

Постановление Правительства РФ от 1 ноября 2012 г. N 1119 " Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

В соответствии со статьей 19 Федерального закона «О персональных данных» Правительство Российской Федерации **п о с т а н о в л я е т** :

1. Утвердить прилагаемые требования к защите персональных данных при их обработке в информационных системах персональных данных.

2. Признать утратившим силу постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» (Собрание законодательства Российской Федерации, 2007, № 48, ст. 6001).

Председатель Правительства
Российской Федерации

Д.Медведев

УТВЕРЖДЕНЫ
постановлением Правительства
Российской Федерации
от 1 ноября 2012 г. № 1119

ТРЕБОВАНИЯ к защите персональных данных при их обработке в информационных системах персональных данных

1. Настоящий документ устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных (далее - информационные системы) и уровни защищенности таких данных.

2. **Безопасность персональных данных** при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона «О персональных данных».

Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

3. **Безопасность персональных данных** при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные (далее - оператор), или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора (далее - уполномоченное лицо). Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.

4. **Выбор средств защиты информации** для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона «О персональных данных».

5. **Информационная система** является информационной системой, обрабатывающей специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

Информационная система является информационной системой, обрабатывающей биометрические персональные данные, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

Информационная система является информационной системой, обрабатывающей общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона «О персональных данных».

Информационная система является информационной системой, обрабатывающей иные категории персональных данных, если в ней не обрабатываются персональные данные, указанные в абзацах первом - третьем настоящего пункта.

Информационная система является информационной системой, обрабатывающей персональные данные сотрудников оператора, если в ней обрабатываются персональные данные только указанных сотрудников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора.

6. Под **актуальными угрозами безопасности персональных данных** понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

7. **Определение типа угроз безопасности персональных данных**, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18 Федерального закона «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона «О персональных данных».

8. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

9. Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

14. **Для обеспечения 3-го уровня защищенности персональных данных** при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 13 настоящего документа, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

15. **Для обеспечения 2-го уровня защищенности персональных данных** при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 14 настоящего документа, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

16. **Для обеспечения 1-го уровня защищенности персональных данных** при их обработке в информационных системах помимо требований, предусмотренных пунктом 15 настоящего документа, необходимо выполнение следующих требований:

а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

17. **Контроль за выполнением настоящих требований** организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

**Постановление от 21 марта 2012 г. № 211 "Об
утверждении перечня мер, направленных на
обеспечение выполнения обязанностей,
предусмотренных федеральным законом "О
персональных данных" и принятыми в
соответствии с ним нормативными правовыми
актами, ..."**

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ
от 21 марта 2012 г. N 211

ОБ УТВЕРЖДЕНИИ ПЕРЕЧНЯ
МЕР, НАПРАВЛЕННЫХ НА ОБЕСПЕЧЕНИЕ ВЫПОЛНЕНИЯ ОБЯЗАННОСТЕЙ,
ПРЕДУСМОТРЕННЫХ ФЕДЕРАЛЬНЫМ ЗАКОНОМ "О ПЕРСОНАЛЬНЫХ ДАННЫХ"
И ПРИНЯТЫМИ В СООТВЕТСТВИИ С НИМ НОРМАТИВНЫМИ ПРАВОВЫМИ
АКТАМИ, ОПЕРАТОРАМИ, ЯВЛЯЮЩИМИСЯ ГОСУДАРСТВЕННЫМИ
ИЛИ МУНИЦИПАЛЬНЫМИ ОРГАНАМИ

Список изменяющих документов

(в ред. Постановлений Правительства РФ от 20.07.2013 N 607,
от 06.09.2014 N 911)

В соответствии с частью 3 статьи 18.1 Федерального закона "О персональных данных"
Правительство Российской Федерации постановляет:

Утвердить прилагаемый перечень мер, направленных на обеспечение выполнения
обязанностей, предусмотренных Федеральным законом "О персональных данных" и
принятыми в соответствии с ним нормативными правовыми актами, операторами,
являющимися государственными или муниципальными органами.

Председатель Правительства
Российской Федерации
В.ПУТИН

Утвержден
постановлением Правительства
Российской Федерации
от 21 марта 2012 г. N 211

ПЕРЕЧЕНЬ
МЕР, НАПРАВЛЕННЫХ НА ОБЕСПЕЧЕНИЕ ВЫПОЛНЕНИЯ ОБЯЗАННОСТЕЙ,

ПРЕДУСМОТРЕННЫХ ФЕДЕРАЛЬНЫМ ЗАКОНОМ "О ПЕРСОНАЛЬНЫХ ДАННЫХ"
И ПРИНЯТЫМИ В СООТВЕТСТВИИ С НИМ НОРМАТИВНЫМИ ПРАВОВЫМИ
АКТАМИ, ОПЕРАТОРАМИ, ЯВЛЯЮЩИМИСЯ ГОСУДАРСТВЕННЫМИ
ИЛИ МУНИЦИПАЛЬНЫМИ ОРГАНАМИ

Список изменяющих документов

(в ред. Постановлений Правительства РФ от 20.07.2013 N 607,
от 06.09.2014 N 911)

1. Операторы, являющиеся государственными или муниципальными органами, принимают следующие меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами:

а) назначают ответственного за организацию обработки персональных данных в государственном или муниципальном органе из числа государственных или муниципальных служащих (далее - служащие) данного органа;

(в ред. Постановления Правительства РФ от 20.07.2013 N 607)

