**МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**имени М.В.Ломоносова**

ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра коммерческого права и основ правоведения

# Регулирование и защита информации при использовании облачных технологий

***Дипломная работа***

Студентки 4 курса 413 группы

Черкасовой Софьи

***Научный руководитель***

Доктор юридических наук

Северин Виталий Андреевич

***Рецензент***

Кандидат юридических наук

Филиппова Софья Юрьевна

Москва, 2018

**Оглавление:**

## Введение

Согласно данным, представленным Правительством Российской Федерации в Программе «Цифровая экономика», рынок облачных услуг стабильно растет примерно на 40% ежегодно.[1] Независимые аналитики прогнозируют, что к 2025 году до 80% всех данных будут находиться в «облаке».[2]

Данная дипломная работа направлена на изучение отношений, складывающихся при использовании облачных технологий с целью стимулирования темпов внедрения данной технологии в российскую экономику. Актуальность данной темы подчеркивается принятием ряда подзаконных нормативных актов, направленных на развитие информационных технологий в Российской Федерации.[3] В частности, в Стратегии развития информационного общества на 2017-2030, утвержденной Указом Президента РФ от 09.05.2017 №203 (*далее* - Указ Президента №203), одной из основных задач формирования новой технологической основы в экономике названа разработка мер по внедрению в российские организации облачных технологий.[4]

В сравнении с другими иностранными государствами российский рынок облачных услуг значительно отстает по объему: так, в Германии объем данного рынка превышает 12.2 миллиарда евро[5], в Великобритании - 5.1 миллиардов фунтов стерлингов[6], а в России эта цифра составляет 28.3

[1] Распоряжение Правительства РФ от 28.07.2017 N 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации»// СЗ РФ. N 32. 2017. Ст. 5138.
[2] Журавлева А. Колосс на облачных ногах // URL: http://expert.ru/ (дата обращения: 09.12.2017).
[3] Распоряжение Правительства РФ от 20.07.2013 №1268-р «Об утверждении плана мероприятий («дорожной карты«) «Развитие отрасли информационных технологий»// СЗ РФ. 2013. N 30. Ст. 4168; Распоряжение Правительства РФ от 28.07.2017 N 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации»// СЗ РФ. N 32. 2017. Ст. 5138.; Распоряжение Правительства РФ от 01.11.2013 №2036-р «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года»// СЗ РФ. 2013. N 46. Ст. 5954.
[4] Ст. 41 Указа Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»// СЗ РФ. 2017. N 20. Ст. 2901.
[5] URL: https://de.statista.com/themen/ (дата обращения: 09.12.2017).
[6] URL: www.techmarketview.com/news/archive/(дата обращения: 09.12.2017).

миллиарда рублей.[7] Эти данные свидетельствуют о том, что, несмотря на бесспорные преимущества облачных услуг (которые будут подробно описаны ниже), российские организации не готовы переходить на новые технологии, в частности, из-за отсутствия правового регулирования и четкого понимания, как обеспечить безопасность и конфиденциальность данных. Хотя российское законодательство действительно требует некоторых изменений, в связи с повсеместными использованием облачных технологий, представляется, что даже в рамках существующих норм возможно принятие определенных мер, которые позволили бы пользователю и провайдеру эффективно осуществлять свое взаимодействие, безопасно обмениваясь данными.

Несмотря на актуальность данной темы, как в России, так и за рубежом, правовое регулирование облачных технологий остается почти совсем не изученной темой. Фундаментальные работы по данной тематике проведены только И.А. Нестеровой, А.В. Морозовым и Т.А. Полякова. Нельзя не отметить одну из первых всеобъемлющих работ по праву облачных вычислений профессора К. Милларда. Однако чаще всего специалистами обсуждаются только отдельные аспекты использованиям облачных технологий. В этом отношении следует отметить отечественные работы таких авторов, как Н.И. Глухов и П.С.Волошина, Я.О. Кучина, У.А. Меликов, А.С. Паус и О.А. Целовальникова, А.И. Савельев, В.А. Северин, Н.В. Шакель. Из зарубежных специалистов облачными технологиями также занимаются С. Годес, К. Клири, П. Мелл и Т. Гранс.

Целью настоящей работы является анализ различных проблем регулирования и защиты информации при использовании облачных технологий, а также выработка оптимальных способов их решения. Для достижения поставленной цели необходимо решить следующие задачи: определить основные понятия, формы, виды, особенности облачных

[7] URL: http://www.tadviser.ru/index (дата обращения: 09.12.2017).

технологий, изучить существующее правовое регулирование в России и за рубежом, адресованное непосредственно этому институту, выявить распространенные на практике договорные формы отношений по использованию облачных технологий, определить главные риски, препятствующие использованию всего потенциала облачных серверов российскими пользователями, а также разработать комплекс мер, необходимых для минимизации указанных рисков.

# Глава 1. Правовое регулирование отношений при использовании облачных технологий

## 1.1. Общие положения об облачных технологиях

Прежде чем приступить к анализу правового регулирования института облачных технологий, представляется необходимым определить основные понятия, связанные с ним, и различные формы и модели его применения.

Установление единообразного определения облачных технологий является проблемным вопросом, в связи с отсутствием общепринятой дефиниции.[8] Наиболее авторитетное определение облачным технологиям дал Национальный институт стандартизации и технологий США (*далее* - NIST) как модели предоставления удобного сетевого доступа в режиме «по требованию» к коллективно используемому набору конфигурируемых вычислительных ресурсов (например, сетей, серверов, хранилищ данных, приложений или сервисов), которые могут быть оперативно задействованы и высвобождены при минимальном взаимодействии с поставщиком услуги и минимальных собственных управленческих усилиях.[9] Схожее определение дано в Указе Президента №203. [10] Главной особенностью облачных технологий выделяется оперативное предоставление доступа к необходимому объему вычислительных ресурсов при минимальном участии провайдера.

Также на Сорок седьмой сессии Комиссии ООН по праву международной торговли (*далее* - Комиссия ЮНСИТРАЛ) Правительство Канады предложило определить «облако» как вычислительные услуги (например, данные хостинга или обработки данных), когда технология применяется не на базе персонального компьютера или на базе компьютерной системы, находящейся в собственности, но в ином другом

[8] *Кучина Я.О.* Облачные технологии: понятие и основы правового регулирования // Азиатско-Тихоокеанский регион: экономика, политика, право. 2016. № 4.
[9] *Mell P., Grance T.* The NIST Definition of Cloud Computing// URL: http://nvlpubs.nist.gov/ (дата обращения: 09.12.2017).
[10] Ст. 4 (и) Указа Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»// СЗ РФ. 2017. N 20. Ст. 2901.

месте через Интернет-соединение, благодаря форме ограниченного доступа, который предоставляется определённой группе индивидов.[11]

Технически данная модель обеспечивается благодаря двум технологиям: виртуализации и фрагментации данных. Виртуализация позволяет создавать на базе одного физического сервера несколько Виртуальных Машин (ВМ), каждую из которых может использовать отдельный пользователь, улучшая таким образом эффективность и оптимальность использования серверов. Также виртуализация облегчает процесс увеличения или снижения объема вычислительных мощностей, исключая необходимость покупки или продажи физических серверов. А фрагментация данных обеспечивает распределение хранимой информации между разными дисками, совокупность которых составляют один логический диск. Это позволяет улучшить доступность этой информации, благодаря более высокой скорости извлечения маленьких объемов информации.

Рабочая группа IV по Электронной торговле Комиссии ЮНСИТРАЛ на 55 сессии в Нью-Йорке в конце апреля 2017 года выделила шесть особенностей облачных технологий, которые необходимо учитывать при составлении договоров о предоставлении облачных услуг. Так, к ним относятся широкий доступ к сети (доступ в любой момент из любой точки мира, где есть сеть Интернет), количественное измерение услуги (по аналогии с коммунальными услугами), работа в режиме коллективной аренды (выделение виртуальных ресурсов нескольким пользователям одновременно, чьи данные являются изолированными и недоступными для других), самообслуживание по мере необходимости, быстрая адаптируемость (способность оперативно расширять и ограничивать масштабы доступа), объединение ресурсов (провайдер может без ведома пользователя

[11] Предложение правительства Канады: возможная будущая работа в области электронной торговли – правовые вопросы, связанные с облачной обработкой компьютерных данных, материалы 47 сессии, 7-8 июля 2014// URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/V14/041/32/PDF/V1404132.pdf?OpenElement (дата обращения: 04.04.2018).

объединить как виртуальные, так и физические ресурсы для оптимизации обслуживания пользователя).[12]

Исходя из этих особенностей, выделяются следующие преимущества облачных технологий: экономическая эффективность, мобильность, отсутствие потребности в собственной инфраструктуре, низкая стоимость обслуживания. [13] Недостатками являются отсутствие правового регулирования этого института, ограниченные возможности контроля за безопасностью.[14]

При этом облачные технологии не являются однородными и традиционно выделяется три формы предоставления облачных услуг, в зависимости от объема предоставляемых услуг и уровня контроля пользователя: в форме программы (Software as a service, *далее* - SaaS) , в форме платформы (Platform as a service, *далее* - PaaS) и в форме инфраструктуры (Infrastructure as a service, *далее* - IaaS).[15]

При предоставлении услуг в форме программы, пользователь использует программное обеспечение на основе облачных технологий. Такая форма является самой распространенной, в силу наибольшей доступности для пользователей и минимальных требований к его технической осведомленности.[16] В частности, на основе этой формы облачных технологий функционируют большинство почтовых сервисов (Yandex, Mail, Gmail),

---

[12] Доклад рабочей группы IV (Электронная торговля) о работе ее пятьдесят пятой сессии, Комиссия ООН по праву международной торговли, 50 сессия // URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/V17/029/30/PDF/V1702930.pdf?OpenElement (дата обращения: 13.04.2018).

[13] *Терещенко Л.К.* Понятийный аппарат информационного и телекоммуникационного права: проблемы правоприменения//Журнал российского права. 2016. №10; *Берестова В.И.* Перспективы использования облачных технологий в электронном документообороте//Делопроизводство. 2015. № 3.

[14] Там же.

[15] *Christopher J. Millard*. Cloud Computing Law// URL: https://global.oup.com/ (дата обращения: 09.12.2017); *Нестерова И.А*. Правовое регулирование отношений, возникающих при использовании облачных технологий/ Дис. канд. юрид. наук:12.00.03. М. 2016. С.56.

[16] *Ильин И.В., Ильяшенко О.Ю., Борреманс А.Д.* Подход к интеграции облачных технологий типа SaaS при реализации ИТ-проектов// Перспективы науки. N 12 (87). 2016. С.112.

социальные сети (VK, Facebook), а также многие бухгалтерские приложения, офисные пакеты, платформы для проведения вебинаров и т.п.[17]

При облачных услугах в форме платформы, пользователь использует облако для создания или приобретения приложений, разработанных с помощью инструментов провайдера. Таким образом, клиент продвигает свои приложения на основе облачной инфраструктуры, эксплуатируя инструменты и язык провайдера. Эта модель носит узкоцелевой характер, поэтому многие споры решаются в техническом режиме без обращения в юрисдикционные органы.[18]

Наконец, когда облачные услуги предоставляются в форме инфраструктуры, то провайдер предоставляет возможность пользователю самостоятельно управлять всеми вычислительными ресурсами. Эта форма, виртуально заменяя физическую информационную инфраструктуру организации, позволяет создавать свой интернет-сайт или интернет-магазин, организовать внутренний документооборот и т.д.[19]

Существование различных форм облачных технологий, заметно различающихся между собой, усложняет анализ данного института и отражает разнообразие возможных способов использования облачных технологий на практике.

Выделяются также четыре модели предоставления (развертывания) услуг облачных вычислений: частное «облако», общественное, публичное и смешанное. [20] Частное облако предполагает ситуацию, когда соответствующая инфраструктура принадлежит или используется в интересах одного пользователя (чаще всего большой коммерческой

[17] *Савельев А.И.* Правовая природа «облачных« сервисов: свобода договора, авторское право и высокие технологии//Вестник гражданского права.2015. N 5.
[18] Там же.
[19] Там же.
[20] *Christopher J. Millard*. Cloud Computing Law// URL: https://global.oup.com/ (дата обращения: 09.12.2017); *Mell P., Grance T.* The NIST Definition of Cloud Computing// URL: http://nvlpubs.nist.gov/ (дата обращения: 09.12.2017).; п. 18 Приложения к Записке Секретариата Комиссии ООН по праву международной торговли «Договорные аспекты облачной обработки компьютерных данных»// URL: http://undocs.org/ru/A/CN.9/WG.IV/WP.142 (дата обращения: 14.04.18).

организации) или нескольких связанных между собой лиц. Частное облако не обязательно должно располагаться на территории этого пользователя, или принадлежать ему, важно, что его функционирование осуществляется в интересах одного лица или ограниченной группы лиц.[21]

Общественное облако напоминает расширенное частное облако, используемое для лиц с общими интересами, такие как государственные или муниципальные органы или институты финансового сектора.[22]

Публичное облако представляет собой инфраструктуру, используемую многочисленными пользователями на основе одних и тех же программ или физического оборудования. А смешанное облако является смесью вышеперечисленных моделей, где, например, организация, использующая частное облако, может перенаправить некоторые операции по обработке данных на публичное облако, чтобы распределить вычислительную нагрузку.

От того, какая модель развертывания и форма облачных услуг будет использована пользователем будет зависеть степень его управления и контроля над предоставляемыми ресурсами[23], также как и распределение ответственности пользователя и провайдера (вопрос, о котором речь пойдет ниже, см. Главу 2.2.1.).

