В. А. Канашевский*

ЮРИДИЧЕСКИЕ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ РОССИЙСКИМИ БАНКАМИ ОБЛАЧНЫХ УСЛУГ ЗАРУБЕЖНЫХ ПРОВАЙДЕРОВ

Аннотация. *В статье исследуются правовые аспекты использования российскими банками облачных решений зарубежных провайдеров. Несмотря на очевидные преимущества, в законодательстве России имеется множество препятствий для такого использования, в том числе отсутствие общего нормативного регулирования услуг облачных вычислений, требования к обеспечению информационной безопасности (лицензирование шифровальной деятельности, сертификация информационных систем), требования законодательства о локализации баз персональных данных, электронных баз данных банков и др. На основе анализа действующих нормативных актов, в частности отраслевых регуляторов, автор приходит к выводу, что зарубежные поставщики облачных услуг вправе предоставлять услуги российским финансовым организациям при соблюдении ряда условий: облачные решения не должны включать аутсорсинг бизнес-функции целиком и не должны предполагать производство внутренних (внутрироссийских) переводов денежных средств (платежей); зарубежный облачный провайдер принял меры к охране защищаемой информации; трансграничная передача персональных данных и банковской тайны должна осуществляться в обезличенном виде и др.*

Ключевые слова: *услуги облачных вычислений, зарубежный провайдер, персональные данные, банк, финансовая организация, информационная безопасность, конфиденциальная информация, открытая информации, лицензирование шифровальной деятельности, сертификация информационных систем, защита информации, компенсирующие меры, аутсорсинг бизнес-функций, трансграничная передача защищаемой информации, центр обработки данных.*

DOI: 10.17803/1729-5920.2019.148.3.108-115

В настоящее время многие финансовые организации в России стремятся сократить расходы на программное обеспечение и инфраструктуру за счет обращения к облачным решениям. Об этом свидетельствуют многочисленные исследования и данные статистики. Так, по оценкам компании Gartner Group, сегодня более 50 % банковских транзакций по всему миру осуществляется посредством облачной инфраструктуры[1]. Внедрение технологий облачных

[1] См.: *Кораблев А. В.* Идентификация информационных рисков использования облачных технологий в банковской деятельности : дис. … канд. экон. наук. Самара, 2017. С. 3.

* *Канашевский Владимир Александрович,* доктор юридических наук, профессор, профессор кафедры международного частного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
vakanashevskij@msal.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

вычислений позволяет существенно сократить расходы и повысить уровень обслуживания. Наиболее популярными и востребованными на рынке являются облачные решения, предоставляемые зарубежными провайдерами, такими как Microsoft (например, Microsoft Azure), Google (например, Google Cloud Platform), Amazon (например, Amazon Web Services) и др.

Одним из главных препятствий для использования зарубежных облачных решений российскими банками являются требования российского законодательства к обеспечению информационной безопасности. Облачные решения зарубежных провайдеров предполагают передачу информации в центры обработки данных, как правило находящиеся на территории иностранного государства. Как верно отмечается в литературе, предоставление банковских услуг на основе облачных технологий характеризуется возросшим количеством уязвимостей и внешних угроз, что обусловлено использованием открытых каналов связи, а сбои при предоставлении банковских сервисов и разглашение банковской информации могут нанести значительный экономический ущерб банку или его клиентам[2].

Препятствием для использования банками услуг зарубежных облачных провайдеров являются также требования законодательства о локализации баз персональных данных, локализации электронных баз данных банков, локализации информации, распространяемой по сети Интернет и др. Выполнение требований соответствующих нормативных актов приводит к необходимости передачи информации в «первичные» базы данных, расположенные на территории России[3].

