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

Экспертное заключение о возможности использования платформы Microsoft Azure для размещения информационных систем российских операторов, обрабатывающих персональные данные, и содержании основных мероприятий, необходимых для достижения соответствия требованиям российского законодательства в сфере персональных данных

наименование документа

Москва 2014

Оглавление

1. Предмет заключения

Российское законодательство в сфере персональных данных практически не затрагивает вопросы размещения информационных систем персональных данных на вычислительных мощностях, не принадлежащих оператору персональных данных – в коммерческих центрах обработки данных (дата-центрах), в облачной инфраструктуре, в частности, в приватных облаках, одновременно используемых несколькими операторами, в публичных и гибридных облаках. Не раскрыты детально и вопросы размещения информационных систем персональных данных на вычислительной инфраструктуре, находящейся за пределами Российской Федерации, в государствах, как обеспечивающих адекватную защиту прав субъектов персональных данных, так и не удовлетворяющих данному требованию.

В связи с этим в Консалтинговое агентство «Емельянников, Попова и партнеры» поступил запрос от клиента **о возможности использования платформы Microsoft Azure для размещения информационных систем российских операторов, обрабатывающих персональные данные**, содержании основных мероприятий, необходимых для достижения соответствия требованиям российского законодательства в сфере персональных данных, распределении обязанностей и ответственности за выполнение требований законодательства в сфере персональных данных и обеспечение безопасности персональных данных между владельцем облачного сервиса Microsoft Azure, провайдерами облачных услуг и операторами персональных данных.

Запрос содержал следующие возможные сценарии размещения персональных данных в Microsoft Azure:

- в облако передаются **персональные данные, прошедшие процедуру обезличивания**; база данных, соотносящая обезличенные данные и конкретных субъектов, хранится непосредственно у оператора персональных данных и в облаке не размещается;
- в облаке хранятся персональные **данные только работников оператора**, у которых возможно получение согласия на размещение данных в облаке;
- персональные **данные хранятся в облаке в зашифрованном виде** и расшифровываются только на рабочих местах оператора (в России), при этом информация, не относящаяся к персональным данным, хранится в облаке в открытом (незашифрованном) виде (при возможности размещения облачной инфраструктуры только на территории государств Европейского союза, являющихся сторонами Конвенции Совета Европы ETS 108, и без возможности определения конкретной страны, где размещена инфраструктура или ее элементы);
- персональные **данные передаются и хранятся в облаке в открытом виде** (при возможности размещения облачной инфраструктуры только на территории государств Европейского союза, являющихся сторонами Конвенции Совета Европы ETS 108, и без возможности определения конкретной страны, где размещена инфраструктура или ее элементы);

- в облаке **размещаются виртуальные машины, где обрабатываются персональные данные;** к виртуальным машинам подключаются пользователи оператора (при возможности размещения облачной инфраструктуры только на территории государств Европейского союза, являющихся сторонами Конвенции Совета Европы ETS 108, и без возможности определения конкретной страны, где размещена инфраструктура или ее элементы).

Вопрос о допустимости использования платформы Microsoft Azure для размещения информационных систем российских операторов, обрабатывающих персональные данные, и о содержании основных мероприятий, необходимых для достижения соответствия требованиям российского законодательства в сфере персональных данных необходимо рассматривать с учетом следующих факторов:

- цели принятия и содержание Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28.01.1981 ETS № 108 и последствия ее ратификации Российской Федерацией;
- применение международного законодательства в Российской Федерации;
- ограничения, устанавливаемые российским законодательством на передачу персональных данных третьим лицам, привлечение их к обработке персональных данных и требования, которые выдвигаются при таком привлечении.

Одним из важнейших является вопрос о том, **следует ли рассматривать размещение** информационных систем персональных данных в облачной инфраструктуре **поручением на обработку персональных данных**, даваемым оператором провайдеру инфраструктуры или нет, и каковы факторы, влияющие на содержание ответа на данный вопрос.

Предметом настоящего заключения (далее – Экспертное заключение) является **оценка допустимости использования платформы Microsoft Azure для размещения информационных систем российских операторов**, обрабатывающих персональные данные, определение состава и содержания основных мероприятий, необходимых для достижения соответствия требованиям российского законодательства в сфере персональных данных при переносе информационных систем персональных данных в Microsoft Azure, и существенных условий договора между владельцем облачной платформы, провайдером облачных услуг и оператором в части обработки персональных данных.

2. Краткие выводы по результатам рассмотрения вопросов, поставленных клиентом

Ратифицировав Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года ETS № 108, Россия стала стороной международного договора. В соответствии с частью 4 ст.15 Конституции Российской Федерации, общепризнанные принципы и нормы международного права и международные договоры Российской Федерации являются составной частью ее правовой системы. Если международным договором Российской Федерации установлены иные правила, чем предусмотренные законом, то применяются правила международного договора. В рассматриваемом случае такими правилами являются нормы, определяющие порядок трансграничной передачи персональных данных, установленные Конвенцией и рассмотренные в разделе 3 Экспертного заключения.

Часть 3 ст.6 закона «О персональных данных» определяет условия, которые должны выполняться при поручении оператором обработки персональных данных иным лицам. К важнейшим из них относятся два, предусматривающие обязательное наличие:

- согласия субъекта на передачу его персональных данных иному лицу для обработки, если иное не предусмотрено федеральным законом;
- договора с этим лицом, в том числе государственного или муниципального контракта, либо соответствующего акта, принятого государственным или муниципальным органом.

Форма получения согласия не указывается, следовательно, оно может даваться в любом виде, позволяющем оператору, давшему такое поручение, впоследствии доказать наличие согласия субъекта.

Таким образом, в случае поручения обработки персональных данных другому лицу получение согласия субъекта на такую передачу персональных данных является обязательным.

В то же время **нельзя рассматривать как поручение**, например, следующие варианты (примеры) размещения информационных систем персональных данных в дата-центрах и облачной инфраструктуре:

1) Развертывание информационных систем персональных данных на инфраструктуре третьего лица без права доступа персонала дата-центра (облачного сервиса) к этим данным.
2) Размещение персональных данных в зашифрованном виде.
3) Размещение персональных данных, прошедших процедуру обезличивания, когда они не могут быть соотнесены с конкретными субъектами, поскольку база данных, позволяющая установить связь между размещенными данными и субъектами, находится только у оператора и физически отсутствует в облачной инфраструктуре, предоставляемой для размещения информационной системы.

В этих случаях владельцу дата-центра (провайдеру облачного сервиса) персональные данные не передаются, цель обработки не устанавливается, а все действия с ними выполняет оператор персональных данных. Не требуется и согласие субъекта на такое размещение персональных данных в странах, обеспечивающих адекватную защиту прав субъектов персональных данных.

При этом при размещении персональных данных в дата-центре в зашифрованном виде шифрование должно осуществляться оператором в своей информационной системе (на своей территории) сертифицированными средствами криптографической защиты.

Учитывая, что в соответствии с частью 1 ст.9 закона «О персональных данных», субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе, а согласие на обработку персональных данных должно быть конкретным, информированным и сознательным, представляется, что **оператор**, осуществляющий или намеревающийся осуществлять трансграничную передачу персональных данных в дата-центры облачного сервиса Microsoft Azure, до получения персональных данных от субъекта **должен его проинформировать любым доступным способом о такой трансграничной передаче**, например, указав это в общедоступной политике в отношении обработки персональных данных, предусмотренной ст.18.1 закона «О персональных данных», в договоре с субъектом, в том числе – трудовом, публичном или в виде оферты и т.д.

