**СВОДКА**

**предложений по итогам размещения** **текста проекта**

приказа Роскомнадзора «Об утверждении Требований по оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»

ID проекта: **02/08/08-22/00130696**

Ссылка на проект: **https://regulation.gov.ru/projects/List/AdvancedSearch#npa=130696**

Дата проведения публичного обсуждения: **25.08.2022 – 21.09.2022**

Количество экспертов, участвовавших в обсуждении: 8

Отчет сгенерирован:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Участник обсуждения** | **Позиция участника обсуждения** | **Статус рассмотрения** | **Комментарии разработчика** |
| 1 | Дьяков Сергей Николаевич | В соответствии с п.7 Требований к защите....., утв. постановлением Правительства РФ от 01.12.2012 № 1119 определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 ст.18.1. ФЗ "О персональных данных". Проект приказа в полной мере не учитывает данную норму. Проектируемый акт в предлагаемой редакции неприменим к указанному выше постановлению. Необходима его доработка с целью его применения операторами при выполнении норм указанного постановления.Кроме того, в соответствии с пунктом 5 части 1 ст.18.1. ФЗ "О персональных данных" необходима как оценка возможного вреда субъектам, так и соотношение данного вреда к мерам, направленным на выполнение обязанностей оператора. Предлагаемая редакция НПА не позволит выполнить в полной мере требования п. 5 части 1 ст.18.1. ФЗ "О персональных данных" так как не содержит соотношения между вредом и мерами, что повлечет за собой двойное толкование и в случае учета дифференциации вреда в КоАП РФ коррупционные риски.Предлагается предусмотреть актом как вред, так и необходимые меры. | Не учтено | Проект приказа устанавливает требования к оценке вреда применительно к деятельности оператора по обработке персональных данных и не затрагивает вопросы, связанные с обеспечением безопасности персональных данных, регулирование которых отнесено к компетенции ФСБ и ФСТЭК.Таким образом, предлагаемое регулирование не приведет к различному правоприменению.Дополнительно сообщаем, что согласно п. 5 ч. 1 ст. 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Закон) Роскомнадзор устанавливает требования исключительно к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона. Соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом, оператор определяет самостоятельно. |
| 2 | Свистельников Антон | 1. Требования не содержат сведений о том, что является объектом оценки вреда (например, последствия инцидента, процесс обработки персональных данных и т.п.).Таким образом не понятно, данная оценка вреда осуществляется в рамках проводимых ответственным лицом за обработку ПДн мероприятий по внутреннему контролю и аудиту соответствия обработки ПДн законодательству в области обработки ПДн, или же оценка вреда осуществляется после возникновения инцидента?Предложение:1.1. установить в требованиях объект оценки вреда явным образом;1.2. установить в требованиях случаи при которых необходимо проводить оценку вреда;1.3. установить в требованиях цели и назначение оценки вреда. | Не учтено | Предложение не поддерживается ввиду того, что на уровне Закона уже определен предмет оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона (далее – оценка вреда), а именно деятельность по обработке персональных данных.По вопросу о дополнении проекта приказа случаями, при которых проводится оценка вреда, сообщаем, что по смыслу правовой конструкции ч. 1 ст. 18.1 Закона оператор вправе самостоятельно определить случаи проведения оценки вреда. |
| 2. Требования не содержат сведений о том, в какие сроки проводится оценка вреда и с какой периодичностью.Предложение:2.1. установить периодичность и сроки в которые должна быть проведена оценка. | Не учтено | Нормой, во исполнение которой подготовлен проект приказа, установлено, что оператор проводит оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона, в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных.Положениями ч. 1 ст. 18.1 Закона закреплено, что оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами.Определение методики осуществления оценки вреда, а также требований к составу и порядку образования комиссии не является предметом предлагаемого регулирования (предметом приказа). Полномочиями по определению методики, а также требований к составу и порядку образования комиссии Роскомнадзор не наделен.Таким образом, определение срока или периода проведения оценки, а также требований к составу и порядку образования комиссии относится к компетенции оператора.Закрепление на законодательном уровне требований к сроку или периоду проведения оценки вреда, а также составу и порядку образования комиссии будет являться ограничением права оператора на самостоятельное определение мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом. |
| 3. В п.2 не указан минимально допустимый состав комиссии.Предложение:3.1. определить минимальный состав комиссии – 2-3 члена комиссии и председатель;3.2. определить, что ответственный за обработку персональных данных должен являться председателем комиссии;3.3. переформулировать пункт основываясь на том, что оценку может проводить только комиссия утвержденная приказом руководителя организации или ответственным за обработку, в состав комиссии при этом могут входить представители сторонних организаций. |
