УДК 378.1

# Доверие в «облаках»: модель провайдера

***Е.А. Осташова, Ж.А. Рожнёва***

Национальный исследовательский Томский государственный университет, Томск, Россия
e-mail: evgeniya.ostashova@gmail.com; zhar@ido.tsu.ru

***Аннотация:*** *облачные технологии сегодня находят широкое и разнообразное применение как в государственном и корпоративном, так и в частном секторе. В фокусе данной статьи использования «облаков» для решения персонально ориентированных задач. Использование данной технологии подразумевает возникновение доверительных отношений между пользователем и провайдером. Авторы полагают, что модели доверия пользователя и провайдера не идентичны друг другу и на данном этапе исследования, на основе анализа пользовательских соглашений и политик конфиденциальности, размещенных на сайте ведущих поставщиков услуг облачного хранения, предпринимают попытку выявления модели доверия провайдера.*

***Ключевые слова****: облачные технологии, публичные облака, провайдер, пользователь, доверие.*

Рынок облачных сервисов в России в последние три года демонстрирует значительное развитие, по темпам роста опережая как другие информационные технологии [1], так и мировой облачный рынок [2]. «Облака» используются государственными органами и бизнесом для предоставления услуг, обеспечения различных внутренних нужд, а также отдельными людьми для решения персонально ориентированных задач. Мы полагаем, что, как и при осуществлении любой другой сделки, при использовании «облаков» между продавцом (провайдером) и потребителем формируется доверие. На данном этапе исследования мы поставили перед собой цель рассмотреть использование облачных технологий и модель доверия, которая формируется в процессе этого использования именно на уровне индивидуального пользователя.

Оговоримся, что спектр задач, решаемых на персональном уровне с помощью облачных технологий, очень широк. Эти задачи могут варьироваться от сугубо личных (хранение фотографий, видеозаписей и пр.) до организации совместной работы над проектами, «транспортировки» файлов, необходимых для работы и в офисе, и дома. Нам представляется, что, несмотря на разнообразие целей, сфер и способов использования облачных сервисов индивидуумами, механизмы защиты собственных данных при использовании «облаков», которыми обладают государство и бизнес, гораздо мощнее и разнообразнее тех,

которые доступны рядовым пользователям, а степень зависимости последних от обеспечиваемых провайдером условий представления сервиса выше. Во многом это связано с тем, что большинство людей выбирают публичные облака и бесплатные сервисы. Поэтому в ситуации персонального использования значительную роль во взаимоотношениях провайдера облачных услуг и пользователя играет именно доверие.

Мы полагаем, что следует различать две нетождественных друг другу модели доверия: модель доверия пользователя и модель доверия провайдера облачных услуг. Вполне очевидно, что на их формирование оказывает влияние законодательная база, регламентирующая предоставление и использование облачных вычислений путем установления набора обязательных требований к открытости и защищенности данных, способам и средствам их обработки. Таким образом, нам представляется, что общая модель доверия в облаках формируется в области пересечения моделей доверия пользователя и провайдера, и должна не противоречить требованиям законодательства.

Большая работа в области изучения влияния фактора доверия на использование Интернета, включая облачные сервисы, как среды бытования и хранения разнообразной документированной информации ведется в рамках международного проекта InterPARES Trust [3], участниками которого мы также являемся. В российских исследованиях облачных технологий, которые стали появляться не так давно, основной фокус направлен на изучение складывающихся практик использования «облаков» в корпоративном и государственном секторе. Кроме того, имеется ряд работ, в которых «облака» рассматриваются как объект права. В них, в частности, отмечается отсутствие единой трактовки понятия «облачные технологии»/«облачные сервисы»/«облако» и указывается на необходимость выработки общей терминологии, которая бы точно описывала суть предмета регулирования, так как бытующее на данный момент в нормативно-правовых актах множество терминов лишь усложняет развитие законодательной базы [4]. Споры среди юристов вызывает и то, какая отрасль права призвана регулировать различные аспекты бытования, предоставления и использования облаков[5, с. 377, 379; 6, с. 31, 33; 7]. Не являясь специалистами в области права, мы не ставили перед собой задачу детального изучения проблем, связанных с проработкой юридического статуса облачных технологий.