[21] *Christopher J. Millard*. Cloud Computing Law// URL: https://global.oup.com/ (дата обращения: 09.12.2017).
[22] Например, облачный сервис «NYSE Euronext's Capital Markets Community cloud» для фирм, предоставляющих финансовые услуги (*Tom Steinert-Threlkeld*. Cloud Fundamental to NYSE IT Strategy // URL: http://www.information-management.com/news/cloud-fundamental-to-nyse-it-strategy-10023088-1.html?zkPrintable=true (дата обращения: 12.12.2017).
[23] п. 19 Приложения к Записке Секретариата Комиссии ООН по праву международной торговли «Договорные аспекты облачной обработки компьютерных данных»// URL: http://undocs.org/ru/A/CN.9/WG.IV/WP.142 (дата обращения: 14.04.18).

## 1.2. Регулирование облачных отношений

В России отсутствует специальное регулирование облачных технологий, кроме эпизодического упоминания в подзаконных актах. Первые отсылки к этому институту относятся к 2010 году и обозначению необходимости создать национальную платформу облачных вычислений как одного из мероприятий по управлению развития информационного общества.[24] В Распоряжении Правительства от 01.11.2013 N 2036-р «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года» прогнозировалось, что до 2018 года применение облачных технологий в корпоративной среде станет массовым, в связи с чем необходимо внести «корректировки в нормативные правовые акты, позволяющие бизнесу развиваться наиболее эффективно в сервисной парадигме».[25] Тем не менее, на настоящий момент подобных корректировок не наблюдается.

Однако надо признать, что техническое внедрение облачных технологий происходит достаточно успешно и без подобных изменений. На сегодняшний день облачные технологии проникли практически во все сферы жизни общества, включая образование [26] , здравоохранение [27] , судопроизводство[28], финансовую[29] и банковскую[30] деятельность, таможенное дело[31], оказание государственных услуг[32].

---

[24] Распоряжение Правительства РФ от 20.10.2010 N 1815-р (ред. от 26.12.2013) «О государственной программе Российской Федерации «Информационное общество (2011 - 2020 годы)»// СЗ РФ. N 46. 2010. Ст. 6026.

[25] Распоряжение Правительства РФ от 01.11.2013 N 2036-р «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года»// СЗ РФ. N 46. 2013. Ст. 5954.

[26] Письмо Минобрнауки России от 15.02.2012 N АП-147/07 «О методических рекомендациях по внедрению систем ведения журналов успеваемости в электронном виде»// Администратор образования. N 14. 2012; Приказ Минобрнауки России от 15.06.2016 N 715 «Об утверждении Концепции развития школьных информационно-библиотечных центров»// СПС Консультант.

[27] Приказ Росздравнадзора от 20.09.2017 N 8134 «О переходе Федеральной службы по надзору в сфере здравоохранения на использование отечественного офисного программного обеспечения»; Распоряжение Правительства РФ от 29.12.2014 N 2769-р «Об утверждении Концепции региональной информатизации»// СЗ РФ. N 2. 2015. Ст. 544.

[28] Федеральная целевая программа «Развитие судебной системы России на 2013 - 2020 годы», утв. распоряжением Правительства РФ от 20.09.2012 N 1735-р// СЗ РФ. N 40. 2012. Ст. 5474.

В последнее время самым значительными упоминаниями облачных технологий представляется определение облачных вычислений в Указе Президента № 203, в котором также содержится указание на то, что их развитие является одним из основных направлений развития российских информационных и коммуникационных технологий. Также следует отметить включение в Программу «Цифровая экономика Российской Федерации» плана по обеспечению хранения и обработки информации, создаваемой органами публичной власти, на единой облачной платформе, и разработки стандартов информационной безопасности облачных технологий.[33]

Уместным здесь представляется отметить существование законопроектов, подготовленных Минкомсвязи РФ, касающихся регулирования облачных технологий. Ни один из них еще не был внесен на рассмотрение в Государственную Думу. Первый из них - «О внесении изменений в отдельные законодательные акты Российской Федерации в части использования облачных вычислений» - предусматривает введение понятий субъектов, форм облачных технологий, требований к поставщику услуг для органов государственной власти и распределение ответственности поставщика и потребителя.[34] Эти вопросы будут затронуты в следующих

---

[29] Приказ Минфина России от 07.07.2014 N 208 «О Концепции обеспечения безопасности информации в информационных системах Министерства финансов Российской Федерации»// СПС Консультант; «Основные направления развития финансового рынка Российской Федерации на период 2016 - 2018 годов» (одобрено Советом директоров Банка России 26.05.2016)// Вестник Банка России. N 57. 17.06.2016.

[30] Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Предотвращение утечек информации« РС БР ИББС-2.9-2016, утв. Приказом Банка России от 11.04.2016 N ОД-1205)// Вестник Банка России. N 41. 27.04.2016; Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Управление риском нарушения информационной безопасности при аутсорсинге« СТО БР ИББС-1.4-2018, утв. Приказом Банка России от 06.03.2018 N ОД-568)// Вестник Банка России. N 27. 30.03.2018.

[31] Приказ ФТС России от 21.10.2015 N 2133 «Об утверждении основных направлений развития информационно-коммуникационных технологий в таможенных органах Российской Федерации до 2030 года»// Таможенные ведомости. N 1. 2016.

[32] Распоряжение Правительства РФ от 25.12.2013 N 2516-р (ред. от 13.10.2017) «Об утверждении Концепции развития механизмов предоставления государственных и муниципальных услуг в электронном виде»// СЗ РФ. 13.01.2014. N 2 (часть II). Ст. 155; Распоряжение Правительства РФ от 29.12.2014 N 2769-р (ред. от 03.03.2017) «Об утверждении Концепции региональной информатизации»// СЗ РФ. N 2. 12.01.2015. Ст. 544.

[33] Распоряжение Правительства РФ от 28.07.2017 N 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации»// СЗ РФ. N 32. 2017. Ст. 5138.

[34] URL: http://www.consultant.ru/law/hotdocs/33631.html/ (дата обращения: 13.04.2018).

главах данной работы. Два других проекта, подготовленных в 2014[35] и 2016[36] годах, предлагают обширное регулирование различных вопросов деятельности электронного правительства. Однако рассмотрение вопросов, поднимаемых в этих проектах, не входит в рамки настоящей работы, хотя само их существование показывает, что регулирование данной сферы востребовано.

На практике вопрос о необходимости принятия специальных законодательных актов в связи с облачными технологиями является дискуссионным. При изучении и анализе облачных технологий многие проблемы связаны с их технологическими особенностями, что иногда приводит к ошибочному мнению о ненужности правового регулирования данного института. Однако автор данной работы убежден, что право играет важнейшую роль в распространении и внедрении их в работе организаций, в особенности, в работе малых предприятия, которым это позволит существенно снизить свои расходы и увеличить темпы развития. Учитывая важность обеспечения экономического развития экономики государства, в том числе, за счет повышения эффективности работы всех видов организаций в стране (от малого и среднего бизнеса до крупных государственных корпораций), а также принимая во внимание безусловные преимущества облачных технологий и представляющееся неизбежным распространение их применения, необходимо признать, что принятие специального законодательного регулирования является безусловной предпосылкой для более безопасного использования облачных технологий. Однако также не стоит забывать о стремительности развития технологий и, с другой стороны, медлительности законодательного процесса. Поэтому

[35] Законопроект «О внесении изменений в ФЗ «Об информации, информационных технологиях и о защите информации» и в ФЗ «Об организации предоставления государственных и муниципальных услуг»»// СПС Консультант.

[36] Законопроект «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации», Федеральный закон «Об организации предоставления государственных и муниципальных услуг» и Федеральный закон «Об электронной подписи»//URL: http://d-russia.ru/wp-content/uploads/2016/11/edinaya_infrastruktura_proekt_16112016.pdf (дата обращения: 14.04.2018).

вполне вероятна ситуация, когда принятый законодательный акт является устаревшим еще на стадии своего подписания или сразу после. В связи с этим, предлагается ввести отдельные уточнения общего характера в существующие законы, применительно к технологиям, построенным на облачном предоставлении услуг.

Сравнительно-правовое исследование выявило, что в большинстве стран также отсутствует особое регулирование облачных технологий, но в таких странах, как Германия[37], Канада[38] ведутся активные дискуссии о необходимости введения специальных норм, в Индии[39] уже разработаны соответствующие законопроекты.

В индийском проекте предусматривается приведение национальных стандартов по защите частной жизни и безопасности данных в соответствие международным стандартам. Также предлагается интересная норма об экстерриториальном применении норм индийского права в отношении услуг по предоставлению облачных технологий на облачные сервисы, используемые гражданами Индии, или вообще на всю «индийскую» информацию. Более того, для некоторых категорий информации (например, налоговая информация) предусматривается хранение и размещение только на территории Индии, без возможности трансграничной передачи. Обсуждается, вдобавок, положение об обязанности всех провайдеров облачных услуг сообщать по запросу пользователю информацию о том, где находятся данные пользователя и какие нормы права, относительно раскрытия данной информации, применяются.

[37] Data Privacy Radar: How the German C5 affects us all // URL: https://blog.box.com/blog/data-privacy-radar-how-german-c5-affects-us-all/ (дата обращения: 12.04.2018).
[38] URL: https://www.canada.ca/en/shared-services/news/2018/02/cloud_computing.html (дата обращения: 12.04.2018).
[39] Walia H., Chandan A. Cloud Services: Recent Developments And Anticipated Laws// URL: http://www.mondaq.com/india/ (дата обращения: 10.12.2017).

В Саудовской Аравии [40] Комиссия по коммуникациям и информационным технологиям Саудовской Аравии приняла документ «Правовая основа облачных технологий», который призван устранить все неясности и сложности при использовании облаков. [41] Данный документ вступил в силу с 6 февраля 2018 года и применяется с 8 марта 2018 года. Он применяется ко всем случаям, когда услуги облачных технологий предоставляются гражданам Саудовской Аравии или данные хранятся или обрабатываются на территории Королевства. Предусматривается юнеобходимость регистрации провайдеров, устанавливается классификация данных пользователя по уровню необходимой информационной защиты (от первого уровня с неограниченным доступом до четвертого уровня секретности, сравнительного с конфиденциальностью государственной тайны). В отдельных положениях рассматривается вопрос нарушения прав интеллектуальной собственности при использовании облачных технологий.

Показательно, что на международном уровне, рабочая группа IV по Электронной торговле Комиссии ЮНСИТРАЛ в конце апреля 2017 года приняла решение о составлении руководства, касающегося облачной обработки компьютерных данных, и было отдельно отмечено, что нет необходимости принимать подробное законодательное руководство.[42]

Данная точка зрения представляется оправданной в отношении большинства отношений, связанных с использованием облачных технологий, поскольку они регулируются нормами уже существующего законодательства. К таким аспектам, например, относятся проблемы интеллектуальных прав на информацию в «облаке»[43] (в том числе, благодаря

[40] *O'Connel N.* Regulation of Cloud Computing in Saudi Arabia// URL: http://www.tamimi.com/ (дата обращения: 10.12.2017).
[41] Saudi Arabia: new Cloud Computing Regulatory Framework // URL: https://www.jdsupra.com/legalnews/saudi-arabia-new-cloud-computing-10730/ (дата обращения: 12.03.2018).
[42] п.11 Доклада рабочей группы IV (Электронная торговля) о работе ее пятьдесят пятой сессии, Комиссия ООН по праву международной торговли, 50 сессия // URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/V17/029/30/PDF/V1702930.pdf?OpenElement (дата обращения: 13.04.2018).
[43] *Нестерова И.А.* Распространение произведений с использованием облачных технологий//Авторское право и смежные права. 2016. №9.

распространению на провайдера облачных услуг норм об информационном посреднике[44]), вопросы, связанные с защитой персональных данных[45] и требований к их операторам (хотя провайдер облачных услуг может и не являться оператором персональных данных, к примеру, при предоставлении IaaS).

Но существует категория отношений, которые в силу особенностей облачных технологий требуют внесения определенных изменений в существующее регулирование. Сама же Комиссия ЮНСИТРАЛ выделила целый ряд черт, которые характеры исключительно для облачных технологий (они подробно рассмотрены ниже в главе о рисках использования облачных технологий). И хотя большинство проблем можно решить, а риски минимизировать через продуманную договорную политику, в некоторых аспектах необходимо законодательное регулирование (однако данный вопрос является темой для отдельной дискуссии).

Подводя итог, автор данной работы придерживается взгляда, что, учитывая стремительность развития технологий и гибкости форм ее использования, установление многочисленных специальных правовых норм только бы помешало экономическому обороту. Однако является желательным внесение некоторых корректировок и дополнений для усовершенствования регулирования отношений, связанных с облачными технологиями.

**Договорное регулирование**

Правовое регулирование отношений, связанных с облачными технологиями, во многом зависит от выбранной договорной модели. А.И. Савельев отмечает, что ни в судебной практике, ни в доктрине нет однозначного мнения о природе договоров о предоставлении услуг облачных

[44] ст. 1253.1 Гражданского кодекса Российской Федерации от 30.11.1994 N 51-ФЗ (ред. от 29.12.2017) // СЗ РФ. 1994. N 32. Ст. 3301.
[45] Комментарий к Федеральному закону от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»//Савельев А.И. М: Статут. 2015. С. 111.

технологий, но самыми распространенными договорами являются договор аренды, лицензионный договор, договор оказания услуг, смешанный и непоименованный договор.

Несмотря на то, что договор аренды использовался еще в советском праве для аренды «компьютерной программы»[46], а также применяется в практике Верховного суда Германии[47], надо признать, что его использование облачных технологий не вписывается в рамки норм о договоре аренды (так как они в большинстве своем направлены на предоставление материальных объектов в пользование арендатора).

