**Нормативно-правовая база:**

[Федеральный закон РФ 27.07.2006 г. N 152-ФЗ "О персональных данных"](https://b-152.ru/152-FZ_O_personalnykh_dannykh)

[Постановление Правительства РФ от 15 сентября 2008 г. N 687 г."Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"](https://b-152.ru/Postanovleniye_pravitelstva_RF_%E2%84%96687_obrabotka_personalnykh_dannykh_bez_sredstv_avtomatizatsii)

[Постановление Правительства РФ от 6 июля 2008 г. N 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных"](https://b-152.ru/Postanovleniye_pravitelstva_RF_%E2%84%96512_ot_ubverzhdenii_trebovaniya_k_materialnym_nositelyam_personalnykh_dannykh)

[Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 г. "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"](https://b-152.ru/Postanovleniye_pravitelstva_RF_%E2%84%961119_ob_ubverzhdenii_trebovaniy_k_zashchite_personalnykh_dannykh)

[Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных система персональных данных" от 21 февраля 2008 года](https://b-152.ru/Tipovyye_trebovaniya_po_organizatsi_i_obespecheniyu_funktsionirovaniya_shifrovalnykh_sredstv)

[Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации" от 21 февраля 2008 года](https://b-152.ru/Metodicheskiye_rekomendatsii_po_obespecheniyu_s_pomoshchyu_kriptosredstv_bezopasnosti_personalnykh_dannykh)

[Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных](https://b-152.ru/Metodika_opredeleniya_aktualnykh_ugroz_bezopasnosti_personalnykh_dannykh)

[Приказ Министерства связи и массовых коммуникаций Российской Федерации от 14 ноября 2011 г. N 312 «Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства российской федерации в области персональных данных»](https://b-152.ru/Prikaz_Minkomsvjazi_RF_N_312__Ob_utverzhdenii_administranivnogo_reglamenta)

[Приказ Министерства связи и массовых коммуникаций РФ от 21 декабря 2011 г. N 346 «Об утверждении Административного регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги «Введение реестра операторов, осуществляющих обработку персональных данных»](https://b-152.ru/Prikaz_Minkomsvyazi_N_346_Reglament_%C2%ABVvedeniye_reyestra_operatorov_osushchestvlyayushchikh_obrabotku_personalnykh_dannykh%C2%BB)

[Приказ Роскомнадзора от 19 августа 2011 г. №706 "Об утверждении Рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных"](https://b-152.ru/Prikaz_Roscomnadzora_N706_Ob_utverzhdenii_Rekomendatsiy_po_zapolneniyu_obraztsa_formy_uvedomleniya_ob_obrabotke)

# ФЕДЕРАЛЬНЫЙ ЗАКОН N 152-ФЗ "О ПЕРСОНАЛЬНЫХ ДАННЫХ" РФ ОТ 27.07.2006 Г.

**РОССИЙСКАЯ ФЕДЕРАЦИЯ   
ФЕДЕРАЛЬНЫЙ ЗАКОН   
О ПЕРСОНАЛЬНЫХ ДАННЫХ**

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

(в ред. Федеральных законов от 25.11.2009 N 266-ФЗ,   
от 27.12.2009 N 363-ФЗ, от 28.06.2010 N 123-ФЗ,   
от 27.07.2010 N 204-ФЗ, от 27.07.2010 N 227-ФЗ,   
от 29.11.2010 N 313-ФЗ от 23.12.2010 N 359-ФЗ,   
от 04.06.2011 N 123-ФЗ, от 25.07.2011 N 261-ФЗ)

**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) утратил силу. - Федеральный закон от 25.07.2011 N 261-ФЗ;

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".

(п. 5 введен Федеральным законом от 28.06.2010 N 123-ФЗ)

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;

(п. 2.1 введен Федеральным законом от 25.11.2009 N 266-ФЗ)

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

(п. 2.2 введен Федеральным законом от 27.07.2010 N 204-ФЗ)

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-разыскной 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. Утратил силу. - Федеральный закон от 25.07.2011 N 261-ФЗ.

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

# ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РA ОТ 15 СЕНТЯБРЯ 2008 Г. N 687 Г."ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ ОБ ОСОБЕННОСТЯХ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ"

В целях реализации Федерального закона "О персональных данных" Правительство Российской Федерации **постановляет:**

1. Утвердить прилагаемое Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации.

2. Федеральным органам исполнительной власти в месячный срок привести свои акты по вопросам обработки персональных данных, осуществляемой без использования средств автоматизации, в соответствие с настоящим постановлением.

3. Настоящее постановление вступает в силу по истечении одного месяца со дня его официального опубликования.

**Председатель Правительства   
Российской Федерации   
В. Путин**

ПОЛОЖЕНИЕ ОБ ОСОБЕННОСТЯХ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

**I. Общие положения**

1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее - персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

2. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

3. Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации, должны применяться с учетом требований настоящего Положения.

**II. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации**

4. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

5. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

6. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии).

7. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

8. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:

а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

в) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится оператор.

9. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

10. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

11. Правила, предусмотренные пунктами 9 и 10 настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

12. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

**III. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации**

13. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

14. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

15. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

# ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ ОТ 6 ИЮЛЯ 2008 Г. N 512 "ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ К МАТЕРИАЛЬНЫМ НОСИТЕЛЯМ БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ И ТЕХНОЛОГИЯМ ХРАНЕНИЯ ТАКИХ ДАННЫХ ВНЕ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ"

Правительство Российской Федерации **постановляет:**

1. Утвердить прилагаемые требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

2. Настоящее постановление вступает в силу по истечении 6 месяцев со дня его официального опубликования.

**Председатель Правительства Российской Федерации**

**В. Путин**

ТРЕБОВАНИЯ К МАТЕРИАЛЬНЫМ НОСИТЕЛЯМ БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ И ТЕХНОЛОГИЯМ ХРАНЕНИЯ ТАКИХ ДАННЫХ ВНЕ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Настоящие требования применяются при использовании материальных носителей, на которые осуществляется запись биометрических персональных данных, а также при хранении биометрических персональных данных вне информационных систем персональных данных.

2. В настоящих требованиях под материальным носителем понимается машиночитаемый носитель информации (в том числе магнитный и электронный), на котором осуществляются запись и хранение сведений, характеризующих физиологические особенности человека и на основе которых можно установить его личность (далее - материальный носитель).

3. Настоящие требования не распространяются на отношения, возникающие при использовании:

а) оператором информационной системы персональных данных (далее - оператор) материальных носителей для организации функционирования информационной системы персональных данных, оператором которой он является;

б) бумажных носителей для записи и хранения биометрических персональных данных.

4. Материальный носитель должен обеспечивать:

а) защиту от несанкционированной повторной и дополнительной записи информации после ее извлечения из информационной системы персональных данных;

б) возможность доступа к записанным на материальный носитель биометрическим персональным данным, осуществляемого оператором и лицами, уполномоченными в соответствии с законодательством Российской Федерации на работу с биометрическими персональными данными (далее - уполномоченные лица);

в) возможность идентификации информационной системы персональных данных, в которую была осуществлена запись биометрических персональных данных, а также оператора, осуществившего такую запись;

г) невозможность несанкционированного доступа к биометрическим персональным данным, содержащимся на материальном носителе.

5. Оператор утверждает порядок передачи материальных носителей уполномоченным лицам.

6. Материальный носитель должен использоваться в течение срока, установленного оператором, осуществившим запись биометрических персональных данных на материальный носитель, но не более срока эксплуатации, установленного изготовителем материального носителя.

7. Тип материального носителя, который будет использован для обработки биометрических персональных данных, определяет оператор, за исключением случаев, когда нормативными правовыми актами Российской Федерации предписано использование материального носителя определенного типа.

8. Оператор обязан:

а) осуществлять учет количества экземпляров материальных носителей;

б) осуществлять присвоение материальному носителю уникального идентификационного номера, позволяющего точно определить оператора, осуществившего запись биометрических персональных данных на материальный носитель.

9. Технологии хранения биометрических персональных данных вне информационных систем персональных данных должны обеспечивать:

а) доступ к информации, содержащейся на материальном носителе, для уполномоченных лиц;

б) применение средств электронной цифровой подписи или иных информационных технологий, позволяющих сохранить целостность и неизменность биометрических персональных данных, записанных на материальный носитель;

в) проверку наличия письменного согласия субъекта персональных данных на обработку его биометрических персональных данных или наличия иных оснований обработки персональных данных, установленных законодательством Российской Федерации в сфере отношений, связанных с обработкой персональных данных.

10. В случае если на материальном носителе содержится дополнительная информация, имеющая отношение к записанным биометрическим персональным данным, то такая информация должна быть подписана электронной цифровой подписью и (или) защищена иными информационными технологиями, позволяющими сохранить целостность и неизменность информации, записанной на материальный носитель.

Использование шифровальных (криптографических) средств защиты информации осуществляется в соответствии с законодательством Российской Федерации.

11. При хранении биометрических персональных данных вне информационных систем персональных данных должна обеспечиваться регистрация фактов несанкционированной повторной и дополнительной записи информации после ее извлечения из информационной системы персональных данных.

12. Оператор вправе установить не противоречащие требованиям законодательства Российской Федерации дополнительные требования к технологиям хранения биометрических персональных данных вне информационных систем персональных данных в зависимости от методов и способов защиты биометрических персональных данных в информационных системах персональных данных этого оператора.

# ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ОТ 1 НОЯБРЯ 2012 Г. N 1119 Г. "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 **постановляет:**

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. N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" (Собрание законодательства Российской Федерации, 2007, N 48, ст. 6001).

**Председатель Правительства Российской Федерации**

**Д. Медведев**

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 [1] 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;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

10. Необходимость обеспечения 2-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 общедоступные персональные данные;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

11. Необходимость обеспечения 3-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 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

12. Необходимость обеспечения 4-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 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

13. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

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).

# ТИПОВЫЕ ТРЕБОВАНИЯ ПО ОРГАНИЗАЦИИ И ОБЕСПЕЧЕНИЮ ФУНКЦИОНИРОВАНИЯ ШИФРОВАЛЬНЫХ (КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ, ПРЕДНАЗНАЧЕННЫХ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ, НЕ СОДЕРЖАЩЕЙ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ГОСУДАРСТВЕННУЮ ТАЙНУ В СЛУЧАЕ ИХ ИСПОЛЬЗОВАНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ" ОТ 21 ФЕВРАЛЯ 2008 ГОДА

**УТВЕРЖДЕНЫ**  
руководством 8 Центра  
ФСБ России  
21 февраля 2008 года  
№ 149/6/6-622

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Требования определяют порядок организации и обеспечения функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну (далее – криптосредство) в случае их использования для обеспечения безопасностиперсональных данных при их обработке в информационных системах персональных данных (далее – информационная система).

1.2. Настоящие Требования разработаны во исполнение:

- Федерального закона "О персональных данных" от 27 июля 2006г. № 152-ФЗ (Статья 19);

- Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного постановлением Правительства РФ от 17 ноября 2007г. №781 (далее – Положение);

- Положения о Федеральной службе безопасности Российской Федерации, утвержденного Указом Президента Российской Федерации от 11 августа 2003 года № 960.