| 4. Не понятно каким образом при определении степени вреда необходимо учитывать сведения приведенные в п.3 и где эти критерии должны отразиться, например, в протоколе оценки вреда или в акте. В п. 2 Требований к оценке вреда, который может быть причинен субъекта персональных данных в случае нарушения Федерального закона «О персональных данных» (далее – Требования) указано, что Оператор для целей оценки вреда в соответствии с приложением к настоящим Требованиям определяет одну из следующих степеней вреда, который может быть причинен субъекту персональных данных в случае нарушения Закона о персональных данных: а) высокая; б) средняя; в) низкая. В данном приложении указана норма закона, которая может быть нарушена и степень вреда, которая может быть причинена субъекту при нарушении таких требований закона. Вместе с тем, в п. 3 Требований к оценке вреда, который может быть причинен субъекту персональных данных в случае нарушения Федерального закона «О персональных данных» (указываются критерии, которые учитываются при оценке вреда. К ним относятся: цели обработки, количество субъектов ПДн, категории Пдн, перечень действий с ПДн, способы обработки, количество третьих лиц, которым поручена обработка Пдн. Таким образом возникает вопрос, как сопоставляются критерии при оценке степени вреда: по количеству целей, количеству субъектов и пр., или по нарушениям норм законодательства в области ПДн?Предложение:4.1. добавить требование по использованию критериев для оценки вреда и описание их влияния на результат оценки вреда. | Частично учтено | По вопросу о доработке критериев, применяемых при определении степени вреда, сообщаем, что на этапе согласования Приказа с заинтересованными федеральными органами исполнительной власти в п. 3 Приказа внесены изменения. В настоящий момент критериями определения степени вреда являются количество субъектов персональных данных, чьи персональные данные обрабатываются, категории обрабатываемых персональных данных, а также вид нарушения законодательства Российской Федерации в области персональных данных, допущенного оператором.Дополнительно сообщаем, что результат оценки вреда отражается в акте оценки вреда. |
| 5. В п.5 необходимо добавить подпункт со сведениями об объекте оценки и/или причинах, инициировавших проведение оценки. | Не учтено | Нормой, во исполнение которой подготовлен проект приказа, установлено, что оператор проводит оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона, в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных.Положениями ч. 1 ст. 18.1 Закона закреплено, что оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами.Определение объекта и причин оценки вреда не является предметом предлагаемого регулирования (предметом приказа). Полномочиями по определению объекта и причин оценки вреда Роскомнадзор не наделен.Таким образом, определение объекта и причин оценки вреда относится к компетенции оператора.Закрепление на законодательном уровне объекта и причин проведения оценки вреда будет являться ограничением права оператора на самостоятельное определение мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом. |
| 6. Из п.5.д непонятно как должен выглядеть результат оценки вреда. Какой результат оценки будет если нарушены нормы относящиеся к разным степеням вреда. Например, в компании несколько процессов обработки ПДн. По одному процессу средняя степень вреда. По второму есть незначительные нарушения. И по третьему будет, исходя из приложения, высокая степень вреда. Какая степень вреда в таком случае будет результатом оценки? В случае проведения оценки вреда, при наличии нарушения, оно может быть сразу же исправлено. Как отражать результат оценки вреда при отсутствии нарушений?Предложение:6.1. привести пример оценки вреда в приложении к приказу;6.2. привести форму акта в приложении к приказу. | Не учтено | Предметом проекта приказа являются требования к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона.Результат оценки вреда отражается в акте оценки вреда, требования к которому приведены в проекте приказа. |
| 3 | Перова ЕкатеринаПАО "Ростелеком" | Позиция ПАО "Ростелеком" к проекту приказа РКН «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» (https://regulation.gov.ru/projects#npa=130696)В соответствии с пунктом 5 части 1 статьи 18.1 Федерального закона «О персональных данных» (далее – ФЗ), в редакции, вступающей в силу с 1 марта 2023 года, оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных ФЗ и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных ФЗ и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено данным ФЗ или другими федеральными законами. К таким мерам, в частности, относится оценка вреда в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных, который может быть причинен субъектам персональных данных в случае нарушения ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ.Таким образом, оператор обязан самостоятельно провести оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения ФЗ в соответствии с требованиями, установленными Роскомнадзором.Во исполнение приведенной нормы ФЗ Роскомнадзором разработан проект соответствующих Требований, к которому имеются следующие замечания:1. Пунктом 3 проекта Требований устанавливаются критерии, которые должны учитываться оператором при определении степени вреда, который может быть причинен субъекту персональных данных в случае нарушения ФЗ. Полагаем необходимым определить методику применения критериев, указанных в пункте 3 проекта Требований, установив каким образом они влияют на определение степени вреда, в ином случае неясно каким образом данные критерии могут быть применены оператором.