Выявление моделей доверия пользователя и провайдера предполагает необходимость проведения исследований в трех направлениях. Во-первых, необходимо изучение законодательства, регулирующего бытование и использование облачных сервисов, для того, чтобы выявить законодательные требования к облакам, а также существующие в законодательной базе лакуны. Во-вторых, необходимо проанализировать пользовательские соглашения, политики конфиденциальности и условия использования наиболее популярных сервисов, предоставляющих возможность хранения данных в облаках.

В отличие от моделей доверия, формируемых законом и провайдером, которые носят «писаный» характер, модель доверия пользователя проявляется исключительно на уровне его действий, внутренняя логика которых часто не рефлексируется самим пользователем. Представляется, что выявление данной модели и допустимых рисков возможно в рамках интервью, которые пока остаются за рамками настоящего исследования.

Наша задача на данном этапе состояла в выявлении модели доверия, конструируемой провайдерами облачных сервисов, под которыми мы понимаем услуги онлайн хранения информационных ресурсов пользователей и организацию доступа к ним.

Для реконструкции этой модели доверия принципиально важно определить те критерии, на основании которых, по мнению провайдера, пользователь делает выбор в пользу того, доверять или не доверять сервису. С этой целью мы проанализировали пользовательские соглашения, документы, содержащие политику конфиденциальности и условия использования, размещенные на веб-сайтах ведущих компаний, предоставляющих возможность работы в «облаках» (хранения документов, их видоизменения, передачи и т.д.) – Google Drive (Политика конфиденциальности [8] и Условия использования [9]), Dropbox (Условия обслуживания Dropbox [10], Политика конфиденциальности Dropbox [11], Политика допустимого использования Dropbox [12]), Яндекс Диск (Политика конфиденциальности [13], Пользовательское соглашение сервисов Яндекса [14], Условия использования сервиса Яндекс.Диск [15]), OneDrive компании Microsoft (Заявление о конфиденциальности компании Microsoft [16] и Соглашение об использовании служб Microsoft [17]), iCloud компании Apple (Обзор безопасности и конфиденциальности iCloud [18],Политика конфиденциальности Apple [19]).

Рассмотренные документы не требуют формального подписания пользователем (подписание бумажного экземпляра, заверения электронной подписью). Сам факт использования предоставляемых сервисов (не только «облаков») предполагает, что пользователь знаком со всеми документами, определяющими порядок предоставления и использования сервиса и согласен с ними.

Явным образом основные принципы, которые помогают заслужить доверие пользователей, приводятся компанией Microsoft и включают:

1. Управление – предоставление «простых в использовании средств управления конфиденциальностью и понятных вариантов выбора»;

2. Прозрачность – предоставлению пользователю информации о сборе и использовании данных для того, чтобы пользователь мог принять обоснованное решение;

3. Безопасность – компания гарантирует защиту доверенных ей данных «с помощью надежной системы безопасности и шифрования»;

4. Надежная юридическая защита – «уважение» местного законодательства о конфиденциальности и борьба за ее защиту;

5. Отсутствие целевой рекламы на основе содержимого – отказ от использования личных данных пользователя (содержания писем, чатов и пр.) для формирования рекламы;

6. Расширение возможностей пользователя – использование данных собираемых компанией о пользователе исключительно для его пользы и расширения его возможностей [20].

Компания Google ориентируется на пять принципов конфиденциальности, среди которых: 1) «использование информации для повышения качества продуктов и сервиса»; 2) «разработка продуктов в соответствии со строгими стандартами конфиденциальности» (в т.ч. с учетом требований законодательства в области защиты информации); 3) «прозрачность сбора личной информации», т.е. информирование пользователя о том, какие данные собираются и хранятся и для чего они используются; 4) «возможность выбора средств защиты конфиденциальности», т.е. вариативность работы с персональной информацией; 5) «ответственное управления полученной информацией»: защита пользователей и их информации от вредоносных программ, мошенничества, технических сбоев и пр. [21].

В целом, описывая свои сервисы, компании делают акцент на удобство и универсальность их использования (возможность получения доступа из любой точки, с любого устройства, быстрота загрузки файлов, широкие возможности использования, синхронизация файлов на различных устройствах) и защищенности данных от утраты («файлы больше не потеряются» [22], «Вы не потеряете их [файлы], даже если с компьютером или телефоном что-то случится» [23]); гибкость пользовательских настроек и широта инструментария по управлению собственным контентом, в том числе и в области обеспечения его конфиденциальности.

