

Возможные стратегии выполнения требований в отношении локализации баз с персональными данными граждан РФ

Начиная с середины 2014 года не утихают активные дискуссии по поводу изменений в российском законодательстве, вводимых Федеральным законом от 21.07.2014 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации (далее - РФ) в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» (далее - 242-ФЗ) и призванных локализовать обработку персональных данных (далее - ПДн) российских граждан на территории РФ. Дополнительным фактором, подогревающим обсуждение, являлась длительная интрига (которая была разрешена только 31.12.2014 Президентом России) относительно даты вступления в силу норм 242-ФЗ.

Учитывая возможные риски для деятельности операторов в связи с принятием и вступлением в силу 242-ФЗ представляется целесообразным рассмотреть и проанализировать основные положения данного закона, а также сформировать представление о возможных стратегиях выполнения требований 242-ФЗ в отношении размещения баз данных (далее - БД) с ПДн на территории РФ.

Описание политической и правовой ситуации, послужившей фоном для принятия 242-ФЗ

С учетом роста мировой геополитической напряженности в первой половине 2014 года между РФ и рядом зарубежных стран, а также в условиях взаимных и встречных санкций различного характера, представители российской исполнительной и законодательной власти выступили с целым рядом инициатив по обеспечению национальной безопасности РФ в информационной, финансовой и иных сферах.

Так, в марте 2014 года, после того как США ввели санкции против РФ в связи с присоединением Крыма к России и международные платёжные системы «Виза» и «МастерКард» во второй раз в истории остановили обслуживание платежных карт нескольких российских банков в торговых точках и банкоматах международной сети, вновь стало актуальным создание в стране национальной системы платёжных карт, независимой от состояния международных отношений. В РФ был принят Федеральный закон от 05.05.2014 № 112-ФЗ, которым внесены изменения, направленные на обеспечение бесперебойности осуществления переводов денежных средств, осуществляемых в рамках платежной системы на территории РФ. Фактически, власти РФ предприняли попытку инфраструктурно и информационно замкнуть процесс осуществления денежных переводов внутри РФ, то есть операционные центры и платёжные клиринговые центры должны обязательно находиться на территории РФ. Также в законе предусмотрен запрет на передачу и предоставление доступа иностранным государствам к информации о внутривнутрироссийских платёжных транзакциях.

Схожим образом власти РФ стали действовать для обеспечения «информационного и цифрового» суверенитета РФ, элементом обеспечения которого и стало принятие 242-ФЗ. При принятии 242-ФЗ законодатель указал, что предлагаемые изменения соответствуют, в том числе и практике Европейского суда по правам человека: «Так, 13 мая 2014 года Европейский суд по правам человека вынес решение, согласно которому поисковые интернет-сервисы должны обязательно принимать во внимание просьбы физических лиц об удалении, открыто размещенной информации с упоминанием их имени из поисковых результатов. При этом, IT-компании, владеющие поисковыми системами в сети «Интернет», обязаны нести ответственность за распространение персональных данных пользователей, опубликованных на сайтах третьих лиц».

Тем не менее, при анализе норм 242-ФЗ можно прийти к выводу о существовании как минимум еще двух мотивов для властей РФ:

1. возникновение у иностранных компаний (например, операторов социальных сетей), осуществляющих свою деятельность в РФ посредством информационно-телекоммуникационной сети «Интернет», обязанности по обеспечению обработки ПДн российских граждан на территории РФ. Таким образом обеспечивается возможность оперативного доступа к указанным ПДн со стороны правоохранительных органов РФ;
2. обеспечение непрерывности деятельности российских компаний, являющихся дочерними по отношению к иностранным компаниям или пользующихся ИТ-услугами иностранных компаний. В частности, очень многие «дочки» иностранных компаний пользуются ресурсами ИС, предоставляемыми иностранными компаниями, для обработки ПДн в таких целях как кадровый учет, расчет заработной платы или взаимодействие с контрагентами. Блокировка обработки ПДн в подобных ИС из-за санкций может в кратчайшие сроки нанести серьезный удар по бизнесу компаний-резидентов РФ.

Обязанность по размещению БД с ПДн на территории РФ

Согласно тексту изменений, приведенных в ст.2 242-ФЗ, ст.18 «Обязанности оператора при сборе персональных данных» 152-ФЗ дополняется частью 5 следующего содержания: «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».