На практике часто встречается оформление отношений по предоставлению услуг облачных технологий в форме лицензионного договора.[48] Эта тенденция поддерживается рядом отечественных авторов[49] и подтверждается зарубежной практикой[50]. Более того, использование этой договорной конструкции объясняется возможностью применения налоговой льготы, установленной пп.26 п.2 ст.149 Налогового кодекса Российской Федерации (далее - НК РФ). Также Савельев А.И. указывает на два других объяснения. Во-первых, облегчение продвижения продукта конечному пользователю при использовании посредников, благодаря возможности использовать одни и те же контрактные документы и процедуры для распространения лицензий на программное обеспечение и на облачный «сервис». Во-вторых, снижение рисков признания услуг облачных

---

[46] Комментарий к Гражданскому кодексу РСФСР / Отв. ред. С.Н. Братусь, О.Н. Садиков. 3-е изд., испр. и доп. М.: Юрид. лит., 1982 (комментарий к ст. 275); Левковская Н.И. Гражданско-правовая ответственность вычислительных центров в договорных обязательствах по обработке информации и проектированию АСУ: Автореф. дис. ... канд. юрид. наук. М., 1986. С. 3 («Договор «на продажу машинного времени« - договор найма с предоставлением услуг»).

[47] Bandulet F., Faisst W., Eggs H., Otyepka S., Wenzel S. Software-as-a-Service as Disruptive Innovation in the Enterprise Application Market // Software-as-a-Service: Anbieterstrategien, Kundenbedürfnisse und Wertschöpfungsstrukturen/ A. Benlian, Th. Hess, P. Buxmann (Hgs.). Gabler Verlag, 2010. S. 17.

[48] Решение Арбитражного суда г. Москвы от 24 июля 2015 г. по делу N А40-85252/15 // http://sudact.ru/arbitral/doc/sLyGj5OVn9VN/ (дата обращения: 23.02.2018).

[49] *Разуваев В*. Софт как услуга // ЭЖ-Юрист. 2010. N 5; Интернет-интервью с И.А. Близнецом, ректором Российской государственной академии интеллектуальной собственности: «Реализация государственной политики в области интеллектуальной собственности« // URL: http://www.consultant.ru/law/interview/bliznets2/ (дата обращения: 15.03.2018).

[50] *Guth S*. Contract Negotiation Handbook: Software as a Service // Guth Ventures, 2013. P. 20 - 21.

технологий услугами связи (п.32 ст.2 Федерального закона от 7 июля 2003 г. N 126-ФЗ «О связи»), что потребовало бы получение специальной лицензии и признание договора публичным (ст. 426 Гражданского кодекса Российской Федерации[51] (далее - ГК РФ)).

Несмотря на все эти преимущества, с формально-юридической точки зрения, применение данного договора к рассматриваемым отношениям некорректно. Предметом лицензионного договора может выступать только программное обеспечение, охраняемое авторским правом (п.1 ст. 1235 ГК РФ), тогда как услуги облачных вычислений включают в себя и объекты, не охраняемые правом интеллектуальной собственности (такие как, информационные технологии и средства, обеспечивающие оперативное объединение и разъединение ресурсов для адаптации к потребностям пользователя). Более того, нормы ГК РФ о лицензионном договоре предполагают предоставление пользователю экземпляра программного обеспечения[52], тогда как в рамках облачных услуг, зачастую программа для ЭВМ установлено только у провайдера, а пользователь может только удаленно пользоваться некоторыми его функциями. Таким образом, представляется, что облачные технологии лишь частично могут регулироваться нормами о лицензионном договоре.

Самым распространенным и общепризнанным договор для отношений, связанных с облаками, является договор возмездного оказания услуг.[53] Это подтверждается судебной практикой в зарубежных правопорядках [54] и в

[51] Гражданский кодекс Российской Федерации от 30.11.1994 N 51-ФЗ (ред. от 29.12.2017) // СЗ РФ. 1994. N 32. Ст. 3301.
[52] Например, ст.1270, 1272, 1280 Гражданского кодекса Российской Федерации от 30.11.1994 N 51-ФЗ (ред. от 29.12.2017) // СЗ РФ. 1994. N 32. Ст. 3301.
[53] *Савельев А.И.* Правовая природа «облачных« сервисов: свобода договора, авторское право и высокие технологии//Вестник гражданского права.2015. N 5.
[54] Во Франции (Tribunal de grande instance de Nanterre Ordonnance de 30 novembre 2012 // URL: http://www.legans.net/spip.php?page=jurisprudence-decision&id_article=3794 (дата обращения: 13.04.2018)), в США (*Melanson R.* Sales Taxes and the Shadow of Cloud Computing: Searching the Horizon for a Workable, National Solution // Tax Lawyer. 2012. Vol. 65. No. 4. P. 874, 880.).

России[55]. Преимуществами данной модели являются учет специфики оплаты облачных услуг (по системе «биллинга», в отличие от лицензионного договора, который предусматривает оплату за сам факт предоставления программы), возможность договорного определения требований к качеству услуги, применение норм об одностороннем отказе от договора (ст. 782 ГК РФ) и об информационном посреднике (ст. 17 Федерального закона «Об информации, информационных технологиях и защите информации»).

Однако облачные услуги могут предоставляться также и на безвозмездной основе, например публичные почтовые сервисы, предоставление бесплатного дискового пространства для хранения данных (iCloud, Yandex.Disk и т.д.), в отношении которых более уместно говорить о непоименованном договоре (п.2 ст. 421 ГК РФ), так как российское право не содержит специального регулирования безвозмездного оказания услуг. Хотя данная модель предоставляет сторонам большую свободу в определении условий договора, возникает опасность злоупотребления этой свободой провайдерами для обеспечения своих интересов в ущерб пользователей, которые часто не имеют специальных технических знаний об облачных технологиях и заключают договор путем соглашения с Условиями пользовательского соглашения.

Также не исключается использование смешанного договора (п.3 ст. 421 ГК РФ), соединяющего в себе элементы договора возмездного оказания услуг и лицензионного договора, что предоставит сторонам необходимую свободу в определении договорных условий, но при этом появляется больше

[55] Постановление Четвертого арбитражного апелляционного суда от 19 декабря 2014 г. N 04АП-4738/2014 по делу N А78-5032/2014// URL: http://pravosudie.biz/2076742 (дата обращения: 12.04.2018); Решение Арбитражного суда Забайкальского края от 26 января 2015 г. по делу N А78-14182/2014 // URL: http://chita.arbitr.ru/chita/cases/cdoc?docnd=841355499&nd=841134332&prefix=&numdeal=&yeardeal=&fld_12=&fld_14=&fld_16=&fld_140=&pagedoc=1 (дата обращения: 12.03.2018); Постановление Девятого арбитражного апелляционного суда от 16 января 2015 г. N 09АП-55322/2014 по делу N А40-77325/14 // СПС Консультант (дата обращения: 12.03.2018).

оснований для признания договора незаключенным и риск неприменения налоговой льготы, предусмотренной для лицензионного договора[56].

Таким образом, существует множество разных договорных моделей для регулирования отношений по предоставлению облачных услуг. Самыми распространенными из них стоит признать договор возмездного оказания услуг, лучше всего подходящий для целей решения ряда проблемных вопросов при использовании облаков.

Подводя итог данной главы, следует отметить, что облачные услуги остаются в большинстве своем не урегулированными законодательными нормами, что отражает практику большинства зарубежных стран. Поэтому решение проблем, связанных с данной технологией, должно осуществляться на договорной основе.

[56] Постановление Арбитражного суда Московского округа от 18 июня 2015 г. по делу N А40-91072/14 // URL: http://www.5451212.ru/sudebnaya-praktika-mosgorsuda/postanovlenie-arbitrazhnogo-suda-moskovskogo-okruga-ot-18-iyunya-2015-g-n-f05-7093-15-po-delu-n-a40-/ (дата обращения: 12.02.2018); Определение Верховного Суда РФ от 30 сентября 2015 г. N 305-КГ15-12154 // СПС Консультант (дата обращения: 24.03.2018).

## Глава 2. Защита информации при использовании облачных технологий

### 2.1. Угрозы информационной безопасности коммерческих организаций при использовании облачных технологий

В данной главе освещаются основные вопросы, возникающие при использовании облачных технологий коммерческими организациями, требующие особого решения, в связи со спецификой облаков.

Рабочая группа ЮНСИТРАЛ выделила 6 главных рисков в соответствующей области: потеря контроля пользователя (степень которой зависит от формы облачных услуг), возможность кибератак в связи с удаленным доступом к услугам, нечеткое распределение ролей и обязанностей, недостаточность мер безопасности провайдера, отсутствие сведений о местонахождении данных и количестве сторон, участвующих в предоставлении услуг облачных технологий.[57]

Первая и вторая проблемы нераздельно связаны друг с другом. Пользователь вынужден отдавать часть функций по использованию облачных технологий провайдеру, в первую очередь, в связи с отсутствием физического контроля пользователя над инфраструктурой, в которой хранится его информация. Угроза кибератак возникает именно из-за необходимости использования удаленного доступа к информации, с помощью зачастую незащищенных каналов передачи данных.[58] Ярким примером такой ситуации стал скандал в 2014 году, связанный с опубликованием в сети Интернет личных фотографий знаменитостей, загруженных в облачный сервис iCloud. Благодаря подбору ответов на достаточно простые стандартные контрольные вопросы, хакерам удалось

---

[57] п. 18 Приложения к Записке Секретариата Комиссии ООН по праву международной торговли «Договорные аспекты облачной обработки компьютерных данных»// URL: http://undocs.org/ru/A/CN.9/WG.IV/WP.142 (дата обращения: 14.04.18).

[58] Приказ Минюста России от 23.10.2017 N 208 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных Министерства юстиции Российской Федерации, эксплуатируемых при осуществлении Министерством юстиции Российской Федерации и его территориальными органами функций, определенных Указом Президента Российской Федерации от 13.10.2004 N 1313 «Вопросы Министерства юстиции Российской Федерации» // URL: http://www.pravo.gov.ru (дата обращения: 12.04.2018); *Шакель Н.В*. Юридические аспекты использования облачных технологий// URL: http://www.evolutio.info/content/view/2307/235/ (дата обращения: 23.03.2018).

получить доступ к конфиденциальной информации, после чего компания Apple вынуждена была усилить безопасность своего облачного сервиса.[59]

Из-за этих двух проблем контроль за сохранностью информации снижается (например, практически невозможно провести аудит [60]) и возникает необходимость применения дополнительных мер информационной безопасности пользователем и провайдером.[61]

Третий риск - отсутствие ясного распределения прав и обязанностей пользователя и провайдера - напрямую связан с потерей контроля пользователя. Именно благодаря определению объема правоотношений каждой стороны можно снизить риски, связанные с потерей контроля, обеспечив каждой стороне четко определенный круг обязанностей и устранив сомнения, которые могли бы потом привести к спорам и конфликтам.[62] Здесь надо оговориться, что модель распределения прав и обязанностей будет зависеть, в первую очередь, от формы предоставления облачных услуг, так как установить единый механизм для всех форм не представляется возможным в виду коренных отличий одной формы от другой.

Четвертая угроза - недостаточность мер безопасности провайдера - появляется в связи с отсутствием технической подготовки пользователя при заключении договора, поэтому необходимые стандарты безопасности не прописываются настолько подробно, насколько этого требует ситуация. Более того, при заключении договора с потребителями, чаще всего публичных и безвозмездных договоров, провайдеры сами формулируют условия, наиболее выгодные для них, и у пользователя фактически нет возможности внести свои изменения. При такой ситуации провайдеры,

---

[59] Apple усилит безопасность iCloud // Интернет-газета «Вести». 2014. URL: http://hitech.vesti.ru/news/view/id/5556 (дата обращения: 23.03.2018).

[60] *Goodwin Andrew*. Practice Pointers: Risk Allocation in Enterprise Cloud Service Agreements // URL: https://www.dataprivacymonitor.com/cloud-computing/five-practice-pointers-risk-allocation-in-enterprise-cloud-service-agreements/ (дата обращения: 23.03.2018).

[61] *Глухов Н.И., Волошина П.С.* Исследование законодательства Российской Федерации в сфере облачных технологий//Academy. N 6(21). 2017.

[62] *Christopher J. Millard*. Cloud Computing Law// URL: https://global.oup.com/ (дата обращения: 09.12.2017).

которые, как правило, не заинтересованы в установлении дополнительных средств защиты, ведь это связано с дополнительными затратами, оказываются в более выигрышном положении в убыток пользователям.[63]

Отсутствие сведений о местонахождении данных обусловлено особенностью функционирования облачных технологий. Информация, размещенная в «облаках» фактически может находиться в разных юрисдикциях, в силу применения технологии фрагментации данных. Поэтому возникает несколько проблем: определение применимого права в условиях трансграничного характера информации [64], обеспечение целостности и конфиденциальности информации, соблюдение требований законодательства при работе с персональными данными.

Самым ярким примером первой проблемы является регулирование вопросов авторского права при создании объектов интеллектуальной собственности в облаках. В связи с различным национальным регулированием предоставления правовой защиты некоторым объектам, определение применимого права становится ключевым вопросом. В частности, профессор Миллард приводит пример создания базы данных пользователем в Англии (где базы данных охраняются как объект авторского права), но размещение ее на серверах в Соединенных Штатах Америки, где Верховный суд США в деле Feist[65] разъяснил, что не все базы данных защищаются американским правом интеллектуальной собственности, а только те, в которых есть явный творческий элемент.[66] Представляется, что данный пример является актуальным и для России, где, согласно ст. 1228 ГК РФ, базы данных охраняются в качестве объектов авторских прав только при условии внесения творческого вклада автора в ее создание. Возможным способом решения данной проблемы (правда только в рамках отношений

[63] *Christopher J. Millard*. Cloud Computing Law// URL: https://global.oup.com/ (дата обращения: 09.12.2017).
[64] *Царегородцев А.В., Савельев И.А., Романовский С.В.* Обеспечение безопасности данных в облаченных сферах // Экономика. Налоги. Право. 2013. №4; Организационно-правовое обеспечение информационной безопасности: монография / Морозов А.В., Полякова Т.А. М.: РПА Минюста России. 2013. С.244.
[65] Feist Publications, Inc. v. Rural Telephone Service Co. 499 U.S. 340 (1991) // URL: https://supreme.justia.com/cases/federal/us/499/340/case.html (дата обращения: 23.03.2018).
[66] *Christopher J. Millard*. Cloud Computing Law// URL: https://global.oup.com/ (дата обращения: 09.12.2017).

