ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
КОНСАЛТИНГОВОЕ АГЕНТСТВО «ЕМЕЛЬЯННИКОВ, ПОПОВА И ПАРТНЕРЫ»

КОНСАЛТИНГОВОЕ АГЕНТСТВО
Емельянников, Попова и партнеры

Экспертное заключение по вопросам, связанным с использованием облачной платформы Azure и иных облачных сервисов корпорации Microsoft российскими компаниями и требованиями законодательства РФ, которые необходимо выполнить при их использовании

наименование документа

Москва
Январь 2020 года

Оглавление

1. Предмет Экспертного заключения

В связи с недавними существенными изменениями в российском регулировании порядка обработки персональных данных, Общество с ограниченной ответственностью Консалтинговое агентство «Емельянников, Попова и партнеры» (далее – **Исполнитель**) подготовило обновленную версию экспертного заключения по вопросам, связанным с использованием облачной платформы Microsoft Azure и иных облачных сервисов корпорации Microsoft российскими компаниями и требованиями законодательства РФ, которые необходимо выполнить при их использовании (далее – **Экспертное заключение**). В Экспертном заключении разъяснены, включая обоснование и ссылки на законодательные и иные нормативные правовые акты Российской Федерации, официально изложенную позицию уполномоченных федеральных органов исполнительной власти (далее – **законодательство РФ**), следующие вопросы:

1. Определение персональных данных, примеры, когда данные являются и не являются персональными.
2. Что понимается в законодательстве РФ под базой персональных данных.
3. Сценарии использования облачной платформы Microsoft Azure и иных облачных сервисов корпорации Microsoft, соответствующие требованиям Закона о персональных данных.
4. Размещение на облачных платформах и в облачных сервисах данных, прошедших процедуру обезличивания.
5. Возможно ли использование российским оператором сервисов электронной почты, интернет-телефонии, передачи видеоконтента, предоставляемых облачным сервисом Microsoft Office 365.
6. Допускает ли законодательство РФ создание новых сведений о субъекте в зарубежной информационной системе персональных данных.
7. Ограничения, накладываемые на использования облачной платформы Microsoft Azure и иных облачных сервисов Законом о персональных данных.
8. Ответственность за нарушения требований законодательства о локализации персональных данных в период их сбора.
9. Как обеспечивается безопасность персональных данных, обрабатываемых в облачной платформе Microsoft Azure и облачных сервисах.

2. Используемые термины и определения

актуализация персональных данных – изменение, уточнение, обновление персональных данных;

база персональных данных – упорядоченный массив персональных данных, независимый от вида материального носителя информации и используемых средств его обработки (архивы, картотеки, электронные базы данных);

дата-центр – специализированная организация, предоставляющая услуги по размещению серверного и сетевого оборудования, сдаче серверов (в том числе виртуальных) в аренду, а также по подключению к сети Интернет;

доступ к персональным данным – ознакомление определенных лиц с персональными данными субъектов при условии сохранения конфиденциальности этих сведений;

конфиденциальность персональных данных – обязанность лиц, получивших доступ к персональным данным, не раскрывать их третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством РФ;

Минкомсвязь России – Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, в соответствии с Положением о ведомстве, утвержденным Постановлением Правительства РФ от 02.06.2008 № 418, являющееся органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере персональных данных;

обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

облачная платформа – вычислительная инфраструктура, обеспечивающая повсеместный и удобный сетевой доступ «по требованию» к общему пулу конфигурируемых вычислительных ресурсов (например, системам передачи данных, серверам, устройствам хранения данных, приложениям и сервисам — как вместе, так и по отдельности), которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами или обращениями к провайдеру, обладающих 5 основными свойствами:

- самообслуживание по требованию;
- универсальный доступ по сети;
- объединение ресурсов;
- эластичность;
- учёт потребления.

облачное решение – информационная система, размещенная на облачной платформе;

облачный сервис – программное обеспечение, распространяемое по модели SaaS (ПО как услуга) с использованием облачной платформы и доступное широкому кругу заказчиков;

обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение),

извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Роскомнадзор – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, на которую возложены функции уполномоченного органа по защите прав субъектов персональных данных;

сбор персональных данных – любые действия оператора или действующего по его поручению лица, приводящие к появлению у оператора (лица, действующего по его поручению) сведений о новом, ранее неизвестном субъекте персональных данных или новых сведений о ранее известном (идентифицированном) субъекте персональных данных, персональными данными которого оператор уже располагал;

субъект персональных данных – физическое лицо, к которому относятся персональные данные;

трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

3. Используемые при подготовке Экспертного заключения нормативные правовые акты и методические материалы

При подготовке Экспертного заключения Консультантом использовались нормативные правовые акты и методические материалы, указанные в Таблице 1.

Таблица 1

№	Наименование документа	Сокращение наименования, используемое в Экспертном заключении
1	Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»	Закон о персональных данных
2	Федеральный закон от 21.07.2014 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»	Закон 242-ФЗ
3	Федеральный закон от 02.12.2019 № 405-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»	
3	Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	Закон 149-ФЗ
4	Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ	ТК РФ
5	Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ	КоАП РФ
6	Постановление Правительства Российской Федерации от 13.02.2019 № 146 «Об утверждении Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных»	Правила контроля
7	Приказ Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»	Приказ № 996
8	Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»	

№	Наименование документа	Сокращение наименования, используемое в Экспертном заключении
9	Страница «Обработка и хранение персональных данных в РФ. Изменения с 1 сентября 2015 года» на официальном сайте Минкомсвязи России http://minsvyaz.ru/ru/personaldata/	
10	Комментарий Роскомнадзора к Федеральному закону от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» (https://pd.rkn.gov.ru/library/p195/)	Комментарий Роскомнадзора
11	Сайт ПД-ИНФО.рф / PD-info.ru	
12	Федеральный закон «О персональных данных»: научно-практический комментарий (под редакцией заместителя руководителя Роскомнадзора А.А. Приезжевой) (Библиотечка «Российской газеты», выпуск № 11, М., 2015)	Научно-практический комментарий к 152-ФЗ

4. Общий обзор изменений законодательства Российской Федерации о персональных данных, внесенных Федеральным законом от 21.07.2014 № 242-ФЗ

Федеральным законом от 21.07.2014 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» (далее – **Закон 242-ФЗ**) внесены следующие изменения в три федеральных закона:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – **Закон 149-ФЗ**):
    - дополняется новой статьей 15.5, определяющей порядок ограничения доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных;
    - часть 4 статьи 16 этого же закона, определяющая обязанности обладателя информации и оператора информационной системы в случаях, установленных законодательством Российской Федерации, дополняется пунктом 7 следующего содержания: «7) нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление,

изменение), извлечение персональных данных граждан Российской Федерации»;

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – **Закон о персональных данных**):
  - статья 18 дополняется частью 5 следующего содержания: «5. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 настоящего Федерального закона»;
  - часть 3 статьи 22, определяющей содержание уведомления об обработке персональных данных, дополняется пунктом 10.1 следующего содержания: «10.1) сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации»;
  - часть 3 статьи 23, определяющей права уполномоченного органа по защите прав субъектов персональных данных (Роскомнадзора), дополняется пунктом 3.1 следующего содержания: «3.1) ограничивать доступ к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, в порядке, установленном законодательством Российской Федерации»;
- Федеральный закон от 26.12.2008 № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» (далее – **Закон 294-ФЗ**):
  - часть 3.1 статьи 1, определяющая виды государственного контроля (надзора), при осуществлении которых не применяются положения данного Федерального закона, дополняется пунктами 19 и 20 следующего содержания:

    «19) контроль за соблюдением требований в связи с распространением информации в информационно-телекоммуникационной сети "Интернет";

    20) контроль и надзор за обработкой персональных данных».

Фактически указанные изменения означают следующее:

- вводится механизм блокировки доступа к сайтам в сети Интернет, принадлежащим лицам, признанным российским судом нарушителями законодательства о персональных данных, причем не имеет значение, связано ли нарушение с обработкой данных на конкретном сайте (в сети Интернет), или нет;
- вводится требование об обязательности обработки персональных данных российских граждан в период их сбора, а также при их актуализации, с использованием баз данных на территории Российской Федерации;

- порядок организации и проведения проверок за соблюдением законодательства, регламентирующего обработку персональных данных, выводится из-под регулирования Законом 294-ФЗ.

Наибольший интерес для вопросов, поставленных Клиентом, представляют поправки в Закон о персональных данных, касающиеся размещения баз персональных данных российских граждан в период их сбора на территории Российской Федерации.

Анализируя содержание введенной в закон части 5 статьи 18, необходимо отметить следующее:

- ограничения на размещение баз персональных данных вводятся только на период сбора персональных данных и не затрагивают их последующей обработки после завершения сбора, кроме ряда конкретных способов обработки;
- ограничения касаются только персональных данных граждан Российской Федерации и не касаются персональных данных граждан других государств и лиц без гражданства;
- ограничения вводятся только на 9 из 18 способов обработки, установленных частью 3 статьи 3 Закона о персональных данных» (сбор, запись, систематизация, накопление, хранение, уточнение, обновление, изменение, извлечение) и не требуют размещения баз данных на территории России для таких действий с персональными данными, как использование, передача, распространение, предоставление, доступ, обезличивание, блокирование, удаление, уничтожение после локализации данных на территории Российской Федерации.

Последний вывод означает, что после завершения сбора персональных данных они должны находиться (храниться) в базах данных на территории Российской Федерации, при этом изменения в данные (в том числе уточнения и обновления) должны вноситься также в базы на территории Российской Федерации. Базы данных на территории Российской Федерации всегда должны содержать все актуальные персональные данные, используемые оператором и полученные или актуализированные им в период времени, начиная с 1 сентября 2015 года.

Однако указанное требование не накладывает никаких ограничений на передачу персональных данных после их сбора и записи в базу данных на территории России, в том числе на трансграничную передачу, предоставление к персональным данным доступа с территории иных государств, а также на использование персональных данных граждан Российской Федерации после их трансграничной передачи, в том числе на использование данных из информационных систем, находящихся за пределами Российской Федерации.

Закон в редакции Закона 242-ФЗ не вводит запрет на обработку персональных данных в дата-центрах и облачных инфраструктурах, находящихся вне территории Российской Федерации, за исключением периода их сбора.

Анализ требований части 5 статьи 18 Закона о персональных данных и части 4 статьи 16 Закона 149-ФЗ в редакции Закона 242-ФЗ показывает, что в соответствии с данными требованиями с 1 сентября 2015 года российским операторам запрещено размещение персональных данных граждан Российской Федерации на серверах, расположенных за пределами Российской Федерации, без предварительного

размещения их в информационной системе (базе данных) на территории Российской Федерации, за исключением случаев, прямо предусмотренных в тексте закона (обработка персональных данных для достижения целей, предусмотренных международным договором или законом, для осуществления и выполнения возложенных законодательством РФ на оператора функций, полномочий и обязанностей; обработка персональных данных для осуществления правосудия, исполнения судебного акта; обработка персональных данных для исполнения полномочий и функций органов власти, государственных внебюджетных и фондов организаций, участвующих в предоставлении государственных и муниципальных услуг; обработка персональных данных для осуществления профессиональной деятельности журналиста и (или) СМИ, научной, литературной или иной творческой деятельности). Поэтому российский оператор не может использовать, например, веб-формы для непосредственного внесения персональных данных российских граждан в базу данных, находящуюся за рубежом, а также для изменения или уточнения в такой базе ранее внесенных в нее данных.

Таким образом, после 1 сентября 2015 года для использования при обработке персональных данных облачных сервисов, серверы которых расположены за пределами Российской Федерации, российскому оператору необходимо принимать дополнительные меры, в частности, базу персональных данных, предназначенную для их первичного сбора, записи и накопления, а также последующей актуализации (уточнения, обновления, изменения) разместить на территории Российской Федерации и постоянно хранить обрабатываемые персональные данные в такой базе.

5. Экспертное заключение

В Экспертном заключении будут последовательно рассмотрены вопросы, поставленные Заказчиком, и даны ответы на них.

5.1. Определение персональных данных, примеры, когда данные являются и не являются персональными.

Пункт 1 статьи 3 Закона о персональных данных определяет **персональные данные** как любую информацию, относящуюся к прямо или косвенно **определенному или определяемому физическому лицу** (субъекту персональных данных).

Данное определение является весьма неопределенным и допускает сколь угодно широкое его толкование. При таком определении к персональным данным могут быть отнесены практически любые сведения о физическом лице, независимо от того, возможна ли его однозначная идентификация (установление личности) с использованием указанных сведений или нет.

Такой подход к определению персональных данных представляется не вполне соответствующим положениям Конвенции о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года ETS № 108 (далее – Европейская конвенция), подписанной государствами-членами Совета Европы, стороной которой является и Российская Федерация. В Европейской конвенции персональным данным дается следующее определение: «any information

relating to an identified or identifiable individual». Замена терминов «идентифицированному или идентифицируемому» терминами «прямо или косвенно определенному или определяемому» выглядит необоснованной.

Это подтверждается и текстами переводов Европейской конвенции, размещенными на официальных сайтах Совета Европы (перевод Российской Федерации для подготовки к подписанию (https://www.coe.int/ru/web/conventions/full-list/-/conventions/rms/0900001680078c46): «любая информация об определенном или поддающемся определению физическом лице», и Роскомнадзора (http://pd.rkn.gov.ru/law/p131/document170.htm?print=1): «информация, касающаяся конкретного или могущего быть идентифицированным лица».

Таким образом, Европейская конвенция основным признаком персональных данных определяет возможность с их помощью точной идентификации конкретного физического лица.

Российский Закон о персональных данных к этой категории сведений относит любые данные о любом физическом лице вне зависимости от возможности его отождествления (идентификации). При этом набор сведений, составляющих персональные данные, может быть минимальным. Так, пункт 5 части 2 статьи 22 Закона о персональных данных допускает возможность обработки оператором персональных данных, включающих только фамилии, имена и отчества субъектов персональных данных. Очевидно, что само по себе словосочетание типа «Иванов Александр Петрович» не может быть соотнесено с конкретным субъектом персональных данных и не позволяет идентифицировать конкретного человека.