Оператор должен проинформировать субъекта указанными выше способами о факте трансграничной передачи его персональных данных **с указанием государств, где данные могут размещаться**, обеспечении или необеспечении этими государствами адекватной российскому законодательству защиты прав субъектов персональных данных, возможных случаях получения доступа к персональным данным иных лиц, в том числе представителей государственных органов стран, где размещаются персональные данные, персонала дата-цента и/или сервис-провайдера, целях, в которых такой доступ может предоставляться, и способах обработки персональных данных такими лицами.

В дата-центре, находящемся за пределами Российской Федерации, вопросы выбора и использования конкретных средств защиты информации, обязательности наличия у них сертификатов или иных документов, подтверждающих соответствие тем или иным требованиям, определяются законодательством, действующим на территории той страны, где находится дата-центр, в котором размещаются персональные данные, или где находится их обработчик.

Рассмотрение требований федерального законодательства позволяет сделать **следующие выводы**:

- во всех случаях **передача персональных данных третьим** лицам требует получения согласия субъекта персональных данных в любой доказываемой форме;
- закон «О персональных данных» **не содержит запрета на трансграничную передачу персональных данных,** однако такая **передача в страны**, не обеспечивающие адекватной защиты прав субъектов персональных данных, оговаривается дополнительными условиями;

- конкретные **правила технической защиты** персональных данных, подвергаемых автоматизированной обработке, определяются законодательством той страны, на территории которой такая обработка ведется.

Предусмотренные сервисом Microsoft Azure меры по обеспечению информационной безопасности обрабатываемых в облаке данных в целом позволяют обеспечить реализацию требований, предъявляемых в части 2 ст.19 закона «О персональных данных», за исключением применения средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия и учета машинных носителей персональных данных, которые могут быть приняты только в отношении элементов вычислительной инфраструктуры, развернутой на стороне оператора (вне облачной платформы).

При размещении информационных систем персональных данных на облачной платформе **необходимо определить зоны ответственности** оператора, владельца облачной платформы и сервис-провайдера (при его наличии), а также принимаемые каждым из участников отношений меры по технической защите персональных данных, отразить распределение обязанностей в договоре о предоставлении облачных сервисов. Оператору необходимо самостоятельно определить, нейтрализацию каких актуальных угроз безопасности персональных данных он должен обеспечить в той части информационной системы персональных данных, за функционирование которой он отвечает, и принять меры по их нейтрализации за счет использования мер и средств защиты в соответствии с требованиями российских нормативных правовых актов.

В договоре между владельцем облачной платформы (сервис-провайдером облачных услуг) и оператором персональных данных (или приложениях к нему) **целесообразно указать**:

- требование об обеспечении конфиденциальности персональных данных, обрабатываемых на облачной платформе;
- возможность доступа персонала дата-центров и/или сервис-провайдера к обрабатываемым данным оператора, и, при наличии такой возможности, – цели, для достижения которых персонал получает доступ к данным, размещенным клиентом, а также случаи, когда такой доступ возможен, и способы обработки таких данных персоналом дата-центра (сервис-провайдера);
- состав и содержание мер по обеспечению безопасности персональных данных, принимаемых владельцем облачной платформы и сервис-провайдером (при его наличии);
- допустимые случаи предоставления доступа к обрабатываемым данным третьих лиц, в том числе представителей органов власти страны, где размещается дата-центр, и порядок информирования оператора о факте такого доступа;
- отсутствие необходимости получения владельцем облачной платформы и/или сервис-провайдера согласия субъекта на обработку персональных

данных и ответственности владельца платформы и/или сервис-провайдера перед субъектом персональных данных;

- ответственность владельца платформы и/или сервис-провайдера перед оператором за инциденты с обрабатываемыми данными.

Весьма желательным было бы включение в качестве приложения к договору описания угроз обрабатываемым данным, нейтрализация которых обеспечивается владельцем облачной платформы и/или сервис-провайдером (при его наличии).

При соблюдении описанных в Экспертном заключении условий **размещение персональных данных** российскими операторами **на облачной платформе Microsoft Azure** представляется **допустимым и соответствующим закону**.

3. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года ETS № 108

Основные причины принятия Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года ETS №108 (далее – Конвенция) определены в преамбуле документа (здесь и далее будет использоваться перевод Конвенции на русский язык, размещенный на портале «Персональные данные» официального сайта Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора) по адресу http://pd.rkn.gov.ru/law/p131/document170.htm?print=1):

- необходимость усиления гарантий прав и основных свобод каждого человека и в особенности права на неприкосновенность его этичной сферы, вызванную все возрастающим перемещением через границы персональных данных, обработанных с применением автоматизированных средств;
- необходимость совмещения таких фундаментальных ценностей, как неприкосновенность личной сферы и свободный обмен информацией между народами независимо от границ.

Таким образом, при принятии Конвенции ставилась не задача ограничения движения персональных данных между государствами, а создание на территории стран, присоединившихся к Конвенции, условий, обеспечивающих уважение прав и основных свобод каждого человека независимо от его гражданства или места жительства и, в первую очередь – его права на неприкосновенность личной жизни.

Изначально вопрос о подготовке и принятии Конвенции был связан с бурным развитием компьютерных технологий и резким увеличением количества автоматизированных систем, где обрабатываются данные о гражданах, а также ростом объемов обмена информацией между такими системами.

8 ноября 2001 г. в Страсбурге был принят Дополнительный протокол к Конвенции о защите частных лиц в отношении автоматизированной обработки данных

личного характера, о наблюдательных органах и трансграничной передаче информации ETS № 181, определивший дополнительные условия, которые должны выполняться при трансграничной передаче персональных данных получателям, находящимся в странах, не являющихся сторонами Конвенции, и в которых соответствующие нормы права, установленные Конвенцией, не действуют. Однако к настоящему моменту Россия Дополнительный протокол не ратифицировала.

Европейский Парламент и Совет Европейского Союза в развитие Конвенции **приняли ряд директив**, в частности:

- от 24 октября 1995 г. № 95/46/ЕС о защите физических лиц при обработке персональных данных и **о свободном обращении таких данных** и других документов Евросоюза, регламентирующих обработку персональных данных;
- от 7 марта 2002 г. № 2002/22/ЕС **об универсальных услугах** и правах пользователей в отношении сетей электронных коммуникаций и услуг;
- от 12 июля 2002 г. № 2002/58/ЕС **в отношении обработки** персональных данных и защиты конфиденциальности в секторе электронных средств связи.

Хотя нормы этих документов не распространяются на Российскую Федерацию, некоторые подходы, применяемые в них, рассмотреть весьма полезно с точки зрения оценки позиций, используемых при регулировании отдельных вопросов применения законодательства о персональных данных, в частности, их трансграничной передачи, предоставления третьим лицам и поручения их обработки.

Рассматривая нормы Конвенции, регламентирующие трансграничную передачу персональных данных, необходимо обратить особое внимание на пункт 2 статьи 12, которая прямо устанавливает, что **сторона Конвенции не будет запрещать** или ставить под специальный контроль информационные потоки персональных данных, идущие на территорию другой Стороны, исходя исключительно из соображений защиты неприкосновенности личной сферы. Таким образом, вопросы обеспечения конфиденциальности не могут служить причиной установления запретов на трансграничную передачу персональных данных в страны, присоединившиеся к Конвенции, поскольку во всех этих странах действуют идентичные нормы права, изначально обеспечивающие соблюдение прав и законных интересов субъектов персональных данных, неприкосновенность частной жизни.