б) утверждают актом руководителя государственного или муниципального органа следующие документы:

правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований;

правила рассмотрения запросов субъектов персональных данных или их представителей;

правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом "О персональных данных", принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора;

правила работы с обезличенными данными в случае обезличивания персональных данных;

(в ред. Постановления Правительства РФ от 06.09.2014 N 911)

перечень информационных систем персональных данных;

перечни персональных данных, обрабатываемых в государственном или муниципальном органе в связи с реализацией служебных или трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций;

(в ред. Постановления Правительства РФ от 20.07.2013 N 607)

перечень должностей служащих государственного или муниципального органа, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных;

(в ред. Постановления Правительства РФ от 06.09.2014 N 911)

перечень должностей служащих государственного или муниципального органа, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

должностной регламент (должностные обязанности) или должностная инструкция ответственного за организацию обработки персональных данных в государственном или муниципальном органе;

(в ред. Постановления Правительства РФ от 20.07.2013 N 607)

типовое обязательство служащего государственного или муниципального органа, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (контракта) или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей;

(в ред. Постановления Правительства РФ от 20.07.2013 N 607)

типовая форма согласия на обработку персональных данных служащих государственного или муниципального органа, иных субъектов персональных данных, а также типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;

порядок доступа служащих государственного или муниципального органа в помещения, в которых ведется обработка персональных данных;

в) при эксплуатации информационных систем персональных данных в случае, если государственный или муниципальный орган является оператором таких информационных систем, принимают правовые, организационные и технические меры по обеспечению безопасности персональных данных при их обработке, предусмотренные соответствующими нормативными правовыми актами, для выполнения установленных Правительством Российской Федерации требований к защите персональных данных при их обработке, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

г) при обработке персональных данных, осуществляемой без использования средств автоматизации, выполняют требования, установленные постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";

д) в целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям организуют проведение периодических проверок условий обработки персональных данных в государственном или муниципальном органе. Проверки осуществляются ответственным за организацию обработки персональных данных в государственном или муниципальном органе либо комиссией, образуемой руководителем государственного или муниципального органа. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, руководителю государственного или муниципального органа докладывает ответственный за организацию обработки персональных данных в государственном или муниципальном органе либо председатель комиссии;

е) осуществляют ознакомление служащих государственного или муниципального органа, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных и (или) организуют обучение указанных служащих;

ж) уведомляют уполномоченный орган по защите прав субъектов персональных данных об обработке (намерении осуществлять обработку) персональных данных, за исключением случаев, установленных Федеральным законом "О персональных данных";

з) в случаях, установленных нормативными правовыми актами Российской Федерации, в соответствии с требованиями и методами, установленными уполномоченным органом по защите прав субъектов персональных данных, осуществляют обезличивание персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ.

(пп. "з" в ред. Постановления Правительства РФ от 06.09.2014 N 911)

2. Документы, определяющие политику в отношении обработки персональных данных, подлежат опубликованию на официальном сайте государственного или муниципального органа в течение 10 дней после их утверждения.

УКАЗ ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ О МЕРАХ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ МЕЖДУНАРОДНОГО ИНФОРМАЦИОННОГО ОБМЕНА

В целях обеспечения [информационной безопасности](#) Российской Федерации при использовании информационно-телекоммуникационных сетей, позволяющих осуществлять передачу информации через государственную границу Российской Федерации, в том числе при использовании международной компьютерной сети "Интернет", постановляю:

1. Установить, что:

- а) подключение информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к международной компьютерной сети "Интернет" (далее - информационно-телекоммуникационные сети международного информационного обмена), не допускается;
- б) при необходимости подключения информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, указанных в подпункте "а" настоящего пункта, к информационно-телекоммуникационным сетям международного информационного обмена такое подключение производится только с использованием специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю. Выполнение данного требования является обязательным для операторов информационных систем, владельцев информационно-телекоммуникационных сетей и (или) средств вычислительной техники;
- в) государственные органы в целях защиты общедоступной информации, размещаемой в информационно-телекоммуникационных сетях международного информационного обмена, используют только средства защиты информации, прошедшие в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получившие подтверждение соответствия в Федеральной службе по техническому и экспортному контролю;
- г) размещение технических средств, подключаемых к информационно-телекоммуникационным сетям международного информационного обмена, в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну, осуществляется только при наличии сертификата, разрешающего эксплуатацию таких технических средств в указанных помещениях.

Финансирование расходов, связанных с размещением технических средств в указанных помещениях федеральных органов государственной власти, осуществляется в пределах бюджетных ассигнований, предусмотренных в федеральном бюджете на содержание этих органов.

2. Федеральной службе охраны Российской Федерации обеспечивать поддержание и развитие сегмента международной компьютерной сети "Интернет" (далее - сеть "Интернет") для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

3. Администрации Президента Российской Федерации, Аппарату Совета Федерации Федерального Собрания Российской Федерации, Аппарату Государственной Думы Федерального Собрания Российской Федерации, Аппарату Правительства Российской Федерации, аппаратам Конституционного Суда Российской Федерации, Верховного Суда Российской Федерации, Высшего Арбитражного Суда Российской Федерации и Генеральной прокуратуре Российской Федерации осуществлять взаимодействие с сетью "Интернет" и представлять в нее информацию через сегмент сети "Интернет" для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, находящийся в ведении Федеральной службы охраны Российской Федерации. В исключительных случаях по согласованию с Федеральной службой охраны Российской Федерации указанные государственные органы могут осуществлять взаимодействие с сетью "Интернет" и представлять в нее информацию через сегменты сети "Интернет" и технологические серверные площадки, находящиеся в ведении федеральных органов исполнительной власти, подведомственных им учреждений и организаций, Российской академии наук, научных академий и иных научных организаций, имеющих государственный статус, а также государственных образовательных учреждений высшего профессионального образования.