Одним из ключевых вопросов, оговариваемых всеми перечисленными выше поставщиками «облачных» сервисов, является вопрос об обработке персональных данных пользователей. В Российской Федерации понятие «персональных данных», «субъекта» и «оператора персональных данных», правила обработки и использования этих данных определяются Федеральным законом «О персональных данных» [24].

В явном виде ссылки на данный Федеральный закон и на соответствие собственной деятельности этому закону присутствуют в «Политике в отношении обработки персональных данных ООО «Майкрософт Рус» [25] («Майкрософт Рус» – представительство компании Microsoft в России) и в «Политике конфиденциальности» Яндекс [13]. Остальные сервисы ссылаются на международные документы: Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) [26], Система правил трансграничной конфиденциальности АТЭС [27] (iCloud), Рамочное соглашение между США и ЕС «Щит конфиденциальности» [28]

(Google Drive, Dropbox, MS OneDrive), Закон об авторском праве в цифровую эпоху [29].

В документах, отражающих политику конфиденциальности, перечисляются виды собираемых персональных (личных) данных (в данном случае этот термин используется без привязки к российскому законодательству и отражает то, что компания, предоставляющая облачный сервис понимает под такого рода сведениями), способы их использования, называются условия передачи этих данных третьим лицами и очерчивается круг третьих лиц, которым может быть передана персональная информация пользователя. Необходимо отметить, что, так как данные компании предоставляют не только доступ к «облаку», но и другие сервисы (почтовые, поисковые, блоги и форумы, покупки) перечисляемые виды персональных данных собираются для всех предоставляемых компанией сервисов, а не исключительно для «облака».

К собираемым данным относятся сведения об имени и фамилии; физический и электронный адрес; номер телефона; данные кредитной карты; сведения о поле, возрасте и предпочитаемом языке предоставления информации (iCloud, Dropbox, OneDrive, Google Drive), кроме того, могут собираться данные об использовании других сервисов, поисковых запросах, интересах, контактах, часто посещаемых местах (OneDrive, Google Drive) и пр.

В документах с разной степенью подробности описываются цели использования персональных данных. К числу основных можно отнести:

1) обеспечение собственных функций компании (совершенствования существующих и создания новых сервисов, повышение персонализации предоставляемых услуг, релевантности поиска, внутренний анализ и аудит). В этой связи принципиальной позицией компании MS является отказ от использования фраз из писем, чат-сообщений, а также личных файлов пользователей для формирования целевой рекламы;

2) защиту и идентификацию пользователей (например, исходя из данных об устройствах, с которых обычно используется сервис, компания может предупредить пользователя в случае, если в его аккаунт осуществлен вход их необычного места или с нового устройства);

3) информирование пользователей. Корпорация Apple также заявляет, что использует собираемые персональные данные, если пользователи ее клиенты участвуют в лотерее [19].

Собираемые данные могут передаваться партнерам компаний-провайдеров, компаниям, предоставляющим определенные услуги (например, по обработке информации) самому провайдеру, государственным органам (в соответствии с требованиями закона). Также провайдер предоставляет общедоступные данные о пользователе другим пользователям (пользователь может сам определить, какие данные будут считаться общедоступными).

Таким образом, данная информация, представленная в пользовательских соглашениях, документах, определяющих политику компаний в отношении персональных данных и конфиденциальности, должна сформировать у

пользователя представление о том, что (какие данные), кто, как и для чего собирает, хранит, передает и обрабатывает.

В проанализированных документах практически не содержится описание технологий, используемых компаниями. Соответствующие ссылки дает компания MS (только англоязычный документ) [30]. По всей видимости, краткость технической информации не означает, что провайдеры совершенно не рассматривают технологию как фактор доверия, а, скорее, объясняется желанием сделать пользовательские соглашения максимально понятными для неспециалистов.

Компании, предлагающие облачные сервисы заявляют о предоставлении пользователю широких возможностей по контролю собственного контента: размещение, удаление и другие действия над файлами и данными; изменение пароля; отказ от целевой рассылки, предоставление другим пользователем доступа к собственным материалам или, наоборот, его ограничение и т.д. В контексте сохранения контроля интересным представляется вопрос о судьбе материалов пользователя, выложенных в облако, после того, как они были удалены пользователем (удаление отдельных файлов или удаление учетной записи в целом). Очевидно, что такая информация будет недоступна другим пользователям, но каковы дальнейшие действия провайдера в отношении этих материалов?