Пункт 3 той же статьи допускает, что сторона Конвенции вправе отступить от положений пункта 2 в той мере, в какой ее законодательство устанавливает специальные правила в отношении определенных категорий персональных данных или автоматизированных баз персональных данных, однако это правило не применимо в тех случаях, когда правилами другой стороны предусмотрена равноценная защита.

Ограничения трансграничной передачи также возможны, если конечный получатель персональных данных находится на территории государства, не являющегося Стороной Конвенции.

Статья 4 Конвенции **обязывает каждую сторону принять** необходимые меры для того, чтобы основные принципы защиты данных, изложенные в Конвенции, были

реализованы в ее национальном праве, а статья 25 запрещает сторонам Конвенции делать какие-либо оговорки в отношении ее положений. Под оговоркой в международном праве понимается одностороннее заявление, сделанное государством при подписании, ратификации, принятии или утверждении договора или присоединении к нему, посредством которого оно желает исключить или изменить юридическое действие определенных положений договора в их применении к данному государству. Закрытый (исчерпывающий) перечень допустимых оговорок к Конвенции приведен в части 2 ст.3 документа.

Из **изложенного следует вывод**, что принятие Конвенции и присоединение к ней государств предусматривает устранение ограничений в передаче персональных данных на территорию стран, являющихся сторонами Конвенции, и обеспечение возможности их движения между сторонами Конвенции, поскольку все они должны предусмотреть в национальном законодательстве нормы, обеспечивающие защиту прав субъектов персональных данных, в том числе судебную, и, что необходимо выделить дополнительно, защиту самих персональных данных на уровне, закрепленном в Конвенции. В частности, в соответствии со ст.7 **каждая сторона должна предусматривать обязательность защиты** персональных данных от случайного или несанкционированного разрушения, случайной утраты и от несанкционированного доступа, изменения или распространения.

Ограничения такого движения не допускаются, оговорки в национальном законодательстве не предусмотрены, при осуществлении трансграничной передачи персональных данных стороны Конвенции обеспечивают адекватные меры по защите прав субъектов персональных данных, руководствуясь при этом национальными законами.

Анализируя нормы, введенные в Европейском союзе, можно отметить, что в Директиве от 24 октября 1995 г. № 95/46/ЕС прямо указывается, что экономическая и социальная интеграция, обусловленная созданием и функционированием внутреннего рынка Евросоюза, приводит к существенному увеличению трансграничных потоков персональных данных между всеми государствами-членами ЕС, развивается обмен персональными данными между предприятиями в различных государствах, а органы власти государств-членов ЕС призываются сотрудничать и обмениваться персональными данными с целью исполнения своих обязанностей в контексте пространства без внутренних границ, образованного внутренним рынком.

Увеличение объема научно-технического сотрудничества и скоординированное внедрение в Евросоюзе новых телекоммуникационных сетей неизбежно влекут за собой и облегчают трансграничную передачу персональных данных. Директива предусматривает устранение препятствий потокам персональных данных, для чего необходимо обеспечить **равноценный** во всех государствах-членах ЕС **уровень защиты прав и свобод** граждан при обработке их данных и сближение законодательств в данной сфере в этих государствах. В Директиве отмечается, что трансграничные потоки персональных данных необходимы для расширения международной торговли, а защита физических лиц, гарантированная Директивой, не препятствует передаче персональных данных в третьи страны, которые обеспечивают достаточный уровень их защиты. С другой стороны, передача

персональных данных в страну, которая не обеспечивает достаточный уровень их защиты, должна быть запрещена.

Необходимо отметить, что права субъекта персональных данных, обязанности оператора и лица, осуществляющего обработку персональных данных по поручению оператора персональных данных (далее – обработчик), случаи допустимой обработки персональных данных, в том числе специальных категорий, условия передачи персональных данных в страны, не обеспечивающие адекватной защиты прав субъектов в Директиве определены значительно более подробно и детально, чем в Конвенции, и положения Федерального закона от 27.07.20006 «О персональных данных» во многом совпадают с нормами Директивы.

4. Поручение на обработку персональных данных и размещение персональных данных на вычислительной инфраструктуре третьих лиц

При рассмотрении вопроса о возможности и условиях размещения информационных систем персональных данных в дата-центрах или облачной инфраструктуре, владельцами которых являются третьи лица, не являющиеся участниками правоотношений между субъектом персональных данных и оператором, необходимо исходить из оценки того, имеется ли в случае такого размещения информационных систем поручение на их обработку третьим лицом или нет.

По смыслу части 3 ст.6 закона «О персональных данных», поручение на обработку персональных данных предусматривает предоставление обработчику конкретного набора таких данных или предоставление доступа к ним, а также выполнение обработчиком конкретных действий с персональными данными, определенных оператором с целью достижения поставленных им целей.

В этом случае **нельзя рассматривать как поручение**, например, следующие варианты (примеры) размещения информационных систем персональных данных в дата-центрах и облачной инфраструктуре:

1. Развертывание информационных систем персональных данных на инфраструктуре третьего лица **без права доступа персонала** дата-центра (облачного сервиса) к этим данным.
2. Размещение персональных данных, **предварительно зашифрованных** оператором.
3. Размещение персональных данных, **прошедших процедуру обезличивания**, когда они не могут быть соотнесены с конкретными субъектами, а база данных, позволяющая установить связь между размещенными данными и субъектами, находится у оператора и в инфраструктуре, предоставляемой для размещения информационной системы, физически отсутствует.

Здесь и далее под шифрованием будет пониматься обратимое криптографическое преобразование данных с целью их сокрытия от неавторизованных лиц и предоставления возможности доступа только авторизованным лицам с

обязательным использованием ключа шифрования, обеспечивающего выбор конкретного преобразования из совокупности возможных для конкретного алгоритма.

Под обезличиванием будут пониматься действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных, выполняемые без использования криптографических преобразований. В соответствии с Приказом Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных», к наиболее перспективным и удобным для практического применения относятся **следующие методы обезличивания**:

- введение идентификаторов (замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным);
- изменение состава или семантики (изменение состава или семантики персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений);
- декомпозиция (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств);
- перемешивание (перестановка отдельных записей, а также групп записей в массиве персональных данных).

В первом из рассматриваемых примеров (развертывание информационных систем персональных данных на инфраструктуре третьего лица без права доступа персонала дата-центра (облачного сервиса) к этим данным) наличие технической возможности у персонала дата-центра или сервис-провайдера получить доступ к обрабатываемым данных заказчиков (клиентов) не должно рассматриваться как препятствие для размещения информационных систем, поскольку такие действия являются прямым нарушением условий договора между оператором и провайдером. Нарушение условий договора одной из сторон является возможным при заключении практически любой сделки, однако **не является законным обязательным условием для отказа** от нее.

Аналогичным образом не имеет значения алгоритм и стойкость системы шифрования, используемой в примере 2, или теоретическая возможность сопоставления данных, прошедших процедуру обезличивания, с конкретным субъектом или группой субъектов, с той, или иной вероятностью в примере 3.