4. Признать утратившими силу: Указ Президента Российской Федерации от 12 мая 2004 г. N 611 "О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена" (Собрание законодательства Российской Федерации, 2004, N 20, ст. 1938); пункт 12 приложения N 1 к Указу Президента Российской Федерации от 22 марта 2005 г. N 329 "О внесении изменений в некоторые акты Президента Российской Федерации" (Собрание законодательства Российской Федерации, 2005, N 13, ст. 1137); Указ Президента Российской Федерации от 3 марта 2006 г. N 175 "О внесении изменений в Указ Президента Российской Федерации от 12 мая 2004 г. N 611 "О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена" (Собрание законодательства Российской Федерации, 2006, N 10, ст. 1090).

5. Настоящий Указ вступает в силу со дня его подписания.

Президент
Российской Федерации
В.ПУТИН

Москва, Кремль
17 марта 2008 года

N 351

Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных"
(с изменениями от 25 ноября, 27 декабря 2009 г., 28 июня, 27 июля, 29 ноября, 23 декабря 2010 г.,
4 июня, 25 июля 2011 г.)

Принят Государственной Думой 8 июля 2006 года
Одобен Советом Федерации 14 июля 2006 года

Глава 1. Общие положения

Статья 1. Сфера действия настоящего Федерального закона

1. Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

2. Действие настоящего Федерального закона не распространяется на отношения, возникающие при:

- 1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;
- 2) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;
- 3) обработке подлежащих включению в единый государственный реестр индивидуальных предпринимателей сведений о физических лицах, если такая обработка осуществляется в соответствии с законодательством Российской Федерации в связи с деятельностью физического лица в качестве индивидуального предпринимателя;
- 4) обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;
- 5) предоставлении уполномоченными органами информации о деятельности судов в Российской Федерации в соответствии с Федеральным законом от 22 декабря 2008 года N 262-ФЗ "Об обеспечении доступа к информации о деятельности судов в Российской Федерации".

Статья 2. Цель настоящего Федерального закона

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Статья 3. Основные понятия, используемые в настоящем Федеральном законе

В целях настоящего Федерального закона используются следующие основные понятия:

- 1) персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- 2) оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
- 3) обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
- 4) автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;
- 5) распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- 6) предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
- 7) блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- 8) уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;
- 9) обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- 10) информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- 11) трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Статья 4. Законодательство Российской Федерации в области персональных данных

1. Законодательство Российской Федерации в области персональных данных основывается на Конституции Российской Федерации и международных договорах Российской Федерации и состоит из настоящего Федерального закона и других определяющих случаи и особенности обработки персональных данных федеральных законов.

2. На основании и во исполнение федеральных законов государственные органы, Банк России, органы местного самоуправления в пределах своих полномочий могут принимать нормативные

правовые акты, нормативные акты, правовые акты (далее - нормативные правовые акты) по отдельным вопросам, касающимся обработки персональных данных. Такие акты не могут содержать положения, ограничивающие права субъектов персональных данных, устанавливающие не предусмотренные федеральными законами ограничения деятельности операторов или возлагающие на операторов не предусмотренные федеральными законами обязанности, и подлежат официальному опубликованию.

3. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации, могут быть установлены федеральными законами и иными нормативными правовыми актами Российской Федерации с учетом положений настоящего Федерального закона.

4. Если международным договором Российской Федерации установлены иные правила, чем те, которые предусмотрены настоящим Федеральным законом, применяются правила международного договора.

Глава 2. Принципы и условия обработки персональных данных

Статья 5. Принципы обработки персональных данных

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Статья 6. Условия обработки персональных данных

1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных настоящим Федеральным законом. Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) 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;

3) обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);

4) обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;

5) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

6) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

7) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

8) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

9) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 настоящего Федерального закона, при условии обязательного обезличивания персональных данных;

10) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных);

11) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

2. Особенности обработки специальных категорий персональных данных, а также биометрических персональных данных устанавливаются соответственно статьями 10 и 11 настоящего Федерального закона.

3. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных,

предусмотренные настоящим Федеральным законом. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 настоящего Федерального закона.

4. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

5. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

Статья 7. Конфиденциальность персональных данных

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.

Статья 8. Общедоступные источники персональных данных

1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

2. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

Статья 9. Согласие субъекта персональных данных на обработку его персональных данных

1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным.

Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона.

3. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в

пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона, возлагается на оператора.

4. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

- 1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- 2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- 3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
- 4) цель обработки персональных данных;
- 5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- 6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
- 7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- 8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
- 9) подпись субъекта персональных данных.

5. Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством Российской Федерации.

6. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

7. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

8. Персональные данные могут быть получены оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона.

Статья 10. Специальные категории персональных данных

1. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обработка указанных в части 1 настоящей статьи специальных категорий персональных данных допускается в случаях, если:

1) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

2) персональные данные сделаны общедоступными субъектом персональных данных;

2.1) обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;

2.2) обработка персональных данных осуществляется в соответствии с Федеральным законом от 25 января 2002 года N 8-ФЗ "О Всероссийской переписи населения";

2.3) обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;

3) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

4) обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

5) обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

6) обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;

7) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;

8) обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;

9) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными

органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан.