Тем не менее, оценивая правоприменение в России законодательства о персональных данных, необходимо исходить именно из такой, расширительной трактовки термина в российском законе.

Поскольку Закон о персональных данных и принятые в его исполнение нормативные правовые акты не определяют конкретный состав сведений, относящихся к персональным данным, для оценки того, являются ли конкретные сведения, в частности, номер телефона и адрес электронной почты, персональными данными, следует исходить из сложившейся практики правоприменения закона.

Следует учитывать позицию надзорного органа по данному вопросу. В подготовленном Роскомнадзором комментарии к Закону о персональных данных [1] (далее – **Научно-практический комментарий к 152-ФЗ**) указывается, что «при буквальном толковании (применяемом в правоприменительной практике «по умолчанию») рассматриваемой нормы [закона «О персональных данных»] к понятию «персональные данные» можно отнести широкий круг информации, в том числе выходящий за рамки разумно ожидаемого в данном контексте. В частности, в нем нет указания на связь между информацией и прямой или косвенной определенностью или «определяемостью» физического лица. Соответственно, отсутствует однозначное понимание того, в каких случаях собираемые и обрабатываемые данные будут относиться к персональным, а в каких – нет».

Члены специальной рабочей группы, созданной Роскомнадзором для решения

[1] Федеральный закон «О персональных данных»: научно-практический комментарий. Под редакцией заместителя руководителя Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций А.А. Приезжевой. — М.: Редакция «Российской газеты», 2015. Вып. 11.

вопроса об отнесении тех или иных сведений к персональным данным, пришли к общему выводу, что, если совокупность данных необходима и достаточна для идентификации лица, такие данные следует считать персональными данными, даже если они не включают в себя данные документов, удостоверяющих личность. При этом данные нельзя считать персональными в том случае, если без использования дополнительной информации они не позволяют идентифицировать физическое лицо.

В Научно-практическом комментарии к 152-ФЗ сделан вывод, что следующие данные можно рассматривать как персональные несмотря на то, что в их отношении остается некоторый аспект вероятного совпадения:

- фамилия, имя, отчество, дата рождения, место прописки;
- фамилия, имя, отчество, дата рождения, должность;
- фамилия, имя, отчество (возможно, фамилия и инициалы) плюс любая информация, выделяющая субъекта из уже ограниченного круга лиц.

Авторы издания приходят к выводу, что «если совокупность данных необходима и достаточна для идентификации лица, такие данные следует считать персональными данными, даже если они не включают в себя данные документов, удостоверяющих личность. При этом данные нельзя считать персональными в том случае, если без использования дополнительной информации они не позволяют идентифицировать физическое лицо. Изложенный подход допустимо рассматривать как учитывающий баланс интересов всех участников отношений» (стр.15). Таким образом, например, обезличенные данные, не соотносимые с конкретным субъектом, не могут рассматриваться как персональные и в отношении них не должны применяться нормы части 5 статьи 18 Закона о персональных данных, требующие локализации персональных данных граждан Российской Федерации в период их сбора в базах данных на территории Российской Федерации. Сами же персональные данные, содержащие фамилию, имя, отчество и другие идентифицирующие личность признаки, безусловно, должны размещаться при их сборе в базах данных на территории России.

Далее, в Научно-практическом комментарии к 152-ФЗ указывается (стр.17), что данные нельзя считать персональными в том случае, если без использования дополнительной информации они не позволяют идентифицировать физическое лицо. К числу данных, которые не могут рассматриваться, по крайней мере, по отдельности друг от друга в качестве персональных, могут быть отнесены: фамилия, имя, отчество, адрес проживания, электронный адрес, номер телефона, дата рождения. Другие идентификаторы сами по себе не определяют однозначно конкретное физическое лицо. Такие данные должны быть отнесены к персональным данным только в том случае, если они хранятся и обрабатываются совместно с идентификаторами, которые сами по себе определяют физическое лицо.

Необходимо учитывать, что вопрос отнесения тех или иных сведений к персональным данным часто решается с учетом того, с какой целью и кем они обрабатываются. Так, Тринадцатый арбитражный апелляционный суд, рассматривая в апелляционной инстанции иск ОАО «Третий парк» о признании недействительным предписания Управления Роскомнадзора по Санкт-Петербургу и Ленинградской области, в Постановлении от 21.06.2010 по делу № А56-4788/2010 согласился с выводом суда первой инстанции, что паспортные данные (серия и номер паспорта) не отнесены законом к персональным данным, а серия и номер

паспорта относятся не к личности гражданина, а к бланку документа, удостоверяющего его личность. Учитывая, что контролерами, кондукторами и водителями автобусов при проверке принадлежности проездного документа конкретному лицу производится считывание и вывод на дисплей валидатора сведений об имени, отчестве, фамилии владельца проездного документа, серии и номере его паспорта, однако в памяти валидатора не сохраняются, эти данные не накапливаются, не систематизируются, а также не представляются третьим лицам, судом был сделан еще один вывод: «Суд первой инстанции обоснованно указал, что Общество не является оператором по обработке персональных данных пассажиров».

Более перспективной представляется попытка определить, в каких случаях сведения не могут рассматриваться как персональные данные. Так, данные после проведения процедуры обезличивания, когда становится невозможным без использования дополнительной информации определить принадлежность этих сведений конкретному субъекту, персональными данными не являются. Необходимо обратить внимание, что в Законе о персональных данных не используется широко применяемый в обиходе термин «обезличенные персональные данные», а только термин «обезличивание». Часть 7 статьи 5 Закона о персональных данных практически приравнивает по последствиям для субъекта уничтожение персональных данных и их обезличивание: «Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом».

Также не являются персональными данными сведения о физических лицах, хранящиеся или передающиеся в зашифрованном виде, поскольку без знания ключа шифрования невозможно не только их соотнесение с конкретным субъектом, но и вообще определение того, что скрывается за массивом символов. Необходимо отметить, что в Российской Федерации отсутствует судебная практика разрешения споров, связанных с передачей персональных данных в зашифрованном виде без предоставления ключа, в том числе при размещении персональных данных в зашифрованном виде в дата-центрах и облачных вычислительных инфраструктурах без передачи ключей провайдеру вычислительных услуг, например, зашифрованных резервных копий баз данных.

Необходимо отметить, что в последнее время (2015-2019 гг.) в судебной и правоприменительной практике наметилась тенденция расширительного толкования определения понятия «персональные данные». К ним в ходе проверок и разрешения судебных споров стали относить любой набор сведений, относящихся к определенному физическому лицу, даже если его идентификация оператором не проводится. В первую очередь такой подход просматривается при использовании персональных данных посетителей и пользователей сайтов в сети Интернет.

При этом не имеет значения, является ли полной и достоверной информация, предоставленная некоторыми субъектами, и содержит ли эта информация персональные данные.

Исходя из общей концепции Закона о персональных данных, любой субъект персональных данных, предоставивший их иному лицу – оператору персональных данных, вправе по умолчанию рассчитывать на выполнение в отношении этих сведений всех требований закона, в том числе на обеспечение конфиденциальности

этих данных, запрета на размещение их в общедоступных источниках, в том числе, на сайтах сети Интернет и предоставление их третьим лицам без согласия субъекта.

Так, в 2016-2019 гг. все проверенные Управлением Роскомнадзора по Центральному федеральному округу операторы-юридические лица перед началом проверки получали от надзорного органа «Перечень документов, представление которых необходимо для достижения целей и задач проведения проверки» (приложение № 1 к Плану проведения проверки). В нем, в частности, указывается: «Под данными посетителей и зарегистрированных пользователей сайтов и мобильных приложений Оператора понимаются все данные о посетителях, собираемые с помощью функционала указанных сервисов, а также те данные, которые сервисы сами собирают и обрабатывают на своих вычислительных мощностях, а именно: псевдоним пользователя, адрес пользователя или адрес устройства пользователя, посредством которого пользователь зашел на сайт Оператора, а также сведения о пользователе, включающие ip-адрес, поисковые запросы пользователя, интернет-адреса веб-страниц, посещаемых пользователем, тематику информации, размещённой на посещаемых пользователем интернет-ресурсах Оператора, идентификатор пользователя, преобразованный Оператором при помощи хеш-функции или других модификаций, географический адрес точки подключения пользователя к сети Интернет, информация, **не позволяющая однозначно идентифицировать пользователя или конкретное физическое лицо, но обеспечивающая формирование достаточного для предоставления пользователю рекламной информации**».

Такой подход полностью подтверждается материалами проверок и судебными решениями. Так, в материалах проверок указывалось как нарушение требований закона отсутствие в перечне обрабатываемых оператором персональных данных файлов cookie (несоответствие содержания уведомления оператором Роскомнадзора об обработке персональных данных фактическому состоянию дел).

По мнению Роскомнадзора, использование файлов cookie и функционала интернет-сервисов Google Analytics, Webtrends, Яндекс.Метрика на основании получаемых ими данных позволяет определить уникального посетителя сайта, формировать сведения о его предпочтениях и поведении на сайте, что указывает на обработку его персональных данных. При этом информирование посетителей сайта об обработке их персональных данных с помощью вышеуказанных интернет-сервисов не осуществляется, на сайте отсутствует форма согласия посетителя сайта на обработку его персональных данных с использованием интернет-сервисов Google Analytics, Webtrends, Яндекс.Метрика, что рассматривается надзорным органом как нарушение закона.

Девятый арбитражный апелляционный суд 23 мая 2016 года, рассматривая апелляционную жалобу по делу № А40-14902/2016 о привлечении к ответственности за совершение правонарушения ПАО «МГТС», пришел к выводу, что предоставление оператором связи на основании заключенных с иными лицами договоров информации о запросах абонентов к доступу к сайтам, содержащих обезличенные данные и IP-адреса абонентов, преобразованные в идентификатор абонента/пользователя (id), с целью последующего целевого размещения рекламы, без согласия на это абонентов, нарушает требования законодательства РФ.

Суд согласился с позицией надзорного органа, в соответствии с которой информация, получаемая от оператора связи, позволяет прямо или косвенно

идентифицировать пользователя как определенное физическое лицо (субъект персональных данных).

ПАО «МГТС» передает партнерам сведения об абоненте, включающие поисковые запросы абонентов, Интернет-адреса веб-страниц, посещаемых абонентами, тематику информации, размещенной на посещаемых абонентами Интернет-ресурсах, IP-адрес абонента, достаточной для формирования его рекламного профиля, необходимого для предоставления ему адресной рекламной информации.

Такая обработка данных позволяет косвенно определить субъекта персональных данных, которому впоследствии рекламодатель **персонифицированно** направляет определенную рекламу **в зависимости от предпочтений** субъекта, а именно, ранее просмотренных субъектом интернет-страниц, товаров, работ, услуг, рекламируемых в Интернет и т.п.

В одном из материалов проверки оператора персональных данных Управлением Роскомнадзора по ЦФО были перечислены данные из файлов cookie, которые отнесены к персональным: операционная система, часовой пояс и время браузера в 24-часовом формате, язык браузера, глубина цвета экрана браузера, разрешение экрана браузера, включен ли Java в браузере, поддерживает ли браузер и/или включен JavaScript, версия JavaScript, поддерживаемая браузером, тип соединения, используемый для передачи данных, размер окна браузера.

Тамбовский областной суд 4 октября 2016 г. отказался удовлетворить кассационную жалобу ООО «Тамбовская Городская Юридическая Компания» (ООО «ТГЮК») по делу № 4А-288/2016 на вступившие в законную силу постановление мирового судьи и решение судьи Октябрьского районного суда г. Тамбова, вынесенные в отношении ООО «ТГЮК» по делу об административном правонарушении, предусмотренном ст. 13.11 КоАП РФ. ООО «ТГЮК» было привлечено к административной ответственности за нарушение, заключавшееся в размещении на сайте Общества формы обратной связи, которое рассматривалось Роскомнадзором и судами как сбор персональных данных в сети Интернет, при отсутствии на этом же сайте политики Общества в отношении обработки персональных данных (такое требование введено частью 2 статьи 18.1 Закона о персональных данных). Судами трех инстанций не было принято во внимание разъяснение Общества о том, что форма обратной связи состоит всего из трех элементов: Ваше имя, тема сообщения, сообщение, и определить физическое лицо как субъекта персональных данных с помощью заполнения данной формы не представляется возможным, поскольку идентифицировать физическое лицо по одному имени, без других данных (фамилия, отчество, адрес, заполнение которых в форме обратной связи не предусмотрено) нельзя. Отвергнут и аргумент Общества о том, что в графе «Ваше имя» в форме заполнения данной формы имя не обязательно может быть настоящим.

Комментируя указанное решение изданию «Ведомости», пресс-секретарь Роскомнадзора Вадим Ампелонский сообщил, что сочетание имени и электронной почты уже является персональными данными.

В случае, если данные относятся не к физическим лицам (например, машинные логи, данные по кассовым чекам), такие данные являются персональными только в привязке к конкретному субъекту (чек № … получен при покупке Ивановым Иваном Ивановичем – это персональные данные). Сам по себе номер чека не является персональными данными.

В то же время, по мнению представителей Роскомнадзора, номер телефона или государственный номер автомобиля без привязки к владельцу не являются персональными данными.

Краткие выводы по разделу 5.1

В текущей трактовке Роскомнадзора и российских судов, применяемой в правоприменительной практике, любые сведения, относящиеся к конкретному физическому лицу, даже если оно не идентифицировано оператором (личность его не установлена), но совокупность данных позволяет его выделить среди других лиц, например, в части определения предпочтений или интересов при посещении сайтов сети Интернет, следует рассматривать как персональные данные, и их обработка оператором подпадает под действие Закона о персональных данных.