провайдера и пользователя) является внесение в договор предоставления облачных услуг положения о том, что стороны договариваются применять российское право для квалификации объектов, созданных при использовании облачных технологий. В таком случае, юридическая сила данного положения будет зависеть от применимого права.

Кроме того, правовое регулирование инфраструктуры может различаться в разных странах, и провайдеры должны будут соответствовать требованиям этих юрисдикций, тогда как пользователю неизвестны эти требования, что может значительно затруднять его деятельность.[67]

Что касается второй проблемы, то угроза безопасности информации, фрагментированной и распределенной по разным Центрам обработки данных (*далее* - ЦОД), расположенных в разных местах, усугубляется использованием публичных облаков, в которых степень контроля пользователя ограничена. Более того, нахождение физических серверов в разных юрисдикциях порождает дополнительные риски в связи с различиями степени вмешательства правоохранительных органов в деятельность ЦОД, возможности изъятия серверов и получении доступа к данным на них. Для снижения данных рисков информация должна копироваться и сохраняться в резервных копиях в разных ЦОД, а также храниться в зашифрованном виде для препятствия нарушения режима конфиденциальности.

Также в этом отношении остро встает вопрос о применении норм, связанных с защитой персональных данных. Как отмечает Минюст, использование облачных технологий является одной из основных угроз безопасности персональных данных, защищаемых без использования средств криптографической защиты информации.[68]

---

[67] *Царегородцев А.В., Савельев И.А., Романовский С.В.* Обеспечение безопасности данных в облаченных сферах // Экономика. Налоги. Право. 2013. №4.

[68] Приказ Минюста России от 23.10.2017 N 208 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных Министерства юстиции Российской Федерации, эксплуатируемых при осуществлении Министерством юстиции Российской Федерации и его территориальными органами функций, определенных Указом Президента Российской Федерации от 13.10.2004 N 1313 «Вопросы Министерства юстиции Российской Федерации» // URL: http://www.pravo.gov.ru (дата обращения: 12.04.2018).

Здесь, пожалуй, стоит обратить внимание на два аспекта: соотношение провайдера облачных услуг и оператора персональных данных, и особенности исполнения требований о локализации данных.

Вопрос о правовом статусе провайдера облачных услуг является дискуссионным в научной литературе, в связи с отсутствием законодательного регулирования. Отмечается, что не все провайдеры будут автоматически считаться операторами, ведь в некоторых формах облачных технологий провайдер не знает о том, какая информация загружается в облачный сервер (например, в IaaS, либо в силу использования технологий шифрования данных).[69] Также может быть ситуация, когда пользователь будет являться оператором, который осуществляет сбор персональных данных с помощью провайдера облачных услуг. В таком случае на пользователе будет лежать обязанность убедиться в том, что серверы провайдера находятся на территории Российской Федерации, так как в обратном случае ответственность понесет пользователь как оператор персональных данных (ст.15.5 Федерального закона от 27.07.2006 N 152-ФЗ (ред. от 29.07.2017 «О персональных данных» 70 (*далее* – ФЗ «О персональных данных)).[71] При подобном привлечении сторонних организаций для обработки персональных данных на основании договора, или «аутсорсинге», как это называют в иностранной литературе, когда провайдер облачных услуг может обрабатывать обезличенные данные нескольких организаций одновременно, Роскомнадзор рекомендует выделять

[69] *Christopher J. Millard*. Cloud Computing Law// URL: https://global.oup.com/ (дата обращения: 09.12.2017).; *Емельянников М.Ю.* «Облако в законе»: юридические аспекты использования облачных сервисов в России //URL: http://embeddedday.ru/2016/presentations/.pdf (дата обращения: 24.04.2018); Комментарий к Федеральному закону от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»//Савельев А.И. М: Статут. 2015. С. 82.

70 Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 29.07.2017) «О персональных данных«// СЗ РФ. N 31. Ст. 3451.

[71] *Савельев А.И.* Научно-практический постатейный комментарий к Федеральному закону «О персональных данных« // М.: Статут, 2017. 320 с.

зону ответственности операторов и субъектов, поручивших обработку оператору.[72]

В соответствии с требованием о локализации персональных данных (ч. 5 ст. 18 ФЗ «О персональных данных»), в России необходимо собирать и хранить персональные данные в пределах страны, а обрабатывать их можно и за рубежом.[73] Причем, трансграничная передача персональных данных, согласно ст. 12 ФЗ «О персональных данных», возможна только в страны-участницы Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных или в иные государства, включенные в Перечень стран, обеспечивающих адекватную защиту прав субъектов персональных данных.[74] Если же иностранное государство не входит в этот перечень и не является участницей Конвенции Совета Европы, то провайдеру будет необходимо получить письменное согласие субъекта персональных данных на трансграничную передачу его персональных данных, либо прописать данное положение в договоре с пользователем-субъектом персональных данных. Таким образом, провайдер должен убедиться не только в том, что сбор персональных данных осуществляется с помощью баз данных на территории Российской Федерации, но и что при передаче информации в другие сервера в иностранных государствах не нарушаются требования закона.

Отсутствие сведений о количестве сторон, участвующих в предоставлении услуг объясняется возможностью конструирования нескольких уровней различных форм облачных технологий.

Профессор Миллиард выделяет целых семь подобных уровней. Во-первых, облачные технологии могут состоять из одного уровня IaaS, такие

[72] Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. N 996 «Об утверждении требований и методов по обезличиванию персональных данных, утв. Приказом Роскомнадзором от 13.12.2013// СПС Консультант.

[73] О защите персональных данных на российском и европейских рынках// URL: https://habrahabr.ru/company/it-grad/blog/332396/ (дата обращения: 19.01.2018).

[74] Перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных, утв. Приказом Роскомнадзора от 15.03.2013 N 274 (ред. от 15.06.2017)// Российская Газета. N 92. 26.04.2013.

как Amazon Web Services, RackSpace, GoGrid, или Google Compute Engine. Во-вторых, PaaS может выступать единственным уровнем в таких программах как Google App Engine, Microsoft Windows Azure, Salesforce's force.com. В-третьих, PaaS может строиться на IaaS (dotCloud, Engine Yard, Heroku, основанные на IaaS Amazon'a). В-четвертых, одноуровневый SaaS, например, такие социальные сети как Facebook, Flickr, почтовые сервисы Gmail, Outlook.com. В-пятых, SaaS может быть основан на IaaS, как в Dropbox или Foursquare на инфраструктуре Amazon. В-шестых, SaaS на PaaS. И, наконец, трехуровневая структура, где SaaS функционирует на основе PaaS, которая основана на IaaS, в таких приложениях как dotCloud или Heroku.

Опасность существования такого количества уровней состоит в том, что, как правило, они неизвестны конечным пользователям облачных технологий, несмотря на очевидную важность такой информации для оценки рисков, связанных с качеством предоставления услуг «скрытыми» провайдерами (или провайдерами второго и третьего уровня). В связи с этим, в условиях множественности уровней и сложной системы договорных отношений, остро стоит проблема заверений сторон об обеспечении безопасности данных. Эта опасность также отмечается в Программе «Цифровая экономика Российской Федерации», как одно из обстоятельств, препятствующих развитию цифровой экономии в России и создающих угрозу личности, бизнесу и государству.[75]

Еще одной угрозой, отмечаемой специалистами, является опасность неполного удаления данных при использовании облачных технологий. Это связано с разными «уровнями» удаления информации, о которых зачастую пользователь не осведомлен. Так, при перемещении файла в Корзину, как правило, информация продолжает храниться на облачном сервере в течение

[75] Распоряжение Правительства РФ от 28.07.2017 N 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации»// СЗ РФ. N 32. 2017. Ст. 5138.

30 дней или до «очистки Корзины». Тем не менее, даже после истечения указанного срока или очистки, информация не окончательно удаляется, а стираются только «указатели» о местонахождении отдельных кусков информации в условиях фрагментации данных.[76] Сама же информация продолжает храниться в серверах провайдера (правда теперь как разрозненные части, не соединенные в одно целое), и если случится так, что на одном сервере остался достаточно большой объем информации, то третьи лица могут неправомерно получить доступ к ней (особенно те, кто использует ту же физическую инфраструктуру).[77] Однако надо признать, что вероятность подобной ситуации чрезвычайно мала, и скорее носит теоретический, нежели практический характер. Офис Комиссара по информации (Information Commissioner's Office) в Великобритании сравнил этот случай с вероятностью получения информации из остатков документов после использования шредера.[78]

Проблема также усугубляется несколькими факторами. Во-первых, большим количество резервных копий в разных хранилищах по всему миру, которые провайдеры делают для обеспечения непрерывного доступа к информации и в которых могут сохраняться данные даже после того, как они формально удалены. Во-вторых, тем, что большинство услуг по предоставлению облачных технологий в целях хранения данных (так называемые, облачные хранилища) не дают пользователю возможности определить судьбу информации, размещенной в облаке.[79] Из-за этого удаление с внешнего устройства (мобильный телефон, компьютер) не влечет автоматического удаления информации с учетной записи в облаке, и даже при удалении из учетной записи, стандартные настройки могут

[76] Например, условия пользования Google Apps SaaS указывают, что при закрытии профиля Google удалит информацию «после коммерчески разумного промежутка времени, путем удаления указателей на нее на активных серверах Google и переписывания другой информации поверх нее» (Google Apps (Free) Agreement // URL: http://www.google.com/apps/intl/en/terms/standard_terms.html (дата обращения: 23.03.2018)).

[77] *Christopher J. Millard*. Cloud Computing Law// URL: https://global.oup.com/ (дата обращения: 09.12.2017).

[78] ICO, «Deleting Personal Data«// URL: https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf (дата обращения: 20.04.2018).

[79] *Шакель Н.В*. Юридические аспекты использования облачных технологий// URL: http://www.evolutio.info/content/view/2307/235/ (дата обращения: 23.03.2018).

предусматривать сохранение резервной копии информации на сервере провайдера.[80] Также многие провайдеры облачных технологий в форме SaaS (в том числе Dropbox[81]) предлагают сохранение всех копий документа для обеспечения возможности вернуться к любой из прошлых версий, что значительно усложняет решение рассматриваемого вопроса. [82] Поэтому чрезвычайно важно в договоре установить судьбу удаляемой информации, резервных копий, порядок осуществления этой процедуры.[83]

Таким образом, использование облачных технологий, хоть и связано с большим количеством преимущество, но также предполагает ряд проблемных вопросов, которые осмотрительный и добросовестный пользователь должен иметь в виду при принятии мер обеспечения информационной безопасности, особенно, когда его работа связана с обработкой, хранением, использованием информации, охраняемой правовым режимом коммерческой тайны.

---

[80] *Шакель Н.В*. Юридические аспекты использования облачных технологий// URL: http://www.evolutio.info/content/view/2307/235/ (дата обращения: 23.03.2018); *Тян В*. Облачные технологии: вызовы правового регулирования// URL: https://kapital.kz/gosudarstvo/55665/oblachnye-tehnologii-vyzovy-pravovogo-regulirovaniya.html (дата обращения: 25.03.2018).

[81] Dropbox Terms of Service // URL: https://www.dropbox.com/terms (дата обращения: 23.04.2018).

[82] *Christopher J. Millard*. Cloud Computing Law// URL: https://global.oup.com/ (дата обращения: 09.12.2017).

[83] *Глухов Н.И., Волошина П.С*. Исследование законодательства Российской Федерации в сфере облачных технологий//Academy. N 6(21). 2017.

## 2.2. Меры предупреждения утечки при использовании облачных технологий

Для предотвращения реализации рисков, обозначенных в предыдущей главе, или хотя бы их минимизации, пользователю необходимо принять целый ряд комплексных мер при работе с облачными технологиями. Предлагается разделить их на две большие группы: договорные способы обеспечения информационной безопасности и меры, которые должен обеспечить сам пользователь в одностороннем порядке.

В первую группу («двусторонние меры») входят особые механизмы, которые представляется необходимым включить в договор между провайдером и пользователем, в связи с отсутствием в законодательстве соответствующего регулирования и вероятности возникновения споров на почве правовой неопределенности. На многие из этих механизмов указывалось выше при рассмотрении существующих проблем и рисков, и основными являются закрепление распределения ответственности между провайдером и пользователем, закрепление требований соответствия стандарту качества предоставления облачных услуг, страхования имущественной ответственности провайдера.

Во вторую группу входят «односторонние» меры, которые пользователь должен принять для обеспечения информационной безопасности. Здесь предлагается рассмотреть вопросы, связанные с установлениям режима коммерческой тайны и разработкой, утверждением, эффективной реализации политики информационной безопасности.