3. Обработка персональных данных о судимости может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами.

4. Обработка специальных категорий персональных данных, осуществлявшаяся в случаях, предусмотренных частями 2 и 3 настоящей статьи, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом.

Статья 11. Биометрические персональные данные

1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию.

Статья 12. Трансграничная передача персональных данных

1. Трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с настоящим Федеральным законом и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

2. Уполномоченный орган по защите прав субъектов персональных данных утверждает перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных. Государство, не являющееся стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, может быть включено в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, при условии соответствия положениям указанной Конвенции действующих в соответствующем государстве норм права и применяемых мер безопасности персональных данных.

3. Оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав

субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных.

4. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

- 1) наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;
- 2) предусмотренных международными договорами Российской Федерации;
- 3) предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;
- 4) исполнения договора, стороной которого является субъект персональных данных;
- 5) защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

Статья 13. Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных

1. Государственные органы, муниципальные органы создают в пределах своих полномочий, установленных в соответствии с федеральными законами, государственные или муниципальные информационные системы персональных данных.
2. Федеральными законами могут быть установлены особенности учета персональных данных в государственных и муниципальных информационных системах персональных данных, в том числе использование различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей государственной или муниципальной информационной системе персональных данных, конкретному субъекту персональных данных.
3. Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных. Не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных.
4. В целях обеспечения реализации прав субъектов персональных данных в связи с обработкой их персональных данных в государственных или муниципальных информационных системах персональных данных может быть создан государственный регистр населения, правовой статус которого и порядок работы с которым устанавливаются федеральным законом.

Глава 3. Права субъекта персональных данных

Статья 14. Право субъекта персональных данных на доступ к его персональным данным

1. Субъект персональных данных имеет право на получение сведений, указанных в части 7 настоящей статьи, за исключением случаев, предусмотренных частью 8 настоящей статьи. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.
2. Сведения, указанные в части 7 настоящей статьи, должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.
3. Сведения, указанные в части 7 настоящей статьи, предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.
4. В случае, если сведения, указанные в части 7 настоящей статьи, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 настоящей статьи, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.
5. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 настоящей статьи, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в части 4 настоящей статьи, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в части 3 настоящей статьи, должен содержать обоснование направления повторного запроса.
6. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 настоящей статьи. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

7. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- 1) подтверждение факта обработки персональных данных оператором;
- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые оператором способы обработки персональных данных;
- 4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- 5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- 6) сроки обработки персональных данных, в том числе сроки их хранения;
- 7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;
- 8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- 9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- 10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

8. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

- 1) обработка персональных данных, включая персональные данные, полученные в результате оперативно-разыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
- 2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;
- 3) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- 4) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;
- 5) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

Статья 15. Права субъектов персональных данных при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации

1. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта персональных данных, если оператор не докажет, что такое согласие было получено.

2. Оператор обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных, указанную в части 1 настоящей статьи.

Статья 16. Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных

1. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

3. Оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

4. Оператор обязан рассмотреть возражение, указанное в части 3 настоящей статьи, в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

Статья 17. Право на обжалование действий или бездействия оператора

1. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

2. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Глава 4. Обязанности оператора

Статья 18. Обязанности оператора при сборе персональных данных

1. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 настоящего Федерального закона.

2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

3. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных частью 4 настоящей статьи, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

- 1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
- 2) цель обработки персональных данных и ее правовое основание;
- 3) предполагаемые пользователи персональных данных;
- 4) установленные настоящим Федеральным законом права субъекта персональных данных;
- 5) источник получения персональных данных.

4. Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные частью 3 настоящей статьи, в случаях, если:

- 1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;
- 2) персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
- 3) персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
- 4) оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;
- 5) предоставление субъекту персональных данных сведений, предусмотренных частью 3 настоящей статьи, нарушает права и законные интересы третьих лиц.

Статья 18.1. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом

1. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами. К таким мерам могут, в частности, относиться:

- 1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;
- 2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки

персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

- 3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 настоящего Федерального закона;
- 4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;
- 5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;
- 6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

2. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

3. Правительство Российской Федерации устанавливает перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами.

4. Оператор обязан представить документы и локальные акты, указанные в части 1 настоящей статьи, и (или) иным образом подтвердить принятие мер, указанных в части 1 настоящей статьи, по запросу уполномоченного органа по защите прав субъектов персональных данных.

Статья 19. Меры по обеспечению безопасности персональных данных при их обработке

1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2. Обеспечение безопасности персональных данных достигается, в частности:

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

системах персональных данных;

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

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

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

5) учетом машинных носителей персональных данных;

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

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

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

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

3. Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

2) требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

3) требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

4. Состав и содержание необходимых для выполнения установленных Правительством Российской Федерации в соответствии с частью 3 настоящей статьи требований к защите персональных данных для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

5. Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органы государственной власти субъектов Российской Федерации, Банк России, органы государственных внебюджетных фондов, иные государственные органы в пределах своих

полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки.

6. Наряду с угрозами безопасности персональных данных, определенных в нормативных правовых актах, принятых в соответствии с частью 5 настоящей статьи, ассоциации, союзы и иные объединения операторов своими решениями вправе определить дополнительные угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с учетом содержания персональных данных, характера и способов их обработки.