5.2. Что понимается в законодательстве РФ под базой персональных данных

В Комментарии Роскомнадзора к Закону 242-ФЗ, размещенном в разделе «Методические рекомендации» Электронной библиотеки по защите прав субъектов персональных данных на странице «Портал персональных данных уполномоченного органа по защите прав субъектов персональных данных» официального сайта ведомства на странице по адресу https://pd.rkn.gov.ru/library/p195/ (далее – **Комментарий Роскомнадзора**), указывается:

«При определении понятия «база данных» следует учитывать, что в законодательстве Российской Федерации существует много понятий баз данных, тем не менее все они сводятся к одному общему значению, согласно которому база данных – это упорядоченный массив данных, независимый от вида материального носителя информации и используемых средств его обработки (архивы, картотеки, электронные базы данных). Так, например, базой данных можно считать таблицу в формате Excel, Word, в которой содержатся персональные данные граждан.

При этом единственным законным признаком, которым должна обладать база данных, является ее место нахождения – территория Российской Федерации».

Способ фиксации данных в базе на территории Российской Федерации и вид такой базы (электронная или на бумажных носителях) играет вторичную роль по отношению к месту нахождения базы персональных данных.

В соответствии с пунктом 1 «Положения о Министерстве связи и массовых коммуникаций Российской Федерации» (далее – **Минкомсвязь России**), утвержденного Постановлением Правительства РФ от 02.06.2008 № 418 «О Министерстве связи и массовых коммуникаций Российской Федерации», Минкомсвязи России является федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере обработки персональных данных.

Минкомсвязь России на своем официальном сайте в сети Интернет создало специальную страницу, разъясняющую позицию ведомства по вопросам, вызванным принятием Закона 242-ФЗ и внесением изменений в Закон «О персональных данных», которая находится по адресу http://minsvyaz.ru/ru/personaldata/.

На данной странице в разделе вопросов и ответов дается следующее разъяснение в отношении баз данных, создаваемых в виде собрания документов на бумажных носителях:

«… нередко сбор персональных данных первоначально осуществляется в «бумажной» форме (заполненные бланки заявлений, анкет и пр.), с последующим их занесением сотрудником организации в общекорпоративную электронную базу данных, расположенную за рубежом. Возложение на оператора обязанности по локализации каждой из таких баз данных приводит к существенному возрастанию затрат, не сопровождающихся усилением защиты субъектов персональных данных (поскольку их данные уже были локализованы на территории РФ). К тому же в некоторых случаях особенности построения информационной инфраструктуры компании не позволяют осуществить локализацию всех баз данных без кардинальной перестройки своей глобальной инфраструктуры».

Таким образом, в качестве базы данных на территории Российской Федерации при использовании облачного решения может использоваться любая база персональных данных, в том числе – систематизированное собрание документов на бумажных носителях (анкет, карточек учета, резюме, трудовых книжек и т.д.), откуда данные могут переносится в электронную базу данных для их последующей обработки с использованием облачного решения.

5.3. Сценарии использования облачной платформы Microsoft Azure и иных облачных сервисов корпорации Microsoft, соответствующие требованиям Закона о персональных данных

Исходя из нормы части 5 статьи Закона о персональных данных, рассмотренной в разделе 4 Экспертного заключения, сбор любых персональных данных российских граждан любыми организациями, независимо от форм их собственности, места нахождения и юрисдикции, должен производиться только с использованием баз данных, расположенных на серверах на территории Российской Федерации. В этих же базах данных на территории России персональные данные должны систематизироваться, накапливаться, храниться, актуализироваться (то есть уточняться, обновляться, изменяться), из них персональные данные должны и извлекаться для последующей их трансграничной передачи зарубежным органам власти, юридическим и физическим лицам, в том числе в дата-центры и облачные вычислительные инфраструктуры, находящиеся за пределами территории Российской Федерации.

На странице http://minsvyaz.ru/ru/personaldata/ своего официального сайта Минкомсвязь России разъясняет, что «В соответствии с частью 5 статьи 18 ФЗ «О персональных данных» сбор персональных данных, их обновление и изменение должны производиться с использованием баз данных, расположенных на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 ФЗ «О персональных данных». Однако при этом следует иметь в виду, что изменения в ФЗ «О персональных данных», внесенные ФЗ-242, не затронули положений закона о трансграничной передаче данных. Соответственно передача персональных данных за пределы Российской Федерации возможна, как и ранее, с соблюдением условий, указанных в ст. 12 ФЗ «О персональных данных». Тем самым требование о локализации отдельных процессов обработки

персональных данных, содержащееся в ч. 5 ст. 18 ФЗ «О персональных данных», следует толковать в системном единстве с положениями ст. 12 о трансграничной передаче данных и с учетом определения данного понятия… Таким образом, **персональные данные** гражданина Российской Федерации, **первоначально внесенные в базу данных на территории Российской Федерации** и актуализируемые в ней («первичная база данных»), **могут далее передаваться в базы данных, расположенные за пределами России** («вторичные базы данных»), администрируемые иными лицами, с соблюдением положений о трансграничной передаче данных».

Аналогичное разъяснение дается на сайте Минкомсвязи России на вопрос «Распространяется ли требование локализации на случаи внесения персональных данных российских граждан в базы данных, которые расположены за пределами Российской Федерации, если такие персональные данные ранее уже были локализованы в соответствии с ФЗ-242?»:

«Как следует из текста ч. 5 ст. 18 ФЗ «О персональных данных», обязанность оператора обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, считается исполненной, когда указанные действия были совершены при сборе персональных данных с использованием базы данных, находящейся на территории Российской Федерации. При этом статья не содержит указания на то, что такие действия должны совершаться исключительно с использованием баз данных, размещенных на территории России. В связи с этим, если в отношении определенного набора персональных данных уже были ранее выполнены требования ФЗ-242, повторная локализация таких персональных данных не требуется, поскольку цели закона уже достигнуты. Соответственно, **если персональные данные были при сборе записаны в базу данных, расположенную на территории Российской Федерации, то впоследствии такие персональные данные могут вноситься работником (представителем) оператора в принадлежащую ему электронную базу данных, находящуюся за пределами РФ**».

Подводя итог рассмотрению позиции Минкомсвязи России по вопросу использования баз данных персональных данных, находящихся за рубежом, необходимо привести еще два разъяснения, размещенные на сайте ведомства:

«Обработка персональных данных граждан Российской Федерации посредством сбора, записи, систематизации, накопления, хранения, уточнения, извлечения может осуществляться с использованием баз данных, не находящихся на территории Российской Федерации в следующих случаях:

- если такая деятельность подпадает под случаи, предусмотренные пунктами 2–4, 8 части 1 статьи 6 закона «О персональных данных»;
- если такая деятельность не подпадает под случаи, предусмотренные пунктами 2–4, 8 части 1 статьи 6 закона «О персональных данных», и на территории Российской Федерации находятся используемые для такой обработки персональных данных базы данных, в которых содержится больший объем персональных данных или равный находящемуся за пределами территории Российской Федерации (в этом случае недопустимо нахождение за пределами территории Российской Федерации персональных

данных, которые одновременно не находятся в пределах территории Российской Федерации)».

«Закон налагает на оператора обязанность при осуществлении обработки собранных персональных данных путем систематизации, накопления, хранения, уточнения, извлечения, использовать базы данных, находящиеся на территории Российской Федерации. Таким образом, если для составления отчетности, либо анализа информации, содержащей персональные данные, оператору требуется осуществить упомянутые формы обработки персональных данных, то такие действия должны осуществляться с использованием баз данных, находящихся на территории Российской Федерации».

Позиция Роскомнадзора как органа, осуществляющего контроль и надзор за соблюдением требований Закона о персональных данных, по рассматриваемым в Экспертном заключении вопросам отражается, без прямого указания на надзорный орган, на сайте проекта ПД-Инфо.рф / PD-info.ru, который посвящен обсуждению вопросов, связанных с особенностями реализации Закона 242-ФЗ. На сайте указывается: «Проект реализуется силами РАЭК (Ассоциация электронных коммуникаций), РОЦИТ (Региональный общественный Центр интернет-технологий) и Роскомнадзора, при участии партнеров проекта: theRunet, rspectr.com и Журнал «Интернет в цифрах». Принципиально важна роль Роскомнадзора в данном проекте как представителя государства и контролирующего органа, готового к диалогу с отраслью, экспертизе закона и возникающих в связи с его исполнением нюансов, а также к постоянному взаимодействию с игроками Рунета и IT-компаниями».

Ответы, разъясняющие нормы, установленные Законом 242-ФЗ, размещены по адресу http://pd-info.ru/questions/.

В частности, в ответе на вопрос «Позволяет ли 242-ФЗ передавать/отражать персональные данные российских граждан после их сбора, обработки и хранения на территории РФ на иностранный сервер (стран-участниц Конвенции 108 и иных государств)? Если да, то на каких условиях?» на сайте Проекта ПД-Инфо.рф указывается:

«Требования 242-ФЗ не исключают трансграничную передачу персональных данных, более того не затрагивают положений, связанных с вопросами передачи персональных данных на территорию иностранного государства.

Так, в соответствии с международными обязательствами, взятыми на себя Российской Федерацией при ратификации Конвенции о защите физических лиц при автоматизированной обработке персональных данных российская Сторона не должна запрещать или обусловливать специальным разрешением трансграничные потоки персональных данных, идущие на территорию другой Стороны, с единственной целью защиты частной жизни…

Трансграничная передача данных в разрезе положений Закона 242-ФЗ представляет собой передачу сведений из одной базы данных, расположенных на территории России, в другую базу данных, расположенных на территории иностранного государства. Такая передача данных должна иметь заранее определенную цель обработки, при достижении которой субъекту персональных данных должно быть гарантировано уничтожение переданных данных на территории иностранного государства».

В ответе на другой вопрос на том же сайте разъясняется:

«… 242-ФЗ не вводится обязанность оператора персональных данных осуществлять передачу данных только в базы данных на территории Российской Федерации.

242-ФЗ не вносит изменений в статью 12 Федерального закона «О персональных данных», которая регламентирует вопрос трансграничной передачи персональных данных. В связи с чем, трансграничная передача персональных данных российских граждан, полученных при сборе с использованием баз данных, расположенных на территории Российской Федерации, может осуществляться при соблюдении принципа соответствия целям обработки персональных данных, собранных на территории Российской Федерации.

Хранение персональных данных на территории иностранного государства в контексте 242-ФЗ не запрещено при условии соблюдения условий сбора персональных данных на территории Российской Федерации и соблюдения порядка трансграничной передачи персональных данных, установленных ст. 12 Федерального закона «О персональных данных».

На сайте имеется и такое разъяснение:

«242-ФЗ устанавливает обязанность оператора персональных данных при сборе персональных данных граждан Российской Федерации обеспечить их запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение с использованием баз данных, находящихся на территории Российской Федерации.

Закон не содержит требований по размещению всех сайтов для граждан Российской Федерации на российском хостинге. Достаточно хранить сами персональные данные граждан Российской Федерации в базах данных, находящихся на территории Российской Федерации (например, на российском хостинге).

При этом следует учитывать, что указанные требования к хранению персональных данных предъявляются к операторам персональных данных только при сборе персональных данных».

Анализ требований части 5 статьи 18 Закона о персональных данных и части 4 статьи 16 Закона 149-ФЗ в редакции Закона 242-ФЗ, рассмотренных в разделе 4 Экспертного заключения, показывает, что в соответствии с данными требованиями, с 1 сентября 2015 года прямо и конкретно запрещено размещение персональных данных российских граждан на серверах, расположенных за пределами Российской Федерации, без предварительного размещения их в информационной системе (базе данных) на территории Российской Федерации. Невозможно использовать, например, веб-формы для непосредственного внесения персональных данных российских граждан в базу данных, находящуюся за рубежом, а также для изменения или уточнения в такой базе ранее внесенных в нее данных.

Таким образом, использование для обработки персональных данных информационных систем, серверы которых расположены за пределами Российской Федерации, без использования дополнительных мер, обеспечивающих фиксацию данных на территории России или иным способом реализующих требований законодательства Российской Федерации, является незаконным.

Для выполнения рассматриваемых требований законодательства Российской Федерации в случае использования оператором информационных систем

персональных данных, находящихся за рубежом, возможна реализация трех сценариев:

1) базу персональных данных, предназначенную для первичного сбора персональных данных, их записи и накопления, а также последующей актуализации (уточнения, обновления, изменения), разместить на территории Российской Федерации и постоянно хранить обрабатываемые персональные данные российских граждан в такой базе;
2) обезличить размещаемые за рубежом персональные данные;
3) зашифровать персональные данные, размещаемые за рубежом, и не предоставлять зарубежному оператору информационной системы (провайдеру вычислительных услуг) ключи шифрования.

При необходимости трансграничной передачи персональных данных российских граждан, в порядок осуществления которой Законом о персональных данных никаких изменений не вносится, персональные данные российских граждан должны извлекаться из базы данных, находящейся на территории Российской Федерации, и передаваться для дальнейшего использования в другие информационные системы, расположенные вне Российской Федерации, обезличиваться или шифроваться перед такой передачей.

Исходя из анализа сложившейся в России правоприменительной и судебной практики, для реализации первого сценария оператору необходимо разместить у себя, или в дата-центре на территории Российской Федерации, или в облачной вычислительной инфраструктуре, технические средства которой находятся целиком и полностью в России, базу данных, в которую будет осуществляться сбор персональных данных граждан Российской Федерации и в которых будет осуществляться их актуализация.

Эффективным механизмом для выполнения этого требования является Azure Stack Hub – расширение облачной платформы Microsoft Azure, которое позволяет запускать приложения в локальной среде и предоставлять службы Azure в дата-центре, используемом заказчиком облачной платформы. В частности, Azure Stack Hub содержит базу данных как сервис, включая SQL Server 2019, SQL resource provider, MySQL resource provider.

Интегрированные системы Azure Stack Hub состоят из 4–16 объединенных в стойку серверов в дата-центре пользователя облачной платформы и позволяют создать гибридные решения, которые хранят и обрабатывают персональные данные локально в Azure Stack Hub, но имеют возможность передавать их платформе Azure для дополнительной обработки и анализа и использованием всех современных технологи, предоставляемых облачной платформой.

Azure Stack Hub использует облачную службу управления удостоверениями и доступом Azure Active Directory (Azure AD) или службы федерации Active Directory (AD FS). В большинстве гибридных сценариев с подключенным к Интернету развертыванием в качестве хранилища идентификаторов используется Azure AD.