### 2.2.1. Распределение ответственности между участниками облачных отношений

Данный вопрос является одним из ключевых для обеспечения безопасности информации при использовании облачных технологий [84] и

[84] п.20 Доклада рабочей группы IV (Электронная торговля) о работе ее пятьдесят пятой сессии, Комиссия ООН по праву международной торговли, 50 сессия // URL: https://documents-dds-

зависит от формы предоставления облачных услуг. [85] Так, при предоставлении услуг в форме программы, пользователь получает возможность воспользоваться программным обеспечением провайдера, оставляя все остальные вычислительные ресурсы под контролем провайдера (серверы, устройства хранения данных, вычислительные мощности и т.д.). Если пользователь получает услугу в форме платформы, то он самостоятельно управляет вычислительными мощностями для создания или приобретения приложений, но провайдер определяет инструменты и язык программирования, которыми может пользоваться пользователь. Наконец, когда облачные услуги предоставляются в форме инфраструктуры, то провайдер отвечает только за функционирование оборудования, на основе которого пользователь самостоятельно использует все вычислительные ресурсы (приложения, вычислительные мощности, устройства хранения данных). Такое распределение рисков отражает сложившуюся практику, как отмечается в зарубежной[86] и отечественной[87] литературе.

Представляется необходимым закреплять подобное распределение ответственности в договорах, вместе с общей обязанностью провайдера обеспечивать конфиденциальность, доступность и целостность информации. Именно грамотное формулирование условий договора о предоставлении услуг облачных технологий позволит создать эффективный механизм минимизации рисков утечки информации.

В данном отношении стоит также проанализировать соотношение понятия провайдера облачных технологий с пересекающимися понятиями «информационного посредника» (ст. 1253.1 Гражданского кодекса РФ), «обладателя информации» (ст. 6 ФЗ «Об информации, информационных технологиях и о защите информации» (*далее* - ФЗ «Об информации»)),

---

ny.un.org/doc/UNDOC/GEN/V17/029/30/PDF/V1702930.pdf?OpenElement (дата обращения: 13.04.2018); Предпринимательская деятельность в сети Интернет: Монография/ Демьянец М.В., Елин В.М., Жарова А.К. М: Юркомпани. 2014. С.76.

[85] *Christopher J. Millard*. Cloud Computing Law// URL: https://global.oup.com/ (дата обращения: 09.12.2017).

[86] Там же.

[87] *Нестерова И.А*. Правовое регулирование отношений, возникающих при использовании облачных технологий/ Дис. канд. юрид. наук:12.00.03. М. 2016. С.56.

«провайдера хостинга» (п.18 ст.2 ФЗ «Об информации»)), «организатора распространения информации» (ст.10.1 ФЗ «Об информации»).

Несмотря на то, что провайдер облачных услуг попадает под определение информационного посредника как лицо, предоставляющее возможность размещения материала с использованием информационно-телекоммуникационной сети, на практике возникают проблемы с определением правового статуса провайдера.[88] Поэтому предлагается внести указание в договоре о применении норм об информационном посреднике к провайдеру. Это необходимо для разрешения ряда проблем, связанных с охраной результатов интеллектуальной деятельности при использовании облачных технологий, в частности, снятия ответственности с провайдера за материалы, размещенные пользователем облачных услуг, и устранения любых сомнений при разрешении споров.

Стоит учитывать, что провайдер облачных услуг не является обладателем информации, как разъяснил Конституционный суд в отношении сервиса электронной почты (облачные услуги в форме SaaS).[89] В этой связи представляет интерес резонансное дело между ООО «В Контакте» и ООО «Дабл». Ответчик в этом деле использовал данные из открытых аккаунтов пользователей социальной сети в коммерческих целях для выявления кредитных историй лиц. Суд апелляционной инстанции поддержал требования истца, признав, что «Социальная сеть» является базой данных в смысле ст. 1260 ГК РФ, использование которой нарушает авторские права В Контакте. Тот факт, что данные пользователей были в открытом доступе не повлиял на решение суда, который указал, что сбор информации ООО «Дабл» происходит, в том числе, в Социальной сети, на что истец не давал согласия. Более того, суд решил, что «истец гарантировал пользователям

[88] *Нестерова И.* Распространение произведений с использованием облачных технологий//Авторское право и смежные права. 2016. №9.

[89] Постановление Конституционного Суда РФ от 26.10.2017 N 25-П «По делу о проверке конституционности пункта 5 статьи 2 Федерального закона "Об информации, информационных технологиях и о защите информации" в связи с жалобой гражданина А.И. Сушкова»// СЗ. 2017. № 45. Ст. 6735.

защиту информации от посторонних лиц, независимо от того, является ли информация открытой иди приватной», следовательно, не санкционированное истцом получения информации пользователей противозаконно.[90] В настоящий момент дело находится в кассационной инстанции.[91] Интересен тот факт, что спустя несколько месяцев после вынесения данного решения, В Контакте приняло решение разрешить Национальному Бюро кредитных историй собирать и использовать данные пользователей-заемщиков.[92] Таким образом, хотя облачный сервер формально не является обладателем информации, это не препятствует социальным сетям использовать данные пользователей по своему усмотрению.

Соотношение провайдера облачных услуг и провайдера хостинга является неоднозначной проблемой. С технической точки зрения это две разные модели предоставления сервиса. Провайдер хостинга размещает информацию на одном физическом сервере, тогда как провайдер облачных услуг обеспечивает размещение информации на нескольких серверах, связанных между собой с помощью облачных технологий.[93] Тем не менее с юридической точки зрения представляется возможным распространить некоторых правил о провайдере хостинга на провайдера облачных услуг[94] для определения обязанностей провайдера при выявлении нарушений порядка обработки персональных данных, при ограничении доступа к заблокированным сайтам, а также установления ответственности провайдера при ограничении доступа к информации (п. 4 ст. 17 ФЗ «Об информации»).

---

[90] Решение Арбитражного суда города Москвы от 12.10.2017 по делу N А40-18827/17 // СПС Консультант (дата обращения: 23.03.2018).

[91] Определение Суда по интеллектуальным правам от 17.04.2018 N С01-201/2018 по делу N А40-18827/2017 «Об отложении судебного заседания суда кассационной инстанции» // СПС Консультант (дата обращения: 23.04.2018).

[92] Как «ВКонтакте» разрешила анализировать данные пользователей // URL: https://www.rbc.ru/technology_and_media/02/04/2018/5abe534d9a7947350e3a7dfa (дата обращения: 23.04.2018).

[93] *Паус А.С., Целовальникова О.А*. Тенденции развития облачных технологий на российском рынке // Новые информационные технологии в автоматизированных системах. 2014. №17.

[94] Комментарий к Федеральному закону от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»//Савельев А.И. М: Статут. 2015. С. 111.

Для организатора распространения информации данных нет необходимости вводить специальное регулирование, так как провайдер облачных услуг может не обладать данными правовыми статусами. Например, при предоставлении облачных услуг в форме инфраструктуры, когда провайдер не имеет доступа к информации пользователя, обрабатываемой с помощью облачных технологий.[95]

### 2.2.2. Иные договорные меры повышения безопасности технологии

Помимо распределения ответственности, в договоре необходимо прописать также комплекс мер для повышения безопасности облачных технологий. Как указывают данные статистики, основным препятствием перехода на облачные технологии являются соображения обеспечения безопасности и конфиденциальности данных.[96] Поэтому представляется крайне важным устанавливать обязанность провайдера, осуществляющего хранение, использование или обработку информации, распространение которой ограничено федеральными законами (например, коммерческой тайны или персональных данных), страховать свою имущественную ответственность, а также соответствовать стандартам безопасности облачных технологий.

Страхование имущественной ответственности позволит повысить доверие пользователей к использованию облачных технологий и предоставит экономическую защиту их имущественных интересов. На настоящий момент страхование ответственности является рекомендованной и широко распространенной практикой.[97] Более того, в США возможность введения обязательного страхования обсуждается на уровне Департамента внутренней

[95] Там же. С. 82.
[96] URL: http://www.tadviser.ru/index (дата обращения: 09.12.2017).
[97] *Godes S., Cleary K., Fessler H.* The Cloud: Selected Benefits, Risks, and Insurance Coverage Issues/ URL: https://www.lexology.com/library/ (дата обращения: 09.12.2017).

безопасности[98], в Европе идут аналогичные дискуссии в связи с принятием Директивы о безопасности сети и информационных сетей.[99]

Установление обязанности провайдера соответствовать стандарту безопасности является одним из самых важных и эффективных инструментов для снижения различного рода рисков, связанных с облаками.[100] На сегодняшний день в России не принят национальный стандарт в области облачных технологий, однако уже подготовлен проект ГОСТа «Требования по защите информации, обрабатываемой с использованием технологий облачных вычислений», принятие которого предусмотрено в рамках Программы «Цифровая экономика» ко 2 кварталу 2020 года.[101] Вместе с тем в зарубежных юрисдикциях уже действуют подобные стандарты. Так, в США Федеральная стратегия облачных вычислений предусматривает разработку таких стандартов NIST[102], в Японии принята Программа оценки технологической безопасности и сертификации.[103]

Однако отсутствие национального стандарта не должно препятствовать включению данного условия в договор между провайдером и пользователем, ведь существуют широко используемые международные стандарты, на основе которых национальные стандарты и будут вырабатываться (ст. 15 Федерального закона «О стандартизации в РФ»). Например, принятые в 2016 и 2017 годах стандарты Cloud Computing Service level agreement (ISO/IEC 19086104) и Cloud Services and devices: Data flow, data categories and data use

---

[98] Insurance for Cyber-related critical infrastructure loss // URL: https://www.dhs.gov/cybersecurity-insurance (дата обращения: 09.12.2017).

[99] Cyber Insurance: A look at recent advances, good practices and challenges by ENISA// URL: https://www.enisa.europa.eu/news/enisa-news/cyber-insurance-a-look-at-recent-advances-good-practices-and-challenges-by-enisa (дата обращения: 09.12.2017).

[100] *Царегородцев А.В., Савельев И.А., Романовский С.В.* Обеспечение безопасности данных в облаченных сферах // Экономика. Налоги. Право. 2013. №4; Организационно-правовое обеспечение информационной безопасности: монография / Морозов А.В., Полякова Т.А. М.: РПА Минюста России. 2013. С.244.

[101] Распоряжение Правительства РФ от 28.07.2017 N 1632-р «Об утверждении программы "Цифровая экономика Российской Федерации»// СЗ РФ. N 32. 2017. Ст. 5138.

[102] *Kundra V.* Federal Cloud Computing Strategy/ URL: https://www.dhs.gov/ (дата обращения: 09.12.2017).

[103] URL: http://cloudscorecard.bsa.org/ (дата обращения: 09.12.2017).

104 ISO/IEC 19086-1:2016 // URL: https://www.iso.org/standard/67545.html?browse=tc (Дата обращения: 20.04.2018).

(ISO/IEC 19944 105 ), а также около десятка подобных международных стандартов, устанавливающих типичные условия для использования облачных технологий. Эти стандарты приняты Международной организацией стандартизации (International Standards Organization), совместно с Международной электротехнической комиссией (International Electrotechnical Commission), в условиях отсутствия законодательного регулирования в большинстве стран мира, с одной стороны, и острой потребности пользователей в определенном руководстве при составлении договоров, с другой стороны. Предлагается использовать именно эти разработки при установлении договорных требований к качеству работы или услуги провайдера.

Более того, обязательное соответствие национальному стандарту позволит разрешить проблему обеспечения безопасности облачных услуг в условиях сложных договорных связей между провайдером и третьими лицами. При наличии сертификата соответствия стандарту пользователи могут уверено полагаться на провайдера, без необходимости проверять лиц, которые обеспечивают деятельность провайдера.

Некоторые специалисты и ученые в группу мер по повышению безопасности технологии включают также обеспечение возможности пользователю проводить аудит провайдера.[106] Данный вопрос является дискуссионным, в связи с особенностями облачных технологий.[107] Из-за использования технологии фрагментации данных, информация «разбросана» по разным серверам, иногда на разных континентах, и пользователь практически не способен посетить каждый из них. Но даже если бы он мог

105 ISO/IEC 19944:2017 // URL: https://www.iso.org/standard/66674.html?browse=tc (дата обращения: 20.04.2018).

[106] *Меликов У.А*. Гражданско-правовые проблемы, связанные с сервером // Вестник ЮУрГУ. Серия: Право. 2016. №1. URL: https://cyberleninka.ru/article/n/grazhdansko-pravovye-problemy-svyazannye-s-serverom (дата обращения: 29.04.2018).

[107] *Полякова Т.А., Химченко А.И*. Актуальные организационно-правовые вопросы трансграничной передачи персональных данных // Право. Журнал Высшей школы экономики. 2013. №1. URL: https://cyberleninka.ru/article/n/aktualnye-organizatsionno-pravovye-voprosy-transgranichnoy-peredachi-personalnyh-dannyh (дата обращения: 29.04.2018); Организационно-правовое обеспечение информационной безопасности: монография / Морозов А.В., Полякова Т.А. М.: РПА Минюста России. 2013. С.244.

это сделать, проведение аудита все равно было бы проблематично, так как в условиях виртуализации данных на одном сервере находятся данные больше чем одного пользователя. Соображения безопасности и конфиденциальности данных третьих лиц ограничивают пользователя в проведении соответствующей процедуры проверки.[108] Тем не менее, некоторые авторы предлагают выход из данной ситуации путем закрепления обязанности провайдера предоставлять заверения в надлежащем качестве обеспечения безопасности облачных технологий в форме отчетов о проведении аудита третьей стороной.[109] Наиболее популярным таким отчетом является SOC Type 2 (Контроль за организацией предоставления услуг Типа 2), который представляет собой анализ качества обеспечения безопасности провайдером по определенному набору критериев, которые сам пользователь выбирает в зависимости от его нужд и особенностей деятельности.[110]

### 2.2.3. Принятие мер самим пользователем

Помимо договорных, или «двусторонних» мер, требующих согласования между провайдером и пользователем, последнему также необходимо самому принять целый ряд мер для предотвращения утечки информации. Причем стоит обратить внимание на основные риски, которые могут привести к утечке информации. К ним относятся: сложности при необходимости оперативно реагирования служб безопасности организации на изменения в работе компании, противоречивость требований к работникам и практикой их выполнения, объективная невозможность выполнения некоторых функций работников служб безопасности и неэффективная система ответственности за невыполнение или ненадлежащее

---

[108] *Goodwin Andrew*. Practice Pointers: Risk Allocation in Enterprise Cloud Service Agreements // URL: https://www.dataprivacymonitor.com/cloud-computing/five-practice-pointers-risk-allocation-in-enterprise-cloud-service-agreements/ (дата обращения: 23.03.2018).