1.3. Настоящие Требования:

- являются обязательными для оператора, осуществляющего обработку персональных данных, а также лица,  которому на основании договора оператор поручает обработку персональных данных и (или) лица, которому на основании договора оператор поручает оказание услуг по организации и обеспечению безопасности защиты персональных данных при их обработке в информационной системе с использованием криптосредств. При этом существенным условием договора является обязанность уполномоченного лица обеспечить конфиденциальность персональных данных и безопасность персональных данных при их обработке в информационной системе в случаях, предусмотренных действующим законодательством;

- распространяются на криптосредства, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, все технические средства которых находятся в пределах Российской Федерации, а также в системах, технические средства которых частично или целиком находятся за пределами Российской Федерации.

- не отменяют требования иных документов, регламентирующих порядок обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти.

Оператор с учетом особенностей своей деятельности может разрабатывать не противоречащие настоящим Требованиям методические рекомендации по их применению.

Используемые для целей настоящих Требований термины и определения приведены в приложении 1.

## 2. ОРГАНИЗАЦИЯ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБРАБОТКИ С ИСПОЛЬЗОВАНИЕМ ШИФРОВАЛЬНЫХ (КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Безопасность обработки персональных данных с использованием криптосредств организуют и обеспечивают операторы, а также лица, которым на основании договора оператор поручает обработку персональных данных и (или) лица, которым на основании договора оператор поручает оказание услуг по организации и обеспечению безопасности обработки в информационной системе персональных данных с использованием криптосредств.

Обеспечение безопасности персональных данных с использованием криптосредств должно осуществляться в соответствии с:

1) Приказом ФСБ России от 9 февраля 2005 г. № 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005);

2)  Постановлением Правительства РФ от 29 декабря 2007 г. № 957 "Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами";

3)  Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (№ 149/54-144, 2008 г. ФСБ России),

4) Настоящими Требованиями.

2.2. Операторы несут ответственность за соответствие проводимых ими мероприятий по организации и обеспечению безопасности обработки с использованием криптосредств персональных данных лицензионным требованиям и условиям, эксплуатационной и технической документации к криптосредствам, а также настоящим Требованиям.

При этом операторы должны обеспечивать комплексность защиты персональных данных, в том числе посредством применения некриптографических средств защиты.

2.3. При разработке и реализации мероприятий по организации и обеспечению безопасности персональных данных при их обработке в информационной системе оператор или уполномоченное оператором лицо осуществляет:

- разработку для каждой информационной системы персональных данных модели угроз безопасности персональных данных при их обработке;

- разработку на основе модели угроз системы безопасности персональных данных, обеспечивающей нейтрализацию всех перечисленных в модели угроз;

- определение необходимости использования криптосредств для обеспечения безопасности персональных данных и, в случае положительного решения, определение на основе модели угроз цели использования криптосредств для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных и (или) иных неправомерных действий при их обработке;

- установку и ввод в эксплуатацию криптосредств в соответствии с эксплуатационной и технической документацией к этим средствам;

- проверку готовности криптосредств к использованию с составлением заключений о возможности их эксплуатации;

- обучение лиц, использующих криптосредства, работе с ними;

- поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним, носителей персональных данных;

- учет лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационной системе (пользователи криптосредств);

- контроль за соблюдением условий использования криптосредств, предусмотренных  эксплуатационной и технической документацией к ним;

- разбирательство и составление заключений по фактам нарушения условий хранения носителей персональных данных, использования криптосредств, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

- описание организационных и технических мер, которые оператор обязуется осуществлять при обеспечении безопасности персональных данных с использованием криптосредств при их обработке в информационных системах, с указанием в частности:

а) индекса, условного наименования и регистрационных номеров используемых криптосредств;

б) соответствия размещения и монтажа аппаратуры и оборудования, входящего в состав криптосредств, требованиям нормативной документации и правилам пользования криптосредствами;

в) соответствия помещений, в котором размещены криптосредства и хранится ключевая документация к ним, настоящим Требованиям с описанием основных средств защиты;

г) выполнения Требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Описание принятых мер должно быть включено в уведомление, предусмотренное частью 1 статьи 22 Федерального закона " О персональных данных".

2.4. Пользователи криптосредств допускаются к работе с ними по решению, утверждаемому оператором. При наличии двух и более  пользователей криптосредств обязанности между ними должны быть распределены с учетом персональной ответственности за сохранность криптосредств, ключевой, эксплуатационной и технической документации, а также за порученные участки работы.

2.5. Пользователи криптосредств обязаны:

- не разглашать информацию, к которой они допущены, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты;

- соблюдать требования к обеспечению безопасности персональных данных, требования к обеспечению безопасности криптосредств и ключевых документов к ним;

- сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним;

- немедленно уведомлять оператора о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных.

- сдать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящими Требованиями, при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств;

2.6 Обеспечение функционирования и безопасности криптосредств возлагается на ответственного пользователя криптосредств, имеющего необходимый уровень квалификации, назначаемого приказом оператора (далее – ответственный пользователь криптосредств).

Допускается возложение функций ответственного пользователя криптосредств на:

- одного из пользователей криптосредств;

- на структурное подразделение или должностное лицо (работника), ответственных за обеспечение безопасности персональных данных, назначаемых оператором;

- на специальное структурное подразделение по защите государственной тайны, использующее для этого шифровальные средства.

2.7. Ответственные пользователи криптосредств должны иметь функциональные обязанности, разработанные в соответствии с настоящими Требованиями.

2.8. При определении обязанностей пользователя криптосредств необходимо учитывать, что безопасность обработки с использованием криптосредств персональных данных обеспечивается:

- соблюдением пользователями криптосредств конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых криптосредств и ключевых документах к ним;

- точным выполнением пользователями криптосредств требований к обеспечению безопасности персональных данных;

- надежным хранением эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей информации ограниченного распространения;

- обеспечением принятых в соответствии с Требованиями к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных мер.

- своевременным выявлением попыток посторонних лиц получить сведения о защищаемых персональных данных, об используемых криптосредствах или ключевых документах к ним;

- немедленным принятием мер по предупреждению разглашения защищаемых персональных данных, а также возможной их утечки при выявлении фактов утраты или недостачи криптосредств, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

2.9. Лица, оформляемые на работу в качестве пользователей (ответственных пользователей) криптосредств, должны быть ознакомлены с настоящими Требованиями и другими документами, регламентирующими организацию и обеспечение безопасности персональных данных при их обработке в информационных системах, под расписку и несут ответственность за несоблюдение ими требований указанных документов в соответствии с законодательством Российской Федерации.

2.10. Текущий контроль за организацией и обеспечением функционирования криптосредств возлагается на оператора и ответственного пользователя криптосредств в пределах их служебных полномочий.

2.11. Контроль за организацией, обеспечением функционирования и безопасности криптосредств, предназначенных для защиты персональных данных при их обработке в информационных системах персональных данных, осуществляется в соответствии с действующим законодательством Российской Федерации.

2.12. В случае необходимости взаимодействия операторов информационных систем при использовании криптосредств для обеспечения безопасности обработки персональных данных для организации взаимодействия криптосредств по решению операторов персональных данных выделяется координирующий орган, ответственный за обеспечение безопасности персональных данных, указания которого являются обязательными для всех пользователей криптосредств.

## 3. ПОРЯДОК ОБРАЩЕНИЯ С КРИПТОСРЕДСТВАМИ И КРИПТОКЛЮЧАМИ К НИМ. МЕРОПРИЯТИЯ ПРИ КОМПРОМЕТАЦИИ КРИПТОКЛЮЧЕЙ.

3.1. Пользователи криптосредств обязаны:

- не разглашать информацию о ключевых документах;

- не допускать снятие копий с ключевых документов;

- не допускать вывод ключевых документов на дисплей (монитор) ПЭВМ или принтер;

- не допускать записи на ключевой носитель посторонней информации;

- не допускать установки ключевых документов в другие ПЭВМ.

3.2. При необходимости передачи по техническим средствам связи служебных сообщений ограниченного доступа, касающихся организации и обеспечения функционирования криптосредств, указанные сообщения необходимо передавать только с использованием криптосредств. Передача по техническим средствам связи криптоключей не допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами.

3.3. Криптосредства, используемые для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров.

Перечень индексов, условных наименований и регистрационных номеров криптосредств определяется Федеральной службой безопасности Российской Федерации.

3.4. Используемые или хранимые криптосредства, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету. Рекомендуемые формы приведены в Приложении №2. При этом программные криптосредства должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные криптосредства подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие криптосредства учитываются также совместно с соответствующими аппаратными средствами.

Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

3.5. Все полученные экземпляры криптосредств, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета пользователям криптосредств, несущим персональную ответственность за их сохранность.

Ответственный пользователь криптосредств заводит и ведет на каждого пользователя криптосредств лицевой счет, в котором регистрирует числящиеся за ними криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы.

3.6. Если эксплуатационной и технической документацией к криптосредствам предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в криптосредствах, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в техническом (аппаратном) журнале, ведущемся непосредственно пользователем криптосредств. В техническом (аппаратном) журнале отражают также данные об эксплуатации криптосредств и другие сведения, предусмотренные эксплуатационной и технической документацией. В иных случаях технический (аппаратный) журнал на криптосредства не заводится (если нет прямых указаний о его ведении в эксплуатационной или технической документации к криптосредствам). Типовая форма технического (аппаратного) журнала приведена в приложении № 3.

3.7  Передача криптосредств, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями криптосредств и (или) ответственным пользователем криптосредствпод расписку в соответствующих журналах поэкземплярного учета. Такая передача между пользователями криптосредств должна быть санкционирована ответственным пользователем криптосредств.

 3.8. Пользователи криптосредств хранят инсталлирующие криптосредства носители, эксплуатационную и техническую документацию к криптосредствам, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

Пользователи криптосредств предусматривают также раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов.

3.9. Аппаратные средства, с которыми осуществляется штатное функционирование криптосредств, а также аппаратные и аппаратно-программные криптосредства должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) криптосредств, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. При наличии технической возможности на время отсутствия пользователей криптосредств указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

3.10. Криптосредства и ключевые документы могут доставляться фельдъегерской (в том числе ведомственной) связью или со специально выделенными оператором ответственными пользователями криптосредств и сотрудниками при соблюдении мер, исключающих бесконтрольный доступ к криптосредствам и ключевым документам во время доставки.

Эксплуатационную и техническую документацию к криптосредствам можно пересылать заказными или ценными почтовыми отправлениями.

3.11. Для пересылки криптосредств и ключевых документов они должны быть помещены в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия, в особенности на записанную ключевую информацию. Криптосредства пересылают отдельно от ключевых документов к ним. На упаковках указывают оператора или ответственного пользователя криптосредств, для которых эти упаковки предназначены. На таких упаковках делают пометку «Лично». Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения упаковок и оттисков печати.

До первоначальной высылки (или возвращения) адресату сообщают отдельным письмом описание высылаемых ему упаковок и печатей, которыми они могут быть опечатаны.

3.12. Для пересылки криптосредств, эксплуатационной и технической документации к ним, ключевых документов следует подготовить сопроводительное письмо, в котором необходимо указать: что посылается и в каком количестве, учетные номера изделий или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Сопроводительное письмо вкладывают в одну из упаковок.