В свою очередь Azure AD может быть развернута с использованием гибридного решения, позволяющего синхронизировать локальную AD, созданную пользователем облачного сервиса на территории Российской Федерации, с облачной. При этом в облачную службу сетевых каталогов могут передаваться

только те данные из локальной AD, которые считает необходимыми пользователь облачного сервиса, а не все данные, используемые локальной AD.

Схема использования гибридной идентификации, предусматривающей синхронизацию локальной и облачной AD, приведена на рисунке 1.

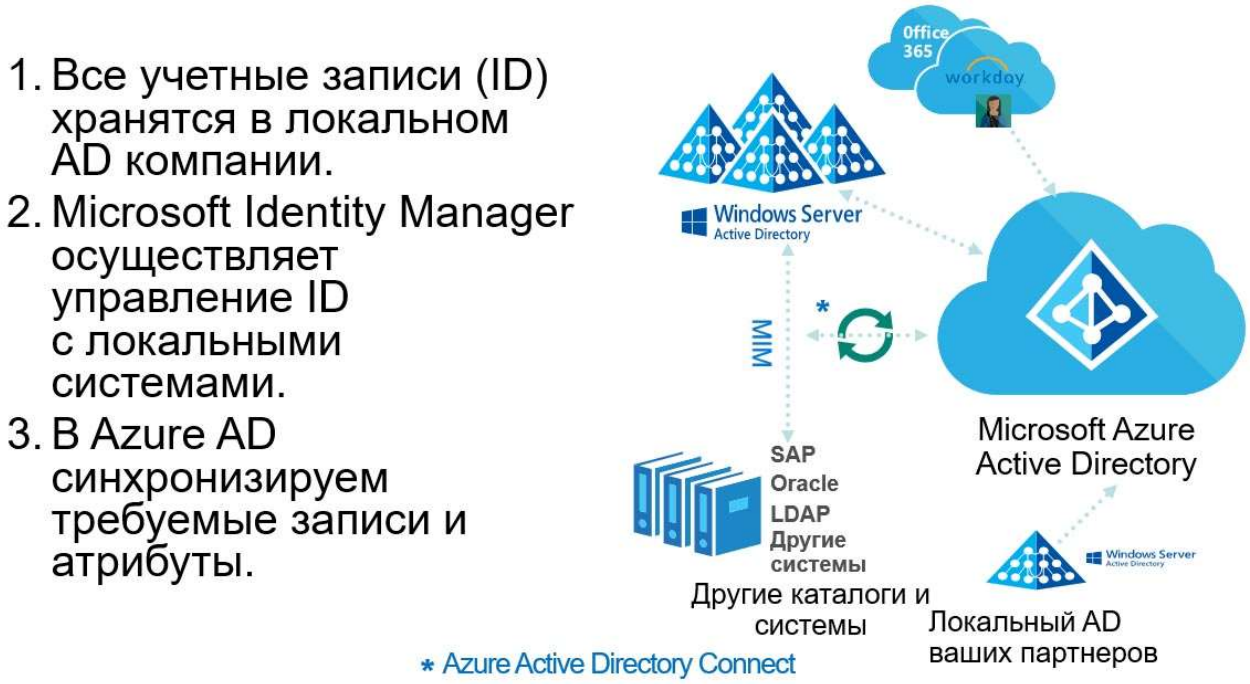

Рисунок 1. Гибридная идентификация

Особого внимания требует анализ допустимости размещения в облаке, находящемся за пределами Российской Федерации, сервера с запущенным на нем приложением, в веб-форму которого вводятся персональные данные, и используемого для сбора персональных данных, в случае, если данные вносятся в базу на территории Российской Федерации и не сохраняются в период сбора в базе, находящейся за рубежом.

В этом случае при заполнении пользователем веб-формы с персональными данными все вносимые данные попадают в оперативную память сервера, находящегося в облаке, где кратковременно хранятся в защищенной области памяти, к которой невозможен доступ пользователей и из которой данные не могут быть произвольно извлечены.

Данные в оперативную память сервера в облаке попадают из веб-браузера пользователя и находятся на сервере в течение примерно нескольких миллисекунд, после чего вносятся в базу данных пользователя на территории Российской Федерации. Исходя из определения базы персональных данных, приведенного в разделе 5.2 Экспертного заключения, оперативная память сервера, в которой кратковременно обрабатываются персональные данные, не является базой персональных данных, и описываемая схема соответствует требованиям части 5 статьи 18 Закона о персональных данных.

Сценарий размещения в облаке данных, прошедших процедуру обезличивания, будет рассмотрен в разделе 5.4 Экспертного заключения.

Как отмечалось ранее, в разделе 5.1 Экспертного заключения, отсутствует судебная практика разрешения споров, связанных с передачей персональных данных в зашифрованном виде без предоставления ключа, в том числе при размещении персональных данных в зашифрованном виде в дата-центрах и облачных вычислительных инфраструктурах без передачи ключей провайдеру вычислительных услуг.

Краткие выводы по разделу 5.3

В случае, если персональные данные первично копируются и/или актуализируются в базы данных на территории Российской Федерации, а затем сохраняются для дальнейшего использования в информационной системе, расположенной за пределами территории Российской Федерации, например, в облаке Microsoft Azure, такая схема полностью соответствует требованиям законодательства Российской Федерации, касающимся территориального расположения баз персональных данных российских граждан.

Эффективным механизмом выполнения такого требования является использование гибридных решений Azure Stack Hub и Azure Active Directory, предусматривающих локализацию персональных данных пользователей и субъектов, чьи данные обрабатываются в облаке, непосредственно на серверах, территориально находящихся у пользователя облачной платформы на территории Российской Федерации.

5.4. Размещение на облачных платформах и в облачных сервисах данных, прошедших процедуру обезличивания

Процедура обезличивания определяется пунктом 9 статьи 3 Закона о персональных данных как действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных. Фактически полученные в результате обезличивания данные нельзя рассматривать как персональные, так как невозможно определить, к какому определенному или определяемому физическому лицу – субъекту персональных данных они относятся. Конкретные требования к обезличиванию персональных данных операторами, являющимися государственными или муниципальными органами, установлены приказом Роскомнадзора от 05.09.2013 № 996 (далее – **Приказ № 996**). Для иных операторов положения Приказа № 996 носят рекомендательный характер.

Среди свойств обезличенных данных, определенных Приказом № 996, необходимо выделить анонимность, то есть невозможность однозначной идентификации субъектов данных, полученных в результате обезличивания, без применения дополнительной информации.

К наиболее перспективным и удобным для практического применения Приказ № 996 относит такой метод обезличивания, как введение идентификаторов (замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным).

Метод введения идентификаторов реализуется путем замены части персональных данных, позволяющих идентифицировать субъекта, их идентификаторами и созданием таблицы соответствия.

Метод обеспечивает такие свойства обезличенных данных, как полнота, структурированность, семантическая целостность, применимость и обеспечивает наличие всех свойств обезличенных данных, установленных Приказом № 996.

Закон о персональных данных рассматривает процедуру обезличивания как идентичную по своим последствиям уничтожению персональных данных. Так, часть 7 статьи 5 Закона о персональных данных устанавливает, что «Обрабатываемые персональные данные подлежат **уничтожению** либо **обезличиванию** по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом».

Таким образом, персональные данные, находящиеся и постоянно хранящиеся в базе данных на территории России, после их обезличивания могут быть размещены в любой информационной системе, в том числе и в системах класса Microsoft Dynamics, для их последующей обработки, при этом территориальное расположение такой системы значения не имеет. В этом случае, поскольку размещаемые в облачной системе данные не являются персональными и не могут быть соотнесены с определенным или определяемым на их основании субъектом персональных данных, не требуется и согласие субъекта персональных данных на трансграничную передачу его данных в страны, не обеспечивающие адекватную защиту прав субъектов персональных данных, в частности, в облачную систему, созданную на платформе дата-центров, находящихся на территории Соединенных Штатов Америки или иной страны, не отнесенной законодательством к странам, обеспечивающим адекватную защиту прав субъектов персональных данных в соответствии с критериями, установленными частями 1 и 2 статьи 12 Закона о персональных данных.

Трансграничная передача данных, прошедших процедуру обезличивания, которые после этого не могут рассматриваться как персональные данные, в том числе и в страны, не обеспечивающие адекватную защиту прав субъектов персональных данных, не требует получения согласия субъектов, так как по своему смыслу такая передача не является передачей персональных данных.

Таким образом, в случае, если персональные данные сохраняются в системе, расположенной на территории РФ, а в облачную систему, например, Microsoft Dynamics, будут передаваться данные, прошедшие процедуру обезличивания, такая схема работы будет соответствовать изменениям, вступившим в силу 1 сентября 2015 года, и предусматривающим, что при сборе персональных данных, в том числе посредством сети Интернет, оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, предусмотренных Законом о персональных данных. В этом случае соблюдаются все требования новой редакции закона, касающиеся ограничения мест расположения баз персональных данных российских граждан в период сбора таких данных и их последующей обработки способами, указанными в части 5 статьи 18 закона.

Использование облачных систем, таких, например, как Microsoft Dynamics, совместно с решением по деперсонализации (Depersonalization solution, DPL solution, далее – DPL-решение), предназначенным для обезличивания персональных данных, после вступления в силу 1 сентября 2015 года поправок в законодательство РФ о персональных данных, касающихся территориального расположения серверов, на которых хранятся персональные данные граждан Российской Федерации, представляется допустимым и соответствующим требованиям законодательства РФ при условии, что базы персональных данных, в отношении которых выполняется процедура обезличивания, полностью находятся на территории Российской Федерации, а все изменения персональных данных производятся первоначально именно в этих базах данных. Для обезличивания используется программное обеспечение и плагины для облачных решений, разработанные партнерами компании Microsoft.

Организация обработки персональных данных в этом случае должна осуществляться **по следующей схеме**:

1. Персональные данные российских граждан после их получения оператором фиксируются в базе данных (осуществляется запись персональных данных в базу данных), находящейся на территории Российской Федерации, которая хранится и поддерживается в актуальном состоянии в течение всего периода обработки персональных данных. В этой же базе осуществляется систематизация и накопление персональных данных.
2. После этого персональные данные могут извлекаться из базы данных для их трансграничной передачи в систему Microsoft Dynamics для последующей обработки и использования, но, при таком извлечении, фамилии, имена и отчества (при наличии) субъектов, а также, при необходимости, иные идентифицирующие сведения, такие, как ИНН, СНИЛС, паспортные данные, в некоторых случаях – адрес электронной почты, заменяются на условные идентификаторы, состоящие из произвольной комбинации символов, и таким образом проходят процедуру обезличивания. Таблица соответствия между идентифицирующими персональными данными (фамилией, именем и отчеством) и условными идентификаторами также должна находиться на территории Российской Федерации.
3. Все последующие изменения (уточнение, обновление, изменение) персональных данных должны производиться также в базе данных, находящейся на территории Российской Федерации, и только после того, как они будут сделаны, модифицированные данные могут извлекаться для последующего использования за пределами Российской Федерации.

С целью выполнения требований Закона о персональных данных в части территориальности размещения баз персональных данных в период их сбора, архитектурный дизайн DPL-решения обеспечивает хранение всех персональных данных локально (на стороне заказчика, в дата-центрах или облачных вычислительных инфраструктурах), на территории Российской Федерации.

Основная идея этого решения заключается в сохранении данных, относящихся к персональным, в отдельной базе данных и последующей передачи ссылок (кодов) на эти данные в систему Microsoft Dynamics.

Безотносительно к тому, где территориально будет находиться MS SQL сервер, все персональные данные будут храниться в отдельном хранилище данных, которое будет располагаться на территории Российской Федерации.

Если установка DPL-решения производится для системы с уже имеющимися в ней персональными данными, необходимо наличие инструмента, позволяющего производить обновление записей после установки DPL-решения.

DPL-решение позволяет выбрать и настроить конкретные поля записей о субъектах персональных данных, подлежащих обезличиванию (например, имя, фамилия, полное имя, дата рождения, СНИЛС, номер мобильного телефона и др.). Обезличиваемые данные заменяются идентификаторами, как правило – значениями хэш-функций от них.

DPL-решение устанавливается на сервер Microsoft Dynamics, который расположен в одном из европейских дата-центров в Дублине (Ирландия) либо Амстердаме (Нидерланды), а плагин, развернутый между веб-приложением и базой данных, работает следующим образом.

При заполнении пользователем Microsoft Dynamics веб-формы с персональными данными все данные попадают в оперативную память сервера, где плагин их разделяет на персональные (идентифицирующие субъекта) и не персональные данные, которые далее обрабатываются по-разному. Не персональные данные попадают в базу данных, развернутую в облаке Microsoft Dynamics, а персональные данные либо заменяются на идентификаторы, которые передаются в облачную базу данных, путем хэширования значения персональных данных, а идентификаторы сохраняются в базе данных на территории РФ, либо персональные данные полностью сохраняются в базе на территории РФ и после успешного завершения этой операции передаются на хранение в облачную базу данных Microsoft Dynamics.

При этом персональные данные кратковременно находятся в оперативной памяти сервера в облаке, и в этот период времени к ним невозможен доступ или их извлечение, поскольку данные находятся в защищенной области памяти.

Данные в оперативную память сервера в облаке попадают по протоколу https из веб-браузера пользователя и находятся на сервере в течение примерно 100-200 мс для того, чтобы они могли быть обработаны плагином согласно описанному выше алгоритму.

Используемый в DPL-решении способ обезличивания персональных данных соответствует требованиям Приказа № 996.

Как отмечалось выше, пункт 11 «Требований и методов обезличивания персональных данных», утвержденных Приказом № 996, относит используемый в DPL-решении метод обезличивания путем введения идентификаторов (замены части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным) к наиболее перспективным и удобным для практического применения методам. Пункт 12 Приказа № 996 требует для реализации данного метода обезличивания установить атрибуты персональных данных, записи которых подлежат замене идентификаторами, разработать систему идентификации, обеспечить ведение и хранение таблиц соответствия, что полностью реализовано в программном продукте.