Рассмотренные пользовательские соглашения предусматривают, что провайдер прекратит обработку таких данных, но только Dropbox заявляет, что после удаления аккаунта пользователем, будет удалена и вся связанная с ним информация. При этом пользователя предупреждают о возможных задержках в удалении информации, связанных с техническими особенностями процесса, а также о возможности сохранения информации, в случаях, когда это требуется законом, необходимо для разрешения судебных споров или исполнения существующих договоренностей [11].

Проведенный анализ пользовательских соглашений, условий предоставления и использования облачных сервисов показывает, что для провайдера сервис, которому можно доверять, – это, в первую очередь, сервис, защищенный от несанкционированного доступа со стороны неоговоренных в указанных документах третьих лиц. При этом пользовательские соглашения предусматривают, что содержание размещаемых данных находится исключительно в сфере ответственности пользователя. В тоже время провайдер может просматривать контент и удалять его в случае нарушения требований закона или политики компании, хотя и не берет на себя такого обязательства и не несет ответственности за размещаемые пользователями материалы.

Кроме того, соглашения оговаривают некоторые объективные условия, при которых сохранение информации или обеспечение доступа к ней становится невозможным (технические сбои, катаклизмы и т.д.), подчеркивая, что пользователь использует сервис «на свой риск», а сам сервис предоставляется «as is» («как есть» – данный термин используется провайдерами в текстах

пользовательских соглашений и подразумевает отказ от ответственности за проблемы, возникающие в процессе использования облачного сервиса). Таким образом, модель доверия, конструируемая провайдером, основывается, прежде всего, на тех гарантиях безопасности данных, которые предусматриваются законодательством и которые он сам считает необходимыми и достаточными для привлечения пользователей к собственному сервису. С точки зрения провайдера, защищенность пользовательских данных от несанкционированного доступа является фактором доверия, так как во всех пользовательских соглашениях воспроизводится это положение. Однако представляется, что эти модели ориентируются, скорее, не на пользователя, а на успешное осуществление собственной деятельности компанией-провайдером.

## СПИСОК ЛИТЕРАТУРЫ


1.Рост облаков – результат технологических, экономических и законодательных изменений [Электронный ресурс] : интервью со С. Другалевым // CNews: аналитика: интернет-издание о высоких технологиях. – М., 2015. – URL: http://www.cnews.ru/articles/2015-12-01_stanislav_drugalev_rost_oblakov_rezultat_tehnologicheskih (дата обращения: 07.06.2017).

2.Коптелов, А. Как совместить преимущества публичного и частного облака? [Электронный ресурс] // CNews: аналитика: интернет-издание о высоких технологиях. – М., 2014. – http://www.cnews.ru/reviews/cloud_2014/articles/kak_sovmestit_preimushchestva_chastnogo_i_publichnogo_oblakov/ (дата обращения: 07.06.2017).

3.InterPARES Trust [офиц. сайт]. – Vancouver, BC, Canada, [2013-1018]. – URL: https://interparestrust.org/trust/contact (дата обращения: 07.06.2017).

4.Кожевникова, Ю.С. Сущность информационно-правовых отношений, формирующихся при использовании облачных технологий в Российской Федерации // Труды по интеллектуальной собственности. – 2013. – № 2, том XIII. – С. 211–284.

5.Кожевникова, Ю.С. Проблемы регулирования деятельности провайдеров облачных вычислений в информационном законодательстве России и ФРГ (сравнительно-правовой анализ) // European Social Science Journal. – 2012. – № 12. – С. 376–379.

6.Кожевникова, Ю.С. Проблемы регламентации отношений, формирующихся при использовании информационных облачных технологий: сочетание регулирования и саморегулирования // Юрист. – 2014. – № 13. – С. 30–35.

7.Савельев, А.С. Правовая природа «облачных» сервисов: свобода договора, авторское право и высокие технологии // Вестник гражданского права. – 2015. – № 5. – С. 62–99.

8.Политика конфиденциальности Google [Электронный ресурс]. – Mountain View, CA USA, 2017. – URL: https://www.google.com/intl/ru/policies/privacy/ (дата обращения: 07.06.2017).

9.Условия использования Google [Электронный ресурс]. – Mountain View, CA USA, 2014. – URL: https://www.google.com/intl/ru/policies/terms/ (дата обращения: 07.06.2017).