7. Проекты нормативных правовых актов, указанных в части 5 настоящей статьи, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации. Проекты решений, указанных в части 6 настоящей статьи, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в порядке, установленном Правительством Российской Федерации. Решение федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, об отказе в согласовании проектов решений, указанных в части 6 настоящей статьи, должно быть мотивированным.

8. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при обработке персональных данных в государственных информационных системах персональных данных осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

9. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, решением Правительства Российской Федерации с учетом значимости и содержания обрабатываемых персональных данных могут быть наделены полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при их обработке в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными информационными системами персональных данных, без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

10. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

11. Для целей настоящей статьи под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Статья 20. Обязанности оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных

1. Оператор обязан сообщить в порядке, предусмотренном статьей 14 настоящего Федерального закона, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

2. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 настоящего Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

3. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять

разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

4. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

Статья 21. Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных

1. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

2. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

4. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

5. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

6. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в частях 3 - 5 настоящей статьи, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

Статья 22. Уведомление об обработке персональных данных

1. Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

1) обрабатываемых в соответствии с трудовым законодательством;

2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной

организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных;

4) сделанных субъектом персональных данных общедоступными;

5) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

7) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;

9) обрабатываемых в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

3. Уведомление, предусмотренное частью 1 настоящей статьи, направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление должно содержать следующие сведения:

1) наименование (фамилия, имя, отчество), адрес оператора;

2) цель обработки персональных данных;

3) категории персональных данных;

4) категории субъектов, персональные данные которых обрабатываются;

5) правовое основание обработки персональных данных;

6) перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;

7) описание мер, предусмотренных статьями 18.1 и 19 настоящего Федерального закона, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

7.1) фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;

8) дата начала обработки персональных данных;

9) срок или условие прекращения обработки персональных данных;

10) сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

11) сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

4. Уполномоченный орган по защите прав субъектов персональных данных в течение тридцати дней с даты поступления уведомления об обработке персональных данных вносит сведения, указанные в части 3 настоящей статьи, а также сведения о дате направления указанного уведомления в реестр операторов. Сведения, содержащиеся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными.
5. На оператора не могут возлагаться расходы в связи с рассмотрением уведомления об обработке персональных данных уполномоченным органом по защите прав субъектов персональных данных, а также в связи с внесением сведений в реестр операторов.
6. В случае предоставления неполных или недостоверных сведений, указанных в части 3 настоящей статьи, уполномоченный орган по защите прав субъектов персональных данных вправе требовать от оператора уточнения предоставленных сведений до их внесения в реестр операторов.
7. В случае изменения сведений, указанных в части 3 настоящей статьи, а также в случае прекращения обработки персональных данных оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

Статья 22.1. Лица, ответственные за организацию обработки персональных данных в организациях

1. Оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных.
2. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа организации, являющейся оператором, и подотчетно ему.
3. Оператор обязан предоставлять лицу, ответственному за организацию обработки персональных данных, сведения, указанные в части 3 статьи 22 настоящего Федерального закона.
4. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:
 - 1) осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
 - 2) доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
 - 3) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

Глава 5. Контроль и надзор за обработкой персональных данных. Ответственность за нарушение требований настоящего Федерального закона

Статья 23. Уполномоченный орган по защите прав субъектов персональных данных

1. Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям настоящего Федерального закона, является федеральный орган исполнительной

власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи.

2. Уполномоченный орган по защите прав субъектов персональных данных рассматривает обращения субъекта персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки и принимает соответствующее решение.

3. Уполномоченный орган по защите прав субъектов персональных данных имеет право:

1) запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;

2) осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;

3) требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

4) принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований настоящего Федерального закона;

5) обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных, в том числе в защиту прав неопределенного круга лиц, и представлять интересы субъектов персональных данных в суде;

5.1) направлять в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, применительно к сфере их деятельности, сведения, указанные в пункте 7 части 3 статьи 22 настоящего Федерального закона;

6) направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством Российской Федерации порядке, если условием лицензии на осуществление такой деятельности является запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных;

7) направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью;

8) вносить в Правительство Российской Федерации предложения о совершенствовании нормативного правового регулирования защиты прав субъектов персональных данных;

9) привлекать к административной ответственности лиц, виновных в нарушении настоящего Федерального закона.

4. В отношении персональных данных, ставших известными уполномоченному органу по защите прав субъектов персональных данных в ходе осуществления им своей деятельности, должна обеспечиваться конфиденциальность персональных данных.

5. Уполномоченный орган по защите прав субъектов персональных данных обязан:

1) организовывать в соответствии с требованиями настоящего Федерального закона и других федеральных законов защиту прав субъектов персональных данных;

- 2) рассматривать жалобы и обращения граждан или юридических лиц по вопросам, связанным с обработкой персональных данных, а также принимать в пределах своих полномочий решения по результатам рассмотрения указанных жалоб и обращений;
- 3) вести реестр операторов;
- 4) осуществлять меры, направленные на совершенствование защиты прав субъектов персональных данных;
- 5) принимать в установленном законодательством Российской Федерации порядке по представлению федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, или федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, меры по приостановлению или прекращению обработки персональных данных;
- 6) информировать государственные органы, а также субъектов персональных данных по их обращениям или запросам о положении дел в области защиты прав субъектов персональных данных;
- 7) выполнять иные предусмотренные законодательством Российской Федерации обязанности.