Кратковременное нахождение персональных данных в защищенной памяти сервера, размещенного за рубежом, не противоречит законодательству РФ, поскольку при такой схеме предусмотренные Законом о персональных данных действия – сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных, выполняются только в базе данных, находящейся на территории Российской Федерации, а на зарубежном сервере сохраняются либо обезличенные данные, идентификаторы которых зафиксированы в Российской Федерации, либо персональные данные, предварительно размещенные в базе данных на территории Российской Федерации.

Краткие выводы по разделу 5.4.

На основании изложенного можно сделать вывод, что в случае, если персональные данные сохраняются в системе, расположенной на территории Российской Федерации, а в облачную систему, например, такую, как Microsoft Dynamics, передаются данные, прошедшие процедуру обезличивания, такая схема будет соответствовать требованиям законодательства РФ, касающимся территориального расположения баз персональных данных российских граждан, поскольку такие данные не являются персональными, их передача за рубеж и обработка в системах, расположенных за рубежом, не регламентируется Законом о персональных данных.

5.5. Возможно ли использование российским оператором сервисов электронной почты, интернет-телефонии, передачи видеоконтента, предоставляемых облачным сервисом Microsoft Office 365

При оценке возможности использования российским оператором сервисов электронной почты, интернет-телефонии, передачи видеоконтента, предоставляемых облачным сервисом Microsoft Office 365 (Outlook, Exchange Online, Teams, Video/Stream), необходимо оценить, **являются ли такие сервисы информационными системами персональных данных или компонентами таких систем**.

В соответствии с пунктом 10 статьи 3 Закона о персональных данных, информационная система персональных данных – это совокупность содержащихся в **базах данных** персональных данных и обеспечивающих их обработку **информационных технологий** и **технических средств**.

Необходимо учитывать, что сервисы электронной почты, интернет-телефонии, передачи видеоконтента, предоставляемые облачным сервисом Microsoft Office 365 (Outlook, Exchange Online, Teams, Video/Stream) не предназначены для непосредственной обработки персональных данных, оператор не определяет цели обработки персональных данных, содержащиеся в почтовых сообщениях и сообщениях мессенджера, их адресных книгах, видеопотоке, состав этих данных и не может их контролировать. Так, отправка незапрашиваемой оператором информации, содержащей специальные категории персональных данных или биометрические персональные данные, приводит к несоответствию установленного оператором уровня защищенности такой информационной системы и необходимости принятия дополнительных мер обеспечения безопасности при том, что контроль содержимого почтовых ящиков, содержания электронных сообщений, передаваемого пользователями видеоконтента не является обязанностью

оператора, и без согласия пользователя или вступившего в силу судебного акта не может выполняться оператором, поскольку нарушает законные права пользователей системы.

В связи с изложенным **представляется нецелесообразным рассматривать сервисы электронной почты, интернет-телефонии, передачи видеоконтента в качестве информационных систем персональных данных и распространять на нее требования законодательства РФ о персональных данных.**

Получение персональных данных в процессе использования сервисов электронной почты, интернет-телефонии, передачи видеоконтента не может рассматриваться как сбор персональных данных и, в связи с этим, не требует обязательной локализации на территории Российской Федерации, что вытекает из разъяснений на сайте Минкомсвязи России: «Обязанности по локализации отдельных процессов обработки персональных данных возникают **лишь при сборе** персональных данных. Из ч. 1 ст. 18 ФЗ «О персональных данных», посвященной обязанностям оператора при сборе персональных данных, можно сделать вывод, что **под сбором можно понимать целенаправленный процесс получения персональных данных** оператором непосредственно от субъекта персональных данных либо через специально привлеченных для этого третьих лиц. Таким образом, **локализации подлежат только те персональные данные**, которые были получены оператором **в результате осуществляемой им целенаправленной деятельности** по организации сбора таких данных, **а не в результате случайного (незапрошенного) попадания к нему** персональных данных, например, **вследствие получения писем по электронной или иной почте**, в которых содержатся персональные данные. Аналогичным образом, не является сбором получение одним юридическим лицом персональных данных от другого юридического лица, если такие данные представляют собой контактную информацию работников или представителей такого юридического лица, переданную в ходе осуществления ими своей законной деятельности».

Исключения составляют случаи создания почтовых ящиков специально для сбора персональных данных, например, соискателей вакантных должностей, таких как recruting@company.ru, vacancies@bank.ru.

Такие ящики электронной почты необходимо рассматривать как элементы информационной системы персональных данных и обеспечивать в отношении них локализацию на территории Российской Федерации, для чего использовать имеющиеся гибридные решения производителей программного обеспечения для систем электронной почты.

Тем не менее вопрос мест расположения хранилищ данных, используемых различными сервисами передачи данных, в частности Teams, вызывает обычно много вопросов при принятии решения российской компанией о целесообразности использования сервиса.

В соответствии с политикой компании Microsoft, данные пользователей сервисов хранятся в зависимости от места первичной регистрации пользователя. Для пользователей из России это «Глобальная география 1-EMEA», включающая в себя вычислительные мощности на территории Австрии, Ирландии, Нидерландов, Финляндии и Франции. Для сервисов Exchange Online, OneDrive и SharePoint Online доступна опция Мульти-Гео, позволяющая пользователю при необходимости разместить данные и в других локациях.

5.6. Допускает ли законодательство РФ создание новых сведений о субъекте в зарубежной информационной системе персональных данных

Необходимо обратить внимание, что часть 5 статьи 18 Закона о персональных данных требует от оператора использовать базу данных на территории Российской Федерации в период сбора персональных данных и для выполнения таких действий как запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.

Закон не вводит требования о том, что такой способ обработки, как **использование** персональных данных должен выполняться исключительно в базе данных на территории Российской Федерации, что делает возможным перенос персональных данных, локализованных в России, для их дальнейшей обработки в информационные системы, находящиеся за пределами Российской Федерации, как это рассмотрено и обосновано в разделе 5.3 Экспертного заключения.

Закон о персональных данных не дает определения понятиям «сбор» и «использование» персональных данных.

На упоминавшейся ранее веб-странице официального сайта Минкомсвязи России, посвященной изменениям в Закон 152-ФЗ, внесенным Законом 242-ФЗ, http://minsvyaz.ru/ru/personaldata/ указывается:

«Обязанности по локализации отдельных процессов обработки персональных данных возникают лишь при сборе персональных данных. Из ч. 1 ст. 18 ФЗ «О персональных данных», посвященной обязанностям оператора при сборе персональных данных, можно сделать вывод, что под сбором можно понимать целенаправленный процесс получения персональных данных оператором непосредственно от субъекта персональных данных либо через специально привлеченных для этого третьих лиц. Таким образом, **локализации подлежат только те персональные данные**, которые были получены оператором в результате осуществляемой им **целенаправленной деятельности по организации сбора таких данных**».

Аналогичное разъяснение дается и на сайте ПД-ИНФО.РФ:

«Сбор персональных данных – это получение персональных данных непосредственно от субъекта персональных данных и оператор обязан обеспечить их запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение с использованием баз данных на территории Российской Федерации, указанные виды обработки составляют единый процесс формирования и поддержания в актуальном состоянии базы данных, что должно осуществляться на территории Российской Федерации».

В Комментарии Роскомнадзора на «Портале персональных данных Уполномоченного органа по защите прав субъектов персональных данных» указывается: «Реализация обязанности *«при сборе данных»* означает, что оператор должен их получать непосредственно у первоисточника, то есть у субъекта персональных данных или его представителя. В таком случае речь идет о сборе информации, а не о случаях передачи данных третьему лицу для обработки в каких-либо целях. Так, оператор, получив данные субъекта, обязан обеспечить их запись,

систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение с использованием баз данных, находящихся в России».

Определение термина «использование персональных данных» имелось в настоящее время не действующих редакциях Закона о персональных данных (до принятия редакции закона, установленной в соответствии с Федеральным законом от 25.07.2011 № 261-ФЗ «О внесении изменений в Федеральный закон "О персональных данных"». Данное понятие определялось в пункте 5 статьи 3 следующим образом: «использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц».

Таким образом, если в информационной системе, находящей за рубежом и обрабатывающей персональные данные, которые в период их сбора были локализованы на территории Российской Федерации, на основании собранных данных выполняются какие-либо действия, затрагивающие субъекта персональных данных и позволяющие получить новые сведения о нем, то такие действия не подпадают под ограничения, установленные частью 5 статьи 18 Закона о персональных данных. Так, если, например, в системе Microsoft Dynamics 365 for Talent на основании собранных и локализованных в России данных о работнике определяется его грейд, делается вывод о необходимости направления на повышение квалификации или продвижения по службе, такие данные нельзя рассматривать как получаемые во время сбора, то есть они не были получены от субъекта или через уполномоченных оператором лиц.

Соответственно, Закон о персональных данных не содержит требования об обязательной локализации таких данных на территории Российской Федерации.

5.7. Ограничения, накладываемые на использования облачной платформы Microsoft Azure и иных облачных сервисов Законом о персональных данных

Закон о персональных данных не водит каких-либо ограничений на использование конкретных технологий обработки персональных данных, в том числе облачных.

На портале ПД-ИНФО.РФ дается ответ на вопрос: «Можно ли в качестве базы данных использовать **облачные технологии** (SaaS, PaaS, SAP)? В том числе если эти технологии предоставляются компаниями, у которых, в том числе, есть в России свои или арендуемые серверы (как у того же SAP), но у клиента нет точной информации о том, какие именно серверы будут задействованы в конкретный миг работы?». Ответ звучит следующим образом: «242-ФЗ, а также проекты подзаконных актов, разработанных во исполнение указанного закона, **не устанавливают каких-либо технических требований**, предписывающих необходимость оператора персональных данных использовать какие-то конкретные технологии при сборе и хранении персональных данных. Так, **оператор может использовать облачные технологии**, но при этом обязан обеспечить, и при необходимости знать и иметь возможность документально подтвердить нахождение баз персональных данных **на территории Российской Федерации**».

Таким образом, ни при каких обстоятельствах, кроме случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 Закона о персональных данных, недопустимо внесение персональных данных при их сборе в базы, находящиеся за рубежом без предварительной локализации данных на территории России, в том числе – с использованием веб-форм, а также обновление (изменение, уточнение) персональных данных в зарубежной безе без предварительного выполнения этих действий в базе на территории России.

Отдельного анализа при использовании рассматриваемых в разделе 5.3 Экспертного заключения сценариев использования облачной платформы Microsoft Azure и иных облачных сервисов для обработки персональных данных требует вопрос, необходимо ли согласие субъектов персональных данных на трансграничную передачу их персональных данных на территории государств, обеспечивающих и не обеспечивающих адекватную защиту прав субъектов персональных данных в соответствии с критериями, установленными Законом о персональных данных.

Статья 12 Закона о персональных данных разделяет все государства на две группы: иностранные государства, обеспечивающие адекватную защиту прав субъектов персональных данных, и иностранные государства, не обеспечивающие адекватную защиту прав субъектов персональных данных.

Для трансграничной передачи персональных данных в государства, обеспечивающие адекватную защиту прав субъектов персональных данных, в общем случае не требуется получения согласия субъектов на такую передачу.

К этой группе относятся государства, являющиеся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных ETS № 108 (их перечень публикуется на официальном сайте Совета Европы по адресу http://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/108/signatures), а также государства, включенные в 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, утверждаемый приказом Роскомнадзора. На сегодняшний день действует перечень, утвержденный приказом Роскомнадзора от 15.03.2013 № 274 (в редакции от 14.01.2019).

Полный перечень государств, обеспечивающих адекватную защиту прав субъектов персональных данных приведен в таблице 2:

Таблица 2

№	Наименование государства
Являющиеся членами Совета Европы	
1	Австрия
2	Азербайджан
3	Албания
4	Андорра
5	Армения
6	Бельгия

№	Наименование государства
7	Болгария
8	Босния и Герцеговина
9	Великобритания
10	Венгрия
11	Германия
12	Греция
13	Грузия
14	Дания
15	Ирландия
16	Исландия
17	Испания
18	Италия
19	Кипр
20	Латвия
21	Литва
22	Лихтенштейн
23	Люксембург
24	Мальта
25	Монако
26	Нидерланды
27	Норвегия
28	Польша
29	Португалия
30	Республика Молдова
31	Российская Федерация
32	Румыния
33	Сан-Марино
34	Северная Македония
35	Сербия
36	Словацкая Республика
37	Словения
38	Турция
39	Украина
40	Финляндия
41	Франция
42	Хорватия
43	Черногория
44	Чешская республика
45	Швейцария
46	Швеция

№	Наименование государства
47	Эстония
Не являющиеся членами Совета Европы, но ратифицировавшие Конвенцию ETS-108	
48	Аргентина
49	Буркина Фасо
50	Кабо-Верде
51	Марокко
52	Мексика
53	Остров Маврикий
54	Сенегал
55	Тунис
56	Уругвай
Включенные в перечень Роскомнадзора	
57	Австралия - Австралийский союз
58	Аргентинская Республика
59	Габонская Республика
60	Государство Израиль
61	Государство Катар
62	Канада
63	Королевство Марокко
64	Малайзия
65	Монголия
66	Новая Зеландия
67	Республика Ангола
68	Республика Бенин
69	Республика Казахстан
70	Республика Корея
71	Республика Коста-Рика
72	Республика Мали
73	Республика Перу
74	Республика Сингапур
75	Тунисская Республика
76	Республика Чили
77	Южно-Африканская Республика
78	Япония

Часть 4 статьи 12 Закона о персональных данных устанавливает, что трансграничная передача любых персональных данных на территории иностранных государств, не обеспечивающих адекватную защиту прав субъектов персональных данных, допускается только в следующих случаях:

1) наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;

2) предусмотренных международными договорами Российской Федерации;

3) предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

4) исполнения договора, стороной которого является субъект персональных данных;

5) защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

Это означает, что российские операторы, желающие разместить персональные данные для обработки в дата-центрах и облачных вычислительных инфраструктурах на территории государств, не обеспечивающих адекватную защиту прав субъектов персональных данных, должны в подавляющем большинстве случаев получать согласие в письменной форме у всех субъектов персональных данных на их трансграничную передачу для последующей обработки. Такое согласие фактически не нужно лишь в случаях, когда субъект персональных данных является стороной договора, в котором трансграничная передача уже прямо предусмотрена.