Поскольку описанные выше примеры размещения персональных данных **не являются поручением** оператора владельцу дата-центра или сервис-провайдеру на обработку персональных данных, и сами персональные данные для обработки, в том числе хранения, не передаются, **не требуется и согласие** субъекта на такое размещение персональных в странах, обеспечивающих адекватную защиту прав субъектов персональных данных.

5. Требования российского законодательства к трансграничной передаче персональных данных и к поручению обработки персональных данных другому лицу

Статья 12 Федерального закона от 27.07.2006 «О персональных данных», следуя нормам Конвенции, не устанавливает никаких ограничений или дополнительных требований, касающихся трансграничной передачи персональных данных на территорию иностранных государств, являющихся сторонами Конвенции, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, перечень которых устанавливается Роскомнадзором (Приказ Роскомнадзора от 15 марта 2013 г. № 274 «Об утверждении Перечня 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»). Часть 1 этой статьи лишь устанавливает возможность запрета или ограничения такой передачи в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

Не требует закон и получения согласия субъекта на трансграничную передачу его персональных данных в страны, являющиеся сторонами Конвенции или обеспечивающие адекватную защиту прав субъектов персональных данных, не только в письменной, но и любой другой форме.

В то же время надо учитывать, что предоставление субъектом своих персональных данных оператору в любой форме фактически является конклюдентным действиями, подтверждающими согласие субъекта с их обработкой оператором. Учитывая, что в соответствии с частью 1 ст.9 закона «О персональных данных», субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе, а согласие на обработку персональных данных должно быть конкретным, информированным и сознательным, представляется, что **оператор до получения персональных данных от субъекта должен его проинформировать любым доступным способом о трансграничной передаче персональных данных**, например, указав это в общедоступной политике в отношении обработки персональных данных, предусмотренной ст.18.1 закона «О персональных данных», в договоре с клиентом, в том числе – трудовом, публичном, в виде оферты и т.д.

В отношении стран, не обеспечивающих адекватную защиту прав субъектов персональных данных, часть 4 ст.12 закона определяет закрытый перечень случаев, когда трансграничная **передача в эти государства допустима**:

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

2) случаи, предусмотренные **международными договорами** Российской Федерации (представляется, что к таковым можно отнести, например, соглашения, касающиеся порядка получения виз или отказа от визовых формальностей);

3) случаи, предусмотренные 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) **для исполнения договора**, стороной которого является субъект персональных данных (например, оказания туристических услуг в странах, не обеспечивающих адекватной защиты или перевод туда денежных средств, для чего необходима передача персональных данных отправителя и получателя);

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

Во всех случаях, независимо от факта наличия или отсутствия трансграничной передачи персональных данных, в соответствии со ст.7 Федерального закона операторы и иные лица, получившие доступ к персональным данным, **обязаны не раскрывать третьим лицам и не распространять персональные данные** без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Часть 3 ст.6 закона «О персональных данных» определяет условия, которые должны выполняться при поручении оператором обработки персональных данных иным лицам. К **важнейшим из них относятся два**, предусматривающие обязательное наличие:

- **согласия субъекта** на передачу его персональных данных иному лицу, если иное не предусмотрено федеральным законом;
- **договора с этим лицом**, в том числе государственного или муниципального контракта, либо соответствующего акта, принятого государственным или муниципальным органом.

Форма получения согласия не указывается, следовательно, **оно может даваться в любом виде**, позволяющем оператору, давшему такое поручение, впоследствии доказать наличие согласия субъекта.

При этом к содержанию договора поручения выдвигаются достаточно жесткие требования. В частности, **в нем должны быть**:

- определены перечень действий (операций) с персональными данными, которые будут совершаться обработчиком, и цели обработки,
- установлена обязанность обработчика соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке,
- указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 закона «О персональных данных».

На **обработчика возлагается обязанность** соблюдать принципы и правила обработки персональных данных, предусмотренные законом «О персональных данных».

В случае, если **обработчик находится вне юрисдикции Российской Федерации**, при организации обработки персональных данных он будет руководствоваться законодательством страны пребывания. Как уже отмечалось выше, присоединение к Конвенции предусматривает и гармонизацию национального законодательства с ее требованиями, поэтому требования к защите персональных данных в договоре поручения на обработку в этом случае будут определяться, исходя из положений ст.7 Конвенции: **обработчик обязан** «принимать надлежащие меры для охраны персональных данных, накопленных в автоматизированных базах данных, от случайного или несанкционированного разрушения или случайной утраты, а равно от несанкционированного доступа, изменения или распространения».

В **случае поручения обработки** персональных данных лицу, находящемуся вне юрисдикции Российской Федерации, **получение согласия** субъекта на передачу персональных данных такому лицу также **является обязательным**, независимо от того, обеспечивается ли в стране пребывания адекватная защита прав субъектов или нет.

При этом вопросы выбора и использования конкретных средств защиты информации, обязательности наличия у них сертификатов или иных документов, подтверждающих соответствие тем или иным требованиям, **определяются законодательством, действующим на территории той страны, где находится дата-центр**, в котором размещаются персональные данные, или где находится их обработчик. В соответствии с нормами Конвенции, каждая ее сторона самостоятельно определяет конкретные правила защиты персональных данных на своей территории, как это сделала, например, Россия, установив перечень требований в ст.19 закона «О персональных данных», Постановлении Правительства РФ от 01.11.2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и приказе ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Необходимо также учитывать, что использование для обеспечения безопасности персональных данных, обрабатываемых за рубежом, средств защиты информации российского производства **не всегда возможно**. Например, средства защиты, имеющие в своем составе модули шифрования, являются товарами, в отношении которых действуют ограничения на ввоз и вывоз, как, например, в странах, входящих в Таможенный союз (Россия, Белоруссия, Казахстан). Есть такие ограничения в ряде европейских и иных зарубежных стран.

Рассмотренные требования федерального законодательства позволяют сделать следующие выводы:

- закон «О персональных данных» **не содержит запрета** на трансграничную передачу персональных данных, однако такая передача в страны, не

обеспечивающие адекватной защиты прав субъектов персональных данных, **оговаривается дополнительными условиями**;

- во всех случаях передача персональных данных **третьим лицам требует получения согласия** субъекта персональных данных в любой доказываемой форме;
- конкретные **правила технической защиты** персональных данных, подвергаемых автоматизированной обработке, определяются законодательством той страны, на территории которой такая обработка ведется.

6. Влияние расположения серверов облачного сервиса Microsoft Azure на возможность размещения на них персональных данных российскими операторами

Как уже отмечалось выше, **трансграничная передача** персональных данных в страны, обеспечивающие **адекватную защиту** прав субъектов персональных данных, **не требует получения согласия** субъекта. В связи с этим важное значение имеет географическое расположение дата-центров, используемых платформой Microsoft Azure при предоставлении облачных сервисов.

В соответствии с информацией, размещенной на странице «Конфиденциальность» Центра управления безопасностью Microsoft Azure (http://www.windowsazure.com/ru-ru/support/trust-center/privacy/), пользователи сервиса могут указывать географическое положение («территории» или «регионы») центров обработки данных Microsoft, в которых будут храниться их данные: Азиатско-Тихоокеанский регион (Гонконг и Сингапур), Европа (Ирландия и Нидерланды) или США. В частности, **возможно использование только дата-центров, расположенных в Европе** и в странах, являющихся сторонами Конвенции – Ирландии (сторона Конвенции с 1990 года) и Нидерландах (сторона Конвенции с 1993 года).