5.1. Уполномоченный орган по защите прав субъектов персональных данных осуществляет сотрудничество с органами, уполномоченными по защите прав субъектов персональных данных в иностранных государствах, в частности международный обмен информацией о защите прав субъектов персональных данных, утверждает перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных.

6. Решения уполномоченного органа по защите прав субъектов персональных данных могут быть обжалованы в судебном порядке.

7. Уполномоченный орган по защите прав субъектов персональных данных ежегодно направляет отчет о своей деятельности Президенту Российской Федерации, в Правительство Российской Федерации и Федеральное Собрание Российской Федерации. Указанный отчет подлежит опубликованию в средствах массовой информации.

8. Финансирование уполномоченного органа по защите прав субъектов персональных данных осуществляется за счет средств федерального бюджета.

9. При уполномоченном органе по защите прав субъектов персональных данных создается на общественных началах консультативный совет, порядок формирования и порядок деятельности которого определяются уполномоченным органом по защите прав субъектов персональных данных.

Статья 24. Ответственность за нарушение требований настоящего Федерального закона

1. Лица, виновные в нарушении требований настоящего Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность.

2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с настоящим Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Глава 6. Заключительные положения

Статья 25. Заключительные положения

1. Настоящий Федеральный закон вступает в силу по истечении ста восьмидесяти дней после дня его официального опубликования.
2. После дня вступления в силу настоящего Федерального закона обработка персональных данных, включенных в информационные системы персональных данных до дня его вступления в силу, осуществляется в соответствии с настоящим Федеральным законом.
 - 2.1. Операторы, которые осуществляли обработку персональных данных до 1 июля 2011 года, обязаны представить в уполномоченный орган по защите прав субъектов персональных данных сведения, указанные в пунктах 5, 7.1, 10 и 11 части 3 статьи 22 настоящего Федерального закона, не позднее 1 января 2013 года.
3. Утратила силу с 1 июля 2011 г.
4. Операторы, которые осуществляют обработку персональных данных до дня вступления в силу настоящего Федерального закона и продолжают осуществлять такую обработку после дня его вступления в силу, обязаны направить в уполномоченный орган по защите прав субъектов персональных данных, за исключением случаев, предусмотренных частью 2 статьи 22 настоящего Федерального закона, уведомление, предусмотренное частью 3 статьи 22 настоящего Федерального закона, не позднее 1 января 2008 года.

Президент Российской Федерации

В. Путин

Москва, Кремль

27 июля 2006 г.

№ 152-ФЗ

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН
ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ
И О ЗАЩИТЕ ИНФОРМАЦИИ

Принят
Государственной Думой
8 июля 2006 года
Одобен
Советом Федерации
14 июля 2006 года

Статья 1. Сфера действия настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, возникающие при:

- 1) осуществлении права на поиск, получение, передачу, производство и распространение информации;
- 2) применении информационных технологий;
- 3) обеспечении защиты информации.

2. Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации.

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

В настоящем Федеральном законе используются следующие основные понятия:

- 1) информация - сведения (сообщения, данные) независимо от формы их представления;
- 2) информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
- 3) информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
- 4) информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;
- 5) обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
- 6) доступ к информации - возможность получения информации и ее использования;
- 7) конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
- 8) предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;
- 9) распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;
- 10) электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

11) документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

12) оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Статья 3. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

- 1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
- 2) установление ограничений доступа к информации только федеральными законами;
- 3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
- 4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
- 5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
- 6) достоверность информации и своевременность ее предоставления;
- 7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
- 8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Статья 4. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации

1. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации основывается на Конституции Российской Федерации, международных договорах Российской Федерации и состоит из настоящего Федерального закона и других регулирующих отношения по использованию информации федеральных законов.

2. Правовое регулирование отношений, связанных с организацией и деятельностью средств массовой информации, осуществляется в соответствии с законодательством Российской Федерации о средствах массовой информации.

3. Порядок хранения и использования включенной в состав архивных фондов документированной информации устанавливается законодательством об архивном деле в Российской Федерации.

Статья 5. Информация как объект правовых отношений

1. Информация может являться объектом публичных, гражданских и иных правовых отношений.

Информация может свободно использоваться любым лицом и передаваться одним лицом другому

лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

2. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

3. Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

- 1) информацию, свободно распространяемую;
- 2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- 3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- 4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

4. Законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя.

Статья 6. Обладатель информации

1. Обладателем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.

2. От имени Российской Федерации, субъекта Российской Федерации, муниципального образования полномочия обладателя информации осуществляются соответственно государственными органами и органами местного самоуправления в пределах их полномочий, установленных соответствующими нормативными правовыми актами.

3. Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

- 1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- 2) использовать информацию, в том числе распространять ее, по своему усмотрению;
- 3) передавать информацию другим лицам по договору или на ином установленном законом основании;
- 4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
- 5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

4. Обладатель информации при осуществлении своих прав обязан:

- 1) соблюдать права и законные интересы иных лиц;
- 2) принимать меры по защите информации;
- 3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Статья 7. Общедоступная информация

1. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

2. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

3. Владелец информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

Статья 8. Право на доступ к информации

1. Граждане (физические лица) и организации (юридические лица) (далее - организации) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных настоящим Федеральным законом и другими федеральными законами.

2. Гражданин (физическое лицо) имеет право на получение от государственных органов, органов местного самоуправления, их должностных лиц в порядке, установленном законодательством Российской Федерации, информации, непосредственно затрагивающей его права и свободы.