Кроме того, проектируемый перечень критериев носит исчерпывающий характер и в нем отсутствует указание на то, что степень вреда оценивается, в том числе, исходя из вида нарушения ФЗ. При этом в приложении к проекту Требований приведен перечень всех возможных нарушений ФЗ, ранжированный по степеням вреда. Следовательно, степень вреда не будет подлежать самостоятельной оценке операторами в соответствии с критериями, установленными пунктом 3 проекта Требований, а заранее определена в приложении к проекту Требований, исходя только из одного критерия – вида нарушения ФЗ, что представляется не отвечающим требованиям ФЗ. | Не учтено | Нормой, во исполнение которой подготовлен проект приказа, установлено, что оператор проводит оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона, в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных.Положениями ч. 1 ст. 18.1 Закона закреплено, что оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами.Определение методики осуществления оценки вреда не является предметом предлагаемого регулирования (предметом приказа). Полномочиями по определению методики Роскомнадзор не наделен.Положениями ч. 1 ст. 18.1 Закона закреплено, что оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено указанным Федеральным законом или другими федеральными законами. Таким образом, определение методики проведения оценки вреда относится к компетенции оператора, в связи с чем указание в Приказе данных положений выходит за пределы полномочий Роскомнадзора. |
| 2. Полагаем целесообразным пункт 5 проекта Требований дополнить указанием на цель обработки персональных данных, а также наименованием информационной системы персональных данных, поскольку, в соответствии с ФЗ, объединение БД персональных данных, обрабатываемых в различных целях, не допускается. Соответственно, в целях эффективной оценки вреда полагаем целесообразным проводить оценку, оформляемую актом оценки вреда, в отношении каждой информационной системы персональных данных, содержащей персональные данные, обрабатываемые в соответствии с конкретной целью. | Не учтено | Проектом приказа предлагается издание оператором акта оценки вреда в качестве подтверждения соблюдения оператором обязательного требования.Так, в акте должно быть указано наименование (ФИО) и адрес оператора, дата издания акта, дата проведения оценки, ФИО и должность лиц, проводивших оценку, а также ее результат (т.е. определенные степени вреда).Оператор вправе проводить оценку вреда по самостоятельному усмотрению применительно к видам осуществляемой деятельности. Положения Закона и проекта приказа не ограничивают право оператора осуществлять оценку применительно к каждой информационной системе персональных данных либо в их совокупности, при осуществлении конкретных видов деятельности, предусматривающих конкретные цели обработки персональных данных. |
| 3. Приложение к проекту Требований предлагается исключить либо скорректировать и изложить его в целях удобства проведения оценки вреда операторами в качестве информационного материала, перечисляющего те нарушения требований ФЗ, которые могут повлечь вред для субъекта персональных данных. При этом обращаем внимание, что ряд нарушений ФЗ, содержащихся в разделе «Низкая степень вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона о персональных данных», связанных с ненаправлением в Роскомнадзор различной информации и сведений, не может повлечь причинение вреда субъектам персональных данных, поскольку не оказывает непосредственного влияния на обработку персональных данных оператором. | Не учтено | Нормой, во исполнение которой подготовлен проект приказа, установлено, что оператор проводит оценку вреда в случае нарушения Закона, в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных.Исходя из положений Закона, соответствующие требования к оценке вреда должны быть закреплены на законодательном уровне.Следовательно, исключение приложения к проекту приказа, которым определены степени вреда в зависимости от нарушений Закона, невозможно в силу требований Закона.Указание на то, что непредставление информации по запросу Роскомнадзора не оказывает непосредственного влияния на обработку персональных данных, является некорректным.Своевременное предоставление информации оператором напрямую влияет на право субъекта персональных данных на получение информации, касающейся обработки его персональных данных, которое закреплено Законом. Кроме того, предоставление оператором информации в установленный срок позволяет Роскомнадзору принимать меры реагирования в случае выявления неправомерной обработки персональных данных, что прежде всего направлено на защиту прав и законных интересов граждан. |