На сайте указывается, что корпорация **Microsoft не передает данные пользователей за пределы указанных территорий** (например, из Европы в США или из США в Азию), **за исключением** случаев, когда корпорации Microsoft необходимо предоставить поддержку пользователям, устранить неполадки или выполнить требования законодательства, или **пользователь разрешает это** в настройках учетной записи, чтобы включить такую передачу своих данных, в том числе посредством использования следующих компонентов:

- компоненты, которые не позволяют выбирать территорию, такие как сеть доставки содержимого, предоставляющая глобальную службу кэша;
- веб-роли и рабочие роли, которые выполняют резервное копирование пакетов развертывания программного обеспечения в США независимо от территории развертывания;
- функции, доступные в предварительных или бета-версиях, которые могут хранить или передавать данные пользователей в США независимо от территории развертывания;

- служба Microsoft Azure Active Directory (кроме Access Control), которая может передавать данные о пользователях Active Directory из Европы в США или из Азии в США или Европу;
- многофакторная проверка подлинности Microsoft Azure, которая хранит данные проверки подлинности в США.

(следует отметить, что Microsoft Azure Active Directory в зависимости от выбранного клиентом способа наполнения каталога данными может и не содержать персональных данных пользователей информационной системы).

США также не входят в перечень стран, которые Роскомнадзор определил как обеспечивающие адекватную защиту прав субъектов персональных данных. Однако следует учитывать, что Европейская комиссия заключила соглашение с Министерством торговли США, согласно которому организации США могут выполнять **самостоятельную сертификацию** на соответствие требованиям программы **«Безопасная гавань»** (Safe Harbor) в целях обеспечения бесперебойности передачи данных между странами в рамках международной деловой деятельности, **включая передачу персональных данных**. Сертификация **подтверждает выполнение требований** к защите персональных данных, установленных Директивой Евросоюза от 24 октября 1995 г. № 95/46/EC, которые, как отмечалось выше, **аналогичны требованиям, установленным российским законодательством**. Корпорация **Microsoft** (включая все ее дочерние организации в США) **имеет такие сертификаты**, выданные Министерством торговли США. Помимо стран-участниц ЕС, страны-участницы Европейской экономической зоны (Исландия, Лихтенштейн и Норвегия) также признают организации, сертифицированные по программе «Безопасная гавань», как **обеспечивающие надлежащий уровень защиты** личных данных при их передаче из страны, в которой расположена организация, в США.

Сертификация по программе «Безопасная гавань» **позволяет осуществлять законную передачу** личных данных из Европейского союза в Microsoft в целях ее обработки. В рамках Директивы ЕС о защите данных и данного соглашения Microsoft действует как обработчик данных, в то время как пользователь является владельцем данных, ответственным за обеспечение законности передачи этих данных в Microsoft. Корпорация Microsoft взяла на себя обязательство передавать данные пользователей из Европейского союза за пределы данного региона **только в случае крайней необходимости**.

В документах корпорации нет прямого указания на то, что данные требования распространяются на данные, размещаемые на платформе Microsoft Azure операторами других стран, в частности, России, однако уровень защиты информации в дата-центрах, обеспечивающих предоставление облачного сервиса, для них будет идентичен описанному выше.

7. Меры по обеспечению безопасности данных, размещенных на платформе Microsoft Azure

В соответствии с информацией, размещенной на сайте Microsoft Azure, для обеспечения безопасности данных клиентов, размещенных на платформе,

используется **комплекс правовых, организационных и технических мер**, обеспечивающих защиту обрабатываемых данных клиентов от неправомерных и несанкционированных воздействий, нейтрализацию угроз безопасности антропогенного, технологического и природного характера.

Правовые меры, помимо упоминавшегося выше соглашения с Европейским союзом в рамках программы «Безопасная гавань» о сертификации дата-центров на соответствие требованиям к защите персональных данных, включают в себя зафиксированную в договоре на оказание услуг ответственность за обеспечение безопасности, подкрепленную финансовыми гарантиями. Выполнение требований безопасности **подтверждается результатами внешнего аудита** на соответствие международному стандарту **ISO/IEC 27001:2005** Information security management systems requirements specification («Системы менеджмента информационной безопасности. Требования»), причем в область сертификации включены виртуальные машины, облачные службы, хранилище и виртуальная сеть. Проведены также аудиты на соответствие стандартам PCI DSS, HIPAA, FISMA, FedRAMP и другим.

Для Microsoft Azure был проведен аудит в соответствии со спецификацией Cloud Controls Matrix (CCM), разработанной организацией Cloud Security Alliance (CSA).

Организационные и технические меры обеспечивают безопасность на физическом и сетевом уровнях, на уровне программного обеспечения и в среде виртуализации.

Физическая безопасность включает круглосуточный контроль доступа в дата-центры с использованием средств сигнализации, датчиков движения, видеонаблюдения и биометрических систем идентификации при доступе, обеспечение пожарной безопасности и резервного электропитания.

Сетевая безопасность предусматривает автоматическое управление конфигурациями, многоуровневое межсетевое экранирование, включая экранирование на уровне приложений, систему предупреждения вторжений (IPS) и защиту от DDoS атак, изоляцию сетевых сегментов, доменов и подсетей с использованием фильтрующих маршрутизаторов, межсетевых экранов и балансировщиков нагрузки (средств преобразования сетевых адресов), что позволяет разделить внутреннюю сеть на локальные сети для веб-серверов и серверов приложений, хранилищ данных и центра администрирования. Подключение к облаку осуществляется с использованием VPN, работающей по протоколу TLS с криптографическими ключами длиной минимум 128 разрядов.

Уровень безопасности отслеживается с помощью централизованных систем мониторинга, корреляции и анализа, которые предоставляют соответствующие уведомления и оповещения.

Безопасность программного обеспечения достигается за счет безопасной разработки приложений (Microsoft Security Development Lifecycle), использования урезанных версий операционных систем и «золотых образов», управления обновлениями.

Для нейтрализации угроз антропогенного характера, помимо обязательной проверки персонала перед приемом на работу, применяются следующие меры: предоставление персоналу дата-центров минимальных полномочий, необходимых

для выполнения их обязанностей, разделение обязанностей между работниками, исключающее дублирование функций и излишние права при доступе в вычислительную инфраструктуру. **По умолчанию у персонала дата-центров нет доступа к данным клиентов**, он может быть предоставлен только в строго регламентированных случаях на временной основе и/или после согласования такого доступа с клиентом и руководством дата-центра. Используется двухфакторная аутентификация администраторов сети.

Для **защиты от несанкционированного доступа** к данным, обрабатываемым в виртуальной среде, используются методы тотальной абстракции, когда виртуальные машины клиента не могут получить и не получают какой-либо информации о других виртуальных машинах, имеющихся на том же хосте, фильтрация трафика на уровне хоста, контроль потребляемых виртуальными машинами ресурсов, а в случае выявления неправомерных действий – блокирование зловредных виртуальных машин.

Обеспечивается резервное копирование обрабатываемых и хранящихся в дата-центрах данных клиентов, причем создается минимум три копии в каждом дата-центре, причем **все данные резервных копий хранятся в зашифрованном виде**, по желанию клиента резервное копирование может осуществляться в другие дата-центры (см. раздел 7 Заключения).

В качестве сервисов безопасности (SecaaS) по желанию клиента могут предоставляться управление электронными правами (RMS – Rights Management services), многофакторная аутентификация, а также службы каталогов Active Directory и Active Directory Premium.