Необходимо отметить, что новое требование распространяется на всех операторов ПДн, за исключением некоторых случаев

обработки ПДн СМИ и органами государственной власти. К исключениям также относится п.2 ч.1 ст.6 152-ФЗ: «обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей». Однако, по нашему мнению, такое исключение может применяться только в тех случаях, при которых на оператора возлагается обязанность по сбору и дальнейшей обработке ПДн за рубежом.

Важной особенностью положений 242-ФЗ является акцент на гражданстве субъектов ПДн. Ранее законодательство РФ в области ПДн было направлено на защиту прав субъектов ПДн в целом, безотносительно их гражданства. Теперь операторы оказываются перед выбором:

1. не разделять субъектов ПДн по наличию гражданства РФ и обрабатывать ПДн всех субъектов в БД, находящихся на территории РФ;
2. разделять субъектов ПДн по наличию гражданства РФ, обрабатывая при этом дополнительную категорию ПДн – сведения о гражданстве субъектов ПДн¹.

В случае если оператор поручает другому лицу обработку ПДн, включая сбор ПДн, указанное требование распространяется также и на такое лицо. Оператор при поручении сбора ПДн другим лицам также обязан обеспечить (например, включением требования в поручение обработки ПДн) размещение БД с ПДн на территории РФ. Указанное требование применяется вне зависимости от технологии сбора ПДн².

Действующее законодательство РФ не располагает необходимым и достаточным понятийным аппаратом, позволяющим решить задачу надлежащей трактовки норм 242-ФЗ: в частности, термин «сбор персональных данных» не определен в 152-ФЗ. Выход из сложившейся ситуации может быть найден в обращении к ст.2 «Модельного закона о персональных данных», принятого в городе Санкт-Петербурге 16.10.1999 Постановлением 14-19 на 14-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ. В соответствии с «Модельным законом» под сбором ПДн понимаются действия, направленные на получение оператором ПДн от субъектов этих данных. Необходимо отметить, что получение ПДн от субъектов этих данных может быть осуществлено как в непосредственной форме (например, путем устного или письменного сообщения ПДн, передачи материальных носителей ПДн, заполнения различных электронных форм), так и в опосредованной форме – при взаимодействии оператора с другими физическими или юридическими лицами (например, представителями субъекта). Кроме того, исходя из комментариев Минкомсвязи РФ, можно сформулировать следующее определение сбора ПДн – целенаправленные действия оператора или специально привлеченных оператором для этого третьих лиц по получению ПДн непосредственно от субъекта ПДн.

Другими словами, операторы обязаны при получении ПДн от субъектов-граждан РФ обеспечивать запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн с использованием БД на территории РФ. Необходимо отметить, что требование распространяется только на обработку ПДн при их сборе. Таким образом, можно сделать вывод о том, что последующие действия с ПДн могут производиться в БД на территории иностранных государств. Кроме того, изменения в 152-ФЗ не затрагивают трансграничную передачу ПДн.

Стратегии выполнения требований 242-ФЗ в отношении размещения БД с ПДн

В связи с противоречивостью и фрагментарностью правоприменительной практики и разъяснений от уполномоченных органов по новым требованиям к обработке ПДн в настоящий момент затруднительно сделать однозначные выводы о наиболее оптимальных стратегиях выполнения указанных требований операторами, обладающими БД с ПДн российских граждан за пределами территории РФ.

Однако могут быть определены следующие возможные стратегии, которые можно комбинировать между собой:

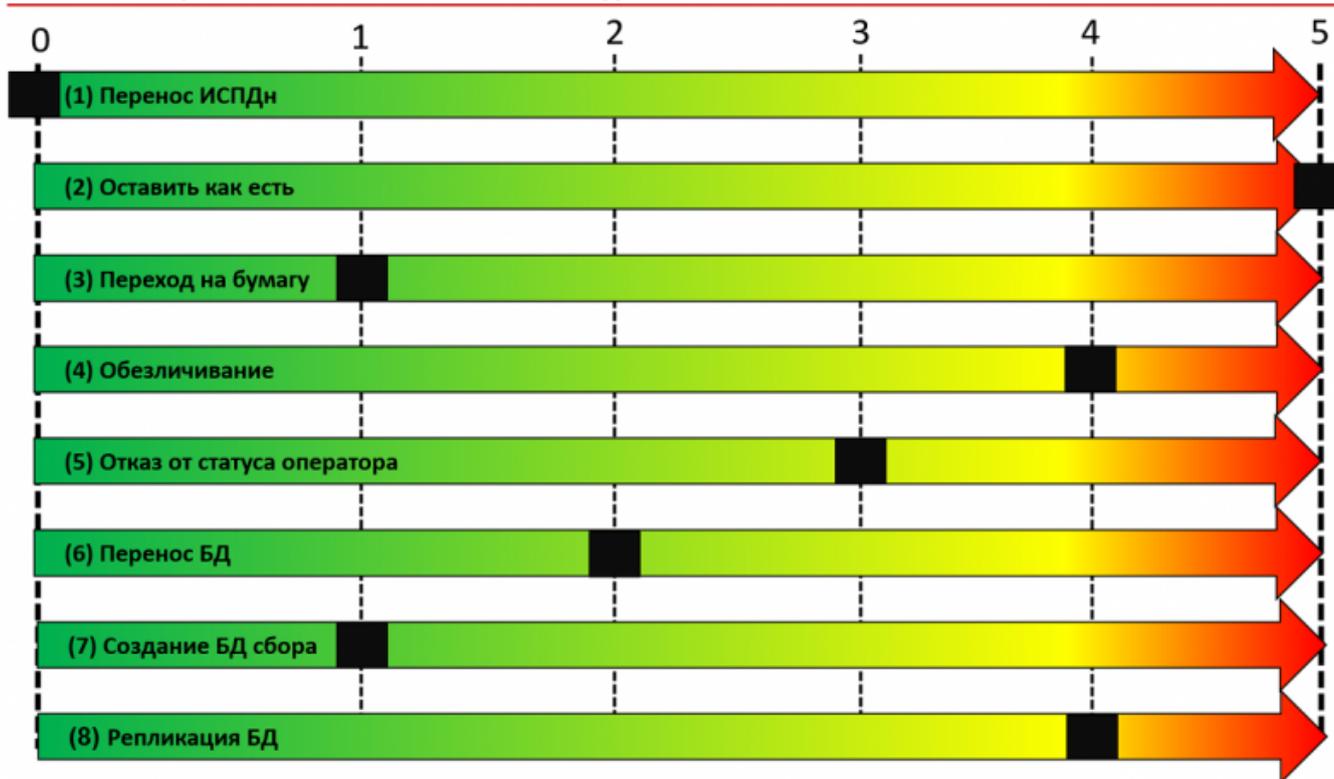
1. перенос информационной системы с ПДн (далее - ИСПДн) целиком на территорию РФ;
2. не осуществление действий, связанных с модификацией порядка функционирования и (или) структуры ИСПДн;
3. отказ от обработки ПДн с помощью средств вычислительной техники (автоматизированной обработки ПДн);
4. обезличивание ПДн (с возможностью обратного сопоставления и без такового) при передаче в зарубежные БД;
5. передача ИСПДн иностранным юридическим лицам. При этом операторами ПДн при обработке в подобных системах становятся иностранные юридические лица, не работающие на территории РФ;
6. отделение БД от серверов приложений, с последующим переносом БД с ПДн на территорию РФ;
7. создание на территории РФ промежуточной БД с целью хранения, использования и актуализации в ней собранных в РФ ПДн, с возможностью последующей передачи таких ПДн для обработки другому оператору, в том числе за границу;
8. репликация БД, которая находится вне территории РФ. Реплика БД помещается на территорию РФ и синхронизируется с зарубежной БД на регулярной основе.

Вышеперечисленные стратегии формировались исходя из презумпции, что обработка ПДн в рамках осуществления процедур по обеспечению непрерывности ИТ-инфраструктуры и восстановления её после сбоев, разработки и тестирования программных модулей информационных систем (далее - ИС), не регулируется напрямую требованиями 242-ФЗ в части размещения БД с ПДн на территории РФ. Данное предположение основывается на следующем доводе: в рамках резервной ИТ-инфраструктуры и сред разработки и тестирования программных модулей ИС не осуществляется сбор ПДн субъектов. ПДн передаются в указанную инфраструктуру и среды из иных БД с ПДн. В целях минимизации юридических рисков, связанных с вышеуказанной обработкой ПДн в средах разработки и тестирования программных модулей ИС, Оператору рекомендуется рассмотреть возможность применения технологий обезличивания (обратимого и необратимого) ПДн.