3.13. Полученные упаковки вскрывает только оператор или ответственный пользователь криптосредств, для которых они предназначены. Если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то получатель составляет акт, который высылает отправителю. Полученные с такими отправлениями криптосредства и ключевые документы до получения указаний от отправителя применять не разрешается.

3.14. При обнаружении бракованных ключевых документов или криптоключей один экземпляр бракованного изделия следует возвратить изготовителю для установления причин происшедшего и их устранения в дальнейшем, а оставшиеся экземпляры хранить до поступления дополнительных указаний от изготовителя.

3.15. Получение криптосредств, эксплуатационной и технической документации к ним, ключевых документов должно быть подтверждено отправителю в соответствии с порядком, указанным в сопроводительном письме. Отправитель обязан контролировать доставку своих отправлений адресатам. Если от адресата своевременно не поступило соответствующего подтверждения, то отправитель должен направить ему запрос и принять меры к уточнению местонахождения отправлений.

3.16. Заказ на изготовление очередных ключевых документов, их изготовление и рассылку на места использования для своевременной замены действующих ключевых документов следует производить заблаговременно. Указание о вводе в действие очередных ключевых документов может быть дано ответственным пользователем криптосредств только после поступления от всех заинтересованных пользователей криптосредств подтверждения о получении ими очередных ключевых документов.

3.17. Неиспользованные или выведенные из действия ключевые документы подлежат возвращению ответственному пользователю криптосредств или по его указанию должны быть уничтожены на месте.

3.18. Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков (CD-ROM), Data Key, Smart Card, Touch Memory и т.п.). Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим криптосредствам, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к соответствующим криптосредствам, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к криптосредствам уничтожают путем сжигания или с помощью любых бумагорезательных машин.

3.19.  Криптосредства уничтожают (утилизируют) по решению оператора, владеющего криптосредствами, и с уведомлением организации, ответственной в соответствии с ПКЗ-2005 за организацию поэкземплярного учета криптосредств.

Намеченные к уничтожению (утилизации) криптосредства подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом криптосредства считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к криптосредствам процедура удаления программного обеспечения криптосредств и они полностью отсоединены от аппаратных средств.

3.20. Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций криптосредств, а также совместно работающее с криптосредствами оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.), разрешается использовать после уничтожения криптосредств без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

3.21. Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в соответствующих журналах поэкземплярного учета. В эти же сроки с отметкой в техническом (аппаратном) журнале подлежат уничтожению разовые ключевые носители и ранее введенная и хранящаяся в криптосредствах или иных дополнительных устройствах ключевая информация, соответствующая выведенным из действия криптоключам; хранящиеся в криптографически защищенном виде данные следует перешифровать на новых криптоключах.

3.22. Разовые ключевые носители, а также электронные записи ключевой информации, соответствующей выведенным из действия криптоключам, непосредственно в криптосредствах или иных дополнительных устройствах уничтожаются пользователями этих криптосредств самостоятельно под расписку в техническом (аппаратном) журнале.

Ключевые документы уничтожаются либо пользователями криптосредств, либоответственным пользователем криптосредствпод расписку в соответствующих журналах поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом. При этом пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. После уничтожения пользователи криптосредств должны уведомить об этом (телефонограммой, устным сообщением по телефону и т.п.) ответственного пользователя криптосредств для списания уничтоженных документов с их лицевых счетов.

Уничтожение по акту производит комиссия в составе не менее двух человек из числа лиц, допущенных к пользованию криптосредств. В акте указывается что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов, инсталлирующих криптосредства носителей, эксплуатационной и технической документации. Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делаются отметки в соответствующих журналах поэкземплярного учета.

3.23. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению ответственного пользователя криптосредств, согласованного с оператором, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а защищаемая информация как можно менее ценной.

3.24. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшихся (хранящихся) с их использованием персональных данных, пользователи криптосредств обязаны сообщать ответственному пользователю криптосредств и (или) оператору.

Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения).

В случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

3.25. Мероприятия по розыску и локализации последствий компрометации ключевых документов организует и осуществляет оператор.

3.26. Ключевые документы для криптосредств или исходная ключевая информация для выработки ключевых документов изготавливаются ФСБ России на договорной основе или лицами, имеющими лицензию ФСБ России на деятельность по изготовлению ключевых документов для криптосредств.

Изготовлять ключевые документы из исходной ключевой информации могут операторы или ответственные пользователи криптосредств, применяя штатные криптосредства, если такая возможность предусмотрена эксплуатационной и технической документацией к криптосредствам.

## 4. РАЗМЕЩЕНИЕ, СПЕЦИАЛЬНОЕ ОБОРУДОВАНИЕ, ОХРАНА И ОРГАНИЗАЦИЯ РЕЖИМА В ПОМЕЩЕНИЯХ, ГДЕ УСТАНОВЛЕНЫ КРИПТОСРЕДСТВА ИЛИ ХРАНЯТСЯ КЛЮЧЕВЫЕ ДОКУМЕНТЫ К НИМ.

4.1 Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним (далее - режимные помещения), должны обеспечивать сохранность персональных данных, криптосредств и ключевых документов к ним.

При оборудовании режимных помещений должны выполняться требования к размещению, монтажу криптосредств, а также другого оборудования, функционирующего с криптосредствами.

Перечисленные в настоящем документе требования к режимным помещениям могут не предъявляться, если это предусмотрено правилами пользования криптосредствами, согласованными с ФСБ России.

4.2. Режимные помещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к криптосредствам. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

4.3. Размещение, специальное оборудование, охрана и организация режима в помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

4.4. Режим охраны помещений, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает ответственный пользователь криптосредств по согласованию, при необходимости, с оператором, в помещениях которого установлены криптосредства или хранятся ключевые документы к ним. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения настоящих Требований.

4.5. Двери спецпомещений должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода сотрудников и посетителей. Ключи от входных дверей нумеруют, учитывают и выдают сотрудникам, имеющим право допуска в режимные помещения, под расписку в журнале учета хранилищ. Дубликаты ключей от входных дверей таких помещений следует хранить в сейфе оператора или ответственного пользователя криптосредствами.

4.6. Для предотвращения просмотра извне режимных помещений их окна должны быть защищены.

4.7. Режимные помещения, как правило, должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации. Исправность сигнализации периодически необходимо проверять ответственному пользователю криптосредств совместно с представителем службы охраны или дежурным по организации с отметкой в соответствующих журналах.

4.8.  Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих криптосредства носителей должно быть предусмотрено необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у сотрудника, ответственного за хранилище. Дубликаты ключей от хранилищ сотрудники хранят в сейфе ответственного пользователя криптосредств. Дубликат ключа от хранилища ответственного пользователя криптосредств в опечатанной упаковке должен быть передан на хранение оператору под расписку в соответствующем журнале.

4.9. По окончании рабочего дня режимное помещение и установленные в нем хранилища должны быть закрыты, хранилища опечатаны. Находящиеся в пользовании ключи от хранилищ должны быть сданы под расписку в соответствующем журнале ответственному пользователю криптосредств или уполномоченному (дежурному), которые хранят эти ключи в личном или специально выделенном хранилище.

Ключи от режимных помещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ режимного помещения, в опечатанном виде должны быть сданы под расписку в соответствующем журнале службы охраны или дежурному по организации одновременно с передачей под охрану самих режимных помещений. Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей криптосредств, ответственных за эти хранилища.

4.10. При утрате ключа от хранилища или от входной двери в режимное помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает оператор или ответственный пользователь криптосредств.

4.11. В обычных условиях режимные помещения, находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями криптосредств, ответственным пользователем криптосредств или оператором.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному пользователю криптосредств или оператору. Прибывший ответственный пользователь криптосредств должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации персональных данных и к замене скомпрометированных криптоключей.

4.12. Размещение и монтаж криптосредств, а также другого оборудования, функционирующего с криптосредствами, в режимных помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

На время отсутствия пользователей криптосредств указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с ответственным пользователем криптосредств необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

Приложение 1

## ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Блокирование персональных данных** - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

**Доступ к информации**- возможность получения информации и ее использования.

**Информационная система**- совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

**Информационная система персональных данных** - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

**Контролируемая зона** - пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств.

Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

**Конфиденциальность персональных данных** - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания

**Криптосредство** - шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В частности, к криптосредствам относятся средства криптографической защиты информации (СКЗИ) - шифровальные (криптографические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну

**Модель нарушителя**- предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

**Модель угроз**- перечень возможных угроз.

**Обработка персональных данных** - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

**Общедоступные персональные данные**- персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

**Оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

**Персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

**Пользователь**- лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

**Распространение персональных данных** - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

**Режимные помещения** - помещения, где установлены криптосредства или хранятся ключевые документы к ним.

**Средство защиты информации**- техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

**Шифровальные (криптографические) средства - криптосредства:**

а) средства шифрования – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;

б) средства имитозащиты – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;

в) средства электронной цифровой подписи – аппаратные, программные и аппаратно–программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи;

г) средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;

д) средства изготовления ключевых документов (независимо от вида носителя ключевой информации);

е) ключевые документы (независимо от вида носителя ключевой информации).

Приложение 2

## ТИПОВАЯ ФОРМА

## ЖУРНАЛА ПОЭКЗЕМПЛЯРНОГО УЧЕТА КРИПТОСРЕДСТВ, ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ, КЛЮЧЕВЫХ ДОКУМЕНТОВ

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № п.п. | Наименование криптосредства, эксплуатационной и технической документации к ним, ключевых документов | Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых докумен-тов | Номера экземпляров (криптографичес-кие номера) ключевых документов | Отметка о получении | | Отметка о выдаче | |
| От кого получены | Дата и номер сопроводи-тельного письма | Ф.И.О. пользователя криптосредств | Дата и расписка в получении |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Отметка о подключении (установке) СКЗИ | | | Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов | | | Примечание |
| Ф.И.О. пользователя криптосредств, производившего подключение (установку) | Дата подключения  (установки) и подписи лиц, произведших подключение (установку) | Номера аппаратных средств, в которые установлены или к кото-рым подклю-чены крипто-средства | Дата изъятия (уничто-жения) | Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение) | Номер акта или расписка об уничтожении |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 |

Приложение 3

## ТИПОВАЯ ФОРМА

## ТЕХНИЧЕСКОГО (АППАРАТНОГО) ЖУРНАЛА

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № п.п. | Дата | Тип и регистра-ционные номера использу-емых крипто-средств | Записи по обслужи-ванию крипто-средств | Используемые криптоключи | | | Отметка об уничтожении (стирании) | | Приме-чание |
| Тип ключево-го доку-мента | Серийный, криптографи-ческий номер и номер экземп-ляра ключево-го документа | Номер разово-го ключевого носителя или зоны криптосредств, в которую вве-дены крипто-ключи | Дата | Подпись пользо-вателя криптосредств |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |

# МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ С ПОМОЩЬЮ КРИПТОСРЕДСТВ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ" ОТ 21 ФЕВРАЛЯ 2008 ГОДА

УТВЕРЖДЕНЫ  
руководством 8 Центра  
ФСБ России  
21 февраля 2008 года  
№ 149/54-144

## ВВЕДЕНИЕ

Настоящие Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (далее – Методические рекомендации) разработаны в соответствии с п. 2 постановления Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

Методические рекомендации предназначены для операторов и разработчиков информационных систем персональных данных и охватывают вопросы защиты персональных данных с помощью криптосредств.