[109] *Christopher J. Millard*. Cloud Computing Law// URL: https://global.oup.com/ (дата обращения: 09.12.2017); *Goodwin Andrew*. Practice Pointers: Risk Allocation in Enterprise Cloud Service Agreements // URL: https://www.dataprivacymonitor.com/cloud-computing/five-practice-pointers-risk-allocation-in-enterprise-cloud-service-agreements/ (дата обращения: 23.03.2018).

[110] URL: http://www.onlinetech.com/resources/references/what-is-a-soc-2-report-an-easy-explanation (дата обращения: 20.04.2018).

выполнение обязанностей, связанных с обеспечением безопасности информации.[111]

Важно понимать, что большинство из данных мер нужны для каждой коммерческой организации или индивидуального предпринимателя, вне зависимости от использования облачных технологий, хотя, конечно, внедрение облаков в коммерческую деятельность превращает данные меры из «настоятельно рекомендованных» в «жизненно необходимые». Данный раздел будет посвящен двум блокам односторонних мер обеспечения и повышения безопасности информации: установление режима коммерческой тайны и проведение грамотной политики информационной безопасности.

**Установление режима коммерческой тайны**

Институт коммерческой тайны является способом установить дополнительный уровень безопасности некоторой категории данных, обеспеченный законодательным регулированием и нормативно установленными санкциями. Согласно ст.3 Федерального закона от 29.07.2004 N 98-ФЗ «О коммерческой тайне» (далее - ФЗ «О коммерческой тайне»[112]) под коммерческой тайной понимается режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду. К информации, составляющей коммерческую тайну, относятся сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность

[111] *Северин В.А*. Теоретико-методологические основы обеспечения безопасности коммерческих структур в информационной сфере // Информационное право. 2016. N 4. С. 13 - 19.
[112] Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 18.04.2018) «О коммерческой тайне»// СЗ РФ. 2004. N 32. Ст. 3283.

в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Согласно ч. 1 и 2 ст. 10 ФЗ «О коммерческой тайне» режим коммерческой тайны считается установленным после принятия обладателем информации следующих мер: определение перечня информации, составляющей коммерческую тайну, ограничение доступа к информации, составляющей коммерческую тайну, учет лиц, получивших доступ к данной информации, введение грифа «Коммерческая тайна» для соответствующих материальных носителей и реквизитов документов. В случае отсутствия установленного режима коммерческой тайны правила о ее защите не подлежат применению.[113]

Подтверждением установления режима коммерческой тайны могут служить локальные нормативные акты, изданные владельцем информации, документы, регулирующие отношения владельца информации с третьими лицами[114] и иные документы, содержащие требования к охране коммерческой тайны.

За нарушение режима коммерческой тайны российским законодательством предусмотрены несколько видов ответственности: дисциплинарная[115], материальная[116], гражданская[117], административная[118], уголовная[119].

---

[113] Апелляционное определение Санкт-Петербургского городского суда от 27.09.2016 N 33-17808/2016 // СПС Консультант (дата обращения: 12.02.2018).
[114] Постановление Двадцатого арбитражного апелляционного суда от 09.11.2016 по делу N А68-2206/2016 // СПС Консультант (дата обращения: 13.02.2018).
[115] п. 6 ст. 81 Трудового кодекса Российской Федерации от 30.12.2001 N 197-ФЗ (ред. от 05.02.2018)// СЗ РФ. 2002. N 1. Ст. 3.
[116] ст.243 Трудового кодекса Российской Федерации от 30.12.2001 N 197-ФЗ (ред. от 05.02.2018)// СЗ РФ. 2002. N 1. Ст. 3.
[117] ч.2 ст. 6.1 Федерального закона от 29.07.2004 N 98-ФЗ (ред. от 18.04.2018) «О коммерческой тайне»// СЗ РФ. 2004. N 32. Ст. 3283.
[118] ст.13.14 Кодекса Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ (ред. от 03.04.2018)// СЗ РФ. 2002. N 1. Ст. 1.
[119] ст.183 Уголовного кодекса Российской Федерации« от 13.06.1996 N 63-ФЗ (ред. от 19.02.2018, с изм. от 25.04.2018) // СЗ РФ. 1996. N 25. Ст. 2954.

При всех видимых преимуществах установления режима коммерческой тайны необходимо учитывать риск злоупотребления данным институтом, который приведет к излишнему засекречиванию информации, препятствия доступа к ней, что может затруднить и затормозить работу всей организации. Как отмечает В.А. Северин, различают три категории коммерческой тайны в зависимости от последствий ее нарушения: первой (причинение ущерба организации), второй (причинение крупного ущерба) и третьей категории (такие тяжкие последствия, как признание несостоятельности компании).[120] Представляется целесообразным отразить данную классификацию в локальных нормативных актах компании для использования мер защиты информации, соответствующих каждой из категорий коммерческой тайны.

Ввиду особой важности информации, защищаемой режимом коммерческой тайны, для тех организаций, которые могут себе это позволить, рекомендуется использование частного облака, а не публичного, для обеспечения большего контроля за местонахождением, уровнем качества и безопасности обслуживания. В связи с этим в таких предприятиях следует предусмотреть запрет на использование публичных облачных хранилищ, таких как Google Drive, Dropbox, Yandex.Disk, Apple iCloud, OneDrive для размещения, хранения, распространения конфиденциальной информации. Вместо этих ресурсов можно использовать более безопасные и защищенные сервисы файлового обмена, например, путем эксплуатации программ DataRoom или Synology. Надо обратить внимание, что даже при использовании таких защищенных сервисов, не рекомендуется хранить информацию в этих сервисах, и стоит удалять ее сразу после завершения обмена файлами, оставляя копию только на частном облаке.

Также стоит предусмотреть, что охраняемая информация не будет храниться в публичных облаках не только на рабочих устройствах сотрудников, но и на их личных учетных записях. Более того, в отношениях с

[120] *Северин В.А.* Теоретико-методологические основы обеспечения безопасности коммерческих структур в информационной сфере // Информационное право. 2016. N 4. С. 13 - 19.

третьими лицами желательно обговаривать, что информация будет передаваться и храниться с использованием защищенных каналов связи.

Проблема возникает для тех организаций, у которых нет возможности обслуживать частное облако. В таком случае представляется, что необходимо максимально использовать возможности правовых, организационных, инженерных и воспитательных мер, о которых речь пойдет ниже.

**Установление политики информационной безопасности**

В. А. Северин разделяет данные меры на четыре основные группы: правовые, организационные, инженерно-технические и воспитательные. [121] Под правовыми мерами можно понимать необходимость принятия специального локального нормативного акта, чаще всего называющийся «Политика информационной безопасности», в котором должны подробно расписываться три других группы мер, направленных на обеспечение безопасности и конфиденциальности данных, а также механизмы контроля за их соблюдением и ответственность за нарушение данных мер. Также к правовым мерам можно отнести и необходимость включения в трудовые договоры специальных обязанностей по обеспечению информационной безопасности.

В организационных мерах выделяется установление ряда ограничений по использованию Интернет-сервисов, таких как, почты, мессенджеров, социальных сетей и общедоступных публичных облачных хранилищ.

Одним из самых распространенных способов утечки информации является использование почтовых сервисов.[122] Так, например, Конституционный суд признал, что отправление конфиденциальной информации с корпоративной почты на личную является нарушением, так как создает «условия для ее

[121] *Северин В.А*. Концептуальные аспекты безопасности информации при производстве и реализации товаров // Безопасность бизнеса. 2017. N 1. С. 30 - 35.
[122] *Слесарев С*. Коммерческая тайна и контроль за работником// Трудовое право. 2017. N 9.

дальнейшего неконтролируемого распространения», несмотря на то, что сам публичный почтовый сервис (Mail.ru, являющийся SaaS) не становится обладателем пересланной информации.[123] Более того, суды признают, что мотивы подобной отправки информации не является существенными, и даже просьба контрагента не может освободить лица, совершившего несанкционированную операцию, от ответственности.[124] Этот вывод также поддерживается многочисленно судебной практикой.[125]

Также важным механизмом обеспечения информационной безопасности является запрет доступа к соцсетям на рабочем месте. Так, И., разместившим фотографии с рабочего места в соцсети, у работодателя в локальном нормативном акте (ЛНА), в частности в Правилах внутреннего трудового распорядка, был закреплен запрет на несанкционированное фотографирование на рабочем месте, а также установлен особый режим работы с информацией, регламентирован порядок работы с документами, попавшими в руки работнику. И суд, принимая решение, активно ссылался на соответствующие положения ЛНА, с которыми работник был ознакомлен и которые обязан был соблюдать.[126] Также важно уточнить, что социальными сетями нельзя пользоваться не только на рабочем месте, но и вне его с использованием служебной техники (рабочие компьютеры, телефоны, планшеты).

---

[123] Постановление Конституционного Суда РФ от 26.10.2017 N 25-П «По делу о проверке конституционности пункта 5 статьи 2 Федерального закона «Об информации, информационных технологиях и о защите информации« в связи с жалобой гражданина А.И. Сушкова»// СЗ. 2017. № 45. Ст. 6735.

[124] Апелляционное определение Московского городского суда от 08.02.2017 по делу N 33-1393/2017 // СПС Консультант (дата обращения: 23.03.2018); Апелляционное определение Московского городского суда от 04.08.2015 по делу N 33-24617/15 // СПС Консультант (дата обращения: 12.03.2018); Определение Московского городского суда от 20.10.2014 N 4г/9-9007/2014 // СПС Консультант (дата обращения: 23.12.2017); Апелляционное определение Свердловского областного суда от 24.04.2015 по делу N 33-5570/2015 // СПС Консультант (дата обращения: 20.03.2018).

[125] Апелляционное определение Московского городского суда от 08.02.2017 по делу N 33-1393/2017// СПС Консультант (дата обращения: 25.03.2018); Апелляционное определение Московского городского суда от 04.08.2015 по делу N 33-24617/15 // СПС Консультант (дата обращения: 22.02.2018); Определение Московского городского суда от 20.10.2014 N 4г/9-9007/2014 // СПС Консультант (дата обращения: 12.02.2018); Апелляционное определение Свердловского областного суда от 24.04.2015 по делу N 33-5570/2015 // СПС Консультант (дата обращения 12.02.2018).

[126] Определение Самарского областного суда от 29.06.2011 по делу N 33-6586/2011 // URL: http://daywork.ru/fas2/44257B06005C4ACF44257B020011B658.html (дата обращения: 12.04.2018).

Работник должен использовать оборудование работодателя только для исполнения трудовой функции, поэтому работодатель вправе регламентировать, какие виды работы (деятельности) сотрудник может осуществлять на оборудовании, например ПК или ином устройстве. В частности, запрет на компьютерные игры и прочие развлекательные программы законен. Даже если работник по какой-то причине свободен от работы (например, «окно» в обслуживании), он не вправе использовать рабочее время в непроизводственных целях.[127]

К организационным мерам стоит также отнести установление правил поведения работников, с целью противодействия разглашения конфиденциальной информации. Такими правилами могут быть ограничение на использование имени клиента или ключевых слов по проекту в одном или ряде сообщений, чтобы исключить возможность так называемого, correspondence trail. С той же целью следует использовать кодовые слова для различных проектов, воздерживаться от упоминания излишней информации в переписке. Не стоит забывать и правила, касающиеся публичных облачных хранилищах, о которых упоминалось ранее.

Для контроля за соблюдением запрета, а также активностью пользователя работодатель может использовать различные методы контроля - от визуального (в т.ч. видеонаблюдение) до специального программного обеспечения, которое отслеживает трафик, использование ресурсов компьютера (в т.ч. копирование и изменение файлов). Суды при этом принимают в качестве доказательств акты осмотров компьютера и браузера Интернета или электронной почты со скриншотами, сведения (распечатки) протоколов (отчетов) специальных программ отслеживания активности пользователя или контроля за сетью, служебные записки и т.п.[128]

---

[127] Апелляционное определение Тульского областного суда от 26.05.2016 по делу N 33-1715/2016 // СПС Консультант (дата обращения: 13.02.2018); Кассационное определение Ростовского областного суда от 30.08.2010 по делу N 33-9782 // СПС Консультант (дата обращения: 22.03.2018).

[128] Апелляционное определение Рязанского областного суда от 11.02.2015 N 33-335// СПС Консультант (дата обращения: 12.03.2018); Апелляционное определение Свердловского областного суда от 12.07.2016 по делу

При описании инженерно-технических мер, необходимых для обеспечения физической безопасности, представляется целесообразным вновь обратиться с классификации В.А. Северина, который разделяет данные меры на три группы.[129] В первую группу входит оборудование техническими средствами мест разработки и обращения изделий и документов (такие как экранизация помещений, безэховые камеры и т.д.). Во второй группе техническое обеспечение защиты помещений, в которых проводятся конфиденциальных работ или хранятся документы (сигнализация, блокировка и т.д.). И в третьей группе находятся меры по оснащению средствами охраны периметра режимных территорий организаций (пропускная и контрольная системы).