Необходимо отметить, что представленные стратегии рассматривают только вопросы логики распределения информационных

потоков внутри и между ИСПДн, но не затрагивают вопросы правового характера. Также стоит отметить, что каждой из вышеозначенных стратегий выполнения требований 242-ФЗ сопутствует соответствующий набор юридических рисков, который может быть проиллюстрирован интегральным показателем (см. Рисунок 1), состоящим из оценки вероятности выявления правонарушения (осуществить выявление несоответствия могут органы государственной власти, в лице Роскомнадзора и Прокуратуры, субъекты ПДн, контрагенты оператора и иные лица), а также оценки вероятности дальнейшего доказывания факта правонарушения в суде.

Рисунок 1. Оценка интегрального уровня юридических рисков в зависимости от стратегии



Оценка вероятности выявления правонарушения и его доказывания представляет собой экспертное мнение, основанное на соответствующих знаниях, навыках и опыте, и не учитывает оценку возможности нарушения оператором требования об уведомлении Роскомнадзора в части местонахождения БД с ПДн и привлечения оператора к юридической ответственности по ст.19.7 КоАП РФ – так как информационное письмо от имени оператора о внесении изменений в сведения в реестре операторов (в части местонахождения БД с ПДн), осуществляющих обработку ПДн, формируется и направляется в Роскомнадзор централизованно, вне зависимости от выбора той или иной стратегии выполнения требований 242-ФЗ.

Общей юридической рекомендацией для операторов ИСПДн является соблюдение оператором следующих принципов в отношении ПДн граждан РФ:

1. сбор ПДн, в том числе с территории иностранных государств, ведется только в БД на территории РФ;
2. объем и актуальность ПДн, хранящихся в БД на территории РФ, должны быть равны или превосходить соответствующие показатели в отношении ПДн, хранящихся в зарубежных БД;
3. получение новых ПДн посредством использования (анализа) имеющихся в наличии ПДн, которые были ранее собраны в БД на территории РФ и переданы за рубеж, может производиться посредством зарубежных БД и без предварительной локализации в РФ;
4. желательным, но не обязательным³⁾, является размещение на территории РФ тех БД с ПДн, которые оператор официально (согласно собственным локальным актам, описывающим ИСПДн) считает составной частью своих ИСПДн.

Рекомендуется отслеживать пояснения и мнения Минкомсвязи, Роскомнадзора и других органов государственной власти РФ по поводу выполнения новых требований и следить за правоприменительной и судебной практикой реализации норм 242-ФЗ.

[персональные данные, аналитика](#)

¹⁾ В качестве примера можно привести работу различных Интернет-ресурсов с удаленной регистрацией пользователей: операторам этих ресурсов придется либо собирать сведения о гражданстве своих пользователей с последующей обработкой персональных данных в разных базах данных, либо полностью локализовать обработку персональных данных в базах данных на территории РФ.

²⁾ Хотя законодатель отдельно и выделяет использование информационно-телекоммуникационной сети «Интернет».

³⁾ Если оператор, например, выбирает стратегии использования промежуточной БД или репликации БД, то находящиеся за рубежом БД не должны юридически относиться к российским ИСПДн, и в отношении этих БД должен быть определен свой оператор – орган власти иностранного государства, иностранное физическое лицо или иностранное юридическое лицо. Организация передачи ПДн из БД сбора в БД дальнейшей обработки или синхронизация между российской БД и зарубежной БД должны оформляться (посредством соответствующих соглашений или поручений) как трансграничная передача ПДн. Если же

оператор решит отнести оставшиеся за границей БД с ПДн к своим ИСПДн, то соответствующие сведения об иностранном местонахождении БД необходимо будет включить в уведомление об обработке ПДн, направляемое в Роскомнадзор. Это серьезно увеличит шансы оператора попасть в план проверок Роскомнадзора или иным образом почувствовать на себе его пристальное внимание.

From:

<https://sps-ib.ru:80/> - **Справочно-правовая система по информационной безопасности**

Permanent link:

<https://sps-ib.ru:80/analitika:242-fz>



Last update: **2018/05/23 14:02**