На трансграничную передачу персональных данных на территории стран, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных ETS № 108 и иных стран, обеспечивающих адекватную защиту прав субъектов персональных данных, в общем случае не требуется согласия субъектов персональных данных. Государствами, обеспечивающими адекватную защиту прав субъектов персональных данных, среди прочих являются Ирландия, Нидерланды и Сингапур, в которых размещаются серверные мощности компании Microsoft, поддерживающие функционирование облачной платформы Microsoft Azure.

В соответствии с частью 3 статьи 6 Закона о персональных данных также требуется согласие субъекта персональных данных на передачу его данных иным лицам в случае, если оператор дает таким лицам поручение на обработку персональных данных.

В то же время, если в договоре между заказчиком и провайдером облачной инфраструктуры, в которой размещается информационная система персональных данных, предусматривается полный запрет на доступ персонала дата-центра (работников корпорации Microsoft) и/или сервис-провайдера к данным заказчика, в получении согласия субъекта на передачу его данных третьим лицам необходимости нет, так как в этом случае поручение на обработку отсутствует.

Необходимо также учитывать, что соответствии со статьей 88 Трудового кодекса РФ от 30.12.2001 № 197-ФЗ, при передаче персональных данных работника работодатель обязан не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в

других случаях, предусмотренных Трудовым кодексом РФ или иными федеральными законами.

Таким образом, если персонал дата-центра или персонал, эксплуатирующий облачную вычислительную инфраструктуру, имеет доступ к обрабатываемым облачными сервисами персональным данным, то есть данные передаются в дата-центр или провайдеру как лицу, осуществляющему обработку персональных данных по поручению оператора, необходимо получать согласие субъектов на передачу их персональных данных в облако Microsoft Azure и иные облачные сервисы компании Microsoft установленным законодательством порядком. Согласие работников в письменной форме потребуется, если работодателем будут передаваться с целью исполнения поручения персональные данные работников, если в облаке размещаются персональные данные специальных категорий или биометрические персональные данные, создается общедоступный источник персональных данных. В остальных случаях, например, при размещении контактных данных покупателей в CRM-системе согласие на передачу данных с целью исполнения поручения может быть получено в любой доказываемой форме.

Краткие выводы по разделу 5.5

В случаях использования облачной платформы Microsoft Azure и иных облачных сервисов на территории государств, обеспечивающих адекватную защиту прав субъектов персональных данных, не требуется получения согласия субъектов на трансграничную передачу персональных данных, если персоналу дата-центра или персоналу, эксплуатирующему облачную платформу, запрещен доступ к обрабатываем данным, что закреплено в договоре между заказчиком и провайдером.

Передача персональных данных в облачную инфраструктуру, вычислительные мощности которой расположены на территории государств, не обеспечивающих адекватную защиту прав субъектов персональных данных, требует получения согласия субъекта на такую передачу в письменной форме, соответствующей требованиям, установленным частью 4 статьи 9 Закона о персональных данных, за исключением случаев, допускающих такую передачу без согласия субъекта и указанных в части 4 статьи 12 Закона о персональных данных.

5.8. Ответственность за нарушения требований законодательства о локализации персональных данных в период их сбора

Вступившей в силу с 1 июля 2017 года новой редакции статьи 13.11 Кодекса Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (далее – **КоАП РФ**) «Нарушение законодательства Российской Федерации в области персональных данных» предусматривается 7 новых составов административных правонарушений, связанных с обработкой персональных данных:

- Часть 1. Обработка персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработка персональных данных, не совместимая с целями сбора персональных данных, за исключением случаев, предусмотренных частью 2

настоящей статьи, если эти действия не содержат уголовно наказуемого деяния.

- Часть 2. Обработка персональных данных без согласия в письменной форме субъекта персональных данных на обработку его персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством Российской Федерации в области персональных данных, если эти действия не содержат уголовно наказуемого деяния, либо обработка персональных данных с нарушением установленных законодательством Российской Федерации в области персональных данных требований к составу сведений, включаемых в согласие в письменной форме субъекта персональных данных на обработку его персональных данных.
- Часть 3. Невыполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки персональных данных, или сведениям о реализуемых требованиях к защите персональных данных.
- Часть 4. Невыполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных.
- Часть 5. Невыполнение оператором в сроки, установленные законодательством Российской Федерации в области персональных данных, требования субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.
- Часть 6. Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих в соответствии с законодательством Российской Федерации в области персональных данных сохранность персональных данных при хранении материальных носителей персональных данных и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении персональных данных, при отсутствии признаков уголовно наказуемого деяния.
- Часть 7. Невыполнение оператором, являющимся государственным или муниципальным органом, предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обезличиванию персональных данных либо несоблюдение установленных требований или методов по обезличиванию персональных данных.

В случае, если оператор, осуществляющий сбор персональных данных российских граждан, использует базу данных, находящуюся не на территории Российской Федерации, он и его должностные лица могут быть привлечены к административной

ответственности по основаниям, предусмотренным частью 1 статьи КоАП РФ (обработка персональных данных в случаях, не предусмотренных законодательством Российской Федерации), поскольку невыполнение требования о месте нахождения баз персональных данных при их сборе является прямым нарушением нормы Закона о персональных данных.

Рассматриваемое административное правонарушение влечет предупреждение или наложение административного штрафа на должностных лиц от 500 до 1000 рублей; на юридических лиц – от 5 000 до 10 000 рублей.

В случае, если использование зарубежной облачной платформы или облачного сервиса предполагает получение согласия субъекта в письменной форме (какие случаи рассмотрены в разделе 5.7 Экспертного заключения), а согласие получено не было или не соответствует требованиям части 4 статьи 9 Закона о персональных данных, такие бездействие или действие оператора влекут административную ответственность, предусмотренную частью 3 статьи 13.11 КоАП и предусматривают наложение административного штрафа на должностных лиц от 10 000 до 20 000 рублей; на юридических лиц - от 15 000 до 75 000 рублей.

Со 2 декабря 2019 года вступили в силу поправки в КоАП РФ, внесенные Федеральным законом от 02.12.2019 № 405-ФЗ. Данным законом статья 13.11 КоАП РФ дополнена частями 8 и 9 следующего содержания:

- Часть 8. Невыполнение оператором при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации.
- Часть 9. Повторное совершение административного правонарушения, предусмотренного частью 8 настоящей статьи.

Административное правонарушение, квалифицируемое по части 8 статьи 13.11 КоАП РФ, влечет наложение административного штрафа на граждан в размере от 30 000 до 50 000 рублей; на должностных лиц – от 100 000 до 200 000 рублей; на юридических лиц – от 1 миллиона до 6 миллионов рублей; по части 9 данной статьи – наложение административного штрафа на граждан в размере от 50 000 тысяч до 100 000 рублей; на должностных лиц - от 500 000 до 800 000 рублей; на юридических лиц – от 6 миллионов до 18 миллионов рублей.

Анализируя вопрос, возможно ли получение российской компанией предписания о запрете использовать облачную платформу или облачный сервис, и о возможных последствиях невыполнения такого предписания, необходимо отметить, что нормы статьи 13.11, других статей КоАП РФ не предполагают наложения запрета на какие-либо действия оператора, такие, например, как запрет на полную или частичную обработку персональных данных, запрет использования для обработки конкретных информационных систем, инфраструктур или платформ. Рассматриваемые применительно к нарушениям законодательства РФ о персональных данных статьи КоАП РФ предусматривают только наложение штрафа на физических, должностных, юридических лиц, а также конфискацию несертифицированных средств защиты информации, когда их сертификация является обязательной, а также выдачу предписания об устранении выявленных нарушений. Иных мер административного

воздействия, таких как административное прекращение деятельности юридического лица, виновного в нарушении требований законодательства РФ, дисквалификация должностных лиц, рассматриваемые статьи КоАП РФ не предусматривают.

В соответствии с пунктом 58 части 2 статьи 28.3 КоАП РФ в редакции, вступившей в силу с 1 июля 2017 года, право составлять протоколы об административных правонарушениях, предусмотренных статьей 13.11 КоАП РФ, перешло от должностных лиц прокуратуры к должностным лица органа, осуществляющего функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора).

Тем не менее работники прокуратуры, ссылаясь на часть 1 статьи 28.4 КоАП РФ «Возбуждение дел об административных правонарушениях прокурором», наделяющей прокуроров при осуществлении надзора за соблюдением Конституции Российской Федерации и исполнением законов, действующих на территории Российской Федерации, правом возбуждать дела о любом другом административном правонарушении, ответственность за которое предусмотрена настоящим Кодексом или законом субъекта Российской Федерации, продолжают инициировать в судах привлечение к ответственности физических, должностных и юридических лиц в случае выявления в ходе проверок нарушений, квалифицируемых по статье 13.11 КоАП РФ.

Последний такой случай отмечен Исполнителем в октябре 2019 года, когда прокуратура Новосибирска обнаружила в местном филиале еврейского агентства «Сохнут» нарушения законодательства о защите персональных данных. Нарушения касались персональных данных слушателей, обучающихся по программам «Сохнут», а также тех, кто собирался перебраться в Израиль. Прокурорская проверка установила, что для защиты информации не применялись сертифицированные средства криптографической защиты. Антивирусные программы, установленные на офисных компьютерах, не были сертифицированы ФСТЭК России, журналы учета носителей информации не велись, ответственный за организацию работы с персональными данными в новосибирском филиале АНО «Сохнут» не был назначен, указывается в материалах проверки. Прокуратура составила несколько административных протоколов о нарушениях в сфере защиты персональных данных.

В соответствии с подпунктом «в» пункта 21 «Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных» (далее – **Правила контроля**), утвержденных Постановлением Правительства Российской Федерации от 13.02.2019 № 146, вступивших в силу 23 февраля 2019 года, должностные лица при осуществлении государственного контроля и надзора вправе выдавать по итогам проведения проверки **предписание об устранении выявленных нарушений**.

Основная проблема, возникающая при выявлении у оператора нарушений требований законодательства РФ о персональных данных, заключается в том, что такое нарушение обязательно связано с выдачей предписания об устранении выявленного нарушения и устранении причин и условий, способствовавших совершению нарушения.

Статья 19.5 КоАП РФ вводит ответственность за невыполнение в срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль), муниципальный

контроль, об устранении нарушений законодательства РФ, что влечет наложение административного штрафа на граждан в размере от 300 до 500 рублей; на должностных лиц - от 1 000 до 2 000 рублей или дисквалификацию на срок до 3-х лет; на юридических лиц - от 10 000 до 20 000 рублей.

Статья 19.6 КоАП РФ предусматривает привлечение к административной ответственности за непринятие по постановлению (представлению) органа (должностного лица), рассмотревшего дело об административном правонарушении, мер по устранению причин и условий, способствовавших совершению административного правонарушения, и влечет наложение административного штрафа на должностных лиц в размере от 4 000 до 5 000 рублей.

Устранение нарушения и причин его возникновения будет контролироваться надзорным органом вплоть до полного выполнения выданного предписания в ходе внеплановых проверок, количество которых законодательством РФ не ограничивается, а частота определяется указанным в предписании сроком устранения выявленного нарушения.

Подпункт «ж» пункта 21 Правил контроля предусматривает, что должностные лица при осуществлении государственного контроля и надзора вправе по итогам проведения проверки или мероприятия по контролю без взаимодействия с операторами принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований, а подпункт «з» того же пункта наделяет должностных лиц Роскомнадзора правом требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных по итогам проведения мероприятия по контролю без взаимодействия с оператором.

Порядок принятия мер по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением закона, а также оспаривания этого требования нормативными правовыми актами не определен, хотя реализация данного права надзорного органа может быть обеспечена путем выдачи предписания об устранении нарушения.

Исполнителю не известно о случаях применения на практике надзорным органом таких мер, как выдвижение требования о приостановлении или прекращении обработки персональных данных, а также об уточнении, блокировании или уничтожении недостоверных или полученных незаконным путем персональных данных.

Предписание должно быть выполнено, а нарушения устранены в установленный надзорным органом срок, не превышающий 6 месяцев с даты выявления нарушения.

Невыполнение в срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль), в соответствии со статьей 19.5 КоАП РФ влечет наложение административного штрафа на должностных лиц – от 1 000 до 2 000 рублей или **дисквалификацию на срок до трех лет**; на юридических лиц - от 10 000 до 20 000 рублей.

Как отмечалось в разделе 4 Экспертного заключения, с 1 сентября 2015 года действуют положения Закона о персональных данных и Федерального закона 149-ФЗ, в соответствии с которыми **доступ к информации в сети Интернет, обрабатываемой с нарушением законодательства в области персональных**

данных, может быть ограничен на основании вступившего в законную силу судебного акта. С этой целью Роскомнадзором создан «Реестр нарушителей прав субъектов персональных данных», сведения из которого выгружаются российскими операторами связи (интернет-сервис провайдерами) для блокирования на территории Российской Федерации доступа к сайтам, включенным в Реестр.

5.8.1. Правоприменительная и судебная практика, связанная с выполнением требования законодательства о локализации персональных данных

Проверки, проводимые территориальными управлениями Роскомнадзора, выявляют редкие единичные случаи нарушения требований законодательства, предусматривающих локализацию персональных данных граждан России в период их сбора в базах данных на территории Российской Федерации.

Данные нарушения не упоминаются в Результатах анализа сведений о выполнении мероприятий плана деятельности Роскомнадзора (Сведениях о результатах деятельности Роскомнадзора), ежеквартально публикуемых на сайте Роскомнадзора (https://rkn.gov.ru/plan-and-reports/reports/p449/) и ежегодных Публичных докладах ведомства (https://rkn.gov.ru/press/annual_reports/).

