования программ по бухгалтерскому учету в облачных сервисах число параметров оценки увеличивается, и, более того, некоторые из них сложно количественно оценить. Основным видом оценки рисков в данном случае должна выступать экспертная оценка работы облачного провайдера. Этот вид работ может осуществляться в несколько этапов: на этапе заключения договора с провайдером и в процессе эксплуатации программы.

На наш взгляд, на первом этапе следует обратить внимание на деловую репутацию провайдера, наличие опыта работа в данной области, сертифицированных специалистов по платформе «1С: Предприятие 8.3» и бухгалтерскому учету, а также предоставление возможности поддержки по ведению бухгалтерского учета в программах 1С по многоканальному телефону.

Первоочередная задача провайдера – обеспечить соответствие облака требованиям нормативных документов и стандартов в области информационной безопасности. Следует предварительно, самостоятельно или с привлечением лицензиата Оперативно-аналитического центра при Президенте Республики Беларусь (ОАЦ) провести анализ выполнения требований нормативных правовых актов по защите информации в информационной системе.

Приказом ОАЦ от 16 января 2015 г. № 3 утверждены правовые акты, регламентирующие сертификацию средств криптографической защиты информации, и документов на соответствие требованиям безопасности.

Приказ определяет необходимость создания доступных в ценовом и техническом аспекте механизмов и средств, обеспечивающих идентификацию и аутентификацию пользователей, конфиденциальность и целостность сообщений в системах и сетях общего пользования и др. Грамотное использование надежных криптографических механизмов позволяет минимизировать риски использования облачных технологий.

Следующим шагом является заключение договора на предоставление облачного сервиса по использованию программ по автоматизации бухгалтерского учета. В основе договорных отношений часто лежит принцип «все или ничего», когда пользователю предлагается принять условия договора без каких-либо изменений или отказаться от использования сервиса.

Пользователям при вступлении в такие соглашения рекомендуется оценивать риск прекращения провайдером соответствующей деятельности (по возможности получать информацию о его финансовой состоятельности, опыте деятельности на рынке и т. п.).

При анализе договоров следует обратить внимание на следующее:

- Прописаны ли технические характеристики (уровень сервиса, устанавливающий качественные параметры предоставляемой услуги).

- Имеется ли ответственность за недоступность (временную или постоянную) сервера.
- Указана ли информация о том, в какой стране (странах) находятся серверы.
- Предусматривается ли обязанность по сохранению и восстановлению информации (например, создание резервных копий данных), и каковы последствия ее несоблюдения.
- Зафиксированы ли обязательства провайдера облачных услуг по сохранению конфиденциальности данных пользователя, защите его данных, в том числе с помощью криптографических средств, шифрования.
- Какие существуют основания и последствия расторжения договора (имеется ли обязанность удалить информацию с сервера после расторжения договора, установлен ли срок удаления информации; если информация не удаляется, в каких пределах возможно ее дальнейшее использование провайдером).
- Каковы последствия неоплаты услуг (удаление информации, приостановление доступа к информации и др.) [4].

С нашей точки зрения, с целью минимизации технических и информационных рисков и увеличения ответственности провайдера за их возникновение в договоре также необходимо предусмотреть:

- возможность круглосуточного доступа к облаку 7 дней в неделю и круглосуточное обслуживание серверов техническими специалистами;
- ежедневное резервное копирование и архивирование информационных баз (срок хранения каждой копии архива – не менее 30 дней);
- возможность доступа пользователя к своим резервным копиям для скачивания на свой компьютер (при необходимости);
- шифрование каналов связи;
- организацию зонирования выделенной для пользователя сети, очистку дисков после обращения к ним, аутентификацию файловой системы;
- необходимость установки обновлений бухгалтерской программы сразу после их выхода без взимания дополнительной оплаты;
- наличие службы поддержки, консультанты которой должны отвечать на вопросы пользователя по чату или многоканальному телефону.

Большинство рисков может быть нивелировано именно на этапе заключения договора посредством установления гарантий, штрафов и т. д. Первое, на что следует обратить внимание, – это наличие в договоре так называемых выкупных платежей, т. е. предусмотренной суммы, которая взимается с потребителя за изъятие информации до определенного в договоре срока. Если такой пункт есть, то у организации могут возникнуть затруднения при ее переходе на обслуживание к другому поставщику услуг. В договоре должны быть четко прописаны конкретные размеры штрафов и те санкции, которые будут наложены на поставщика облачных услуг при утрате или повреждении хранящейся у него информации.

Для минимизации рисков у пользователя бухгалтерской программы важно обратить внимание на обеспечение информационной безопасности непосредственно в программе по автоматизации бухгалтерского учета, которая может гарантироваться двухуровневой защитой. Во-первых, это автоматическое шифрование канала передачи данных по средствам SSL-сертификатов, что обеспечивает безопасность передаваемой информации и защиту от несанкционированных действий злоумышленников по ее перехвату. Во-вторых, это защищенный авторизацией доступ пользователя к программе. При любом типе подключения – через опубликованное приложение или терминальный доступ – должна прилагаться антивирусная защита.

Отдельное место занимает ответственность бухгалтеров за несанкционированный доступ к данным. С целью минимизации данных рисков в контрактах с работниками в должностных инструкциях следует указывать меру ответственности за передачу паролей и конфиденциальной информации третьим лицам.

При выполнении вышеназванных условий по минимизации рисков использование облачных технологий в бухгалтерском учете имеет определенные перспективы, прежде всего, в среде малого и среднего бизнеса, что связано с более низкой стоимостью внедрения и эксплуатации программ.

Список использованной литературы

1. **Облачные** вычисления: статистика и прогнозы [Электронный ресурс]. – Режим доступа : <http://www.bytemag.ru/articles/detail.php?-ID=24720>. – Дата доступа : 18.05.2015.
2. **Официальный сайт** ООО «1С» [Электронный ресурс]. – Режим доступа : <http://www.v8.1c.ru>. – Дата доступа : 17.05.2015.
3. **Разумников, С. В.** Моделирование оценки рисков при использовании облачных ИТ-серверов / С. В. Разумников // *Фундам. исслед.* – 2014. – № 5. – С. 39 – 44.
4. **Шакель, Н. В.** Юридические аспекты использования облачных технологий / Н. В. Шакель // *Журн. междунар. права и междунар. отношений.* – 2014. – № 4. – С. 3–7.