Выполняется постоянное тестирование платформы Microsoft Azure на предмет защиты от несанкционированного доступа, причем **клиенты могут выполнять такое тестирование в отношении своих приложений**, размещенных в Microsoft Azure, и самостоятельно после получения предварительного одобрения от службы поддержки.

Предусмотренные сервисом Microsoft Azure меры по обеспечению информационной безопасности обрабатываемой в облаке информации в целом позволяют обеспечить реализацию требований, предъявляемых в части 2 ст.19 закона «О персональных данных», за исключением применения средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия и учета машинных носителей персональных данных, которые могут быть приняты только в отношении элементов вычислительной инфраструктуры, развернутой на стороне оператора (вне облачной платформы).

8. Распределение обязанностей и ответственности за выполнение требований законодательства в сфере персональных данных и обеспечение безопасности персональных данных между владельцем облачного сервиса Microsoft Azure, провайдерами облачных услуг и операторами персональных данных при различных сценариях использования платформы Microsoft Azure

При возможном использовании российскими операторами персональных данных облачного сервиса Microsoft Azure сторонами правоотношений являются:

- сам оператор персональных данных (российская компания (организация), **использующая** на основании договора **сервис Microsoft Azure** и размещающая (обрабатывающая) в облаке среди прочих данных и персональные данные);
- корпорация Microsoft, предоставляющая облачный сервис Microsoft Azure;
- сервис-провайдеры - партнеры корпорации Microsoft CSV (Cloud Software Vendor), **создающие свои сервисы** на платформе Microsoft Azure и заключающие договоры с российскими операторами о предоставлении им своих сервисов на платформе Microsoft Azure;
- агенты партнеры корпорации Microsoft (LAR партнеры), действующие в ее интересах и по ее поручению и **предоставляющие право доступа** к платформе Microsoft Azure всем заказчикам, как тем, кто использует Azure для внутренних задач (операторам персональных данных), так и другим партнерам, которые создают сервисы для продажи (сервис-провайдерам)

Агенты корпорации Microsoft (LAR партнеры) никаких мер по обеспечению безопасности обрабатываемых данных самостоятельно принимать не могут и **никакой ответственности за обеспечение безопасности не несут**.

Для определения зон ответственности остальных участников правоотношений и состава принимаемых мер по обеспечению безопасности обрабатываемых данных, а также оценки необходимости получения согласия субъектов на размещение их персональных данных в информационной системе, развернутой на платформе Microsoft Azure, рассмотрим варианты (сценарии) такого размещения, указанные в запросе на подготовку Экспертного заключения.

8.1. Размещение персональных данных, прошедших процедуру обезличивания

При данном сценарии в облако передаются только персональные данные, прошедшие процедуру обезличивания. База данных, соотносящая обезличенные данные и конкретных субъектов, хранится непосредственно у оператора персональных данных и в облаке не размещается. Закон «О персональных данных» не содержит прямого ответа на вопрос о том, являются ли данные после обезличивания персональными, однако исходя из смысла процедуры обезличивания, полученные в результате ее **данные не требуют обеспечения конфиденциальности**. В этом случае должна быть обеспечена только

целостность и доступность таких данных, что достигается в значительной степени за счет выполнения резервного копирования, обрабатываемых в дата-центрах Microsoft Azure данных клиентов (в рассматриваемом случае – оператора персональных данных). Частота (периодичность) такого резервного копирования должна определяться оператором и отражаться в договоре на предоставление сервиса.

Оператор, со своей стороны, в информационной системе на своей территории **должен принять все меры**, предусмотренные российским законодательством в отношении данных, обрабатываемых в этой системе, включая меры по предотвращению несанкционированного доступа к ним и обеспечению конфиденциальности. **Согласия субъекта** на передачу данных в облако после их обезличивания **не требуется**, т.к. их невозможно соотнести с конкретным физическим лицом.

8.2. Размещение в облаке персональных данных только работников оператора

Как отмечалось в разделе 6 Экспертного заключения, одним из важнейших факторов, влияющих на состав мер, необходимых для выполнения требований российского законодательства в сфере персональных данных, а также распределение обязанностей между оператором, владельцем сервиса и сервис-провайдером, является возможность доступа персонала дата-центра и/или провайдера, к обрабатываемым данным.

Если в договоре на предоставление услуг оператору по использованию облачной платформы **предусматривается полный запрет** на доступ персонала дата-центра (работников корпорации Microsoft) и/или сервис-провайдера к данным клиента, в получении согласия субъекта на передачу его данных третьим лицам необходимости нет, так как в этом случае **поручение на обработку отсутствует**.

В случаях, когда размещение информационной системы персональных данных на платформе Microsoft Azure **не исключает доступ персонала** дата-центров и/или сервис-провайдера к обрабатываемым персональным данным, такое размещение необходимо рассматривать **как поручение оператора** на обработку персональных данных корпорации Microsoft или сервис-провайдеру с определением в договоре **конкретных действий**, которые персонал может совершать в отношении персональных данных, размещенных оператором (определить используемые способы обработки), а **также целей** такой обработки (например, «предотвращение, обнаружение и устранение проблем с работой служб, предоставленных на платформе клиенту, улучшение возможностей обнаружения угроз для пользователей, таких как вредоносные программы и нежелательная почта (спам) и защита от них», как это указано на сайте Microsoft Azure).

Размещение в облаке информационной системы, обрабатывающей персональные данные **только работников оператора**, предполагает, что у каждого из них возможно получения согласия на передачу персональных данных для обработки иному лицу (корпорации Microsoft или сервис-провайдеру). Такое согласие может быть дано в том числе непосредственно в трудовом договоре или дополнительном соглашении к нему. При этом если размещение дата-центров

облачной платформы ограничено только территорией Ирландии, Нидерландов или Гонконга, согласие должно даваться **в любой доказываемой форме**, а если допускается возможность обработки на территории Сингапура и США, то согласие должно быть получено **только в письменной форме** и соответствовать по содержанию требованиям, установленным частью 4 ст.9 закона «О персональных данных». Особое внимание необходимо уделить персональным данным бывших работников, с которыми у оператора может быть потеряна связь, и получение их согласия окажется невозможным.

Как отмечалось в разделе 5 Экспертного заключения, во всех случаях размещения персональных данных в открытом виде на платформе Microsoft Azure, в том числе персональных данных работников оператора, **оператор должен проинформировать** работника любым доступным способом о трансграничной передаче его персональных данных, например, указав это в политике в отношении обработки персональных данных, в трудовом договоре (дополнительном соглашении к нему) или ином документе, предусматривающем необходимость и возможность ознакомления в ним работника.

Далее оператор должен определить уровень защищенности персональных данных. При признании **актуальными угроз только третьего типа** (не связанных с наличием не декларированных возможностей в системном и прикладном программном обеспечении, используемом при обработке персональных данных) и отсутствии в системе персональных данных специальных категорий и биометрических персональных данных, необходимо **обеспечение минимального, четвертого уровня защищенности**, независимо от количества работников, чьи персональные данные обрабатываются.

Исходя из типа актуальных угроз, особенностей функционирования информационной системы в облаке оператору необходимо построить частную модель актуальных угроз и меры, принятие которых необходимо для данного уровня защищенности в соответствии с перечнем, установленным приказом ФСТЭК от 18.02.2013 № 21.