Представляется, что к инженерно-техническим мерам также стоит отнести один из самых важных инструментов для обеспечения безопасности данных - шифрование. В условиях использования облачных технологий оно становится еще более важным, помогая сохранить конфиденциальность информации даже при получении третьих лиц доступа к ней. Уместным здесь является применением по аналогии классификации уровней коммерческой тайны. Чем важнее и секретнее информация, тем уровень шифрования должен быть выше.

Еще одна не менее важная мера - создание резервных копий данных, которые должны храниться на одном или нескольких защищенных серверах. Это поможет избежать утери данных, снизит вероятность приостановления деятельности в случае сбоев в работе основного сервера, а также позволит минимизировать риски прерывания деятельности при попытках конкурентов

---

N 33-12012/2016 // СПС Консультант (дата обращения: 10.03.2018); Апелляционное определение Московского городского суда от 16.06.2016 по делу N 33-23105/2016 // СПС Консультант (дата обращения: 12.02.2018); Апелляционное определение Московского городского суда от 08.09.2014 по делу N 33-18661/2014 // СПС Консультант (дата обращения: 13.02.2018).

[129] *Северин В.А.* Концептуальные аспекты безопасности информации при производстве и реализации товаров // Безопасность бизнеса. 2017. N 1. С. 30 - 35.

помешать работе организации, в том числе через дезорганизацию системы коммуникаций.

В инженерно-технические нормы рекомендуется также включить целую серию мероприятий по защите от кибератак. Здесь главную роль играют IT-работники организации, задача которых установить наиболее эффективные и оптимальные средства защиты на технических устройствах в компании и обеспечить их непрерывную и качественную работу. Более того, обычно именно на этих работниках лежит обязанность рассказать, показать и проследить за исполнением всех вышеперечисленных требований, связанных с информационной безопасностью. Поэтому руководителю организации следует очень ответственно подходить к кадровой политике в этой области.

Главной мерой по защите от кибератак является установка антивирусной защиты и поддержание ее в рабочем состоянии, в обновленной версии. Следует также выбрать надлежащую защиту, отвечающую всем требованиям локальных нормативных актов. При технической, финансовой и организационной возможности, желательным является создание собственной системы корпоративных информационных ресурсов: например, создание корпоративного Интернет-шлюза для рабочих устройств для защищенного и быстрого доступа к Интернету или использование VPN (Virtual Private Network) при подключении к Интернету вне рабочего места с внешнего устройства (ноутбук, планшет, телефон).

Немаловажным аспектом обеспечения безопасности является принятие воспитательных мер, необходимых для просвещения работников о способах и мерах противодействия утечки информации, а также для выработки «информационного правосознания», призванного обеспечить ответственное отношение к соблюдению правил информационной безопасности. С этой целью предлагается проводить регулярные тренинги, курсы по повышению квалификации и компьютерной грамотности, а также целесообразно обращение особого внимания на важность сохранения конфиденциальности

информации в локальных нормативных актах, при реализации политики компании. Ключевым элементом данных мер является регулярность их проведения, чтобы не утрачивалось осознание важности соблюдения соответствующих правил.

## Заключение

В настоящей работе проанализированы различные аспекты регулирования и защиты информации, возникающие при использовании облачных технологий. В связи с широкой распространенностью использования облаков, как обычными гражданами (в основном, в форме социальных сетей и почтовых сервисов), так и предпринимателями и юридическими лицами (в самых различных формах), необходимость разрешения проблем, связанных с безопасностью и конфиденциальностью данных, стоит очень остро.

В рамках проведенного исследования проанализированы существующие определения облачных технологий, как в законодательстве, так и в доктринальных разработках российских и зарубежных ученых, также выделены основные формы, виды облачных услуг, которые влияют на особенности условий заключаемых договоров. Осуществлен анализ существующего законодательного регулирования облачных технологий, как в России, так и за рубежом, совместно с сформировавшимися на практике договорными формами оформления отношений между пользователем и провайдером.

Также детально разобраны основные риски и особенности, связанные с использованием «облаков», на основе классификации, предложенной рабочей группой ЮНСИТРАЛ, с учетом выработавшейся российской и иностранной практики. В прямой связи с выявленными рисками разработан целый ряд мер, направленных на минимизацию их последствий, в целях повышения привлекательности использования облачных технологий и устранения высказываемых опасений пользователей. Для систематизации данных мер предложена их классификация на двусторонние и односторонние меры, с превалированием последних в обеспечении безопасности информации. В первую группу включаются меры по договорному регулированию, то есть предложены механизмы, рекомендованные к

включению в договор между провайдером и пользователем. Особое внимание уделено механизму распределения ответственности между провайдером и пользователем в условиях дифференциированности услуг по предоставлению облачных технологий. Во вторую группу предложено отнести два блока мер: установление режима коммерческой тайны для особо важной информации и проведение грамотной политики информационной безопасности (которая в свою очередь включает правовые, организационные, инженерно-технические и воспитательные меры).

В результате настоящего исследования была предпринята попытка выявить главные риски, свойственные институту облачных технологий, в связи с технологическими особенностями реализации облачного сервиса, а также определить основные доступные способы снижения влияния данных рисков на безопасность и конфиденциальность информации.

Представляется, что использование «облаков» является неизбежной реальностью современного мира, и в будущем сфера распространения данного института будет только расширяться. И на сегодняшний день, учитывая широкую распространенность применения облачных технологий, необходимо признать, что существующее на сегодняшний день нормативное регулирование представляется не адекватным в сравнении с потребностями рынка и распространением института, а правоприменительная практика зачастую отражает непонимание технологических тонкостей облачных технологий. Жертвами этих явлений являются пользователи, которые вынуждены прибегать к более ресурсозатратным, неэффективным и устаревшим способам обработки и передачи информации в попытке обеспечить ее защиту.

Более того, при анализе мер по защите информации в облачных серверах выявлено, что хотя способы минимизации рисков общеизвестны и относительно просты, их реализация представляет собой отдельную сложность в виду ряда факторов, в том числе, неэффективной организации

работы на производстве, непонимания работником значения требуемых правил, а также не реалистичности предъявляемых требований.

В связи с этим, можно констатировать, что на данный момент проблема регулирования и защиты информации при использовании облачных технологий нуждается в дальнейшей разработке и совершенствовании.

**Список использованной литературы**


**I. Федеральное законодательство**

1. Гражданский кодекс Российской Федерации от 30.11.1994 N 51-ФЗ (ред. от 29.12.2017) // СЗ РФ. 1994. N 32. Ст. 3301.
2. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ (ред. от 03.04.2018)// СЗ РФ. 2002. N 1. Ст. 1.
3. Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (ред. от 05.02.2018)// СЗ РФ. 2002. N 1. Ст. 3.
4. Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 19.02.2018, с изм. от 25.04.2018) // СЗ РФ. 1996. N 25. Ст. 2954.
5. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 29.07.2017) «О персональных данных»// СЗ РФ. N 31. Ст. 3451.
6. Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 18.04.2018) «О коммерческой тайне»// СЗ РФ. 2004. N 32. Ст. 3283.

**II. Подзаконные нормативные акты**

1. Законопроект «О внесении изменений в ФЗ «Об информации, информационных технологиях и о защите информации» и в ФЗ «Об организации предоставления государственных и муниципальных услуг»»// СПС Консультант (дата обращения: 13.04.2018)
2. Законопроект «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации», Федеральный закон «Об организации предоставления государственных и муниципальных услуг» и Федеральный закон «Об электронной подписи»// URL: http://d-russia.ru/wp-content/uploads/2016/11/edinaya_infrastruktura_proekt_16112016.pdf (дата обращения: 14.04.2018)
3. Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. N 996 "Об утверждении требований и методов

по обезличиванию персональных данных, утв. Приказом Роскомнадзором от 13.12.2013// СПС Консультант

4. Перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных, утв. Приказом Роскомнадзора от 15.03.2013 N 274 (ред. от 15.06.2017)// Российская Газета. N 92. 26.04.2013.
5. Письмо Минобрнауки России от 15.02.2012 N АП-147/07 «О методических рекомендациях по внедрению систем ведения журналов успеваемости в электронном виде»// Администратор образования. N 14. 2012; Приказ Минобрнауки России от 15.06.2016 N 715 «Об утверждении Концепции развития школьных информационно-библиотечных центров»// СПС Консультант
6. Приказ Минфина России от 07.07.2014 N 208 "О Концепции обеспечения безопасности информации в информационных системах Министерства финансов Российской Федерации»// СПС Консультант; "Основные направления развития финансового рынка Российской Федерации на период 2016 - 2018 годов» (одобрено Советом директоров Банка России 26.05.2016)// Вестник Банка России. N 57. 17.06.2016.
7. Приказ Минюста России от 23.10.2017 N 208 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных Министерства юстиции Российской Федерации, эксплуатируемых при осуществлении Министерством юстиции Российской Федерации и его территориальными органами функций, определенных Указом Президента Российской Федерации от 13.10.2004 N 1313 «Вопросы Министерства юстиции Российской

Федерации» // URL: http://www.pravo.gov.ru (дата обращения: 12.04.2018)

8. Приказ Росздравнадзора от 20.09.2017 N 8134 «О переходе Федеральной службы по надзору в сфере здравоохранения на использование отечественного офисного программного обеспечения»; Распоряжение Правительства РФ от 29.12.2014 N 2769-р «Об утверждении Концепции региональной информатизации»// СЗ РФ. N 2. 2015. Ст. 544.
9. Приказ ФТС России от 21.10.2015 N 2133 «Об утверждении основных направлений развития информационно-коммуникационных технологий в таможенных органах Российской Федерации до 2030 года»// Таможенные ведомости. N 1. 2016.
10. Распоряжение Правительства РФ от 01.11.2013 №2036-р «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года»// СЗ РФ. 2013. N 46. Ст. 5954.
11. Распоряжение Правительства РФ от 20.07.2013 №1268-р «Об утверждении плана мероприятий ("дорожной карты") "Развитие отрасли информационных технологий»// СЗ РФ. 2013. N 30. Ст. 4168;
12. Распоряжение Правительства РФ от 20.10.2010 N 1815-р (ред. от 26.12.2013) "О государственной программе Российской Федерации "Информационное общество (2011 - 2020 годы)»// СЗ РФ. N 46. 2010. Ст. 6026.
13. Распоряжение Правительства РФ от 25.12.2013 N 2516-р (ред. от 13.10.2017) «Об утверждении Концепции развития механизмов предоставления государственных и муниципальных услуг в электронном виде»// СЗ РФ. 13.01.2014. N 2 (часть II). Ст. 155; Распоряжение Правительства РФ от 29.12.2014 N 2769-р (ред. от 03.03.2017) «Об утверждении Концепции региональной информатизации»// СЗ РФ. N 2. 12.01.2015. Ст. 544.

14. Распоряжение Правительства РФ от 28.07.2017 N 1632-р «Об утверждении программы "Цифровая экономика Российской Федерации»// СЗ РФ. N 32. 2017. Ст. 5138.;
15. Рекомендации в области стандартизации Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Предотвращение утечек информации" РС БР ИББС-2.9-2016, утв. Приказом Банка России от 11.04.2016 N ОД-1205)// Вестник Банка России. N 41. 27.04.2016; Стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Управление риском нарушения информационной безопасности при аутсорсинге" СТО БР ИББС-1.4-2018, утв. Приказом Банка России от 06.03.2018 N ОД-568)// Вестник Банка России. N 27. 30.03.2018.
16. Указа Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»// СЗ РФ. 2017. N 20. Ст. 2901.
17. Федеральная целевая программа «Развитие судебной системы России на 2013 - 2020 годы», утв. распоряжением Правительства РФ от 20.09.2012 N 1735-р// СЗ РФ. N 40. 2012. Ст. 5474.

**III. Правоприменительная практика**

1. Апелляционное определение Московского городского суда от 04.08.2015 по делу N 33-24617/15 // СПС Консультант (дата обращения: 12.03.2018)
2. Апелляционное определение Московского городского суда от 08.02.2017 по делу N 33-1393/2017 // СПС Консультант (дата обращения: 23.03.2018)
3. Апелляционное определение Московского городского суда от 08.09.2014 по делу N 33-18661/2014 // СПС Консультант (дата обращения: 13.02.2018).