Вопрос о гражданско-правовой природе отношений между провайдером облачных решений и пользователями является дискуссионным[4]. Следует согласиться с мнением, что отношения по использованию облачных решений[5] могут быть квалифицированы как смешанные, имеющие признаки лицензионного договора и договора оказания услуг, причем черты последнего преобладают. Один из основных аргументов против лицензионно-правовой природы облачных решений состоит в том, что «используемый клиентом “облачный” сервис может рассматриваться в качестве информационной системы… <…> Предоставление лицензии на информационную систему в целом, в том числе на использование информационных технологий и технических средств, невозможно, поскольку данные объекты не могут выступать объектом лицензионного договора»[6].

В настоящее время в России отсутствует какой-либо нормативный акт, регулирующий предоставление услуг облачных вычислений, в том числе услуг зарубежных облачных провайдеров. Согласно планам Правительства РФ, к концу 2015 г. должны были быть разработаны проекты нормативных актов, направленные на развитие и внедрение технологий облачных вычислений[7], которые до настоящего времени еще не приняты. В 2014—2017 гг. опубликованы проекты федеральных законов касательно технологий облачных вычислений. Перспективы указанных законопроектов в настоящее время неясны.

Проект Закона об облачных вычислениях 2014 г.[8] предлагает ввести ограничения на использование облачных сервисов органами и организациями государственного и муниципального секторов. В частности, проект исходит из того, что только российские юридические лица, которые имеют свою облачную инфраструктуру в России, могут предоставлять облачные услуги

---

2 *Кораблев А. В.* Указ. соч. С. 3.

3 См.: *Канашевский В. А.* Об обязательном хранении информации на территории России (требование локализации) // Международное публичное и частное право. 2017. № 6.

4 См.: *Савельев А. И.* Правовая природа «облачных» сервисов: свобода договора, авторское право и высокие технологии // Вестник гражданского права. 2015. № 5.

5 Традиционными способами организации предоставления облачных решений являются программное обеспечение как услуга (SaaS, Software-as-a-Service), платформа как услуга (PaaS, Platform-as-a-Service) и инфраструктура как услуга (IaaS, Infrastructure-as-a-Service).

6 *Савельев А. И.* Указ. соч.

7 См.: План мероприятий («дорожная карта») «Развитие отрасли информационных технологий», утв. распоряжением Правительства РФ № 2602-р от 30.12.2013 (в ред. от 05.12.2014) // СПС «КонсультантПлюс».

8 Федеральный портал проектов нормативных правовых актов. URL: http://regulation.gov.ru/projects#npa=23163.

для государственного и муниципального секторов. В литературе высказано мнение, что требование законопроекта о наличии у провайдера облачных услуг лицензий в области обеспечения информационной безопасности, выданных Федеральной службой по техническому и экспортному контролю (ФСТЭК) и Федеральной службой безопасности РФ (ФСБ), а также о наличии аттестата по требованиям безопасности на облачную инфраструктуру означает фактический запрет зарубежным облачным провайдерам предоставлять свои услуги российским государственным (муниципальным) органам и не позволяет это делать многим российским облачным провайдерам, которые используют зарубежные сервисы в качестве платформы IaaS или резервной площадки[9].

В 2016 г.[10] и в 2017 г.[11] были опубликованы еще два проекта федеральных законов, ориентированные главным образом на создание государственной инфраструктуры облачных вычислений для использования органами государственной власти, местного самоуправления, государственными и муниципальными предприятиями и учреждениями. Законопроекты 2016 и 2017 гг. не регулируют использование услуг облачных вычислений, предоставляемых иными (то есть негосударственными, немуниципальными и пр.) провайдерами. В частности, в законопроекте 2016 г. отмечается: «В целях создания экономически обоснованных условий для сосредоточения вычислительных ресурсов, а также хранения и обработки персональных данных граждан РФ на территории РФ систему центров обработки данных целесообразно создавать в виде сети федеральных и региональных центров обработки данных, связанных резервированными магистральными каналами связи высокой пропускной способности в единый катастрофоустойчивый кластер. Защита от компьютерных атак должна быть реализована с использованием надежных программно-аппаратных средств и соблюдением принципа невыхода трафика указанного кластера за пределы Российской Федерации». Думается, что законодатель (разработчиком законопроектов выступило Министерство связи и массовых коммуникаций РФ) в качестве своей главной стратегии принял курс на создание в России «государственной инфраструктуры облачных вычислений», услугами которой будут пользоваться как государственные и муниципальные органы и организации, так и третьи лица («электронные коммерческие услуги»). Об услугах зарубежных облачных провайдеров законопроекты умалчивают.