Затем необходимо проанализировать состав мер безопасности, обеспечиваемых владельцем облачной платформы и провайдером (при его наличии), развернувшим свои сервисы на платформе Microsoft Azure и предоставившим их оператору персональных данных, наличие описания состава таких мер в договоре на предоставление услуг, оценить, какие актуальные угрозы, указанные в частной модели, могут быть нейтрализованы при их выполнении.

Все остальные меры по нейтрализации актуальных угроз безопасности, в том числе в отношении рабочих мест пользователей и тех, реализация которых возможна на стороне оператора, должны быть обеспечены самим оператором.

Во всех случаях **при передаче персональных данных** между оператором и дата-центром должно быть обеспечено шифрование данных при использовании в качестве транспорта интернета или сети связи общего пользования.

8.3. Размещение персональных данных в облаке в зашифрованном виде

Данный сценарий предполагает, что персональные данные хранятся в облаке только в зашифрованном виде и расшифровываются на рабочих местах оператора на территории Российской Федерации, при этом информация, не относящаяся к персональным данным, может храниться в облаке в открытом (незашифрованном) виде. При данном сценарии **географическое место расположения дата-центров** платформы Microsoft Azure только на территории государств, входящих в Совет Европы и являющихся сторонами Конвенции, или без возможности определения конкретной страны, где размещена инфраструктура или ее элементы, **значения не имеет**, поскольку трансграничная передача персональных данных не осуществляется (в облаке размещен только массив данных в зашифрованном виде, значение которых владельцу облачной платформы неизвестно), **обработки данных в облаке не происходит**.

Обеспечение конфиденциальности таких данных не требуется, оператор должен лишь **предусмотреть их целостность** (путем определения порядка резервного копирования и восстановления модифицированных или уничтоженных данных) и доступность (возможно, за счет создания резервных каналов связи с дата-центром). Состав мер, принимаемых оператором в отношении безопасности персональных данных, полностью идентичен описанному в сценарии в разделе 9.1 Экспертного заключения. В этом случае **согласие субъекта** на передачу данных в облако в зашифрованном виде также **не требуется**, сами данные не распространяются, никому не передаются, и трансграничная их передача не осуществляется.

8.4. Размещение персональных данных в облаке в открытом виде на территории государств, входящих в Совет Европы

В данном сценарии предполагается, что персональные данные хранятся в облаке в открытом виде, при этом облачная инфраструктура находится только на территории государств, входящих в Совет Европы и являющихся сторонами Европейской конвенции.

Обязанности и ответственность сторон (оператора, владельца облачной платформы и сервис-провайдера) в этом случае почти полностью идентичны описанным в сценарии раздела 9.2 Экспертного заключения, с той лишь разницей, что уровень защищенности персональных данных в этом случае может быть выше (даже при признании актуальными угроз только 3-го типа – вплоть до 2-го уровня защищенности в случае обработки персональных данных специальных категорий более чем 100 тысяч субъектов персональных данных) и состав мер по обеспечению безопасности может быть гораздо шире.

В случае наличия возможности доступа к персональным данным работников дата-центра (корпорации Microsoft) и/или сервис-провайдера, **необходимо получение согласия субъектов** на передачу их персональных данных для обработки иному лицу в любой доказываемой форме. В то же время, в случае отражения в договоре на предоставление услуг оператору по использованию облачной платформы **полного запрета на доступ персонала** дата-центра и/или сервис-

провайдера к данным клиента, в **получении такого согласия необходимости нет**, так как в этом случае поручение на обработку отсутствует, а трансграничная передача данных осуществляется только на территорию государств, обеспечивающих адекватную защиту прав субъектов персональных данных.

8.5. Обработка персональных данных в облаке на виртуальных машинах

Данный сценарий предполагает, что в облаке размещаются виртуальные машины, предоставленные оператору, на которых обрабатываются персональные данные. Пользователи оператора подключаются к виртуальным машинам с использованием технологии Remote Desktop как при размещении облачной инфраструктуры только на территории государств, являющихся стороной Конвенции, так и без возможности определения конкретной страны, где размещена инфраструктура или ее элементы.

При размещение дата-центров, где развернута виртуальная инфраструктура и находятся хосты с виртуальными машинами, на территории государств, являющихся сторонами Конвенции, ситуация является полностью аналогичной той, которая описана в предыдущем сценарии (раздел 9.4) лишь с тем отличием, что в договоре оператора на предоставление ему услуг облачной инфраструктуры **необходимо описание мер**, которые принимаются владельцем облачной платформы и/или сервис-провайдером **для нейтрализации специфических угроз** безопасности, обусловленных использованием аппаратной системы виртуализации Hyper-V.

Выводы же о необходимости получения согласия субъектов персональных данных, сделанные в предыдущем разделе, остаются справедливыми и для рассматриваемого случая – оно необходимо в случае, если не исключается доступ персонала дата-центра и/или сервис-провайдера к обрабатываемым данным, такую передачу необходимо рассматривать как поручение на обработку персональных данных, и в получении согласия нет необходимости, если договором о предоставлении облачной платформы предусмотрен запрет на доступ персонала к обрабатываемым данным заказчика (клиента).

В случае, если определение конкретной страны, где размещена облачная инфраструктура или ее элементы, невозможно, и допускается размещение персональных данных на территории стран, не обеспечивающих адекватную защиту прав субъектов персональных данных, состав мер по обеспечению безопасности и распределение ответственности между оператором, владельцем облачной платформы и сервис-провайдером не отличается от описанных выше.

Однако в этом случае является обязательным получение согласия субъекта на трансграничную передачу персональных данных в письменной форме, предусмотренной частью 4 ст.9 закона «О персональных данных» даже в случае запрета на доступ персонала дата-центра к обрабатываемым данным. Это обусловлено тем, что порядок получения доступа к обрабатываемым в дата-центре персональным данным иных лиц, в том числе органов власти, спецслужб, правоохранительных органов, органов следствия и дознания определяется национальным законодательством страны, где размещен дата-центр, и которое не

обеспечивает адекватную российскому законодательству защиту прав субъектов персональных данных.

Несмотря на отсутствие требования об обязательном шифровании персональных данных, передаваемых по открытым (незащищенным) каналам связи и сети интернет в прямой постановке в российских законодательных и иных нормативно-правовых актах, регламентирующих обеспечение безопасности персональных данных, необходимость применения шифрования при использовании незащищенных каналов связи вытекает из требования части 1 ст.19 закона «О персональных данных», обязывающих оператора принимать необходимые 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. Применение иных, некриптографических, способов защиты персональных данных от несанкционированного доступа при передаче их через сеть интернет или сети связи общего пользования практически невозможно. Таким образом, необходимо сделать вывод, что при размещении в облаке персональных данных в незашифрованном или необезличенном виде должно предусматривать шифрование этих данных при передаче по незащищенным каналам связи, в том числе – через интернет. При этом представляется **допустимым использование несертифицированных средств криптографической защиты** информации, встроенных в сетевое оборудование (например, межсетевые экраны) и браузеры ввиду наличия упоминавшихся в разделе 4 Экспертного заключения ограничений на ввоз и вывоз средств, содержащих в своем составе средства шифрования, а также в связи с необходимостью соблюдения дата-центрами законодательства стран, на территории которых они размещены.