| 4 | Обухова Евгения | В отношении проекта приказа РКН «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных».С учетом принятого 266-ФЗ, оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных законодательством, если иное не предусмотрено федеральными законами.Перечень мер является открытым (ст.18.1 152-ФЗ) и включает оценку вреда субъектам ПДн в случае нарушения закона в соответствии с требованиями, установленными РКН (а также соотношение вреда и принимаемых оператором мер). Таким образом, оператор обязан самостоятельно провести оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения ФЗ в соответствии с требованиями, установленными Роскомнадзором.1. Пунктом 3 проекта Требований устанавливаются факторы, которые учитываются при определении степени вреда, причем перечень факторов закрытый.При этом в приложении к проекту приведен перечень всех возможных нарушений 152-ФЗ, заранее ранжированный по степени причиненного субъекту вреда (формальный состав). В этой связи непонятно, какова роль факторов для проведения оценки в принципе, поскольку при наступлении любого из условий, приведенных в Приложении, степень вреда считается установленной. Предлагает уточнить особенности применения Приложения к проекту Требований.Предлагаем сформулировать перечень открытым, в противном случае необходима методика учета каждого из факторов в общем весе оценки степени возможного вреда. | Не учтено | Нормой, во исполнение которой подготовлен проект приказа, установлено, что оператор проводит оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона, в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных.Положениями ч. 1 ст. 18.1 Закона закреплено, что оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами.Определение методики осуществления оценки вреда не является предметом предлагаемого регулирования (предметом приказа). Полномочиями по определению методики Роскомнадзор не наделен.Положениями ч. 1 ст. 18.1 Закона закреплено, что оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено указанным Федеральным законом или другими федеральными законами. Таким образом, определение методики проведения оценки вреда относится к компетенции оператора, в связи с чем указание в Приказе данных положений выходит за пределы полномочий Роскомнадзора. |
| 2. Приложение к проекту Требований предлагается дополнить условиями его применения (с учетом положений самих Требований). Также обращаем внимание, что для ряд нарушений 152-ФЗ, которые не влекут причинения вреда субъектам ПДн, отнесены к низкой степени вреда (например, ненаправление в РКН различной информации и сведений, которое само по себе никак не причиняет вред правам субъектов ПДн). | Не учтено | Проектом приказа установлены критерии определения оператором степени вреда в зависимости от нарушения обязательных требований, предусмотренных Законом.Определение методики (условий) осуществления соответствующей оценки, не является предметом предлагаемого регулирования (предметом приказа), в связи с чем оператор вправе разработать указанную методику (условия) самостоятельно.Указание на то, что непредставление информации по запросу Роскомнадзора не оказывает непосредственного влияния на обработку персональных данных, является некорректным.Своевременное предоставление информации оператором напрямую влияет на право субъекта персональных данных на получение информации, касающейся обработки его персональных данных, которое закреплено Законом. Кроме того, предоставление оператором информации в установленный срок позволяет Роскомнадзору принимать меры реагирования в случае выявления неправомерной обработки персональных данных, что прежде всего направлено на защиту прав и законных интересов граждан. |
| 5 | ПАО Сбербанк | С целью исключения рисков неоднозначного толкования и обеспечения практической применимости формируемых требований предлагаем закрепить в тексте, следующие положения: 1) предмет проведения оценки вреда - процессы в деятельности оператора ПДн, предусматривающие обработку ПДн; 2) обязанность оператора персональных данных самостоятельно определить порядок и методику проведения оценки вреда;3) случаи проведения оценки вреда (до начала обработки, при изменении условий обработки, в случае установления факта неправомерной передачи ПДн и т.п.); 4) дальнейшие действия оператора ПДн, исходя из определенной степени вреда. | Не учтено | Обязанность оператора проводить оценку вреда в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных, установлена п. 5 ч. 1 ст. 18.1 Закона. Указанная норма не возлагает на Роскомнадзор полномочия по установлению методики осуществления оценки вреда.Положениями ч. 1 ст. 18.1 Закона закреплено, что оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено указанным Федеральным законом или другими федеральными законами. Таким образом, определение методики проведения оценки вреда относится к компетенции оператора, в связи с чем указание в Приказе данных положений выходит за пределы полномочий Роскомнадзора.По вопросу о дополнении Приказа случаями, при которых проводится оценка вреда, сообщаем, что по смыслу правовой конструкции ч. 1 ст. 18.1 Закона оператор вправе самостоятельно определить случаи проведения оценки вреда.Предложение ПАО Сбербанк о закреплении предмета оценки вреда в Приказе Роскомнадзора не поддерживается ввиду того, что на уровне Закона уже определен предмет оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона (далее – вред), а именно деятельность оператора по обработке персональных данных. |
| Необходимо обеспечить корреляцию между степенями вреда, установленным п. 2 Требований, и критериев, установленных п. 3 Требований.При определении степени вреда необходимо также учитывать такие критерии, как: - категории субъектов ПДн (работники, клиенты и т.п.), перечень и объем обрабатываемых ПДн; - используемые при их обработке информационные технологии (Big data, облачные сервисы, AI и т.п.). Предлагаем конкретизировать перечень действий с ПДн, которые фактически могут влиять на уровень вреда субъекту ПДн. - передача третьим лицам (в т.ч. трансграничная), распространение) ПДн/ | Не учтено | По вопросу о доработке критериев, применяемых при определении степени вреда, сообщаем, что на этапе согласования Приказа с заинтересованными федеральными органами исполнительной власти в п. 3 Приказа внесены изменения. В настоящий момент критериями определения степени вреда являются количество субъектов персональных данных, чьи персональные данные обрабатываются, категории обрабатываемых персональных данных, а также вид нарушения законодательства Российской Федерации в области персональных данных, допущенного оператором. |