В последнее время в действующее законодательство были внесены существенные изменения, в том числе направленные на расширение полномочий регулирующих органов по осуществлению контроля над информационным содержанием («контентом»), распространяемым в сети Интернет, и предусматривающие обязательства по хранению данных на территории России. Однако эти изменения напрямую не запрещают передачу контента зарубежным провайдерам облачных сервисов и хранение такой информации в центрах обработки данных за пределами Российской Федерации.

Несмотря на отсутствие специального законодательства, можно отметить, что хранение (размещение) информации в зарубежном публичном облаке per se (само по себе) не запрещено и, следовательно, разрешено при условии соблюдения отдельных требований и ограничений, предусмотренных законами и отраслевыми стандартами.

Федеральным агентством по техническому регулированию и метрологии (Росстандарт) принят ГОСТ ISO/IEC 17788-2016 «Информационные технологии. Облачные вычисления. Общие положения и терминология», который был разработан на основе международного стандарта ISO/IEC 17788:2014 «Information technology — Cloud computing — Overview and vocabulary» и применяется с 1 ноября 2017 г.[12]. Продвижению в России технологий облачных вычисле-

---

[9] См.: *Савельев А. И.* Комментарий к Федеральному закону от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» (постатейный). М. : Статут, 2015 (см. комментарий к ст. 12 «Государственное регулирование в сфере применения информационных технологий»).

[10] Федеральный портал проектов нормативных правовых актов. URL: http://regulation.gov.ru/projects#npa=59054.

[11] Федеральный портал проектов нормативных правовых актов. URL: http://regulation.gov.ru/projects#npa=67812.

[12] Информационный портал по международной стандартизации. Национальные стандарты РФ. URL: http://iso.gost.ru/wps/portal.

ний могли бы существенно поспособствовать разработка и принятие в России национальных стандартов по использованию облачных решений на основе стандартов Международной организации по стандартизации (ISO/IEC 27001[13], BS ISO/IEC 27017[14], ISO/IEC 27018[15]).

Перед принятием решения об использовании зарубежных облачных решений российским финансовым организациям необходимо выделить «чувствительную» (конфиденциальную) информацию, которая может быть передана в зарубежное облако только при соблюдении определенных условий. Примерный список такой чувствительной (конфиденциальной) информации включает финансовую информацию, информацию о технической и информационной безопасности, внутренние корпоративные документы, банковскую тайну, персональные данные, информацию о кредитной истории, налоговую информацию, тайну страхования и тайну ломбарда, а также иную информацию, признанную финансовой организацией в качестве «конфиденциальной»[16]. При хранении и обработке чувствительной (конфиденциальной) информации облачный провайдер должен принять определенные меры по защите переданной ему информации, которые (методы) описываются в ряде нормативных актов[17].

К нечувствительной (открытой) информации относится вся иная информация, которая не относится к информации конфиденциального характера. Она может передаваться и обрабатываться в зарубежном публичном облаке без каких-либо ограничений.

Хранение и обработка определенной информации кредитных организаций облачными провайдерами может вызвать также вопросы лицензирования и сертификации (лицензирование шифровальной деятельности, сертификация информационных систем, используемых для хранения и обработки данных и др.). На практике только российские организации могут соответствовать всем требованиям российского законодательства в данной области, и это обстоятельство может служить практическим препятствием для использования услуг зарубежного облачного провайдера. Например, согласно постановлению Правительства РФ № 1119[18] персональные данные (далее — ПДн) подлежат шифрованию в обязательном порядке, если соответствующая информационная система, используемая для обработки ПДн, относится к системам одного из четырех уровней защищенности, определенных постановлением Правительства РФ № 1119 (уровень защищенности присваивается в зависимости от угроз безопасности ПДн). Оценку угроз безопасности проводит оператор ПДн (то есть сам банк). Кроме того, применение средств шифрования для защиты ПДн предусмотрено Методическими рекомендациями ФСБ № 149/7/2/6-432 от 31.03.2015[19].