За период времени после 1 сентября 2015 года – даты вступления в силу части 5 статьи 18 Закона о персональных данных – только в 2017 году Управление Роскомнадзора по ЦФО в «Отчете о результатах деятельности Управления…» единственный раз упомянуло, что при проверке операторов на соответствие требований части 5 статьи 18 Закона о персональных данных был выявлен факт нарушения указанной нормы Централизованной религиозной организацией «Религиозная Ассоциация Церкви Иисуса Христа Святых последних дней в России», база данных которой располагалась на территории США в г. Прово (https://77.rkn.gov.ru/p23422/p23490/p24610/).

В этом же 2017 году Управлением было проведено 36 плановых и 8 внеплановых проверок выполнения законодательства о персональных данных, в том числе проверялась деятельность таких операторов, как ПАО «Сбербанк России», ООО «Хоум Кредит энд Финанс Банк», АО «КИВИ», ООО «ЛГ «Электроникс РУС», ПАО «Мегафон», ООО «Мобильные ТелеСистемы», ООО «Пфайзер», ООО «ДаВиза», ООО «ГЕТТАКСИ РУС», ЗАО «Делойт и Туш СНГ», ЗАО «ПрайсвотерхаусКуперс Аудит», АО «КПМГ», которые широко и активно используют облачные сервисы в своей деятельности. Ни у одного из них нарушений, связанных с требованием о локализации баз персональных данных в период их сбора, выявлено не было.

В «Информации о результатах анализа сведений о выполнении в 1 квартале мероприятий плана деятельности Роскомнадзора в 2017 году» (https://rkn.gov.ru/plan-and-reports/reports/p449/) отмечается, что в Реестр операторов персональных данных включены 12 операторов в ЦФО, указавшие базы данных вне пределов РФ, к которым необходимо применять меры по выполнению части 5 статьи 18 Закона о персональных данных, однако о наличии каких-либо нарушений у данных операторов не сообщается.

26 сентября 2019 года на официальном сайте Роскомнадзора размещен пресс-релиз «Три иностранные компании проверены на локализацию баз данных россиян на территории РФ», в котором сообщается, что Роскомнадзор завершил плановые

проверки российских представительств иностранных компаний Mercedes-Benz, Sony и Huawei по соблюдению законодательства о персональных данных. В ходе проверок подтвердился факт того, что **все три указанные компании локализовали базы с персональными данными российских граждан на территории России**. Результаты проверок показали, что российские представительства указанных иностранных компаний стремятся соблюдать требования российского законодательства о персональных данных. В отдельных случаях сотрудники Роскомнадзора выявили нарушения условий обработки и уничтожения персональных данных, а также факты использования согласий граждан, не соответствующих установленным требованиям.

Исполнителю неизвестны случаи выдвижения претензий Роскомнадзором к операторам персональных данных в ходе осуществления мероприятий контроля и надзора за соблюдением требований законодательства Российской Федерации о персональных данных в случае использования интернет-сервиса Microsoft Office 365, в то время, как его использование является повсеместным и распространенным.

При рассмотрении Арбитражным судом г. Москвы и Девятым арбитражным апелляционным судом исков ООО «Скартел» о признании недействительными и отмене предписаний Управления Роскомнадзора по ЦФО, выданных по результатом плановой и внеплановой проверок (см., например, http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=MARB009;n=1066376#04782473183458438), суды отмечали, что ООО «Скартел» осуществляется трансграничная передача персональных данных своих работников на территорию Нидерландов в рамках использования облачного сервиса компании Microsoft Office 365, в том числе корпоративной социальной сети Yammer. Никаких претензий и требований ни Роскомнадзором, ни судами по этом поводу не выдвигалось, за исключением требования получить согласие работников в письменной форме на передачу их персональных данных в корпоративную социальную сеть Yammer в порядке, установленном статьей 8 Закона «О персональных данных», поскольку и Роскомнадзор, и суды посчитали Yammer общедоступным источником персональных данных. Исполнитель полагает такую квалификацию корпоративной сети Yammer ошибочной. Кроме того, согласие работников на размещение данных в системе Yammer было работодателем получено, но не соответствовало требованиям части 4 статьи 9 Закона о персональных данных. Данная претензия не была связана с локализацией персональных данных.

5.8.2. Выдвижение требований о локализации персональных данных граждан РФ к иностранным компаниям, не присутствующим на территории России

Летом 2016 года Роскомнадзор обратился в Таганский районный суд г. Москвы с исковым заявлением к LinkedIn Corporation о признании деятельность интернет-ресурсов (http://www.linkedin.com, http://linkedin.com) по сбору, использованию и хранению персональных данных граждан Российской Федерации нарушающей требования Закона «О персональных данных» и права граждан на неприкосновенность частной жизни, личную и семейную тайну.

В исковом заявлении указывается, что в сети Интернет было выявлено нарушение интернет-сайтом, расположенным по адресам: http://www.linkedin.com, http://linkedin.com прав и законных интересов граждан Российской Федерации, как

субъектов персональных данных, посредством сбора информации о пользователях интернет-ресурса, а также гражданах Российской Федерации, не являющихся пользователями интернет-ресурса, её использование и передачу, в том числе посредством указанного сайта, без соответствующего согласия а также с нарушением требований законодательства Российской Федерации в области персональных данных, что является нарушением части 1 статьи 6 и части 5 статьи 18 Закона «О персональных данных».

Поскольку законодательством Российской Федерации в области персональных данных установлено обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требований, предусмотренных Законом о персональных данных, при таких обстоятельствах суд пришел к выводу, что ответчиком, являющимся администратором доменного имени linkedin.com, обрабатывающим персональные данные граждан в сети Интернет, допущено нарушение прав и свобод человека и гражданина при обработке его персональных данных, в том числе право на неприкосновенность его частной жизни, личную и семейную тайну.

Деятельность интернет-ресурсов http://www.linkedin.com, http://linkedin.com была признана незаконной, и суд обязал Роскомнадзор принять меры по ограничению доступа к информации в сети Интернет, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, путем внесения доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в Интернет, в Реестр нарушителей прав субъектов персональных данных.

LinkedIn Corporation обратилась с апелляционной жалобой на решение суда первой инстанции. 10 ноября 2016 года Судебная коллегия по гражданским делам Московского городского суда, рассматривая дело № 33-38783/16, определила решение Таганского районного суда г. Москвы от 04 августа 2016 года оставить без изменения, апелляционную жалобу и дополнения представителя ответчика LinkedIn Corporation – без удовлетворения.

Довод апелляционной жалобы о том, что нарушение прав субъектов персональных данных не доказано, польку данных о наличии жалоб граждан РФ в связи с деятельностью спорного интернет-сайта не представлено, не является основанием к отмене судебного решения.

Предметом спорных отношений является деятельность по сбору персональных данных граждан Российской Федерации и обязанность оператора, собирающего персональные данные, в том числе посредством сети Интернет, обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации.

В соответствии со ст. 15.5 Закона № 149-ФЗ, нарушение правила сбора в сети Интернет персональных данных субъектов влечет применение соответствующей меры воздействия, в том числе ограничение доступа к соответствующей информации.

После многочисленных обращений Роскомнадзора к социальным сетям Твиттер и Фейсбук, в том числе путем проведения рабочих встреч и направления официальных запросов, Управление Роскомнадзора по ЦФО возбудило дело об административном правонарушении, предусмотренном статьей 19.7 КоАП РФ:

непредставление в орган (должностному лицу), осуществляющий государственный контроль, сведений, представление которых предусмотрено законом и необходимо для осуществления этим органом его законной деятельности.

Мировой судья судебного участка № 422 Таганского района г. Москвы Козырев А.И., 5 апреля 2019 года рассмотрел дело № 5-618/19 в отношении компании Твиттер Инк. (Twitter Inc.) и постановил признать иностранное юридическое лицо виновным в совершении административного правонарушения, предусмотренного ст. 19.7 КоАП РФ и назначить ему наказание в виде штрафа в размере 3 000 рублей.

В мотивировочной части постановления отмечается, что Твиттер Инк. (Twitter Inc.), не имеющее регистрации на территории Российской Федерации, в нарушение части 4 статьи 20 Закона о персональных данных не представило в Роскомнадзор сведения (информацию), представление которых предусмотрено законом и необходимо для осуществления этим органом его законной деятельности, а именно информацию о результатах принятых указанной компанией мер по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения персональных данных российских пользователей социальной сети Twitter с использованием баз данных, находящихся на территории Российской Федерации, в том числе: заверенную блок-схему размещения рабочих мест, на которых осуществляется хранение персональных данных российских пользователей; справку о постановке на балансовый учёт организации приобретенных серверных мощностей; договор купли-продажи серверных мощностей; в случае аренды технических площадок (ЦОД, серверные мощности) на территории Российской Федерации необходимо было представить копию договора аренды, заключенного с компанией, представляющей соответствующие услуги.

Таким образом, своими бездействиями Твиттер Инк. (Twitter Inc.) 17 января 2019 года совершило административное правонарушение, предусмотренное ст. 19.7 КоАП РФ.

17 января 2019 года компания Твиттер Инк. ответила на письмо от 17 декабря 2018 года, дополнительно сообщив, что для детального ответа на запрос им нужно время и информация будет представлена, при этом запрашиваемая информация и указанные документы представлены не были, и не представлены на день проведения судебного заседания, что подтверждает нежелание компании Твиттер Инк. предоставлять данную информацию, и неисполнение требований законодательства по локализации баз данных.

Перед тем, как направить письмо в Твиттер от 17 декабря 2018 года, сотрудниками Роскомнадзора был проведен анализ локальных актов, размещенных на сайте Твиттер.ком, а также информации, размещенной в общедоступных источниках. После проведенного анализа информации, размещенной на сайте, была составлена докладная записка на имя ВРИО заместителя руководителя Роскомнадзора и было выявлено, что посредством сайта Твиттер.ком осуществляется сбор персональных данных, а также сведения из общедоступных источников показывали информацию, что серверные мощности находятся на территории США. При анализе локальных актов оператора Твиттер Инк. не скрывал, что использует серверные мощности, размещенные на территории США, Евросоюза и других стран, где находятся его подразделения.

По мнению мирового судьи, отраженном в постановлении, осуществляя обработку персональных данных, оператор, в том числе, иностранное юридическое лицо, независимо от места нахождения и осуществления деятельности, обязано по

запросу уполномоченного органа – Роскомнадзора представить документы и локальные акты или иным образом подтвердить принятие мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

Решением судьи Таганского районного суда г. Москвы Смолина Ю.М., рассмотревшего 8 мая 2019 года дело № 12-0513/2019 по жалобе защитника компании Твиттер Инк. (Twitter Inc.) на постановление мирового судьи судебного участка № 422, постановление мирового судьи оставлено без изменения, а жалоба – без удовлетворения.

В решение отмечается, что судья соглашается с выводами мирового судьи о том, что о направленности Интернет-сайта www.twitter.com на Россию свидетельствует наличие русскоязычной версии указанного Интернет-сайта. При этом использование социальной сети Twitter предполагает обработку сведений, предоставляемых российскими пользователями, которым в обязательном порядке для регистрации на указанном Интернет-ресурсе необходимо предоставить имя пользователя, пароль, адрес электронной почты или номер телефона, что дополнительно свидетельствует о включении российской аудитории в пользование вышеуказанным Интернет-ресурсом.

При этом судья учитывает, что помимо вышеуказанных сведения, предоставление которых в обязательном порядке необходимо при регистрации в социальной сети Twitter, используя сервисы Twitter, зарегистрированные пользователи могут дополнять свои учетные записи сведениями из биографии (включая дату рождения), о местонахождении, фотографическими изображениями, загрузить и синхронизировать список контактов, также использование отдельных сервисов Twitter предполагает предоставление доступа к платежным средствам пользователей (номер кредитной или дебетовой карты, срок действия карты, код CVV, адрес биллинга, адрес доставки товара), администрация сайта может, в том числе, получать и обрабатывать метаданные, сведения о стране и языке, информацию о беспроводных сетях или вышках мобильной связи вблизи от мобильного устройства, или IP-адрес, в связи с чем в соответствии с частью 1 статьи 3 Закона о персональных данных вышеуказанные сведения являются персональными данными.

При таких обстоятельствах, совершая вышеуказанные действия с предоставляемыми пользователями данными, компания Твиттер Инк. является оператором, осуществляющим обработку персональных данных граждан Российской Федерации, на которого распространяются требования части 5 статьи 18 Закона о персональных данных.

Постановлением Московского городского суда от 09.07.2019 № 4а-4186/2019 постановление мирового судьи судебного участка № 422 Таганского района города Москвы от 05.04.2019 и решение судьи Таганского районного суда города Москвы от 08.05.2019 по делу об административном правонарушении по ст. 19.7 КоАП РФ в отношении компании Твиттер Инк. оставлено без изменения, жалоба защитника компании Твиттер Инк. – без удовлетворения.

Верховный суд Российской Федерации в Постановлении от 27.12.2019 № 5-АД19-239 согласился с решениями судов нижестоящих инстанций.

Аналогичное решение было принято судьей мирового участка № 422 Козыревым А.И. в отношении компании Facebook, которая также была оштрафована на 3 000 рублей по основаниям, предусмотренным статьей 19.7 КоАП РФ.

Необходимо иметь в виду, что в отношении российских операторов суды занимают иную позицию.

Арбитражный суд Астраханской области 26 августа 2016 года принял решение по делу № А06-5241/2016 по заявлению администрации муниципального образования «Город Астрахань» к Управлению Роскомнадзора по Астраханской области о признании незаконными акта от 28.04.2016 N А-30/2/42-нд/38 и предписания от 28.04.2016 N П-30/2/42-нд/-/1/1. Среди выявленных нарушений отмечалось отсутствие документов, подтверждающих размещение баз персональных данных на технических площадках (ЦОД, сервера), информационных систем, находящихся на территории Российской Федерации.

Решением суда первой инстанции заявленные требования удовлетворены частично.