| Целесообразно дополнить содержание акта оценки вреда перечнем мер по минимизации вреда. Например, принять дополнительные меры по снижению вреда или ограничению / запрету обработки ПДн, в случае высокой степени вреда. | Не учтено | В отношении предложения о дополнении Приказа положениями о действиях оператора после проведения оценки вреда сообщаем, что согласно п. 5 ч. 1 ст. 18.1 Закона оператор обязан осуществлять соотношение оценки вреда и принимаемых оператором мер, направленных на обеспечение обязанностей, предусмотренных Законом. Данная норма не предусматривает полномочия Роскомнадзора по определению действий оператора после проведения оценки вреда, в связи с чем предложение ПАО Сбербанк не может быть поддержано. |
| Норма:Несоблюдение оператором требований по уведомлению уполномоченного органа по защите прав субъектов персональных данных о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных.Предложение:Предлагаем переместить в категорию «Низкая степень вреда»КомментарийИсходя из природы нарушения и требования, предусмотренного ч. 3.1 ст. 21 152-ФЗ, отсутствует потенциальная причинноследственная связь между нарушением указанного требования и каким-либо вредом субъекту ПДнНорма:Несоблюдение оператором требований по уведомлению уполномоченного органа по защите прав субъектов о своем намерении осуществлять трансграничную передачу персональных данныхПредложение:Предлагаем переместить в категорию «Низкая степень вреда»Комментарий:Исходя из природы нарушения и требования, предусмотренного ч. 3 ст. 12 152-ФЗ, отсутствует потенциальная причинноследственная связь между нарушением указанного требования и каким-либо вредом субъекту ПДнНорма:Несоблюдение оператором требований по предоставлению по запросу уполномоченного органа по защите прав субъектов персональных данных сведений, предусмотренных пунктами 1-3 части 5 статьи 12 Закона о персональных данныхПредложение:Предлагаем переместить в категорию «Средняя степень вреда»Комментарий:Исходя из природы нарушения и требования, предусмотренного ч. 6 ст. 12 152-ФЗ, отсутствует потенциальная причинноследственная связь между нарушением указанного требования существенным вредом субъекту ПДнНорма:Несоблюдение оператором требований по опубликованию или обеспечению неограниченного доступа к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данныхПредложение:Предлагаем переместить в категорию «Низкая степень вреда»Комментарий:Исходя из природы нарушения и требования, предусмотренного ч. 2 ст. 18.1 152-ФЗ, отсутствует потенциальная причинноследственная связь между нарушением указанного требования и каким-либо вредом субъекту ПДнНорма:Неинформирование оператором лиц, осуществляющих обработку персональных данных без использования средств автоматизации, о факте обработке ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработкиПредложение:Предлагаем переместить в категорию «Низкая степень вреда»Комментарий:Исходя из природы нарушения и требования, предусмотренного п. 6 Постановления Правительства РФ от 15.09.2008 № 687, отсутствует потенциальная причинно-следственная связь между нарушением указанного требования и каким-либо вредом субъекту ПДнНорма:Неназначение оператором лица, ответственного за организацию обработки персональных данныхПредложение:Предлагаем переместить в категорию «Низкая степень вреда»Комментарий:Исходя из природы нарушения и требования, предусмотренного ч. 1 ст. 22.1 152-ФЗ, отсутствует потенциальная причинноследственная связь между нарушением указанного требования и каким-либо вредом субъекту ПДн | Не учтено | По предложениям о снижении степени вреда в отношении отдельных нарушений законодательства Российской Федерации в области персональных данных сообщаем следующее.Несоблюдение оператором требований по уведомлению Роскомнадзора об инцидентах с персональными данными в соответствии с ч. 3.1 ст. 21 Закона относится к высокой степени вреда ввиду того, что распространение персональных данных влечет негативные последствия для субъектов персональных данных, в том числе возможное совершение мошеннических действий с использованием персональных данных граждан. Уведомление о произошедшем инциденте с персональными данными позволит Роскомнадзору оперативно принимать меры по пресечению распространения персональных данных граждан, а также иные меры по восстановлению нарушенных прав граждан.По вопросу снижения степени вреда в отношении нарушения, касающегося несоблюдения оператором требований ст. 12 Закона к порядку осуществления трансграничной передачи, сообщаем, что уведомление об осуществлении трансграничной передачи является обязательным условием трансграничной передачи, в связи с чем невыполнение установленных требований расценивается как неправомерная передача персональных данных граждан, в том числе без учета рисков возможного нарушения их прав и законных интересов как субъектов персональных данных.