3. Организация имеет право на получение от государственных органов, органов местного самоуправления информации, непосредственно касающейся прав и обязанностей этой организации, а также информации, необходимой в связи с взаимодействием с указанными органами при осуществлении этой организацией своей уставной деятельности.

4. Не может быть ограничен доступ к:

1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

2) информации о состоянии окружающей среды;

3) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

4) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

5. Государственные органы и органы местного самоуправления обязаны обеспечивать доступ к информации о своей деятельности на русском языке и государственном языке соответствующей республики в составе Российской Федерации в соответствии с федеральными законами, законами субъектов Российской Федерации и нормативными правовыми актами органов местного самоуправления. Лицо, желающее получить доступ к такой информации, не обязано обосновывать необходимость ее получения.

6. Решения и действия (бездействие) государственных органов и органов местного самоуправления, общественных объединений, должностных лиц, нарушающие право на доступ к информации, могут быть обжалованы в вышестоящий орган или вышестоящему должностному лицу либо в суд.

7. В случае, если в результате неправомерного отказа в доступе к информации, несвоевременного ее предоставления, предоставления заведомо недостоверной или не соответствующей содержанию запроса информации были причинены убытки, такие убытки подлежат возмещению в соответствии с гражданским законодательством.

8. Предоставляется бесплатно информация:

- 1) о деятельности государственных органов и органов местного самоуправления, размещенная такими органами в информационно-телекоммуникационных сетях;
 - 2) затрагивающая права и установленные законодательством Российской Федерации обязанности заинтересованного лица;
 - 3) иная установленная законом информация.
9. Установление платы за предоставление государственным органом или органом местного самоуправления информации о своей деятельности возможно только в случаях и на условиях, которые установлены федеральными законами.

Статья 9. Ограничение доступа к информации

1. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.
2. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.
3. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.
4. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.
5. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.
6. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.
7. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.
8. Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.
9. Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

Статья 10. Распространение информации или предоставление информации

1. В Российской Федерации распространение информации осуществляется свободно при соблюдении требований, установленных законодательством Российской Федерации.
2. Информация, распространяемая без использования средств массовой информации, должна включать в себя достоверные сведения о ее обладателе или об ином лице, распространяющем информацию, в форме и в объеме, которые достаточны для идентификации такого лица.
3. При использовании для распространения информации средств, позволяющих определять получателей информации, в том числе почтовых отправлений и электронных сообщений, лицо,

распространяющее информацию, обязано обеспечить получателю информации возможность отказа от такой информации.

4. Предоставление информации осуществляется в порядке, который устанавливается соглашением лиц, участвующих в обмене информацией.

5. Случаи и условия обязательного распространения информации или предоставления информации, в том числе предоставление обязательных экземпляров документов, устанавливаются федеральными законами.

6. Запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

Статья 11. Документирование информации

1. Законодательством Российской Федерации или соглашением сторон могут быть установлены требования к документированию информации.

2. В федеральных органах исполнительной власти документирование информации осуществляется в порядке, устанавливаемом Правительством Российской Федерации. Правила делопроизводства и документооборота, установленные иными государственными органами, органами местного самоуправления в пределах их компетенции, должны соответствовать требованиям, установленным Правительством Российской Федерации в части делопроизводства и документооборота для федеральных органов исполнительной власти.

3. Электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе.

4. В целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной цифровой подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.

5. Право собственности и иные вещные права на материальные носители, содержащие документированную информацию, устанавливаются гражданским законодательством.

Статья 12. Государственное регулирование в сфере применения информационных технологий

1. Государственное регулирование в сфере применения информационных технологий предусматривает:

1) регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации), на основании принципов, установленных настоящим Федеральным законом;

2) развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;

3) создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети "Интернет" и иных подобных информационно-телекоммуникационных сетей.

2. Государственные органы, органы местного самоуправления в соответствии со своими полномочиями:

1) участвуют в разработке и реализации целевых программ применения информационных технологий;

2) создают информационные системы и обеспечивают доступ к содержащейся в них информации на русском языке и государственном языке соответствующей республики в составе Российской Федерации.

Статья 13. Информационные системы

1. Информационные системы включают в себя:

1) государственные информационные системы - федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов;

2) муниципальные информационные системы, созданные на основании решения органа местного самоуправления;

3) иные информационные системы.

2. Если иное не установлено федеральными законами, оператором информационной системы является собственник используемых для обработки содержащейся в базах данных информации технических средств, который правомерно пользуется такими базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы.

3. Права обладателя информации, содержащейся в базах данных информационной системы, подлежат охране независимо от авторских и иных прав на такие базы данных.

4. Установленные настоящим Федеральным законом требования к государственным информационным системам распространяются на муниципальные информационные системы, если иное не предусмотрено законодательством Российской Федерации о местном самоуправлении.

5. Особенности эксплуатации государственных информационных систем и муниципальных информационных систем могут устанавливаться в соответствии с техническими регламентами, нормативными правовыми актами государственных органов, нормативными правовыми актами органов местного самоуправления, принимающих решения о создании таких информационных систем.

6. Порядок создания и эксплуатации информационных систем, не являющихся государственными информационными системами или муниципальными информационными системами, определяется операторами таких информационных систем в соответствии с требованиями, установленными настоящим Федеральным законом или другими федеральными законами.

Статья 14. Государственные информационные системы

1. Государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях.

2. Государственные информационные системы создаются с учетом требований, предусмотренных Федеральным законом от 21 июля 2005 года N 94-ФЗ "О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд".