Методическими рекомендациями необходимо руководствоваться в случае определения оператором необходимости обеспечения безопасности персональных данных с использованием криптосредств (за исключением случая, когда оператором является физическое лицо, использующее персональные данные исключительно для личных и семейных нужд), а также при обеспечении безопасности персональных данных при обработке в  информационных системах, отнесенных к компетенции ФСБ России. В частности, Методическими рекомендациями необходимо руководствоваться в следующих случаях:

-  при обеспечении с использованием криптосредств безопасности персональных данных при их обработке в государственных информационных системах персональных данных (часть 5 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»);

-  при использовании криптосредств для обеспечения персональных данных в случаях, предусмотренных п. 3 Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).

Настоящие Методические рекомендации не распространяются на информационные системы персональных данных, в которых:

-  персональные данные обрабатываются без использования средств автоматизации;

-  обрабатываются персональные данные, отнесенные в установленном порядке к сведениям, составляющим государственную тайну;

-  технические средства частично или целиком находятся за пределами Российской Федерации.

## 1. ОСНОВНЫЕ ТЕРМИНЫ И ИХ ОПРЕДЕЛЕНИЯ

<В настоящих Методических рекомендациях и при взаимодействии с лицензиатами ФСБ России, являющимися разработчиками криптосредств, разработчиками информационных систем персональных данных, в которых используются криптосредства, или специализированными организациями, проводящими тематические исследования криптосредств, используются следующие основные термины.

**Автоматизированная система (АС)** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**Автоматизированная система в защищенном исполнении (АСЗИ)** – автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и (или) иных нормативных документов по защите информации.

**Атака** – целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой криптосредством информации или с целью создания условий для этого.

**Безопасность** **–** состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

**Безопасность объекта** **–** состояние защищенности объекта от внешних и внутренних угроз.

Данное определение распространяется на любой реальный объект, в качестве которого могут выступать технические средства, программные средства, информация, информационные технологии, информационные системы, информационно-телекоммуникационные сети, здания, сооружения и т.д.

**Блокирование персональных данных** – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

**Встраивание криптосредства** – процесс подключения криптосредства к техническим и программным средствам, совместно с которыми предполагается его штатное функционирование, за исключением процесса инсталляции.

**Документированные (декларированные) возможности ПО (ТС)** – функциональные возможности ПО (ТС), описанные в документации на ПО (ТС).

**Доступ к информации** – возможность получения информации и ее использования.

**Жизненно важные интересы** – совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

**Защищаемая информация** – информация, для которой обладателем информации определены характеристики ее безопасности.

**Инсталляция** – установка программного продукта на компьютер. Инсталляция обычно выполняется под управлением инсталлятора – программы, которая приводит состав и структуру устанавливаемого программного изделия в соответствие с конфигурацией компьютера, а также настраивает программные параметры согласно типу имеющейся операционной системы, классам решаемых задач и режимам работы. Таким образом, инсталляция делает программный продукт пригодным для использования в данной вычислительной системе и готовым решать определенный класс задач в определенном режиме работы.

**Информация** – сведения (сообщения, данные) независимо от формы их представления.

**Информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

**Информационная система персональных данных** – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

**Информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**Информационно-телекоммуникационная сеть** – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

**Информационно-телекоммуникационная сеть общего пользования** –информационно-телекоммуникационная сеть, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

**Использование персональных данных** – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

**Канал атаки** – среда переноса от субъекта к объекту атаки (а, возможно, и от объекта к субъекту атаки) действий, осуществляемых при проведении атаки.

**Контролируемая зона** – пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств.

Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

**Конфиденциальность информации** – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

**Конфиденциальность персональных данных** – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

**Криптографически опасная информация (КОИ)** – информация о состояниях криптосредства, знание которой нарушителем позволит ему строить алгоритмы определения ключевой информации (или ее части) или алгоритмы бесключевого чтения.

**Криптосредство** – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В частности, к криптосредствам относятся средства криптографической защиты информации (СКЗИ) - шифровальные (криптографические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

**Модель нарушителя** – предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности».

**Модель угроз** – перечень возможных угроз.

**Нарушитель (субъект атаки)** – лицо (или инициируемый им процесс), проводящее (проводящий) атаку.

**Негативные функциональные возможности** – документированные и недокументированных возможности программных и аппаратных компонентов криптосредства и среды функционирования криптосредства, позволяющие:

-  модифицировать или искажать алгоритм работы криптосредств в процессе их использования;

-  модифицировать или искажать информационные или управляющие потоки и процессы, связанные с функционированием криптосредства;

-  получать доступ нарушителям к хранящейся в открытом виде ключевой, идентификационной и (или) аутентифицирующей информации, а также к защищаемой информации.

**Недокументированные (недекларированные) возможности ПО (ТС)**– функциональные возможности ПО (ТС), не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение характеристик безопасности защищаемой информации.

**Носители сведений, составляющих государственную тайну,** – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Так как по своей природе сведения, составляющие государственную тайну, не отличаются от всех остальных сведений, то приведенное определение можно корректно использовать для любых сведений.

Учитывая определение понятия «информация», термин «носитель информации» можно использовать в качестве синонима термину «носитель сведений».

**Обезличивание персональных данных** – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

**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.

**Обработка персональных данных** – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

**Общедоступные персональные данные** – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

**Объект информатизации** – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

**Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

**Опубликованные возможности ПО или ТС** – возможности, сведения о которых содержатся в общедоступных открытых источниках (технические и любые другие материалы разработчика ПО или ТС, монографии, публикации в СМИ, материалы конференций и других форумов, информация из сети Internet и т.д.).

**Персональные данные** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

**Пользователь**– лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

**ПО –**программное обеспечение.

**Распространение персональных данных** – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

**Специальная защита** – комплекс организационных и технических мероприятий, обеспечивающих защиту информации от утечки по каналам побочных излучений и наводок.

**Среда функционирования криптосредства (СФК)** – совокупность технических и программных средств, совместно с которыми предполагается штатное функционирование криптосредства и которые способны повлиять на выполнение предъявляемых к криптосредству требований.

**Средство защиты информации** – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

**Средство вычислительной техники (СВТ)** - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

**Трансграничная передача персональных данных** – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

**ТС –**техническое средство.

**Угроза безопасности –**совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

**Угроза безопасности объекта** – возможное нарушение характеристики безопасности объекта.

**Уничтожение персональных данных** – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

**Успешная атака** – атака, достигшая своей цели.

**Уровень криптографической защиты информации** – совокупность требований, предъявляемых к криптосредству.

**Характеристика безопасности объекта** – требование к объекту, или к условиям его создания и существования, или к информации об объекте и условиях его создания и существования, выполнение которого необходимо для обеспечения защищенности жизненно важных интересов личности, общества или государства.

**Шифровальные (криптографические) средства**:

а) средства шифрования – аппаратные, программные и аппаратно–

программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;

б) средства имитозащиты – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;

в) средства электронной цифровой подписи – аппаратные, программные и аппаратно–программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи;

г) средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;

д) средства изготовления ключевых документов (независимо от вида носителя ключевой информации);

е) ключевые документы (независимо от вида носителя ключевой информации).

## 2. ОСНОВНЫЕ ПОЛОЖЕНИЯ

2.1.  Работы по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (далее – информационная система) проводятся в соответствии со следующими основными документами:

-  Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

-  Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

-  Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденное постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 (далее – Положение);

-  Порядок проведения классификации информационных систем персональных данных, утвержденный приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 года № 55/86/20 (зарегистрирован Минюстом России 3 апреля 2008 года, регистрационный № 11462) (далее – Порядок);

-  Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное приказом ФСБ России от 9 февраля 2005 года № 66 (зарегистрирован Минюстом России 3 марта 2005 года, регистрационный № 6382);

-  Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (ФСБ России, № 149/6/6-622, 2008);

-  настоящие Методические рекомендации.

2.2.  В соответствии с п. 2 Положения безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

2.3.  В соответствии с п. 12 Положения необходимым условием разработки системы защиты персональных данных является формирование модели угроз безопасности персональных данных (далее – модель угроз).

Кроме этого, в соответствии с п. 16 Порядка модель угроз необходима для определения класса специальной информационной системы.

2.4.  Модель угроз формируется и утверждается оператором в соответствии с методическими документами, разработанными в соответствии с пунктом 2 постановления 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».

В случае обеспечения безопасности персональных данных без использования криптосредств при формировании модели угроз используются методические документы ФСТЭК России.

В случае определения оператором необходимости обеспечения безопасности персональных данных с использованием криптосредств  при формировании модели угроз используются методические документы ФСТЭК России и настоящие Методические рекомендации. При этом из двух содержащихся в документах ФСТЭК России и Методических рекомендациях однотипных угроз выбирается более опасная.

По согласованию с ФСТЭК России и ФСБ России допускается формирование модели угроз только на основании настоящих Методических рекомендаций.

При обеспечении безопасности персональных данных при обработке в информационных системах, отнесенных к компетенции ФСБ России, модели угроз формируются только на основании настоящих Методических рекомендаций.

2.5.  В случае использования в информационной системе криптосредств при необходимости к формированию модели угроз могут привлекаться лицензиаты ФСБ России, являющиеся разработчиками криптосредств или специализированными организациями, проводящими тематические исследования криптосредств.

2.6.  Модель угроз может быть пересмотрена:

-  по решению оператора на основе периодически проводимых им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;

-  по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

## 3. МЕТОДОЛОГИЯ ФОРМИРОВАНИЯ МОДЕЛИ УГРОЗ

### 3.1. Общие принципы

Разработка модели угроз должна базироваться на следующих принципах:

1) Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных (п. 2.2 Методических рекомендаций).

2) При формировании модели угроз необходимо учитывать как угрозы, осуществление которых нарушает безопасность персональных данных (далее – прямая угроза), так и угрозы, создающие условия для появления прямых угроз (далее – косвенные угрозы) или косвенных угроз.

3) Персональные данные обрабатываются и хранятся в информационной системе с использованием определенных информационных технологий и технических средств, порождающих объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы защищаемой информации.

4) Криптосредство штатно функционирует совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к криптосредству требований и которые образуют среду функционирования криптосредства (СФК).

5) Система защиты персональных данных не может обеспечить защиту информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, криптосредство не может обеспечить защиту информации от раскрытия лицами, которым предоставлено право на доступ к этой информации).

6) Нарушитель может действовать на различных этапах жизненного цикла криптосредства и СФК (под этими этапами в настоящем документе понимаются разработка, производство, хранение, транспортировка, ввод в эксплуатацию, эксплуатация программных и технических средств криптосредства и СФК).

7) Для обеспечения безопасности персональных данных при их обработке в информационных системах должны использоваться сертифицированные в системе сертификации ФСБ России (имеющие положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации) криптосредства.

В случае отсутствия готовых сертифицированных криптосредств, функционально пригодных для обеспечения безопасности персональных данных при их обработке в конкретной информационной системе, на этапе аванпроекта или эскизного (эскизно-технического) проекта разработчиком информационной системы с участием оператора и предполагаемого разработчика криптосредства готовится обоснование целесообразности разработки нового типа криптосредства и определяются требования к его функциональным свойствам.

Разработка нового типа криптосредства осуществляется в соответствии с Положением ПКЗ-2005.