10. Условия обслуживания Dropbox [Электронный ресурс]. – [Б.м.], 2016. – URL: https://www.dropbox.com/privacy?#terms (дата обращения: 07.06.2017).

11. Политика конфиденциальности Dropbox [Электронный ресурс]. – [Б.м.], 2016. – URL: https://www.dropbox.com/privacy?#terms (дата обращения: 07.06.2017).

12. Политика допустимого использования Dropbox [Электронный ресурс]. – [Б.м.], 2016. – URL: https://www.dropbox.com/privacy?#acceptable_use (дата обращения: 07.06.2017).

13. Политика конфиденциальности [Электронный ресурс]. – М., 2016. – URL: https://yandex.ru/legal/confidential/index.html (дата обращения: 07.06.2017).

14. Пользовательское соглашение сервисов Яндекса [Электронный ресурс]. – М., 2016. – URL: https://yandex.ru/legal/rules/index.html (дата обращения: 07.06.2017).

15. Условия использования сервиса Яндекс.Диск [Электронный ресурс]. – М., 2016. – URL: https://yandex.ru/legal/disk_termsofuse/ (дата обращения: 07.06.2017).

16. Заявление о конфиденциальности компании Microsoft [Электронный ресурс]. – [Б.м.], 2017. – URL: https://privacy.microsoft.com/ru-ru/privacystatement (дата обращения: 07.06.2017).

17. Соглашение об использовании служб Microsoft [Электронный ресурс]. – [Б.м.], 2016. – URL: https://www.microsoft.com/ru-ru/servicesagreement/ (дата обращения: 07.06.2017).

18. Обзор безопасности и конфиденциальности iCloud [Электронный ресурс]. – [Б.м.], 2017. – URL: https://support.apple.com/ru-ru/HT202303 (дата обращения: 07.06.2017).

19. Политика конфиденциальности Apple [Электронный ресурс]. – [Б.м.], 2016. – URL: https://www.apple.com/ru/legal/privacy/ru/ (дата обращения: 07.06.2017).

20. Шесть принципов конфиденциальности Майкрософт [Электронный ресурс]. – [Б.м.], [2017]. – URL: https://privacy.microsoft.com/ru-RU/ (дата обращения: 07.06.2017).

21. Политика конфиденциальности и условия использования Google: технологии и принципы [Электронный ресурс]. – Mountain View, CA USA, 2017. – URL: https://www.google.com/intl/ru/policies/technologies/ (дата обращения: 07.06.2017).

22. Официальный сайт сервиса Dropbox [Электронный ресурс]. – [Б.м.]. URL: dropbox.com (дата обращения: 07.06.2017).

23. Официальный сайт сервиса Яндекс.Диск [Электронный ресурс]. – М., [2012-2017]. – URL: https://disk.yandex.ru/ (дата обращения: 07.06.2017).

24. О персональных данных [Электронный ресурс] : федер. закон Рос. Федерации от 27 июля 2007 г. № 152-ФЗ // КонсультантПлюс: справочная правовая система. – М., [1997-2017]. – URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 07.06.2017).

25. Политика в отношении обработки персональных данных ООО «Майкрософт Рус» [Электронный ресурс] – [Б.м.], [2017]. – URL: https://www.microsoft.com/ru-ru/about/piidatapolicy/privacy.aspx.

26. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [Электронный ресурс]. – Strasbourg, 1981. – European Treaty Series, № 108. – URL: https://rm.coe.int/1680078b37 (дата обращения: 07.06.2017).

27. APEC Cross-Border Privacy Rules System [Электронный ресурс]. – [Б.м.], 2016. – URL: http://www.cbprs.org/ (дата обращения: 07.06.2017).

28. Privacy Shield Framework [Электронный ресурс]. – Washington, D.C., [2017]. – URL: https://www.privacyshield.gov/EU-US-Framework (дата обращения:07.06.2017).

29. The Digital Millennium Copyright Act of 1998 [Электронный ресурс]. – [Б.м.], 1998. – URL: https://www.copyright.gov/legislation/dmca.pdf (дата обращения: 07.06.2017).

30. Microsoft Enterprise Cloud Red Teaming [Электронный ресурс] – [Б.м.], 2014. – URL: https://download.microsoft.com/download/C/1/9/C1990DBA-502F-4C2A-848D-392B93D9B9C3/Microsoft_Enterprise_Cloud_Red_Teaming.pdf (дата обращения: 07.06.2017).