---

[13] Стандарт ISO/IEC 27001:2013 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

[14] Стандарт BS ISO/IEC 27017:2015 «Информационные технологии. Методы и средства обеспечения безопасности. Свод правил по управлению информационной безопасностью на основе ISO/IEC 27002 для облачных сервисов».

[15] Стандарт ISO/IEC 27018:2014 «Информационные технологии. Методы обеспечения безопасности. Практика защиты персональных данных в публичных облаках, выступающих в роли обработчиков персональных данных».

[16] Примерный состав категорий информации, рекомендуемых для включения в класс «информация конфиденциального характера», содержится в приложении А (справочном) к рекомендациям Банка России в области стандартизации РС БР ИББС-2.9-2016 «Обеспечение информационной безопасности организаций банковской системы РФ. Предотвращение утечек информации».

[17] См. Положение о защите информации в платежной системе (утв. постановлением Правительства РФ от 13.06.2012 № 584); положение Банка России № 382-П (утв. Банком России 09.06.2012, с послед. изменениями); указание Банка России от 09.06.2012 № 2831-У (с послед. изменениями); стандарты Банка России, касающиеся информационной безопасности (СТО БР ИББС-1.0-2014; СТО БР ИББС-1.2-2014); рекомендации Банка России (РС БР ИББС-2.5-2014; РС БР ИББС-2.2-2009; РС БР ИББС-2.7-2015; РС БР ИББС-2.8-2015; РС БР ИББС-2.9-2016) (см.: СПС «КонсультантПлюс»).

[18] Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // СПС «КонсультантПлюс».

[19] См.: Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информаци-

Что касается обязательного шифрования кредитными организациями данных (когда такое шифрование обязательно согласно российскому законодательству), то следует указать следующее.

Во-первых, в России деятельность по шифрованию данных является лицензируемой и при шифровании может использоваться лишь то программное обеспечение и те аппаратные устройства, которые сертифицированы ФСБ[20]. Очевидно, что указанные требования к шифрованию применимы только к российским организациям, поскольку российские регуляторы (ФСБ и др.) не вправе сертифицировать шифровальные средства иностранных организаций (зарегистрированных и действующих за рубежом), а лицензию на шифрование вправе получить лишь российская организация.

Во-вторых, если зарубежный облачный провайдер в рамках оказания им облачных услуг использует информационную систему и меры защиты информации, которые предусматривают такой же уровень защиты информационных систем и такие же меры информационной защиты (включая шифрование данных), которые соответствуют общим техническим и организационным требованиям российского законодательства (либо его меры выше тех требований, которые предъявляются российскими регуляторами), то можно заключить, что данный облачный провайдер вправе осуществлять деятельность по работе с соответствующей информацией (поскольку цель обеспечения информационной безопасности достигнута).

Данный вывод находит поддержку в некоторых нормативных актах. Так, согласно приказу ФСТЭК РФ от 18.02.2013 № 21[21] при невозможности технической реализации отдельных мер по обеспечению безопасности ПДн, предусмотренных постановлением Правительства РФ № 1119, оператор *вправе принимать другие (компенсирующие) меры*, направленные на нейтрализацию актуальных угроз безопасности ПДн. В этом случае в обязательном порядке проводится надлежащее обоснование применения таких компенсирующих мер (п. 10). С учетом вышеизложенного оператор ПДн обязан обеспечить принятие зарубежным облачным провайдером всех необходимых организационных и технических мер, предусмотренных постановлением Правительства РФ № 1119 и приказом ФСТЭК РФ № 21, для надлежащей защиты обрабатываемых ПДн.