Суд признал недействительными акт проверки и предписание в части выводов о совершении Администрацией муниципального образования «Город Астрахань» следующих нарушений, в том числе – части 5 статьи 18 Закона о персональных данных.

Управление Роскомнадзора по Астраханской области не согласилось с принятым решением и обратилось в Двенадцатый арбитражный апелляционный суд с жалобой, в которой просит решение суда первой инстанции отменить, в удовлетворении заявленных Администрацией требований отказать.

Арбитражный суд апелляционной инстанции в удовлетворении жалобы надзорному органу отказал и отметил, что наличие каких-либо документов, подтверждающих нахождение баз персональных данных на технических площадках на территории Российской Федерации, законодательством не предусмотрено. Требование административного органа о необходимости подтверждения места нахождения баз данных соответствующими документами (приказы, блок-схемы), утвержденными главой администрации, выходит за рамки положений закона. Форма таких документов нормативно не установлена, в связи с чем суд апелляционной инстанции соглашается с выводом Арбитражного суда Астраханской области, что указанного в акте проверки нарушения части 5 статьи 18 Закона о персональных данных не имеется, довод административного органа о наличии нарушения названной нормы, является необоснованным.

31 января 2020 года Роскомнадзор после многократных игнорирований требований ведомства к компаниям Facebook и Twitter о локализации баз персональных данных российских граждан в период их сбора на территории Российской Федерации возбудил два первых административных производства по принятой в декабря 2019 года новой части 8 статьи 13.11 КоАП РФ, предусматривающей ответственность за невыполнение оператором при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации в виде штрафа на юридическое лицо от 1 до 6 миллионов рублей.

13 февраля 2020 года мировой судья судебного участка мировых судей № 374 Таганского районного суда Александра Михалева оштрафовала компании Facebook Inc. и Twitter Inc. за отказ выполнить требования о локализации баз данных российских пользователей на 4 миллиона рублей каждую.

В ходе судебных разбирательств было установлено, что по данным, размещенным на сайтах www.facebook.com и www.twitter.com, деятельность сайтов предусматривает сбор информации о пользователях социальных сетей Facebook и Twitter, гражданах Российской Федерации и предполагает обработку личной информации, предоставляемой российскими пользователями в учетных данных.

Сам интернет-сайт размещен на технических площадках, находящихся на территории США, что подтверждается данными сервиса whois.

Указанный факт свидетельствует о том, что личные данные российских пользователей социальных сетей Facebook и Twitter обрабатываются с использованием баз данных, находящихся на территории США.

Достоверных данных, свидетельствующих о выполнении Фейсбук, Инк. (Facebook, Ink.) и Твиттер Инк. (Twitter Inc.) обязанности по обеспечению локализации баз данных российских пользователей социальных сетей на территории Российской Федерации материалы дел не содержат, учитывая также, что Роскомнадзор неоднократно напоминал о необходимости соблюдения вышеуказанных требований закона.

16 марта Twitter попытался оспорить штраф в суде, но Таганский суд оставил решение нижестоящей инстанции в силе.

5.8.3. По информации агентства «Интерфакс», представитель Роскомнадзора Елена Прохорова заявила, что КоАП допускает штраф до 18 млн руб. за повторное нарушение юридическими лицами. Сам факт уплаты текущего штрафа в 4 млн руб. не будет означать исполнения требований Роскомнадзора: ведомство заявило, что оно «вправе провести мероприятие по контролю без взаимодействия с оператором в любое время».***Оспаривание операторами актов проверок и предписаний об устранении нарушений***

Попытки операторов оспорить полностью или частично полученное предписание об устранении нарушения в суде заканчиваются, как правило, отказом в удовлетворении такого требования (см. четыре судебных акта об оспаривании ООО «Скартел» предписания Управления Роскомнадзора по ЦФО в 2016 году (например, Постановление Девятого арбитражного апелляционного суда от 02.08.2016 № 09АП-30590/2016 по делу № А40-32030/16), Постановление Арбитражного суда Московского округа от 15.01.2018 г. по делу № А40-81171/17-149-793 об оспаривании ООО «Суп Медиа» предписания Управления Роскомнадзора по ЦФО, Решение Арбитражного суда города Москвы от 21.03.2018 по делу № А40-7530/18-139-40 об оспаривании ООО «Пфайзер» предписания Управления Роскомнадзора по ЦФО и другие).

Исполнителю известен только один случай удовлетворения судами требований оператора о признании акта проверки и предписания об устранении нарушения в полном объеме (оспаривание ООО «Макдоналдс» акта и предписания Управления Роскомнадзора по ЦФО, Апелляционное определение Московского городского суда

от 18.09.2017 по делу № 33а-4308/2017). Однако Роскомнадзор после решения суда направил материалы в прокуратуру. Замоскворецкая межрайонная прокуратура г. Москвы провела проверку ООО «Макдоналдс». В выданном Замоскворецким межрайонным прокурором г. Москвы представлении № 07-04-2016 от 04.08.2016 были указаны те же нарушения, что в акте проверки и предписании Управления Роскомнадзора по ЦФО, однако Замоскворецким районным судом г. Москвы в первой инстанции и Московским городским судом в апелляционной инстанции ООО «Макдоналдс» было отказано в удовлетворении требований о признании незаконным представления Замоскворецкого межрайонного прокурора г. Москвы.

5.9. Как обеспечивается безопасность персональных данных, обрабатываемых в облачной платформе Microsoft Azure и облачных сервисах

В соответствии с частью 1 статьи 19 Закона о персональных данных, оператор при обработке персональных данных, обязан принимать необходимые правовые, организационные и технические меры **или обеспечивать их принятие** для защиты персональных данных **от неправомерного или случайного доступа к ним**, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от **иных неправомерных действий** в отношении персональных данных.

Часть 2 той же статьи конкретизирует эти требования, устанавливая, что обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

«Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства Российской Федерации от 01.11.2012 № 1119, предусматривают в зависимости от установленного уровнях защищенности 9 групп мер, приведенных в таблице 3.

Таблица 3

Требования	Уровни защищенности			
	1	2	3	4
Организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения	+	+	+	+
Обеспечение сохранности носителей персональных данных	+	+	+	+
Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей	+	+	+	+
Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз	+	+	+	+
Назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе	+	+	+	-
Ограничение доступа к содержанию электронного журнала сообщений, предоставление такого доступа исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей	+	+	-	-
Автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе	+	-	-	-

Создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности	+	-	-	-

Для обеспечения безопасности персональных данных, обрабатываемых в облачной платформе Microsoft Azure и других облачных сервисах, используются следующие меры безопасности, адекватные предусмотренным нормативными правовыми актами Российской Федерации.

Для предотвращения неправомерного или случайного доступа к обрабатываемым данным заказчиков, несанкционированного уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также иных неправомерных действий в отношении персональных данных, **обеспечивается безопасное изолированное размещение данных клиентов**. Хранение и обработка данных каждого клиента осуществляется раздельно с помощью службы сетевых каталогов Active Directory и других средств, разработанных для создания, контроля и обеспечения безопасности многопользовательских сред. Такой подход не позволяет одним клиентам получить доступ к данным других клиентов или поставить под угрозу безопасность этой информации.

Правилами доступа к данным, обрабатываемым в облачной платформе и облачных сервисах, гарантируется защита информации от несанкционированного доступа и обеспечивается сохранность носителей обрабатываемых данных. Персоналу дата-центров предоставляется доступ в помещения, где ведется обработка данных заказчиков, только для выполнения рабочих задач, при этом круг лиц, имеющих такой доступ, ограничен. Контроль физического доступа осуществляется посредством многочисленных процедур аутентификации и обеспечения безопасности, в том числе с использованием смарт-карт, биометрических сканеров, двухфакторной идентификации. Дата-центры оборудованы датчиками движения, системами видеонаблюдения и сигнализации. Предусмотрена инвентаризация всех машинных носителей, на которых хранятся данные клиента.

Доступ персонала к данным клиентов, обрабатываемым в облачной платформе и облачных сервисах, контролируется посредством управления доступом на основе ролей (RBAC) и процессов блокировки, предусматривающими разделение обязанностей и предоставление наименьших привилегий пользователю системы. Доступ к данным клиентов получает только инженер, отвечающий определенным требованиям: его личные данные прошли проверку, отпечатки пальцев совпадают с отпечатками, хранящимися в системе, он прошел обучение по обеспечению безопасности и получил соответствующие допуски. Запрос инженера на выполнение определенных задач попадает в процесс блокировки, который определяет продолжительность и уровень доступа.

Сети дата-центров сегментированы и обеспечивают физическое разделение критически важных внутренних серверов и устройств хранения от общедоступных интерфейсов. Средства безопасности пограничных маршрутизаторов выявляют попытки вторжения и признаки уязвимости системы. Подключение клиентов к облачной платформе и к облачным сервисам происходит по протоколу TLS/SSL,

Microsoft шифрует или разрешает клиенту шифровать его данные, передаваемые по общедоступным сетям связи.

Облачная платформа и облачные сервисы предоставляет клиентам модель безопасности, обеспечивающую целостность и конфиденциальность данных, а также поддерживает эффективный доступ к данным и совместную работу на основании ролевой модели доступа пользователей. Пользователям может предоставляться доступ только к информации, необходимой для выполнения своих задач. С этой целью пользователи категорируются по ролям и им устанавливается и ограничивается доступ в соответствии с этими ролями, включающими в себя набор предопределенных ролей безопасности. Каждая из них объединяет набор прав пользователей для упрощения управления безопасностью. Кроме того, развертываемое в облаке приложение может определять собственные роли для удовлетворения потребностей разных пользователей.

Безопасность на уровне записей в информационных системах и системах управления базами данных, предоставляемыми по модели SaaS, позволяет разграничивать права доступа к определенным записям, безопасность на уровне полей в них позволяет разграничивать доступ к конкретным областям данных между пользователями и группами пользователей.

В облачной платформе и облачных сервисах используются средства защиты от вредоносного программного обеспечения и антивирусное сканирование.

Защита системы от внешних вторжений строится как превентивная, предусматривающая прогнозирование и проактивную защиту. В ее рамках предусмотрено сканирование портов и устранение обнаруженных проблем, выявления уязвимостей периметра, обновления операционной системы для установки актуальных версий средств обеспечения безопасности, обнаружение и предотвращение распределенных атак типа «отказ в обслуживании» (Distributed Denial of Service, DDOS), а также многофакторная аутентификация при предоставлении доступа к службе. Процесс превентивной защиты предполагает пересмотр допусков и действий оператора или администратора и затрагивает как персонал, так и процедуры допуска к выполнению необходимых работ.

Превентивная защита предусматривает автоматическое удаление учетных записей уволенных сотрудников дата-центров. Там, где это возможно, вмешательство человека заменяется автоматическим процессом, выполняемым специальным инструментом; речь идет о таких рутинных операциях, как развертывание, отладка, сбор данных диагностики и перезапуск служб. Используются системы, позволяющие выявлять аномальное и подозрительное поведение и немедленно реагировать на него с целью устранения риска безопасности. Проводятся тесты на защиту от несанкционированного доступа с целью улучшения процедур реагирования на инциденты.

В целях обеспечения регистрации и учета действий, совершаемых с обрабатываемыми данными в облачной платформе и облачных сервисах, запросы персонала дата-центра регистрируются в журнале как запросы на обслуживание, которые впоследствии подвергаются проверке.

Microsoft протоколирует или разрешает клиенту протоколировать данные о доступе и использовании информационных систем, содержащих данные клиента, регистрируя идентификатор доступа, время, авторизацию и соответствующие действия. Используемые политики аудита дают клиентам возможность

регистрировать в электронных журналах такие события, как просмотр, изменение и удаление содержимого электронных сообщений и документов. При включении аудита в состав политики управления информацией администраторы могут получать данные аудита и обобщать использование информации. С помощью этих отчетов можно определить, как используется информация, управлять соответствием нормативным требованиям и анализировать проблемные области.

Microsoft хранит записи о входящих и исходящих носителях, содержащих данные клиента, в том числе сведения о типе носителя, данные об уполномоченных отправителях и получателях, дату и время, количество носителей и типы содержащихся на них данных клиента.

С целью обеспечения возможности восстановления данных клиентов, модифицированных или уничтоженных вследствие несанкционированного доступа к ним, предусмотрены соответствующие процедуры, в частности:

- на постоянной основе, но не реже одного раза в неделю (за исключением случаев, когда в течение этого периода данные клиента не обновлялись) создается несколько копий данных клиента, по которым их можно восстановить;
- копии данных клиента и процедуры восстановления данных хранятся в разных местах, не на основном компьютерном оборудовании, на котором производится обработка данных клиента;
- определяются конкретные процедуры на местах, регламентирующие доступ к копиям данных клиента;
- процедуры восстановления данных пересматриваются каждые шесть месяцев;
- регистрируются попытки восстановления данных, в том числе ответственными лицами, описание восстановленных данных и, если применимо, ответственное лицо, а также какие данные (если таковые имеются) были введены вручную в процессе восстановления данных.

Для обеспечения выполнения требования об осуществлении контроля за принимаемыми мерами по обеспечению безопасности обрабатываемых данных регулярно анализируются процессы управления рисками, используется поддерживаемая в актуальном состоянии структура управления безопасностью, проводятся внутренние проверки и внешние аудиты с привлечением сторонних организаций. Контролируется выполнение требований, содержащихся в нормативных правовых актах, промышленных нормах и стандартах, внутренних политиках и передовых отраслевых практиках. Ведется постоянный анализ новых требований, соответствие которым необходимо обеспечивать, с последующим внедрением соответствующих служебных процессов.

Краткие выводы по разделу 5.9

В облачной платформе Azure и облачных сервисах, предоставляемых корпорацией Microsoft, реализованы все основные требования к обеспечению безопасности обрабатываемых персональных данных, предусмотренные нормативными правовыми актами Российской Федерации, за исключением требования об использовании для нейтрализации актуальных угроз средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства

Российской Федерации в области обеспечения безопасности информации, которое не применимо к вычислительным инфраструктурам и информационным системам, принадлежащих иностранным лицам и находящимся за пределами Российской Федерации.