Опубликование оператором политики в отношении обработки персональных данных согласно ч. 2 ст. 18.1 Закона направлено на соблюдение обязанности по информированию субъекта персональных данных о порядке обработки его персональных данных, в связи с чем полагаем целесообразным отнести нарушение положений ч. 2 ст. 18.1 Закона к средней степени вреда.По предложению о снижении степени вреда в отношении нарушения, связанного с невыполнением обязанности оператора по информированию лиц, осуществляющих обработку персональных данных без использования средств автоматизации, в том числе о правилах такой обработки, сообщаем, что несоблюдение работниками оператора требований законодательства Российской Федерации в области персональных данных может повлечь нарушение законных прав субъектов персональных данных.По вопросу снижения степени вреда в отношении нарушения, связанного с отсутствием ответственного за организацию обработки персональных данных, сообщаем, что на указанное лицо возлагаются обязанности, предусмотренные ч. 4 ст. 22.1 Закона. Несоблюдение данных требований может повлечь нарушение прав и законных интересов субъектов персональных данных. |
| Норма:Несоблюдение оператором требований по разъяснению субъекту персональных данных юридических последствий отказа предоставить его персональные данные, в случае если предоставление персональных данных является обязательным в соответствии с федеральным закономПредложение:Предлагаем переместить в категорию «Высокая степень вреда»Комментарий:Исходя из природы нарушения и требования, предусмотренного ч. 2 ст. 18 152-ФЗ, вред субъекту ПДн, который может быть причинен потенциальным нарушением, соразмерим с отсутствием основания на обработку ПДн, т.е. нарушению, отнесенному к высокой степени вреда. Более того, нарушение прямо связано со взаимодействием оператора ПДн с субъектом ПДн.Норма:Несоблюдение оператором требований по предоставлению субъекту персональных данных информации до начала обработки персональных данных, в случае если персональные данные получены не от субъекта персональных данных, за исключением случаев, предусмотренных частью 4 статьи 18 Закона о персональных данныхПредложение:Предлагаем переместить в категорию «Высокая степень вреда»Комментарий:Исходя из природы нарушения и требования, предусмотренного ч. 3 ст. 18 152-ФЗ, вред субъекту ПДн, который может быть причинен потенциальным нарушением, соразмерим с отсутствием основания на обработку ПДн, т.е. нарушению, отнесенному к высокой степени вреда. Более того, нарушение прямо связано со взаимодействием оператора ПДн с субъектом ПДнНорма:Несоблюдение оператором требований о совместимости обрабатываемых персональных данных с целями сбора персональных данныхПредложение:Предлагаем переместить в категорию «Высокая степень вреда»Комментарий:Исходя из природы нарушения и требования, предусмотренного ч. 2 ст. 5 152-ФЗ, вред субъекту ПДн, который может быть причинен потенциальным нарушением, соразмерим с нарушениями, отнесенными к высокой степени вреда.Норма:Несоблюдение оператором требований к содержанию и объему персональных данных в части соответствия заявленным целям обработкиПредложение:Предлагаем переместить в категорию «Высокая степень вреда»Комментарий:Исходя из природы нарушения и требования, предусмотренного ч. 5 ст. 5 152-ФЗ, вред субъекту ПДн, который может быть причинен потенциальным нарушением, соразмерим с нарушениями, отнесенными к высокой степени вреда.Норма:Несоблюдение оператором требований по уточнению персональных данных в случае подтверждения факта неточности персональных данных на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документовПредложение:Предлагаем переместить в категорию «Высокая степень вреда»Комментарий:Исходя из природы нарушения и требования, предусмотренного ч. 2 ст. 18 152-ФЗ, вред субъекту ПДн, который может быть причинен потенциальным нарушением, соразмерим с отсутствием основания на обработку ПДн, т.е. нарушению, отнесенному к высокой степени вреда. Более того, нарушение прямо связано со взаимодействием оператора ПДн с субъектом ПДн.Норма:Несоблюдение оператором требований к содержанию типовых форм документов, характер информации которых предполагает или допускает включение в них персональных данныхПредложение:Предлагаем переместить в категорию «Средняя степень вреда»Комментарий:Исходя из природы нарушения и требования, предусмотренного п. 7 Постановления Правительства РФ от 15.09.2008 № 687, вред субъекту ПДн, который может быть причинен потенциальным нарушением, соразмерим с нарушениями, отнесенными к средней степени вреда и также связанным с разработкой внутренних нормативных документов.Норма:Несоблюдение оператором требований к условиям ведения журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целяхПредложение:Предлагаем переместить в категорию «Средняя степень вреда»Комментарий:Исходя из природы нарушения и требования, предусмотренного п. 8 Постановления Правительства РФ от 15.09.2008 № 687, вред субъекту ПДн, который может быть причинен потенциальным нарушением, соразмерим с нарушениями, отнесенными к средней степени вреда и также связанным с разработкой внутренних нормативных документов.Норма:Отсутствие у оператора документов, устанавливающих места хранения персональных данных (материальных носителей), а также перечня лиц, осуществляющих обработку персональных данных либо имеющих к ним доступПредложение:Предлагаем переместить в категорию «Средняя степень вреда»Комментарий:Исходя из природы нарушения и требования, предусмотренного п. 13 Постановления Правительства РФ от 15.09.2008 № 687, вред субъекту ПДн, который может быть причинен потенциальным нарушением, соразмерим с нарушениями, отнесенными к средней степени вреда и также связанным с разработкой внутренних нормативных документов.