Согласно ГОСТ Р 57580.1-2017[22] «при невозможности технической реализации отдельных выбранных мер защиты информации, а также с учетом экономической целесообразности на этапах адаптации (уточнения) базового состава мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию угроз безопасности информации, определенных в модели угроз, и нарушителей безопасности информации финансовой организации. В этом случае финансовой организацией должно быть проведено обоснование применения компенсирующих мер защиты информации» (п. 6.4). При этом финансовая организация *самостоятельно определяет* необходимость использования средств криптографической защиты информации (СКЗИ), если иное не установлено нормативными актами, актами Банка России, стандартами профессиональной деятельности или правилами платежной системы. В случае если финансовая организация *применяет СКЗИ российского производителя*, указанные СКЗИ должны иметь сертификаты или разрешения федерального органа, уполномоченного в области обеспечения безопасности (п. 6.12). Таким образом, ГОСТ Р 57580.1-2017 не исключает использования финансовой организацией СКЗИ иностранного производителя, хотя прямо и не разрешает это делать.

онных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, № 149/7/2/6-432 (утв. ФСБ России 31.03.2015) // СПС «КонсультантПлюс».

[20] См.: постановление Правительства РФ от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств…» (в ред. 18.05.2017) // СПС «КонсультантПлюс».

[21] Приказ ФСТЭК РФ от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (в ред. 23.03.2017) // СПС «КонсультантПлюс».

[22] Национальный стандарт России ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утв. приказом Росстандарта от 08.08.2017 № 822-ст, введен в действие с 01.01.2018 // СПС «КонсультантПлюс».

Согласно п. 6.13 ГОСТ Р 57580.1-2017 «юридические лица или индивидуальные предприниматели, привлекаемые финансовой организацией для проведения работ по обеспечению защиты информации, *должны иметь лицензию* на деятельность по технической защите конфиденциальной информации».

Наконец, Банк России принял рекомендации (например, РС БР ИББС-2.2-2009 и РС БР ИББС-2.9-2016), которые хотя и не носят обязательного характера, но применяются банками в силу авторитета Банка России. Эти рекомендации подразумевают, что кредитные организации должны хранить в России определенную чувствительную информацию (которая определена в рекомендациях очень широко и включает в числе прочего любые ПДн). В отсутствие прямого законодательного запрета на размещение большинства данных в инфраструктуре зарубежного облачного провайдера можно заключить, что данные рекомендации Банка России служат наиболее существенным препятствием для передачи банками данных зарубежному облачному провайдеру.

В частности, согласно Стандарту Банка России об управлении риском нарушения информационной безопасности при аутсорсинге[23] допускается передача на аутсорсинг функций, связанных с хранением и обработкой информации, в том числе на внешних центрах обработки данных и облачных сервисах (облачных службах). Стандарт прямо допускает возможность аутсорсинга бизнес-функций, при выполнении которых осуществляется обработка защищаемой информации[24] (в том числе сведений, относящихся к банковской тайне, ПДн и другой конфиденциальной информации). Примерами бизнес-функций, которые могут быть переданы на аутсорсинг, являются, в частности: аутсорсинг центров обработки данных; облачные вычисления (по модели предоставления сервисов SaaS, PaaS, IaaS); обслуживание информационных (автоматизированных) систем организации банковской системы РФ[25].

Согласно Стандарту финансовая организация должна определить критерии, в том числе основанные на законодательстве РФ о лицензировании отдельных видов деятельности. В частности, у поставщика услуг должны быть лицензия на осуществление деятельности по технической защите конфиденциальной информации, выданная ФСТЭК[26], и лицензия на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, выданная ФСБ РФ[27]. В случае несоответствия поставщика услуг данным критериям ему не могут передаваться на выполнение существенные функции (п. 6.5). Отметим, что указанные лицензии могут получить лишь российские юридические лица. Это обстоятельство служит препятствием для зарубежных облачных провайдеров к выполнению функции поставщиков аутсорсинговых услуг.