3. Государственные информационные системы создаются и эксплуатируются на основе статистической и иной документированной информации, предоставляемой гражданами (физическими лицами), организациями, государственными органами, органами местного самоуправления.

4. Перечни видов информации, предоставляемой в обязательном порядке, устанавливаются федеральными законами, условия ее предоставления - Правительством Российской Федерации или соответствующими государственными органами, если иное не предусмотрено федеральными законами.

5. Если иное не установлено решением о создании государственной информационной системы, функции ее оператора осуществляются заказчиком, заключившим государственный контракт на создание такой информационной системы. При этом ввод государственной информационной системы в эксплуатацию осуществляется в порядке, установленном указанным заказчиком.

6. Правительство Российской Федерации вправе устанавливать обязательные требования к порядку ввода в эксплуатацию отдельных государственных информационных систем.

7. Не допускается эксплуатация государственной информационной системы без надлежащего оформления прав на использование ее компонентов, являющихся объектами интеллектуальной собственности.

8. Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании.

9. Информация, содержащаяся в государственных информационных системах, а также иные имеющиеся в распоряжении государственных органов сведения и документы являются государственными информационными ресурсами.

Статья 15. Использование информационно-телекоммуникационных сетей

1. На территории Российской Федерации использование информационно-телекоммуникационных сетей осуществляется с соблюдением требований законодательства Российской Федерации в области связи, настоящего Федерального закона и иных нормативных правовых актов Российской Федерации.

2. Регулирование использования информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, осуществляется в Российской Федерации с учетом общепринятой международной практики деятельности саморегулируемых организаций в этой области. Порядок использования иных информационно-телекоммуникационных сетей определяется владельцами таких сетей с учетом требований, установленных настоящим Федеральным законом.

3. Использование на территории Российской Федерации информационно-телекоммуникационных сетей в хозяйственной или иной деятельности не может служить основанием для установления дополнительных требований или ограничений, касающихся регулирования указанной деятельности, осуществляемой без использования таких сетей, а также для несоблюдения требований, установленных федеральными законами.

4. Федеральными законами может быть предусмотрена обязательная идентификация личности, организаций, использующих информационно-телекоммуникационную сеть при осуществлении предпринимательской деятельности. При этом получатель электронного сообщения, находящийся на территории Российской Федерации, вправе провести проверку, позволяющую установить отправителя электронного сообщения, а в установленных федеральными законами или соглашением сторон случаях обязан провести такую проверку.

5. Передача информации посредством использования информационно-телекоммуникационных сетей осуществляется без ограничений при условии соблюдения установленных федеральными законами требований к распространению информации и охране объектов интеллектуальной собственности. Передача информации может быть ограничена только в порядке и на условиях, которые установлены федеральными законами.

6. Особенности подключения государственных информационных систем к информационно-телекоммуникационным сетям могут быть установлены нормативным правовым актом Президента Российской Федерации или нормативным правовым актом Правительства Российской Федерации.

Статья 16. Защита информации

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

- 1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- 2) соблюдение конфиденциальности информации ограниченного доступа;
- 3) реализацию права на доступ к информации.

2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

3. Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.

4. Владелец информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

- 1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- 2) своевременное обнаружение фактов несанкционированного доступа к информации;
- 3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- 4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- 5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- 6) постоянный контроль за обеспечением уровня защищенности информации.

5. Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области

противодействия техническим разведкам и технической защите информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

6. Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

Статья 17. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации

1. Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2. Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с иском о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

3. В случае, если распространение определенной информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации не несет лицо, оказывающее услуги:

- 1) либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;
- 2) либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.

Статья 18. О признании утратившими силу отдельных законодательных актов (положений законодательных актов) Российской Федерации

Со дня вступления в силу настоящего Федерального закона признать утратившими силу:

- 1) Федеральный закон от 20 февраля 1995 года N 24-ФЗ "Об информации, информатизации и защите информации" (Собрание законодательства Российской Федерации, 1995, N 8, ст. 609);
- 2) Федеральный закон от 4 июля 1996 года N 85-ФЗ "Об участии в международном информационном обмене" (Собрание законодательства Российской Федерации, 1996, N 28, ст. 3347);
- 3) статью 16 Федерального закона от 10 января 2003 года N 15-ФЗ "О внесении изменений и дополнений в некоторые законодательные акты Российской Федерации в связи с принятием Федерального закона "О лицензировании отдельных видов деятельности" (Собрание законодательства Российской Федерации, 2003, N 2, ст. 167);
- 4) статью 21 Федерального закона от 30 июня 2003 года N 86-ФЗ "О внесении изменений и дополнений в некоторые законодательные акты Российской Федерации, признании утратившими силу отдельных законодательных актов Российской Федерации, предоставлении отдельных

гарантий сотрудникам органов внутренних дел, органов по контролю за оборотом наркотических средств и психотропных веществ и упраздняемых федеральных органов налоговой полиции в связи с осуществлением мер по совершенствованию государственного управления" (Собрание законодательства Российской Федерации, 2003, N 27, ст. 2700);

5) статью 39 Федерального закона от 29 июня 2004 года N 58-ФЗ "О внесении изменений в некоторые законодательные акты Российской Федерации и признании утратившими силу некоторых законодательных актов Российской Федерации в связи с осуществлением мер по совершенствованию государственного управления" (Собрание законодательства Российской Федерации, 2004, N 27, ст. 2711).

Президент

Российской Федерации

В.ПУТИН

Москва, Кремль

27 июля 2006 года

N 149-ФЗ