УДК 34

Правовые проблемы и риски использования облачных технологий

Рузаев Евгений Павлович
Приамурский государственный университет имени Шолом-Алейхема
Студент

Аннотация
В данной статье рассматриваются различные аспекты регулирования и защиты информации, возникающие при использовании облачных технологий. В связи с широким распространением использования облаков, как обычными гражданами (в основном в виде социальных сетей и сервисов электронной почты), возникает необходимость решения проблем, связанных с безопасностью и конфиденциальностью данных.
Ключевые слова: персональные данные, информационная безопасность, провайдер

Legal issues and risks of using cloud technology

Ruzaev Evgeny Pavlovich
Sholom-Aleichem Priamursky State University
Student

Abstract
This article discusses various aspects of regulation and protection of information arising from the use of cloud technology. Due to the widespread use of clouds, both by ordinary citizens (mainly in the form of social networks and email services), there is a need to address issues related to data security and privacy.
Keywords: personal data, information security, provider

Важность и актуальность статьи обусловлены тем фактом, что облачные технологии нередко называют технологиями будущего. Вместе с тем, их использование представляется достаточно сложным, с точки зрения юридического оформления таких отношений и последующей защиты прав их участников. В последние годы наблюдаются широкая популяризация и активное развитие облачных хранилищ (соответствующие сервисы сегодня предоставляет большая часть компаний, производящих различные цифровые устройства), что требует осмысления соответствующих процессов с точки зрения права.

Цель данной статьи заключается в исследовании основных правовых проблем и рисков, связанных с использованием облачных технологий в Российской Федерации.

В своей статье М.Р. Акбарова рассмотрела основные типы облаков, статистические данные по использованию облачных технологий и облачную

безопасность нового уровня [2]. В работе Д.А. Боярчук рассмотрел угрозы для облачных технологий, а также предложил подходы для минимизации рисков в облачной среде [3]. Статья А.В. Пантелеева посвящена изучению проблем, связанных с применением облачных сервисов. Автор провел анализ существующего материала, изучить понятие «облачные сервисы» и его основные особенности, проанализировал проблемы безопасности данных и существующие методы оценки безопасности [4].

Основное внимание в нормативных документах уделяется непосредственно вопросам обеспечения информационной безопасности. Две основные проблемы, связанные с использованием облачных технологий на территории Российской Федерации, — это безопасность и расположение технических средств. «Облака» обладают как преимуществами, которые приносят довольно много пользы, так и недостатками, которые могут нанести ущерб, особенно в области безопасности данных. Все, в первую очередь, связано с тем, что исполнитель передает часть функций по использованию облачного сервиса провайдеру, в результате снижается контроль над хранением данных, появляются дополнительные риски и угрозы информационной безопасности. Эти проблемы могут быть решены путем применения определенных мер как со стороны клиента, так и со стороны поставщика.

В связи с тем, что в российском законодательстве отсутствует нормативный документ, непосредственно описывающий требования к обеспечению информационной безопасности при использовании облачных технологий, заказчик практически не располагает достаточной информацией для оценки уровня безопасности облачного сервиса и степени гарантии сохранности конфиденциальной информации.

При работе с облачными сервисами весьма вероятно использование персональных данных. В данном случае основным регулятором является федеральный закон Российской Федерации от 27.07.2006 № 152 — ФЗ «О персональных данных» [1]. Клиенту должно быть либо предоставлено средство для удаления его собственных данных, либо поставщик сам должен удалить эти данные по первому запросу клиента. В соответствии со ст. 5 этого закона, «Принципы обработки персональных данных», обрабатываемые персональные данные должны быть обезличены или уничтожены для достижения целей обработки [1].

Существуют и другие проблемы, связанные с обработкой персональных данных в облачном сервисе. В соответствии со ст. 6 этого же закона «Условия обработки персональных данных», обработка персональных данных может осуществляться только с согласия субъекта персональных данных, ст. 7 данного закона «Конфиденциальность персональных данных» разъясняет, что операторы или другие лица, получившие доступ к персональным данным субъекта персональных данных, обязаны не разглашать эти данные третьим лицам и не распространять их без согласия субъекта, если иное не предусмотрено федеральным законом [1]. Если клиент (он же оператор персональных данных) решил использовать облачные технологии на своем

предприятии и предполагает обработку персональных данных в облаке, то ему необходимо внести изменения в согласие субъекта персональных данных относительно обработки его данных третьей стороной, а именно поставщик облачных услуг.

Можно выделить следующие правовые риски использования облачных технологий:

1) пользователь вынужден передавать часть функций по использованию облачных технологий провайдеру, в первую очередь из-за отсутствия физического контроля пользователя над инфраструктурой, в которой хранится его информация. Угроза кибератак возникает именно из-за необходимости использовать удаленный доступ к информации, используя зачастую незащищенные каналы передачи данных;

2) отсутствие четкого распределения прав и обязанностей пользователя и провайдера напрямую связано с потерей пользовательского контроля. Однако, определив сферу правовых отношений каждой стороны, можно снизить риски, связанные с потерей контроля, предоставив каждой стороне четко определенный круг обязанностей и устранив сомнения, которые затем могут привести к спорам и конфликтам. Здесь необходимо убедиться, что модель распределения прав и обязанностей будет зависеть, прежде всего, от формы предоставления облачных сервисов, поскольку установить единый механизм для всех форм невозможно из-за принципиальных различий между одной формой и другой;