4. Апелляционное определение Московского городского суда от 16.06.2016 по делу N 33-23105/2016 // СПС Консультант (дата обращения: 12.02.2018);
5. Апелляционное определение Рязанского областного суда от 11.02.2015 N 33-335// СПС Консультант (дата обращения: 12.03.2018);
6. Апелляционное определение Санкт-Петербургского городского суда от 27.09.2016 N 33-17808/2016 // СПС Консультант (дата обращения: 12.02.2018).
7. Апелляционное определение Свердловского областного суда от 12.07.2016 по делу N 33-12012/2016 // СПС Консультант (дата обращения: 10.03.2018);
8. Апелляционное определение Свердловского областного суда от 24.04.2015 по делу N 33-5570/2015 // СПС Консультант (дата обращения 12.02.2018).
9. Апелляционное определение Тульского областного суда от 26.05.2016 по делу N 33-1715/2016 // СПС Консультант (дата обращения: 13.02.2018);
10. Доклад рабочей группы IV (Электронная торговля) о работе ее пятьдесят пятой сессии, Комиссия ООН по праву международной торговли, 50 сессия // URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/V17/029/30/PDF/V1702930.pdf?OpenElement (дата обращения: 13.04.2018)
11. Кассационное определение Ростовского областного суда от 30.08.2010 по делу N 33-9782 // СПС Консультант (дата обращения: 22.03.2018).
12. Определение Верховного Суда РФ от 30 сентября 2015 г. N 305-КГ15-12154 // СПС Консультант (дата обращения: 24.03.2018).
13. Определение Московского городского суда от 20.10.2014 N 4г/9-9007/2014 // СПС Консультант (дата обращения: 12.02.2018);

14. Определение Самарского областного суда от 29.06.2011 по делу N 33-6586/2011 // URL: http://daywork.ru/fas2/44257B06005C4ACF44257B020011B658.html (дата обращения: 12.04.2018).
15. Определение Суда по интеллектуальным правам от 17.04.2018 N С01-201/2018 по делу N А40-18827/2017 "Об отложении судебного заседания суда кассационной инстанции»// СПС Консультант (дата обращения: 25.04.2018).
16. Постановление Арбитражного суда Московского округа от 18 июня 2015 г. по делу N А40-91072/14 // URL: http://www.5451212.ru/sudebnaya-praktika-mosgorsuda/postanovlenie-arbitrazhnogo-suda-moskovskogo-okruga-ot-18-iyunya-2015-g-n-f05-7093-15-po-delu-n-a40-/ (дата обращения: 12.02.2018)
17. Постановление Двадцатого арбитражного апелляционного суда от 09.11.2016 по делу N А68-2206/2016 // СПС Консультант (дата обращения: 13.02.2018).
18. Постановление Девятого арбитражного апелляционного суда от 16 января 2015 г. N 09АП-55322/2014 по делу N А40-77325/14 // СПС Консультант (дата обращения: 12.03.2018)
19. Постановление Конституционного Суда РФ от 26.10.2017 N 25-П «По делу о проверке конституционности пункта 5 статьи 2 Федерального закона "Об информации, информационных технологиях и о защите информации" в связи с жалобой гражданина А.И. Сушкова»// СЗ. 2017. № 45. Ст. 6735.
20. Постановление Четвертого арбитражного апелляционного суда от 19 декабря 2014 г. N 04АП-4738/2014 по делу N А78-5032/2014// URL: http://pravosudie.biz/2076742 (дата обращения: 12.04.2018)
21. Предложение правительства Канады: возможная будущая работа в области электронной торговли – правовые вопросы, связанные с облачной обработкой компьютерных данных, материалы 47 сессии, 7-

8 июля 2014// URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/V14/041/32/PDF/V1404132.pdf?OpenElement (дата обращения: 04.04.2018)

22. Приложение к Записке Секретариата Комиссии ООН по праву международной торговли «Договорные аспекты облачной обработки компьютерных данных»// URL: http://undocs.org/ru/A/CN.9/WG.IV/WP.142 (дата обращения: 14.04.18)
23. Решение Арбитражного суда г. Москвы от 24 июля 2015 г. по делу N А40-85252/15 // http://sudact.ru/arbitral/doc/sLyGj5OVn9VN/ (дата обращения: 23.02.2018)
24. Решение Арбитражного суда г. Москвы от 12.10.2017 по делу N А40-18827/17 // СПС Консультант (дата обращения: 23.03.2018).
25. Решение Арбитражного суда Забайкальского края от 26 января 2015 г. по делу N А78-14182/2014 // URL: http://chita.arbitr.ru/chita/cases/cdoc?docnd=841355499&nd=841134332&prefix=&numdeal=&yeardeal=&fld_12=&fld_14=&fld_16=&fld_140=&pagedoc=1 (дата обращения: 12.03.2018)

**IV. Российская научная литература**

1. *Берестова В.И.* Перспективы использования облачных технологий в электронном документообороте //Делопроизводство. 2015. № 3.
2. *Глухов Н.И., Волошина П.С.* Исследование законодательства Российской Федерации в сфере облачных технологий//Academy. N 6(21). 2017.
3. *Емельянников М.Ю.* «Облако в законе»: юридические аспекты использования облачных сервисов в России //URL: http://embeddedday.ru/2016/presentations/.pdf (дата обращения: 24.04.2018)
4. *Ильин И.В., Ильяшенко О.Ю., Борреманс А.Д.* Подход к интеграции облачных технологий типа SaaS при реализации ИТ-проектов// Перспективы науки. N 12 (87). 2016. С.112.

5. Интернет-интервью с И.А. Близнецом, ректором Российской государственной академии интеллектуальной собственности: "Реализация государственной политики в области интеллектуальной собственности" // URL: http://www.consultant.ru/law/interview/bliznets2/ (дата обращения: 15.03.2018).
6. Комментарий к Гражданскому кодексу РСФСР / Отв. ред. С.Н. Братусь, О.Н. Садиков. 3-е изд., испр. и доп. М.: Юрид. лит., 1982 (комментарий к ст. 275);
7. Комментарий к Федеральному закону от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»//Савельев А.И. М: Статут. 2015. С. 111.
8. *Кучина Я.О.* Облачные технологии: понятие и основы правового регулирования // Азиатско-Тихоокеанский регион: экономика, политика, право. 2016. № 4.
9. *Меликов У.А*. Гражданско-правовые проблемы, связанные с сервером // Вестник ЮУрГУ. Серия: Право. 2016. №1. URL: https://cyberleninka.ru/article/n/grazhdansko-pravovye-problemy-svyazannye-s-serverom (дата обращения: 29.04.2018).
10. *Нестерова И.А*. Правовое регулирование отношений, возникающих при использовании облачных технологий/ Дис. канд. юрид. наук:12.00.03. М. 2016. С.56.
11. *Нестерова И.А.* Распространение произведений с использованием облачных технологий//Авторское право и смежные права. 2016. №9.
12. *Левковская Н.И.* Гражданско-правовая ответственность вычислительных центров в договорных обязательствах по обработке информации и проектированию АСУ: Автореф. дис. ... канд. юрид. наук. М., 1986. С. 3 ("Договор "на продажу машинного времени" - договор найма с предоставлением услуг»).

13. Организационно-правовое обеспечение информационной безопасности: монография / Морозов А.В., Полякова Т.А. М.: РПА Минюста России. 2013. С.244.
14. *Паус А.С., Целовальникова О.А*. Тенденции развития облачных технологий на российском рынке // Новые информационные технологии в автоматизированных системах. 2014. №17.
15. Предпринимательская деятельность в сети Интернет: Монография/ Демьянец М.В., Елин В.М., Жарова А.К. М: Юркомпани. 2014. С.76.
16. Подход к интеграции облачных технологий типа SaaS при реализации ИТ-проектов, И.В. Ильин, О.Ю. Ильяшенко, А.Д. Борреманс// Перспективы науки. N 12 (87). 2016. С.112.
17. *Полякова Т.А., Химченко А.И.* Актуальные организационно-правовые вопросы трансграничной передачи персональных данных // Право. Журнал Высшей школы экономики. 2013. №1. URL: https://cyberleninka.ru/article/n/aktualnye-organizatsionno-pravovye-voprosy-transgranichnoy-peredachi-personalnyh-dannyh (дата обращения: 29.04.2018)
18. *Разуваев В*. Софт как услуга // ЭЖ-Юрист. 2010. N 5
19. *Савельев А.И.* Научно-практический постатейный комментарий к Федеральному закону "О персональных данных" // М.: Статут, 2017. 320 с.
20. *Савельев А.И.* Правовая природа "облачных" сервисов: свобода договора, авторское право и высокие технологии//Вестник гражданского права. 2015. N 5.
21. *Северин В.А*. Концептуальные аспекты безопасности информации при производстве и реализации товаров // Безопасность бизнеса. 2017. N 1. С. 30 - 35.

22. *Северин В.А*. Теоретико-методологические основы обеспечения безопасности коммерческих структур в информационной сфере // Информационное право. 2016. N 4. С. 13 - 19.
23. *Слесарев С*. Коммерческая тайна и контроль за работником// Трудовое право. 2017. N 9.
24. *Терещенко Л.К*. Понятийный аппарат информационного и телекоммуникационного права: проблемы правоприменения//Журнал российского права. 2016. №10;
25. *Тян В*. Облачные технологии: вызовы правового регулирования// URL: https://kapital.kz/gosudarstvo/55665/oblachnye-tehnologii-vyzovy-pravovogo-regulirovaniya.html (дата обращения: 25.03.2018)
26. *Царегородцев А.В., Савельев И.А., Романовский С.В.* Обеспечение безопасности данных в облаченных сферах // Экономика. Налоги. Право. 2013. №4
27. *Шакель Н.В*. Юридические аспекты использования облачных технологий// URL: http://www.evolutio.info/content/view/2307/235/ (дата обращения: 23.03.2018).

## V. Зарубежная научная литература

1. *Bandulet F., Faisst W., Eggs H., Otyepka S., Wenzel S*. Software-as-a-Service as Disruptive Innovation in the Enterprise Application Market // Software-as-a-Service: Anbieterstrategien, Kundenbedürfnisse und Wertschöpfungsstrukturen/ A. Benlian, Th. Hess, P. Buxmann (Hgs.). Gabler Verlag, 2010. S. 17.
2. *Christopher J. Millard*. Cloud Computing Law// URL: https://global.oup.com/ (дата обращения: 09.12.2017)
3. Feist Publications, Inc. v. Rural Telephone Service Co. 499 U.S. 340 (1991) // URL: https://supreme.justia.com/cases/federal/us/499/340/case.html (дата обращения: 23.03.2018).

4. *Godes S., Cleary K., Fessler H*. The Cloud: Selected Benefits, Risks, and Insurance Coverage Issues/ URL: https://www.lexology.com/library/ (дата обращения: 09.12.2017).
5. *Goodwin Andrew*. Practice Pointers: Risk Allocation in Enterprise Cloud Service Agreements // URL: https://www.dataprivacymonitor.com/cloud-computing/five-practice-pointers-risk-allocation-in-enterprise-cloud-service-agreements/ (дата обращения: 23.03.2018).
6. *Guth S*. Contract Negotiation Handbook: Software as a Service // Guth Ventures, 2013. P. 20 - 21.
7. Insurance for Cyber-related critical infrastructure loss // URL: https://www.dhs.gov/cybersecurity-insurance (дата обращения: 09.12.2017).
8. *Kundra V*. Federal Cloud Computing Strategy/ URL: https://www.dhs.gov/ (дата обращения: 09.12.2017).
9. *Melanson R*. Sales Taxes and the Shadow of Cloud Computing: Searching the Horizon for a Workable, National Solution // Tax Lawyer. 2012. Vol. 65. No. 4. P. 874, 880.
10. *Mell P., Grance T*. The NIST Definition of Cloud Computing// URL: http://nvlpubs.nist.gov/ (дата обращения: 09.12.2017).
11. *O'Connel N*. Regulation of Cloud Computing in Saudi Arabia// URL: http://www.tamimi.com/ (дата обращения: 10.12.2017).
12. *Tom Steinert-Threlkeld*. Cloud Fundamental to NYSE IT Strategy // URL: http://www.information-management.com/news/cloud-fundamental-to-nyse-it-strategy-10023088-1.html?zkPrintable=true (дата обращения: 12.12.2017).
13. Tribunal de grande instance de Nanterre Ordonnance de 30 novembre 2012 // URL: http://www.legans.net/spip.php?page=jurisprudence-decision&id_article=3794 (дата обращения: 13.04.2018)

14. *Walia H., Chandan A.* Cloud Services: Recent Developments And Anticipated Laws// URL: http://www.mondaq.com/india/ (дата обращения: 10.12.2017).

**VI. Электронные ресурсы**

1. Apple усилит безопасность iCloud // Интернет-газета «Вести». 2014. URL: http://hitech.vesti.ru/news/view/id/5556 (дата обращения: 23.03.2018).
2. Cyber Insurance: A look at recent advances, good practices and challenges by ENISA// URL: https://www.enisa.europa.eu/news/enisa-news/cyber-insurance-a-look-at-recent-advances-good-practices-and-challenges-by-enisa (дата обращения: 09.12.2017).
3. Dropbox Terms of Service // URL: https://www.dropbox.com/terms (дата обращения: 23.04.2018).
4. Data Privacy Radar: How the German C5 affects us all // URL: https://blog.box.com/blog/data-privacy-radar-how-german-c5-affects-us-all/ (дата обращения: 12.04.2018)
5. Google Apps (Free) Agreement // URL: http://www.google.com/apps/intl/en/terms/standard_terms.html (дата обращения: 23.03.2018)
6. http://www.tadviser.ru/index (дата обращения: 09.12.2017).
7. ICO, Deleting Personal Data// URL: https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf (дата обращения: 20.04.2018)
8. ISO/IEC 19086-1:2016 // URL: https://www.iso.org/standard/67545.html?browse=tc (Дата обращения: 20.04.2018)
9. Saudi Arabia: new Cloud Computing Regulatory Framework // URL: https://www.jdsupra.com/legalnews/saudi-arabia-new-cloud-computing-10730/ (дата обращения: 12.03.2018)

10. URL: http://www.consultant.ru/law/hotdocs/33631.html/ (дата обращения: 13.04.2018)
11. URL: http://www.onlinetech.com/resources/references/what-is-a-soc-2-report-an-easy-explanation (дата обращения: 20.04.2018)
12. URL: http://www.tadviser.ru/index (дата обращения: 09.12.2017).
13. URL: http://www.tadviser.ru/index (дата обращения: 09.12.2017).
14. URL: https://de.statista.com/themen/ (дата обращения: 09.12.2017).
15. URL: www.techmarketview.com/news/archive/ (дата обращения: 09.12.2017).
16. URL: https://www.canada.ca/en/shared-services/news/2018/02/cloud_computing.html (дата обращения: 12.04.2018).
17. Журавлева А. Колосс на облачных ногах // URL: http://expert.ru/ (дата обращения: 09.12.2017).
18. Как «ВКонтакте» разрешила анализировать данные пользователей // URL: https://www.rbc.ru/technology_and_media/02/04/2018/5abe534d9a7947350e3a7dfa (дата обращения: 23.04.2018).
19. О защите персональных данных на российском и европейских рынках// URL: https://habrahabr.ru/company/it-grad/blog/332396/ (дата обращения: 19.01.2018)