Стандарт указывает, что финансовой организации при принятии решения об аутсорсинге существенных функций, при котором предполагается трансграничная передача защищаемой информации, следует убедиться в соблюдении ряда требований законодательства РФ: о трансграничной передаче ПДн, включая обязанность обработки и хранения ПДн на территории РФ; о локализации электронных баз данных банков на территории РФ; о лицензировании деятельности по технической защите конфиденциальной информации и работе с шифровальными средствами; об обеспечении безопасности критической информационной инфраструктуры. В случае наличия у поставщика услуг подразделений и (или) дочерних предприятий за пределами РФ, а также при использовании самим поставщиком услуг аутсорсинга поставщик услуг должен предоставить финансовой организации информацию о таких подразделениях,

---

[23] Стандарт Банка России «СТО БР ИББС-1.4-2018. Обеспечение информационной безопасности организаций банковской системы РФ. Управление риском нарушения информационной безопасности при аутсорсинге», принят приказом Банка России от 06.03.2018 № ОД-568 и введен в действие с 01.07.2018 // СПС «КонсультантПлюс».

[24] Введение и п. 6.2 Стандарта СТО БР ИББС-1.4-2018.

[25] Приложение 3 к Стандарту СТО БР ИББС-1.4-2018.

[26] Постановление Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (в ред. 15.06.2016) // СПС «КонсультантПлюс».

[27] Постановление Правительства РФ от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств…».

предприятиях или аутсорсинговых субподрядчиках. Трансграничная передача информации, составляющей банковскую тайну, допускается в обезличенной обобщенной (агрегированной) форме, за исключением случаев, установленных законодательством РФ (п. 6.9).

Таким образом, не исключена возможность использования финансовыми организациями аутсорсинговых услуг зарубежных операторов, привлекаемых российскими поставщиками через свои зарубежные структуры. Однако на поставщике услуг остается обязанность обеспечить соблюдение субподрядчиком требований к защите информации, в том числе в области лицензирования отдельных видов деятельности[28]. Однако наличие данных требований не означает запрет для зарубежных поставщиков предоставлять облачные услуги российским финансовым организациям. Они вправе это делать при соблюдении следующих условий:

1) соответствующие облачные решения не включают аутсорсинг бизнес-функции целиком;
2) зарубежный облачный провайдер принял меры к охране защищаемой информации, в том числе посредством разработки и реализации компенсирующих мер, направленных на нейтрализацию угроз безопасности информации финансовой организации;
3) трансграничная передача ПДн и информации, относящейся к банковской тайне, должна осуществляться в обезличенном виде;
4) передача в зарубежное облако ПДн и банковской информации должна происходить при условии соблюдения требования локализации ПДн и электронных баз данных банков;
5) в соответствующих случаях необходимо обеспечить размещение ПДн в том центре обработки данных, который находится в стране, обеспечивающей адекватную защиту ПДн, либо банк должен получить согласие субъектов ПДн на трансграничную передачу ПДн;
6) сведения, относящиеся к банковской тайне, могут быть переданы в зарубежное облако, если кредитная организация сохраняет контроль за облачной инфраструктурой и у облачного провайдера отсутствует возможность доступа к соответствующим сведениям[29];
7) облачные решения зарубежных провайдеров не должны предполагать производство внутренних (внутрироссийских) переводов денежных средств / платежей;
8) при заведении учетных записей в публичном облаке должна соблюдаться процедура анонимизации ПДн или их шифрования;
9) при невозможности технической реализации отдельных выбранных мер защиты информации, а также с учетом экономической целесообразности финансовая организация совместно с зарубежным провайдером вправе разрабатывать иные (компенсирующие) меры, направленные на нейтрализацию угроз безопасности информации финансовой организации.

Как видим, вышеприведенные требования вполне выполнимы и могут быть соблюдены зарубежными поставщиками при предоставлении финансовым организациям широкого круга облачных решений. А значит, вывод о запрете зарубежным поставщикам предоставлять облачные услуги финансовым организациям является неверным и подлежит корректировке.