Различают модель угроз верхнего уровня и детализированную модель угроз.

Модель угроз верхнего уровня предназначена для определения характеристик безопасности защищаемых персональных данных и других объектов защиты (принципы 2 и 3). Эта модель также определяет исходные данные для детализированной модели угроз.

Детализированная модель угроз предназначена для определения требуемого уровня криптографической защиты.

### 3.2. Методология формирования модели угроз верхнего уровня

Формирование модели угроз верхнего уровня осуществляется на этапе сбора и анализа исходных данных по информационной системе в соответствии с установленным Порядком.

Для правильного определения криптосредств, необходимых для обеспечения безопасности персональных данных, дополнительно к данному этапу предъявляются следующие требования.

**Определение условий создания и использования персональных данных**

Должны быть описаны условия создания и использования персональных данных. Для этого определяются:

-  субъекты, создающие персональные данные (в качестве такого субъекта может выступать лицо или его представитель в виде программного или технического средства);

-  субъекты, которым персональные данные предназначены;

-  правила доступа к защищаемой информации;

-  информационные технологии, базы данных, технические средства, используемые для создания и обработки персональных данных;

-  используемые в процессе создания и использования персональных данных объекты, которые могут быть объектами угроз, создающими условия для появления угроз персональным данным. Такого рода объектами могут быть, например, технические и программные средства.

Степень детализации описания должна быть достаточной для выполнения остальных требований к этапу сбора и анализа исходных данных по информационной системе.

**Описание форм представления персональных данных**

Персональные данные имеют различные формы представления (формы фиксации) с учетом используемых в информационной системе информационных технологий и технических средств.

Необходимо дать описание этих форм представления (форм фиксации) персональных данных. К таким формам относятся области оперативной памяти, файлы, записи баз данных, почтовые отправления и т.д.

**Описание информации, сопутствующей процессам создания и использования персональных данных**

На основе анализа условий создания и использования персональных данных должна быть определена информация, сопутствующая процессам создания и использования персональных данных. При этом представляет интерес только та информация, которая может быть объектом угроз и потребует защиты.

К указанной информации, в частности, относится:

-  ключевая, аутентифицирующая и парольная информация криптосредства;

-  криптографически опасная информация (КОИ);

-  конфигурационная информация;

-  управляющая информация;

-  информация в электронных журналах регистрации;

-  побочные сигналы, которые возникают в процессе функционирования технических средств и в которых полностью или частично отражаются персональные данные или другая защищаемая информация;

-  резервные копии файлов с защищаемой информацией, которые могут создаваться в процессе обработки этих файлов;

-  остаточная информация на носителях информации.

В тех случаях, когда модель угроз разрабатывается лицами, не являющимися специалистами в области защиты информации, рекомендуется ограничиться приведенными выше примерами информации, сопутствующей процессам создания и использования персональных данных.

Разработчики модели угроз - специалисты в области защиты информации могут уточнить указанный выше перечень информации, сопутствующей процессам создания и использования персональных данных, с приведением соответствующих обоснований. Рекомендуется указанное уточнение делать только в случае необходимости разработки нового типа криптосредства.

Уточнение перечня информации, сопутствующей процессам создания и использования персональных данных, должно осуществляться путем:

- исключения типов рассматриваемой информации из указанного выше перечня, которые являются избыточными в силу специфики конкретной информационной системы;

- конкретизации и детализации не исключенных типов рассматриваемой информации с учетом конкретных условий эксплуатации информационной системы;

- описания типов рассматриваемой информации, не указанных в приведенном выше перечне.

**Определение характеристик безопасности**

Необходимо определить характеристики безопасности не только персональных данных, но и характеристики безопасности всех объектов, которые были определены как возможные объекты угроз.

Основными (классическими) характеристиками безопасности являются конфиденциальность, целостность и доступность.

В дополнение к перечисленным выше основным характеристикам безопасности могут рассматриваться также и другие характеристики безопасности. В частности, к таким характеристикам относятся неотказуемость, учетность (иногда в качестве синонима используется термин «подконтрольность»), аутентичность (иногда в качестве синонима используется термин «достоверность») и адекватность.

Приведенный список характеристик безопасности не является исчерпывающим. Возможность большого числа характеристик безопасности кроется в определении понятия «характеристика безопасности объекта»:

«**характеристика безопасности объекта** – требование к объекту, или к условиям его создания и существования, или к информации об объекте и условиях его создания и существования, выполнение которого необходимо для обеспечения защищенности жизненно важных интересов личности, общества или государства».

Как правило, условия создания и существования реальных объектов достаточно сложны и, как следствие, к ним можно предъявить достаточно много самых различных требований.

Так как угроза безопасности объекта – возможное нарушение характеристики безопасности объекта, то перечень всех характеристик безопасности для всех возможных объектов угроз, по сути, определяет модель угроз верхнего уровня.

Например, если в информационной системе требуется обеспечить только защиту от уничтожения, целостность и доступность защищаемой информации (в качестве возможного примера такой информационной системы можно привести информационную систему школьного учителя, содержащую общедоступные персональные данные учащихся), то модель угроз верхнего уровня содержит следующий перечень угроз:

-  угроза уничтожения защищаемой информации;

-  угроза нарушения целостности защищаемой информации;

-  угроза нарушения доступности защищаемой информации.

### 3.3. Методология формирования детализированной модели угроз

Согласно приведенному в Законе Российской Федерации «О безопасности» определению понятия «угроза безопасности», необходимо определить совокупность условий и факторов, создающих опасность нарушения характеристик безопасности возможных объектов угроз. Это и есть содержание работ по созданию детализированной модели угроз.

Можно привести примеры, когда целесообразно создание моделей угроз нескольких уровней детализации.

Очевидным примером может служить объект угроз, представляющий сложную территориально распределенную автоматизированную систему, для которой условия функционирования различных составных частей системы могут существенно различаться. При анализе такой системы, как правило, используется принцип декомпозиции сложного объекта. Если же составные части системы также весьма сложны, то их анализ снова потребует использование принципа декомпозиции сложного объекта. В рассматриваемом случае целесообразно создание моделей угроз для каждого объекта, получающегося в процессе декомпозиции.

При определении угроз безопасности объекта следует различать:

-  угрозы, не являющиеся атакой;

-  атаки.

Рекомендуется использовать следующую структуру угроз, не являющихся атаками:

-  *угрозы, не связанные с деятельностью человека: стихийные бедствия и природные явления* (землетрясения, наводнения, ураганы и т.д.);

-  *угрозы социально–политического характера*: забастовки, саботаж, локальные конфликты и т.д.;

-  *ошибочные действия и (или) нарушения тех или иных требований лицами, санкционировано взаимодействующими с возможными объектами угроз.* Если, например, в качестве объекта угроз выступает автоматизированная система в защищенном исполнении (АСЗИ), то к таким действиям и нарушениям, в частности, относятся:

o  непредумышленное искажение или удаление программных компонентов АСЗИ;

o  внедрение и использование неучтенных программ;

o  игнорирование организационных ограничений (установленных правил) при работе с ресурсами АСЗИ, включая средства защиты информации. В частности:

-  нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (в частности, ключевой, парольной и аутентифицирующей информации);

-  предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований;

-  настройка и конфигурирование средств защиты информации, а также технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, в нарушение нормативных и технических документов;

-  несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа.

-  *угрозы техногенного характера,* основными из которых являются:

o  аварии (отключение электропитания, системы заземления, разрушение инженерных сооружений и т.д.);

o  неисправности, сбои аппаратных средств, нестабильность параметров системы электропитания, заземления и т.д.;

o  помехи и наводки, приводящие к сбоям в работе аппаратных средств.

Следует отметить, что, как правило, защита от угроз, не являющихся атаками, в основном регламентируется инструкциями, разработанными и утвержденными операторами с учетом особенностей эксплуатации информационных систем и действующей нормативной базы.

Как показал мировой и отечественный опыт, атаки являются наиболее опасными угрозами (что обусловлено их тщательной подготовкой, скрытностью проведения, целенаправленным выбором объектов и целей атак).

Атаки готовятся и проводятся нарушителем, причем возможности проведения атак обусловлены возможностями нарушителя. Иными словами, конкретные возможности нарушителя определяют конкретные атаки, которые может провести нарушитель.

Но тогда с учетом определения понятия «модель нарушителя» все возможные атаки определяются моделью нарушителя.

Модель нарушителя тесно связана с моделью угроз и, по сути, является ее частью. Смысловые отношения между ними следующие. В модели угроз содержится максимально полное описание угроз безопасности объекта. Модель нарушителя содержит описание предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

### 3.4. Методология формирования модели нарушителя

Согласно последнему из определенных в п. 3.1 Методических рекомендаций принципу (принцип 7) нарушитель может действовать на различных этапах жизненного цикла криптосредства и СФК (под этими этапами в настоящем документе понимаются разработка, производство, хранение, транспортировка, ввод в эксплуатацию, эксплуатация программных и технических средств криптосредств и СФК).

**Этапы разработки, производства, хранения, транспортировки, ввода в эксплуатацию технических и программных средств криптосредства и СФК**

На этапах разработки, производства, хранения, транспортировки, ввода в эксплуатацию технических и программных средств криптосредства и СФК обработка персональных данных не производится. Поэтому объектами атак могут быть только сами эти средства и документация на них.

В связи с изложенным на указанных этапах возможны следующие атаки:

-  внесение негативных функциональных возможностей в технические и программные компоненты криптосредства и СФК, в том числе с использованием вредоносных программ (компьютерные вирусы, «троянские кони» и т.д.);

-  внесение несанкционированных изменений в документацию на криптосредство и технические и программные компоненты СФК.

Необходимо отметить, что указанные атаки:

-  на этапах разработки, производства и транспортировки технических и программных средств криптосредства и СФК могут проводиться только вне зоны ответственности оператора;

-  на этапе хранения технических и программных средств криптосредства и СФК могут проводиться как в зоне, так и вне зоны ответственности оператора;

-  на этапе ввода в эксплуатацию технических и программных средств криптосредства и СФК могут проводиться в зоне ответственности оператора.

В связи с изложенным операторы должны предусмотреть меры контроля:

-  соответствия технических и программных средств криптосредства и СФК и документации на эти средства, поступающих в зону ответственности оператора, эталонным образцам (например, оператор должен требовать от поставщиков гарантий соответствия технических и программных средств криптосредства и СФК и документации на эти средства, поступающих в зону ответственности оператора, эталонным образцам или механизмы контроля, позволяющие оператору установить самостоятельно такое соответствие);

-  целостности технических и программных средств криптосредства и СФК и документации на эти средства в процессе хранения и ввода в эксплуатацию этих средств (с использованием как механизмов контроля, описанных в документации, например, на криптосредство, так и с использованием организационных и организационно-технических мер, разработанных оператором с учетом требований соответствующих нормативных и методических документов – см. п. 2.1 Методических рекомендаций).

**Этап эксплуатации технических и программных средств криптосредства и СФК**

Атака как любое целенаправленное действие характеризуется рядом существенных признаков. К этим существенным признакам на этапе эксплуатации технических и программных средств криптосредства и СФК вполне естественно можно отнести:

-  нарушителя - субъекта атаки;

-  объект атаки;

-  цель атаки;

-  имеющуюся у нарушителя информацию об объекте атаки;

-  имеющиеся у нарушителя средства атаки;

-  канал атаки.