Норма:Несоблюдение оператором требований по раздельному хранению персональных данных (материальных носителей), обработка которых осуществляется в различных целях без использования средств автоматизацииПредложение:Предлагаем переместить в категорию «Средняя степень вреда»Комментарий:Исходя из природы нарушения и требования, предусмотренного п. 14 Постановления Правительства РФ от 15.09.2008 № 687, вред субъекту ПДн, который может быть причинен потенциальным нарушением, соразмерим с нарушениями, отнесенными к средней степени вреда и также связанным с разработкой внутренних нормативных документов. | Не учтено | По предложениям о повышении степени вреда в отношении отдельных нарушений законодательства Российской Федерации в области персональных данных сообщаем следующее.Положения ч. 2 ст. 18 Закона, устанавливающие обязанность оператора по разъяснению субъекту персональных данных юридических последствий отказа предоставления персональных данных, не предполагает осуществление обработки персональных данных гражданина в случае его отказа, а равно не является ограничением или нарушением его прав непосредственно при обработке его персональных данных.По вопросу повышения степени вреда по нарушению, связанному с несоблюдением оператором требований по уточнению персональных данных в случае подтверждения факта их неточности, сообщаем, что невыполнение требований ч. 2 ст. 21 Закона несет меньшие риски по сравнению с неправомерной обработкой оператором достоверных персональных данных граждан. Несоблюдение требований ч. 3 ст. 18, ч. 2 ст. 5, ч. 5 ст. 5 Закона при условии наличия у оператора правового основания обработки персональных данных не является нарушением, соразмерным несоблюдению обязательных требований, предъявляемых к порядку и условиям обработки персональных данных, в связи с чем представляется целесообразным отнести указанное нарушение к средней степени вреда.Требования к обработке персональных данных без использования средств автоматизации установлены пп. 7, 8, 13, 14 Положения об особенностях обработки персональных данных без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15.09.2008 № 687 (далее – Положение).Указанные требования не увязаны с положениями законодательства Российской Федерации, затрагивающими права и законные интересы граждан, что позволяет отнести несоблюдение данных требований к низкой степени вреда. Дополнительно вывод об отнесении данных нарушений к низкой степени вреда подтверждается отсутствием в Кодексе Российской Федерации об административных правонарушениях составов административных правонарушений за несоблюдение оператором требований пп. 7, 8, 13, 14 Положения. |
| 6 | Национальный Совет финансового рынка | Специалисты НСФР совместно с финансовыми организациями проанализировали Проект 1 и просят разъяснить или учесть при доработке Проекта I следующее.Согласно пункту 2 Проекта оператор для целей оценки вреда в соответствии с приложением к Проекту определяет одну из следующих степеней вреда, который может быть причинен субъекту персональных данных в случае нарушения Федерального закона от 27 июля 2006 г.№ І52-ФЗ «О персональных данных » далее — Закон № І52-ФЗ):а) высокая;6) средняя; в) низкая.В приложении к Проекту указана степень вреда, который может быть причинен субъектам персональных данных, в случае каждого конкретного нарушения Закона № 152-ФЗ (приводится соотнесение нарушения требования Закона № 152-ФЗ (с реквизитами структурных единиц указанного закона) со степенью вреда, который может быть причинен субъектам персональных данных в случае соответствующего нарушения).При этом из Проекта не совсем ясен порядок осуществления оператором оценки вреда в случае нарушения им одновременно (в результате одного действия или события) нескольких положенный Закона № 152-ФЗ. В этой связи просим уточнить, необходимо ли в такой ситуации:— оценивать вред по каждому допущенному нарушению отдельно, не учитывая однократность действия (события), повлекшего нарушение прав субъекта персональных данных;либо— оценивать вред по максимальному уровню из всех допущенных нарушений Закона о персональных данных, приведенных в приложении к Проекту 1,либо— оценивать совокупный вред, но с учетом «весовых» долей нарушений каждого вида с учетом степени вреда субъекту персональных данных, причиненного каждым нарушением? | Не учтено | В случае, если при проведении оценки вреда определены различные степени вреда, подлежит применению наиболее высокая степень вреда. |
| 7 | ПАО «СУРГУТНЕФТЕГАЗ» | Содержание требований, изложенных в Проекте, не соответствует принципу правовой определенности, установленному ст.7 Федерального закона от 31.07.2020 №247-ФЗ «Об обязательных требованиях в Российской Федерации», так как не является ясным, логичным, понятным и, как следствие, является не исполнимым.Проект не содержит правил, процедур, методик проведения оценки вреда, который может быть причинен субъектам персональных данных, нарушением требований Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» (далее Закон №152-ФЗ). Из Проекта не ясно, каким образом оператор при определении степени вреда должен учесть цели, способ обработки персональных данных, количество субъектов, категории персональных данных, перечень действий с персональными данными, если степень вреда за нарушение конкретных требований Закона №152-ФЗ уже определена в приложении к Проекту без учета условий обработки персональных данных.