БИБЛИОГРАФИЯ

1. *Канашевский В. А.* Банковская тайна и использование банками услуг аутсорсинга информационной безопасности // Lex Russica. — 2018. — № 7.
2. *Канашевский В. А.* Об обязательном хранении информации на территории России (требование локализации) // Международное публичное и частное право. — 2017. — № 6.
3. *Кораблев А. В.* Идентификация информационных рисков использования облачных технологий в банковской деятельности : дис. … канд. экон. наук. — Самара, 2017.
4. *Савельев А. И.* Комментарий к Федеральному закону от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» (постатейный). — М. : Статут, 2015.

[28] П. 10.3 Стандарта СТО БР ИББС-1.4-2018.

[29] См.: *Канашевский В. А.* Банковская тайна и использование банками услуг аутсорсинга информационной безопасности // Lex Russica. 2018. № 7.

5. *Савельев А. И.* Правовая природа «облачных» сервисов: свобода договора, авторское право и высокие технологии // Вестник гражданского права. — 2015. — № 5.

Материал поступил в редакцию 4 сентября 2018 г.

LEGAL PROBLEMS OF USING CLOUD SERVICES OF FOREIGN PROVIDERS BY RUSSIAN BANKS

KANASHEVSKIY Vladimir Aleksandrovich, Doctor of Law, Professor, Professor of the Department of International Private Law of the Kutafin Moscow State Law University (MSAL)
vakanashevskij@msal.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

Abstract. *The paper examines the legal aspects of the use of cloud solutions by Russian banks of foreign providers. Despite the obvious advantages, there are many obstacles to such a use in the Russian legislation, including the lack of general regulation of cloud computing services, requirements for information security (licensing of encryption activities, certification of information systems), requirements of legislation on the localization of personal data databases, electronic databases of banks, etc.*
Based on the analysis of existing regulations, in particular the industry regulators, the author comes to the conclusion that foreign cloud service providers have the right to provide services to Russian financial institutions under certain conditions: cloud solutions should not include outsourcing of business functions entirely and should not involve the production of internal (domestic) money transfers (payments); foreign cloud provider has taken measures to protect the protected information; cross-border transfer of personal data and bank secrecy should be carried out in an impersonal form, etc.

Keywords: *cloud computing services, foreign provider, personal data, bank, financial organization, information security, confidential information, open information, licensing of encryption activities, certification of information systems, information protection, compensating measures, outsourcing of business functions, cross-border transmission of protected information, data processing center.*

REFERENCES

1. Kanashevskiy V.A. *Bankovskaya tayna i ispolzovanie bankami uslug autsorsinga informatsionnoy bezopasnosti* [Banking secrecy and use of information security outsourcing services by banks]. Lex Russica. 2018. No. 7.
2. Kanashevskiy V.A. *Ob obyazatelnom khranenii informatsii na territorii Rossii (trebovanie lokalizatsii)* [On mandatory storage of information on the territory of Russia (localization requirement)]. *Mezhdunarodnoe publichnoe i chastnoe pravo* [International public and private law]. 2017. No. 6.
3. Korablev A.V. *Identifikatsiya informatsionnykh riskov ispolzovaniya oblachnykh tekhnologiy v bankovskoy deyatelnosti : dis. … kand. ekon. nauk* [Identification of information risks of using cloud technologies in banking : PhD Thesis]. Samara, 2017.
4. Saveliev A.I. Kommentariy k Federalnomu Zakonu ot 27.07.2006 № 149-FZ «Ob informatsii, informatsionnykh tekhnologiyakh i zashchite informatsii» (postateynyy) [Commentary to the Federal law of 27.07.2006 № 149-FZ “On information, information technologies and information protection “ (article-by-article)]. Moscow: Statut Publ., 2015.
5. Saveliev A.I. *Pravovaya priroda «oblachnykh» servisov: svoboda dogovora, avtorskoe pravo i vysokie tekhnologii* [Legal nature of cloud services: freedom of contract, copyright and high technology]. *Vestnik grazhdanskogo prava* [Civil Law Review]. 2015. No. 5.