**Возможные объекты атак и цели атак определяются на этапе формирования модели угроз верхнего уровня.**

При определении объектов атак, в частности, должны быть рассмотрены как возможные объекты атак и при необходимости конкретизированы с учетом используемых в информационной системе информационных технологий и технических средств следующие объекты:

-  документация на криптосредство и на технические и программные компоненты СФК;

-  защищаемые персональные данные;

-  ключевая, аутентифицирующая и парольная информация;

-  криптографически опасная информация (КОИ);

-  криптосредство (программные и аппаратные компоненты криптосредства);

-  технические и программные компоненты СФК;

-  данные, передаваемые по каналам связи;

-  помещения, в которых находятся защищаемые ресурсы информационной системы.

В тех случаях, когда модель угроз разрабатывается лицами, не являющимися специалистами в области защиты информации, рекомендуется ограничиться приведенными выше примерами возможных объектов атак.

Разработчики модели угроз - специалисты в области защиты информации могут уточнить указанный выше перечень возможных объектов атак с приведением соответствующих обоснований. Рекомендуется указанное уточнение делать только в случае необходимости разработки нового типа криптосредства.

Уточнение перечня возможных объектов атак должно осуществляться путем:

исключения объектов атак из указанного выше перечня, которые являются избыточными в силу специфики конкретной информационной системы;

конкретизации и детализации не исключенных объектов атак с учетом конкретных условий эксплуатации информационной системы;

описания объектов атак, не указанных в приведенном выше перечне.

С учетом изложенного модель нарушителя для этапа эксплуатации технических и программных средств криптосредства и СФК должна иметь следующую структуру:

-  описание нарушителей (субъектов атак);

-  предположения об имеющейся у нарушителя информации об объектах атак;

-  предположения об имеющихся у нарушителя средствах атак;

-  описание каналов атак.

**Описание нарушителей (субъектов атак)**

1) Различают шесть основных типов нарушителей: Н1, Н2, ... , Н6.

Предполагается, что нарушители типа Н5 и Н6 могут ставить работы по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа криптосредств и СФК.

Возможности нарушителя типа Нi+1 включают в себя возможности нарушителя типа Нi (1  i   5).

Если внешний нарушитель обладает возможностями по созданию способов  подготовки атак, аналогичными соответствующим возможностям нарушителя типа Нi (за исключением возможностей, предоставляемых пребыванием в момент атаки в контролируемой зоне), то этот нарушитель также будет обозначаться как нарушитель типа Нi (2  i   6).

2) Данный раздел модели нарушителя должен содержать:

-  перечень лиц, которые не рассматриваются в качестве потенциальных нарушителей, и обоснование этого перечня (при необходимости);

-  предположение о невозможности сговора нарушителей *(для всех типов нарушителей)* или предположения о возможном сговоре нарушителей и о характере сговора, включая перечисление дополнительных возможностей, которые могут использовать находящиеся в сговоре нарушители для подготовки и проведения атак *(для нарушителей типа Н4 - Н6)*.

Примечание

Данный раздел модели нарушителя имеет следующее типовое содержание.

Сначала все физические лица, имеющие доступ к техническим и программным средствам информационной системы, разделяются на следующие категории:

-  категория I – лица, не имеющие права доступа в контролируемую зону информационной системы;

-  категория II – лица, имеющие право постоянного или разового доступа в контролируемую зону информационной системы.

Далее все потенциальные нарушители подразделяются на:

-  *внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны информационной системы;*

-  *внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны информационной системы.*

*Констатируется, что:*

-  *внешними нарушителями могут быть как лица категория I, так и лица категория II;*

-  *внутренними нарушителями могут быть только лица категории II.*

*Дается описание привилегированных пользователей информационной системы (членов группы администраторов), которые назначаются из числа особо доверенных лиц и осуществляют техническое обслуживание технических и программных средств криптосредства и СФК, включая их настройку, конфигурирование и распределение ключевой документации между непривилегированными пользователями.*

*Далее следует обоснование исключения тех или иных типов лиц категории II из числа потенциальных нарушителей. Как правило, привилегированные пользователи информационной системы исключаются из числа потенциальных нарушителей.*

*И, наконец, рассматривается вопрос о возможном сговоре нарушителей.*

**Предположения об имеющейся у нарушителя информации об объектах атак**

Данный раздел модели нарушителя должен содержать:

-  предположение о том, что потенциальные нарушители обладают всей информацией, необходимой для подготовки и проведения атак, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная, аутентифицирующая и ключевая информация.

-  обоснованные ограничения на степень информированности нарушителя (перечень сведений, в отношении которых предполагается, что они нарушителю недоступны).

Примечание

*Обоснованные ограничения на степень информированности нарушителя могут существенно снизить требования к криптосредству при его разработке.*

При определении ограничений на степень информированности нарушителя, в частности, должны быть рассмотрены следующие сведения:

-  содержание технической документации на технические и программные компоненты СФК;

-  долговременные ключи криптосредства;

-  все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного доступа (НСД) к информации организационно-техническими мерами (фазовые пуски, синхропосылки, незашифрованные адреса, команды управления и т.п.);

-  сведения о линиях связи, по которым передается защищаемая информация;

-  все сети связи, работающие на едином ключе;

-  все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, нарушения правил эксплуатации криптосредства и СФК;

-  все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, неисправности и сбои технических средств криптосредства и СФК;

-  сведения, получаемые в результате анализа любых сигналов от технических средств криптосредства и СФК, которые может перехватить нарушитель.

Только нарушителям типа Н3 - Н6 могут быть известны все сети связи, работающие на едином ключе.

Только нарушители типа Н5 - Н6 располагают наряду с доступными в свободной продаже документацией на криптосредство и СФК исходными текстами прикладного программного обеспечения.

Только нарушители типа Н6 располагают все документацией на криптосредство и СФК.

В тех случаях, когда модель угроз разрабатывается лицами, не являющимися специалистами в области защиты информации, рекомендуется ограничиться приведенным выше предположением о том, что потенциальные нарушители обладают всей информацией, необходимой для подготовки и проведения атак.

Разработчики модели угроз - специалисты в области защиты информации могут подготовить обоснованные ограничения на степень информированности нарушителя. Рекомендуется указанное ограничение делать только в случае необходимости разработки нового типа криптосредства.

**Предположения об имеющихся у нарушителя средствах атак**

Данный раздел модели нарушителя должен содержать:

-  предположение о том, что нарушитель имеет все необходимые для проведения атак по доступным ему каналам атак средства, возможности которых не превосходят возможности аналогичных средств атак на информацию, содержащую сведения, составляющие государственную тайну;

-  обоснованные ограничения на имеющиеся у нарушителя средства атак.

Примечание

Обоснованные ограничения на имеющиеся у нарушителя средства атак могут существенно снизить требования к криптосредству при его разработке.

При определении ограничений на имеющиеся у нарушителя средства атак, в частности, должны быть рассмотрены:

-  аппаратные компоненты криптосредства и СФК;

-  доступные в свободной продаже технические средства и программное обеспечение;

-  специально разработанные технические средства и программное обеспечение;

-  штатные средства.

Нарушители типа Н1 и Н2 располагают только доступными в свободной продаже аппаратными компонентами криптосредства и СФК.

Дополнительные возможности нарушителей типа Н3-Н5 по получению аппаратных компонент криптосредства и СФК зависят от реализованных в информационной системе организационных мер.

Нарушители типа Н6 располагают любыми аппаратными компонентами криптосредства и СФК.

Нарушители типа Н1 могут использовать штатные средства только в том случае, если они расположены за пределами контролируемой зоны.

Возможности нарушителей типа Н2-Н6 по использованию штатных средств зависят от реализованных в информационной системе организационных мер.

Нарушители типа Н4-Н6 могут проводить лабораторные исследования криптосредств, используемых за пределами контролируемой зоны информационной системы.

В тех случаях, когда модель угроз разрабатывается лицами, не являющимися специалистами в области защиты информации, рекомендуется ограничиться только приведенными выше средствами атак.

Разработчики модели угроз - специалисты в области защиты информации могут уточнить приведенный выше перечень средств атак. Рекомендуется указанное уточнение делать только в случае необходимости разработки нового типа криптосредства.

**Описание каналов атак**

С практической точки зрения этот раздел является одним из важнейших в модели нарушителя. Его содержание по существу определяется качеством формирования модели угроз верхнего уровня.

Основными каналами атак являются:

-  каналы связи (как внутри, так и вне контролируемой зоны), не защищенные от НСД к информации организационно-техническими мерами;

-  штатные средства.

Возможными каналами атак, в частности, могут быть:

-  каналы непосредственного доступа к объекту атаки (акустический, визуальный, физический);

-  машинные носители информации;

-  носители информации, выведенные из употребления;

-  технические каналы утечки;

-  сигнальные цепи;

-  цепи электропитания;

-  цепи заземления;

-  канал утечки за счет электронных устройств негласного получения информации;

-  информационные и управляющие интерфейсы СВТ.

В тех случаях, когда модель угроз разрабатывается лицами, не являющимися специалистами в области защиты информации, рекомендуется ограничиться только приведенными выше основными каналами атак.

Разработчики модели угроз - специалисты в области защиты информации могут уточнить приведенный выше перечень каналов атак. Рекомендуется указанное уточнение делать только в случае необходимости разработки нового типа криптосредства.

**Определение типа нарушителя**

Нарушитель относится к типу Нi, если среди предположений о его возможностях есть предположение, относящееся к нарушителям типа Нi и нет предположений, относящихся только к нарушителям типа Нj (j > i).

Нарушитель относится к типу Н6 в информационных системах, в которых обрабатываются наиболее важные персональные данные, нарушение характеристик безопасности которых может привести к особо тяжелым последствиям.

Рекомендуется при отнесении оператором нарушителя к типу Н6 согласовывать модель нарушителя с ФСБ России.

## 4. УРОВЕНЬ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ, УРОВНИ СПЕЦИАЛЬНОЙ ЗАЩИТЫ ОТ УТЕЧКИ ПО КАНАЛАМ ПОБОЧНЫХ ИЗЛУЧЕНИЙ И НАВОДОК И УРОВНИ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА.

4.1.  Различают шесть уровней КС1, КС2, КС3, КВ1, КВ2, КА1 криптографической защиты персональных данных, не содержащих сведений, составляющих государственную тайну, определенных в порядке возрастания количества и жесткости предъявляемых к криптосредствам требований, и, соответственно, шесть классов криптосредств, также обозначаемых через КС1, КС2, КС3, КВ1, КВ2, КА1.

Уровень криптографической защиты персональных данных, обеспечиваемой криптосредством, определяется оператором путем отнесения нарушителя, действиям которого должно противостоять криптосредство, к конкретному типу.

При отнесении заказчиком нарушителя к типу Н1 криптосредство должно обеспечить криптографическую защиту по уровню КС1, к типу Н2 – КС2, к типу Н3– КС3, к типу Н4 – КВ1, к типу Н5 – КВ2, к типу Н6 – КА1.

4.2.  Различают три уровня КС, КВ и КА специальной защиты от утечки по каналам побочных излучений и наводок при защите персональных данных с использованием криптосредств.

При отнесении нарушителя к типу Н1-Н3 должна быть обеспечена специальная защита по уровню КС, к типу Н4-Н5 – по уровню КВ, к типу Н6 – по уровню КА.