3) недостаточные меры безопасности провайдера — появляется из-за отсутствия технической подготовки пользователя при заключении контракта, следовательно, необходимые стандарты безопасности прописаны не так подробно, как того требует ситуация. Более того, при заключении договора с потребителями, чаще всего публичных и неплатежных договоров, поставщики сами формулируют наиболее выгодные для них условия, и пользователь фактически не имеет возможности вносить собственные изменения. В такой ситуации провайдеры, которые, как правило, не заинтересованы в установлении дополнительных средств защиты, поскольку это связано с дополнительными расходами, оказываются в более выгодном положении в убыток пользователям. Отсутствие информации о местонахождении данных связано с особенностью функционирования вторичных технологий. Информация, размещенная в «облаках», на самом деле может находиться в разных юрисдикциях из-за использования технологии фрагментации данных. Таким образом, возникает несколько проблем: определение применимого законодательства в контексте трансграничного характера информации, обеспечение целостности и конфиденциальности информации, соблюдение требований законодательства при работе с персональными данными;

4) еще одной угрозой является опасность неполного удаления данных при использовании облачных технологий. Это связано с различными «уровнями» удаления информации, о которых пользователь часто не подозревает. Итак, при перемещении файла в корзину, как правило, информация продолжает храниться на облачном сервере в течение 30 дней или

до тех пор, пока «корзина не будет очищена». Тем не менее, даже по истечении указанного срока или очистки информация не удаляется безвозвратно, а стираются только «указатели» о местоположении отдельных фрагментов информации в условиях фрагментации данных. Сама информация продолжает храниться на серверах провайдера (хотя теперь в виде отдельных частей, не соединенных в одно целое), и если случится так, что на одном сервере останется достаточно большой объем информации, то третьи лица могут незаконно получить к ней доступ (особенно те, кто использует тот же физический инфраструктура).

Проблема также усугубляется несколькими факторами. Во-первых, существует большое количество резервных копий в различных хранилищах по всему миру, которые провайдеры создают для обеспечения непрерывного доступа к информации и в которых данные могут храниться даже после их официального удаления. Во-вторых, тот факт, что большинство сервисов по предоставлению облачных технологий для хранения данных (так называемое облачное хранилище) не дают пользователю возможности определить судьбу информации, размещенной в облаке. Из-за этого подключение с внешнего устройства (мобильного телефона, компьютера) такие сервисы не удаляют автоматически информацию из учетной записи в облаке, и даже при удалении из учетной записи стандартные настройки могут предусматривать сохранение резервной копии информации на сервере провайдера. Также многие поставщики облачных технологий в виде SaaS (включая Dropbox) предлагают сохранять все копии документа, чтобы обеспечить возможность возврата к любой из предыдущих версий, что значительно усложняет решение рассматриваемого вопроса. Поэтому крайне важно в договоре установить судьбу удаленной информации, первых копий, порядок проведения этой процедуры.

Из вышесказанного следует, что провайдер должен учитывать и обеспечивать соблюдение всех требований федерального закона Российской Федерации от 27.07.2006 № 152 — ФЗ «О персональных данных», в том числе технических [1]. Заказчику, в свою очередь, также необходимо учитывать эти требования и, принимая решение об использовании облачных технологий в рабочем процессе своего предприятия, вносить необходимые изменения во внутренние документы, например, в форму согласия на обработку персональных данных субъекта.

Для того чтобы выполняемые операции соответствовали требованиям законодательства, должны быть выполнены следующие условия: — подписание договора с поставщиком облачных услуг на основании требований федерального закона Российской Федерации от 27.07.2006 № 152 — ФЗ «О персональных данных»; организация передачи персональных данных третьим лицам (на основании согласия); трансграничная пере-дача персональных данных; регулирование вопросов, связанных с обезличенными данными; нормативное регулирование в области лицензирования и сертификации [1].

Таким образом, обосновывается необходимость принятия поправок в законодательство, которые обеспечат возможность эффективного регулирования отношений, возникающих при использовании облачных технологий, а также сформулируют их основные положения. Из этого следует, что особое внимание следует уделить формированию такой базы в российском законодательстве, основанной, в том числе, на существующих международных стандартах, активное изучение которых позволит разработать эффективные российские нормативные документы, регулирующие проблемные вопросы использования облачных технологий на территории Российской Федерации, что позволяет повысить их качество, эффективность и безопасность, а также гармонизировать их с отечественной практикой использования облачных сервисов.

Библиографический список

1. О персональных данных: офиц. текст ФЗ № 152-ФЗ от 27.07.2006 г. – СПС КонсультантПлюс.
2. Акбарова М.Р. Безопасность и защита данных в облачных технологиях // Universum: технические науки. 2022. № 10-1. С. 17 – 19.
3. Боярчук Д.А. Угрозы информационной безопасности облачных технологий // Современные проблемы радиоэлектроники и телекоммуникаций. 2022. № 5. С. 207 – 212.
4. Пантелеев А.В. Исследование проблем внедрения облачных технологий с точки зрения эффективности и информационной безопасности // Перспективы науки. 2020. № 6 (129). С. 28 – 31.