В отсутствие пояснений к Проекту не понятно, какими принципами руководствовался, из чего исходил разработчик Проекта, определяя в приложении к Проекту степень вреда за нарушение того или иного требования Федерального закона от 27.072006 №152-ФЗ «О персональных данных». Из анализа приложения к Проекту и положений ст, 13.11 КоАП РФ, ст. 137 УК РФ (в которых установлена ответственность по степени общественной опасности нарушения) взаимосвязь не прослеживается.Учитывая изложенное, считаем, что Проект нуждается в доработке. | Частично учтено | Обязанность оператора проводить оценку вреда в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных, установлена п. 5 ч. 1 ст. 18.1 Закона. Указанная норма не возлагает на Роскомнадзор полномочия по установлению методики осуществления оценки вреда.Положениями ч. 1 ст. 18.1 Закона закреплено, что оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено указанным Федеральным законом или другими федеральными законами. Таким образом, определение методики проведения оценки вреда относится к компетенции оператора, в связи с чем указание в Приказе данных положений выходит за пределы полномочий Роскомнадзора.По вопросу о доработке критериев, применяемых при определении степени вреда, сообщаем, что на этапе согласования Приказа с заинтересованными федеральными органами исполнительной власти в п. 3 Приказа внесены изменения. В настоящий момент критериями определения степени вреда являются количество субъектов персональных данных, чьи персональные данные обрабатываются, категории обрабатываемых персональных данных, а также вид нарушения законодательства Российской Федерации в области персональных данных, допущенного оператором.Дополнительно сообщаем, что в проекте приказа определена степень вреда исходя из тяжести негативных последствий для прав и законных интересов субъектов персональных данных. |
| 8 | sun.2008@mail.ru | Целесообразно установить в законодательстве РФ единую методику расчета уровня (степени) защищенности (вреда) субъекту ПДн. Проект приказа Роскомнадзора России «Об утверждении Требований к оценке вреда, который̆ может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» обязывает операторов ПДн проводить оценку вреда, который может быть причинен субъектам ПДн. В соответствии с пунктом 5) части 2 статьи 18.1 ФЗ № 152 для оператора ПДн установлена обязанность проводить оценку вреда в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов ПДн, который может быть причинен субъектам ПДн в случае нарушения ФЗ № 152, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом. Однако степень вреда (ущерба), который может быть нанесен субъекту ПДн, уже учтена в постановлении Правительства РФ от 01.11.2012 года № 1119. Для степени вреда установлены соответствующие уровни защищенности ПДн. На основе уровней защищенности ПДн в подзаконных НПА установлены меры защиты ПДн. Операторы ПДн определяют уровень защищенности ПДн в соответствии с требованиями постановления Правительства РФ № 1119. В постановлении Правительства РФ используются, в том числе, аналогичные проекту НПА критерии оценки ущерба *«б) количество субъектов персональных данных, персональные данные которых обрабатываются; в) категории обрабатываемых персональных данных»*. Однако шкалы и методики определения степени вреда субъекту ПДн в проекте приказа и в постановлении Правительства РФ различаются. Наличие разных методик и шкал оценки вреда субъекту ПДн в разных НПА приведет к правовым коллизиям. Кроме того, не понятно каким образом цели обработки ПДн, перечень действий с ПДн и т.п. могут влиять на степень вреда субъекту ПДн.В приложении к проекту приказа «Степень вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона о персональных данных» большая часть критериев может быть использована для оценки вероятности нарушения безопасности ПДн, но не для оценки ущерба (вреда) субъекту ПДн. | Частично учтено | Обязанность оператора проводить оценку вреда в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных, установлена п. 5 ч. 1 ст. 18.1 Закона. Указанная норма не возлагает на Роскомнадзор полномочия по установлению методики осуществления оценки вреда.Положениями ч. 1 ст. 18.1 Закона закреплено, что оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено указанным Федеральным законом или другими федеральными законами. Таким образом, определение методики проведения оценки вреда относится к компетенции оператора, в связи с чем указание в Приказе данных положений выходит за пределы полномочий Роскомнадзора.Проект приказа устанавливает требования к оценке вреда применительно к деятельности оператора по обработке персональных данных и не затрагивает вопросы, связанные с обеспечением безопасности персональных данных, регулирование которых отнесено к компетенции ФСБ и ФСТЭК.Таким образом, предлагаемое регулирование не приведет к различному правоприменению.По вопросу о доработке критериев, применяемых при определении степени вреда, сообщаем, что на этапе согласования Приказа с заинтересованными федеральными органами исполнительной власти в п. 3 Приказа внесены изменения. В настоящий момент критериями определения степени вреда являются количество субъектов персональных данных, чьи персональные данные обрабатываются, категории обрабатываемых персональных данных, а также вид нарушения законодательства Российской Федерации в области персональных данных, допущенного оператором. |