4.3.  В случае принятия оператором решения о защите персональных данных в информационной системе от несанкционированного доступа в соответствии с нормативными документами ФСБ России различают шесть уровней АК1, АК2, АК3, АК4, АК5, АК6 защиты от несанкционированного доступа к персональным данным в информационных системах, определенных в порядке возрастания количества и жесткости предъявляемых к системам защиты требований, и, соответственно, шесть классов информационных систем, также обозначаемых через АК1, АК2, АК3, АК4, АК5, АК6.

При отнесении заказчиком нарушителя к типу Н1 в информационной системе должна быть обеспечена защита от несанкционированного доступа к персональным данным по уровню АК1, к типу Н2 – по уровню АК2, к типу Н3 – по уровню АК3, к типу Н4 – по уровню АК4, к типу Н5 – по уровню АК5, к типу Н6 – по уровню АК6.

## 5. ТРЕБОВАНИЯ К КОНТРОЛЮ ВСТРАИВАНИЯ КРИПТОСРЕДСТВА

5.1.  Встраивание криптосредств класса КС1 и КС2 осуществляется без контроля со стороны ФСБ России (если этот контроль не предусмотрен техническим заданием на разработку (модернизацию) информационной системы).

Встраивание криптосредств класса КС3, КВ1, КВ2 и КА1 осуществляется только под контролем со стороны ФСБ России.

5.2.  Встраивание криптосредств класса КС1, КС2 или КС3 может осуществляться либо самим пользователем криптосредства при наличии соответствующей лицензии ФСБ России, либо организацией, имеющей соответствующую лицензию ФСБ России.

Встраивание криптосредства класса КВ1, КВ2 или КА1 осуществляется организацией, имеющей соответствующую лицензию ФСБ России.

5.3.  В ходе контроля со стороны ФСБ России встраивания криптосредства могут решаться, в частности, следующие задачи:

-  проверка требований документации на криптосредство, относящихся к встраиванию криптосредства, в том числе:

o  анализ корректности встраивания;

o  анализ правильности функционирования системы управления ключами;

-  экспериментальная проверка работоспособности криптосредства и правильности выполнения возложенных на него целевых функций;

-  оценка влияния технических и программных средств, совместно с которыми предполагается штатное функционирование криптосредства, на выполнение предъявляемых к криптосредству требований.

Методика и программа контроля встраивания криптосредства разрабатываются и (или) обосновываются специализированной организацией, проводящей тематические исследования криптосредства, и согласовываются с ФСБ России.

# МЕТОДИКА ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

<

Федеральная служба

по техническому и экспортному контролю

Утверждена

Заместителем директора ФСТЭК России

14 февраля 2008 г.

## МЕТОДИКА

## ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Примечание: пометка «для служебного пользования» снята Решением ФСТЭК России от 16 ноября 2009 г.

В книге всего пронумеровано 10 страниц, для служебного пользования

**Введение**

Методика определения актуальных угроз безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн) разработана ФСТЭК России на основании Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных» и «Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного  постановлением Правительства Российской Федерации от 17 ноября 2007 г. N 781, с учетом действующих нормативных документов ФСТЭК России по защите информации. Методика предназначена для использования при проведении работ пообеспечению безопасности персональных данных при их обработке в следующих автоматизированных информационных системах персональных данных:

государственных или муниципальных ИСПДн;

ИСПДн, создаваемых и (или) эксплуатируемых предприятиями, организациями и учреждениями (далее – организациями) независимо от форм собственности, необходимых для выполнения функций этих организаций в соответствии с их назначением;

ИСПДн, создаваемых и используемых физическими лицами, за исключением случаев, когда последние используют указанные системы исключительно для личных и семейных нужд.

Документ предназначен для специалистов по обеспечению безопасности информации, руководителей организаций и предприятий, организующих и проводящих работы по обработке ПДн в ИСПДн.

**1. Общие положения**

Под угрозами безопасности ПДн при их обработке в ИСПДн понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий  при их обработке в информационной системе персональных данных.

В соответствии со статьей 19 Федерального закона N152-ФЗ от 27 июля 2006 г. «О персональных данных» ПДн должны быть защищены от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий. Угрозы безопасности ПДн при их обработке в ИСПДн могут быть связаны как с непреднамеренными действиями персонала ИСПДн и(или) потребителей, пользующихся услугами, предоставляемыми ИСПДн в соответствии с ее назначением, так и со специально осуществляемыми неправомерными действиями иностранных государств, криминальных сообществ, отдельных организаций и граждан, а также иными источниками угроз.

Угрозы безопасности ПДн могут быть реализованы за счет утечки ПДн по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах ИСПДн, технические каналы перехвата информации при ее передаче по каналам связи, технические каналы утечки акустической (речевой) информации) либо за счет несанкционированного доступа с использованием соответствующего программного обеспечения.

Детальное описание угроз, связанных с утечкой ПДн по техническим каналам, приведено в «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Выявление технических каналов утечки ПДн осуществляется на основе нормативных и методических документов ФСТЭК России.

Источниками угроз, реализуемых за счет несанкционированного доступа к базам данных с использованием штатного или специально разработанного программного обеспечения, являются субъекты, действия которых нарушают регламентируемые в ИСПДн правила разграничения доступа к информации. Этими субъектами могут быть:

нарушитель;

носитель вредоносной программы;

аппаратная закладка.

Под нарушителем здесь и далее понимается физическое лицо (лица), случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности ПДн при их обработке техническими средствами в информационных системах. С точки зрения наличия права легального доступа в помещения, в которых размещены аппаратные средства, обеспечивающие доступ к ресурсам ИСПДн, нарушители подразделяются на два типа:

нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена, – внешние нарушители;

нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн, – внутренние нарушители.

Для ИСПДн, предоставляющих информационные услуги удаленным пользователям, внешними нарушителями могут являться лица, имеющие возможность осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий, алгоритмических или программных закладок через автоматизированные рабочие места, терминальные устройства ИСПДн, подключенные к сетям общего пользования.

Возможности внутреннего нарушителя существенным образом зависят   
от установленного порядка допуска физических лиц к информационным ресурсам ИСПДн и мер по контролю порядка проведения работ.

Угрозы несанкционированного доступа от внешних нарушителей реализуются с использованием протоколов межсетевого взаимодействия.

Детальное описание угроз, связанных с несанкционированным доступом в ИСПДн персональных данных, приведено в «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

Выявление угроз НСД к ПДн, реализуемых с применением программных и программно-аппаратных средств, осуществляется на основе экспертного метода, в том числе путем опроса специалистов, персонала ИСПДн, должностных лиц, при этом могут использоваться специальные инструментальные средства (сетевые сканеры) для подтверждения наличия   
и выявления уязвимостей программного и аппаратного обеспечения ИСПДн. Для проведения опроса составляются специальные опросные листы.

Наличие источника угрозы и уязвимого звена, которое может быть использовано для реализации угрозы, свидетельствует о наличии данной угрозы. Формируя на основе опроса перечень источников угроз ПДн, на основе опроса и сетевого сканирования  перечень уязвимых звеньев ИСПДн, а также по данным обследования ИСПДн – перечень технических каналов утечки информации, определяются условия существования в ИСПДн угроз безопасности информации и составляется их полный перечень. На основании этого перечня в соответствии с описанным ниже порядком формируется перечень актуальных угроз безопасности ПДн.

**2. Порядок определения актуальных угроз безопасности персональных данных в информационных системах персональных данных**

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн. Подход к составлению перечня актуальных угроз состоит в следующем.

Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности ИСПДн и частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, приведенных в таблице 1.

Таблица 1

Показатели исходной защищенности ИСПДн

| Технические и эксплуатационные характеристики ИСПДн | Уровень защищенности | | |
| --- | --- | --- | --- |
| Высокий | Средний | Низкий |
| 1. По территориальному размещению:  распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом; | – | – | + |
| городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка); | – | – | + |
| корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации; | – | + | – |
| локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий; | – | + | – |
| локальная ИСПДн, развернутая в пределах одного здания | + | – | – |
| 2. По наличию соединения с сетями общего пользования:  ИСПДн, имеющая многоточечный выход в сеть общего пользования; | – | – | + |
| ИСПДн, имеющая одноточечный выход в сеть общего пользования; | – | + | – |
| ИСПДн, физически отделенная от сети общего пользования | + | – | – |
| 3. По встроенным (легальным) операциям с записями баз персональных данных:  чтение, поиск; | + | – | – |
| запись, удаление, сортировка; | – | + | – |
| модификация, передача | – | – | + |
| 4. По разграничению доступа к персональным данным: | – | + | – |
| ИСПДн, к которой имеют доступ определенные переченем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн; |
| ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн; | – | – | + |
| ИСПДн с открытым доступом | – | – | + |
| 5. По наличию соединений с другими базами ПДн иных ИСПДн:  интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн); | – | – | + |
| ИСПДн, в которой используется  одна база ПДн, принадлежащая организации – владельцу данной ИСПДн | + | – | – |
| 6. По уровню обобщения (обезличивания) ПДн:  ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);  ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;  ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн) | +          –          – | –          +          – | –          –          + |
| 7. По объему  ПДн, которые предоставляются  сторонним пользователям ИСПДн без предварительной обработки:  ИСПДн, предоставляющая всю базу данных  с ПДн; | – | – | + |
| ИСПДн, предоставляющая часть ПДн; | – | + | – |
| ИСПДн, не предоставляющая никакой информации. | + | – | – |

Исходная степень защищенности определяется следующим образом.

1. ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу).

2. ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности,  к общему количеству решений), а остальные – низкому уровню защищенности.

3. ИСПДн имеет низкую степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент, а именно:

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

С учетом изложенного коэффициент реализуемости угрозы Y будет определяться соотношением.

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

если , то возможность реализации угрозы признается низкой;

если , то возможность реализации угрозы признается средней;

если , то возможность реализации угрозы признается высокой;

если , то возможность реализации угрозы признается очень высокой.

Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой ИСПДн. Этот показатель имеет три значения:

низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Затем осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн, в соответствии с правилами, приведенными в таблице 2.

Таблица 2

Правила отнесения угрозы безопасности ПДн к актуальной

|  |  |  |  |
| --- | --- | --- | --- |
| Возможность реализации угрозы | Показатель опасности угрозы | | |
| Низкая | Средняя | Высокая |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

С использованием данных о классе ИСПДн и составленного перечня актуальных угроз, на основе «Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и «Основных мероприятий по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» формулируются конкретные организационно-технические требования по защите ИСПДн от утечки информации по техническим каналам, от несанкционированного доступа и осуществляется выбор программных и технических средств защиты информации, которые могут быть использованы при создании и дальнейшей эксплуатации ИСПДн.