Кроме того, протокол HTTPS, основанный на использовании алгоритма RSA, используют при передаче персональных данных через интернет и веб-сайты органов государственной власти Российской Федерации, в частности, единый портал государственных услуг www.gosuslugi.ru, сайт Федеральной налоговой службы www.nalog.ru, и их функционирование в течение длительного времени косвенно свидетельствует о допустимости использования в определенных случаях штатных средств шифрования сетевого оборудования и встроенных в пользовательское программное обеспечение.

8.6. Организация моделирования актуальных угроз персональным данным, обрабатываемым в информационных системах, размещенных в облаке Microsoft Azure

В соответствии с классификацией, установленной «Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК России (далее – Базовая модель), информационные системы персональных данных (ИСПДн) размещаемые на вычислительной инфраструктуре платформы Microsoft Azure, являются распределенными информационными системами персональных данных,

имеющими подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

Для таких сетей Базовая модель предполагает возможность реализации следующих угроз безопасности персональных данных:

- угрозы утечки информации по техническим каналам (угрозы утечки акустической (речевой) информации; угрозы утечки видовой информации; угрозы утечки информации по каналам, создаваемым побочными электромагнитными излучениями и наводками);
- угрозы несанкционированного доступа (НСД) к персональным данным, обрабатываемым на автоматизированном рабочем месте.

Угрозы НСД связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн, а также нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

Выделяются следующие угрозы НСД, связанные с действиями нарушителей, имеющих доступ к ИСПДн:

- угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой;
- угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.);
- угрозы внедрения вредоносных программ;
- угрозы анализа сетевого трафика с перехватом передаваемой по сети информации;
- угрозы выявления паролей;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

Кроме того, в таких ИСПДн имеют место угрозы, реализуемые с использованием протоколов межсетевого взаимодействия из внешних сетей, в том числе:

- угрозы анализа сетевого трафика с перехватом передаваемой из ИСПДн и принимаемой в ИСПДн из внешних сетей информации;
- угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций

ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;

- угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;
- угрозы подмены доверенного объекта;
- угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях;
- угрозы выявления паролей;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;
- угрозы внедрения вредоносных программ из внешних сетей информации.

В случае размещения информационных систем персональных данных на облачной платформе выполнение указанных выше требований по моделированию угроз персональных данных существенно усложняется тем фактом, что оператор не является владельцем и оператором вычислительной инфраструктуры Microsoft Azure, не определяет ее топологию и состав используемых технических средств и, в силу этого, не может в полном объеме выявить актуальные угрозы безопасности персональных данных, реализация которых возможна на облачной платформе.

В этих условиях **представляется оптимальным следующий путь**: определить зоны ответственности оператора, владельца облачной платформы и сервис-провайдера (при его наличии), а также принимаемые каждым из участников отношений меры по технической защите персональных данных.

Оператор самостоятельно определяет типы актуальных для обрабатываемых персональных данных **угроз** (от 1-го до 3-го), уровень защищенности своей информационной системы персональных данных (от 1-го до 4-го) и **формирует частную модель угроз и требования**, обеспечивающие безопасность персональных данных при их автоматизированной обработке в зависимости от установленного уровня защищенности, состав мер обеспечения безопасности данных для установленного уровня защищенности, определяемый на основании приложения № 1 к документу «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных Приказом ФСТЭК России от 18.02.2013 № 21. При этом оператор исходит из особенностей обработки данных, размещенных на облачной платформе.

На основании анализа мер по обеспечению безопасности, принимаемых дата-центрами и описанных в Соглашении об обработке данных (Data Processing Agreement) и/или договоре с сервис-провайдером, оператор определяет, какие актуальные угрозы нейтрализуются средствами, имеющимися в дата-центре (с использованием средств защиты информации, соответствующих требованиям национального законодательства страны, где размещен дата-центр) и/или развернутыми на облачной платформе сервис-провайдером, и в отношении каких угроз он должен самостоятельно принять меры по их нейтрализации при

размещении информационной системы персональных данных на платформе Microsoft Azure.

Оператор также выявляет, нейтрализацию каких актуальных угроз безопасности персональных данных он должен обеспечить в той части информационной системы персональных данных, функционирование которой он обеспечивает самостоятельно, и обеспечивает их нейтрализацию за счет использования мер и средств защиты в соответствии с требованиями российских нормативных правовых актов.

9. Содержание типового договора между владельцем облачной платформы (сервис-провайдером облачных услуг) и оператором персональных данных в части обработки персональных данных

С учетом изложенного выше, в договоре между владельцем облачной платформы (сервис-провайдером облачных услуг) и оператором персональных данных (или приложениях к нему) целесообразно указать:

- требование об обеспечении конфиденциальности персональных данных, обрабатываемых на облачной платформе;
- возможность доступа персонала дата-центров и/или сервис-провайдера к обрабатываемым данным оператора, и при наличии такой возможности – цели, для достижения которых персонал получает доступ к данным, размещенным клиентом, случаи, когда такой доступ возможен и способы обработки таких данных персоналом дата-центра (сервис-провайдера);
- состав и содержание мер по обеспечению безопасности персональных данных, принимаемых владельцем облачной платформы и сервис-провайдером (при его наличии);
- допустимые случаи предоставления доступа к обрабатываемым данным третьих лиц, в том числе представителей органов власти страны, где размещается дата-центр, и порядок информирования оператора о факте такого доступа;
- отсутствие необходимости получения владельцем облачной платформы и/или сервис-провайдером согласия субъекта на обработку персональных данных и ответственности владельца платформы и/или сервис-провайдера перед субъектом персональных данных;
- ответственность владельца платформы и/или сервис-провайдера перед оператором за инциденты с обрабатываемыми данными.

Весьма желательным было бы включение в качестве приложения к договору описания угроз обрабатываемым данным, нейтрализация которых обеспечивается владельцем облачной платформы и/или сервис-провайдером (при его наличии).

10. Содержание дополнительных мер, принятие которых необходимо оператором персональных данных-пользователем облачных сервисов Microsoft Azure для достижения соответствия требованиям российского законодательства в сфере персональных данных

В разделе 5 Экспертного заключения отмечалось, что в соответствии с законом «О персональных данных» субъект персональных данных принимает решение о предоставлении его персональных данных оператору и дает согласие на их обработку свободно, своей волей и в своем интересе, а согласие на обработку персональных данных должно быть конкретным, информированным и сознательным.

В связи с этим представляется, что оператор, использующий облачную платформу Microsoft Azure, должен указать на это в общедоступной политике в отношении обработки персональных данных, разрабатываемой в соответствии со ст.18.1 закона «О персональных данных», а также в своих локальных актах, регламентирующих вопросы обработки и обеспечения безопасности персональных данных.

В случае, если обработка персональных данных осуществляется на основания договора с клиентом в письменной форме (в том числе трудового), публичного договора или договора в форме оферты, информация о трансграничной передаче персональных данных и размещении их на вычислительной инфраструктуре иного лица должна быть указана в договоре.

Оператор должен проинформировать субъекта указанными выше способами о факте трансграничной передачи его персональных данных с указанием государств, где данные могут размещаться, обеспечении или необеспечении этими государствами адекватной российскому законодательству защиты прав субъектов персональных данных, возможных случаях получения доступа к персональным данным иных лиц, целях, в которых такой доступ может предоставляться, и способах обработки персональных данных такими лицами.

При соблюдении описанных в настоящем Экспертном заключении условий размещение персональных данных российскими операторами на облачной платформе Microsoft Azure представляется допустимым и соответствующим закону.