# ПРИКАЗ МИНИСТЕРСТВА СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ ОТ 14 НОЯБРЯ 2011 Г. N 312 «ОБ УТВЕРЖДЕНИИ АДМИНИСТРАТИВНОГО РЕГЛАМЕНТА ИСПОЛНЕНИЯ ФЕДЕРАЛЬНОЙ СЛУЖБОЙ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ ГОСУДАРСТВЕННОЙ ФУНКЦИИ ПО ОСУЩЕСТВЛЕНИЮ ГОСУДАРСТВЕННОГО КОНТРОЛЯ (НАДЗОРА) ЗА СООТВЕТСТВИЕМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ»

Зарегистрировано в Минюсте РФ 13 декабря 2011 г. N 22595

**МИНИСТЕРСТВО СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ  
  
ПРИКАЗ  
от 14 ноября 2011 г. N 312  
  
ОБ УТВЕРЖДЕНИИ АДМИНИСТРАТИВНОГО РЕГЛАМЕНТА ИСПОЛНЕНИЯ ФЕДЕРАЛЬНОЙ СЛУЖБОЙ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ ГОСУДАРСТВЕННОЙ ФУНКЦИИ ПО ОСУЩЕСТВЛЕНИЮ ГОСУДАРСТВЕННОГО КОНТРОЛЯ (НАДЗОРА) ЗА СООТВЕТСТВИЕМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

В целях реализации части 1 статьи 23 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3451; 2009, N 48, ст. 5716; N 52, ст. 6439; 2010, N 27, ст. 3407; N 31, ст. 4173, ст. 4196; N 49, ст. 6409; N 52, ст. 6974; 2011, N 23, ст. 3263; N 31, ст. 4701), в соответствии с Федеральным законом Российской Федерации от 26 декабря 2008 г. N 294-ФЗ "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля" (Собрание законодательства Российской Федерации, 2008, N 52, ст. 6249; 2009, N 18, ст. 2140; N 29, ст. 3601; N 48, ст. 5711; N 52, ст. 6441; 2010, N 17, ст. 1988; N 18, ст. 2142; N 31, ст. 4160, ст. 4193, ст. 4196; N 32, ст. 4298; 2011, N 1, ст. 20; N 7, ст. 905; N 17, ст. 2310; N 23, ст. 3263; N 27, ст. 3880; N 30, ст. 4590), Постановлением Правительства Российской Федерации от 16 марта 2009 г. N 228 "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций" (Собрание законодательства Российской Федерации, 2009, N 12, ст. 1431; 2010, N 13, ст. 1502; N 26, ст. 3350; 2011, N 3, ст. 542; N 6, ст. 888; N 14, ст. 1935; N 21, ст. 2965), Постановлением Правительства Российской Федерации от 16 мая 2011 г. N 373 "О разработке и утверждении административных регламентов исполнения государственных функций и административных регламентов предоставления государственных услуг" (Собрание законодательства Российской Федерации, 2011, N 22, ст. 3169; N 35, ст. 5092) приказываю:

1. Утвердить прилагаемый Административный регламент исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.

2. Направить настоящий Приказ на государственную регистрацию в Министерство юстиции Российской Федерации.

3. Признать утратившим силу Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 1 декабря 2009 г. N 630 "Об утверждении Административного регламента проведения проверок Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных" (зарегистрирован в Министерстве юстиции Российской Федерации 01.12.2009, регистрационный N 16095).

Министр  
И.О.ЩЕГОЛЕВ

Утвержден  
Приказом Министерства связи  
и массовых коммуникаций  
Российской Федерации  
от 14.11.2011 N 312

## АДМИНИСТРАТИВНЫЙ РЕГЛАМЕНТ ИСПОЛНЕНИЯ ФЕДЕРАЛЬНОЙ СЛУЖБОЙ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ ГОСУДАРСТВЕННОЙ ФУНКЦИИ ПО ОСУЩЕСТВЛЕНИЮ ГОСУДАРСТВЕННОГО КОНТРОЛЯ (НАДЗОРА) ЗА СООТВЕТСТВИЕМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

### I. Общие положения

**Наименование государственной функции**

1. Осуществление государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных (далее - государственная функция).

#### Наименование уполномоченного федерального органа исполнительной власти

2. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее - Служба) и ее территориальные органы, перечень которых приведен в Приложении N 1 к Административному регламенту исполнения Службой и ее территориальными органами государственной функции (далее - Регламент).

3. Настоящий Регламент определяет сроки и последовательность действий (административных процедур) Службы и ее территориальных органов, а также порядок взаимодействия с государственными органами, муниципальными органами, юридическими или физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных (далее - Оператор), в рамках проведения проверок при осуществлении государственной функции.

#### Перечень нормативных правовых актов, регулирующих исполнение государственной функции

4. Проведение проверок осуществляется в соответствии со следующими нормативными правовыми актами:

4.1. Кодекс Российской Федерации об административных правонарушениях (Собрание законодательства Российской Федерации, 2002, N 1, ст. 1; N 18, ст. 1721; N 30, ст. 3029; N 44, ст. 4295, 4298; 2003, N 1, ст. 2; N 27, ст. 2700; N 27, ст. 2708, 2717; N 46, ст. 4434, 4440; N 50, ст. 4847, 4855; N 52, ст. 5037; 2004, N 19, ст. 1838; N 30, ст. 3095; N 31, ст. 3229; N 34, ст. 3529, 3533; N 44, ст. 4266; 2005, N 1, ст. 9, 13, 37, 40, 45; N 10, ст. 762, 763; N 13, ст. 1077, 1079; N 17, ст. 1484; N 19, ст. 1752; N 25, ст. 2431; N 27, ст. 2719, 2721; N 30, ст. 3104; N 30, ст. 3124, 3131; N 40, ст. 3986; N 50, ст. 5247; N 52, ст. 5574, 5596; 2006, N 1, ст. 4, 10; N 2, ст. 172, 175; N 6, ст. 636; N 10, ст. 1067; N 12, ст. 1234; N 17, ст. 1776; N 18, ст. 1907; N 19, ст. 2066; N 23, ст. 2380, 2385; N 28, ст. 2975; N 30, ст. 3287; N 31, ст. 3420, 3432, 3433, 3438, 3452; N 43, ст. 4412; N 45, ст. 4633, 4634, 4641; N 50, ст. 5279, 5281; N 52, ст. 5498; 2007, N 1, ст. 21, ст. 25, ст. 29, ст. 33; N 7, ст. 840; N 15, ст. 1743; N 16, ст. 1824, ст. 1825; N 17, ст. 1930; N 20, ст. 2367; N 21, ст. 2456; N 26, ст. 3089; N 30, ст. 3755; N 31, ст. 4001, 4007, 4008, 4009, 4015; N 41, ст. 4845; N 43, ст. 5084; N 46, ст. 5553; N 49, ст. 6034, 6065; N 50, ст. 6246; 2008, N 10, ст. 896; N 18, ст. 1941; N 20, ст. 2251, 2259; N 29, ст. 3418; N 30, ст. 3582, 3601, 3604; N 45, ст. 5143; N 49, ст. 5738, 5745, 5748; N 52, ст. 6227, 6235, 6236, 6248; 2009, N 1, ст. 17; N 7, ст. 771, 777; N 19, ст. 2276; N 23, ст. 2759, 2767, 2776; N 26, ст. 3120, 3122, 3131, 3132; N 29, ст. 3597, 3599, 3635, 3642; N 30, ст. 3735, 3739; N 45, ст. 5265, 5267; N 48, ст. 5711, 5724, 5755; N 52, ст. 6406, 6412; 2010, N 1, ст. 1; N 11, ст. 1169, 1176; N 15, ст. 1743, 1751; N 18, ст. 2145; N 19, ст. 2291; N 21, ст. 2524, 2525, 2526, 2530; N 23, ст. 2790; N 25, ст. 3070; N 27, ст. 3416, 3429; N 28, ст. 3553; N 30, ст. 4000, 4002, 4005, 4006, 4007; N 31, ст. 4155, 4158, 4164, 4191, 4192, 4193, 4195, 4198, 4206, 4207, 4208; N 32, ст. 4298; N 41, ст. 5192, 5193; N 46, ст. 5918; N 49, ст. 6409; N 50, ст. 6605; N 52, ст. 6984, 6995, 6996; 2011, N 1, ст. 10, ст. 23, 29, 33, 47, 54; N 7, ст. 901, 905; N 15, ст. 2039, 2041; N 17, ст. 2310, 2312; N 19, ст. 2714, 2715, 2769; N 23, ст. 3260, 3267; N 27, ст. 3873; N 29, ст. 4284, ст. 4289, ст. 4290, ст. 4291; N 30, ст. 4573, ст. 4574, ст. 4584, ст. 4590, ст. 4591, ст. 4598, ст. 4601; N 31, ст. 4009).

4.2. Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3451; 2009, N 48, ст. 5716; N 52, ст. 6439; 2010, N 27, ст. 3407; N 31, ст. 4173, ст. 4196; N 49, ст. 6409; N 52, ст. 6974; 2011, N 23, ст. 3263; N 31, ст. 4701).

4.3. Федеральный закон от 26 декабря 2008 г. N 294-ФЗ "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля" (Собрание законодательства Российской Федерации, 2008, N 52, ст. 6249; 2009, N 18, ст. 2140; N 29, ст. 3601; N 48, ст. 5711; N 52, ст. 6441; 2010, N 17, ст. 1988; N 18, ст. 2142; N 31, ст. 4160, 4193, 4196; N 32, ст. 4298; 2011, N 1, ст. 20; N 7, ст. 905; N 17, ст. 2310; N 23, ст. 3263; N 27, ст. 3873, 3880; N 30, ст. 4590).

4.4. Федеральный закон от 2 мая 2006 г. N 59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации" (Собрание законодательства Российской Федерации, 2006, N 19, ст. 2060; 2010, N 27, ст. 3410; N 31, ст. 4196).

4.5. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3448; N 31, ст. 4196; 2011, N 15, ст. 2038).

4.6. Постановление Правительства Российской Федерации от 17 ноября 2007 г. N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" (Собрание законодательства Российской Федерации, 2007, N 48, ст. 6001).

4.7. Постановление Правительства Российской Федерации от 6 июля 2008 г. N 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных" (Собрание законодательства Российской Федерации, 2008, N 28, ст. 3384).

4.8. Постановление Правительства Российской Федерации от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" (Собрание законодательства Российской Федерации, 2008, N 38, ст. 4320).

4.9. Постановление Правительства Российской Федерации от 16 марта 2009 г. N 228 "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций" (Собрание законодательства Российской Федерации, 2009, N 12, ст. 1431; 2010, N 13, ст. 1502; N 26, ст. 3350; 2011, N 3, ст. 542; N 6, ст. 888; N 14, ст. 1935; N 21, ст. 2965).

4.10. Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" (зарегистрирован Министерством юстиции Российской Федерации 3 апреля 2008 г., регистрационный N 11462).

4.11. Приказ Министерства связи и массовых коммуникаций Российской Федерации от 7 апреля 2009 г. N 51 "Об утверждении Типового положения о территориальном органе Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций" (зарегистрирован Министерством юстиции Российской Федерации 13 мая 2009 г., регистрационный N 13919), с изменениями, внесенными Приказом Министерства связи и массовых коммуникаций Российской Федерации от 23 апреля 2010 г. N 61 "О внесении изменений в типовое положение о территориальном органе федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций" (зарегистрирован Министерством юстиции Российской Федерации 19 мая 2010 г., регистрационный N 17288) и Приказом Министерства связи и массовых коммуникаций Российской Федерации от 3 сентября 2010 г. N 113 "О внесении изменений в типовое положение о территориальном органе федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций" (зарегистрирован Министерством юстиции Российской Федерации 7 октября 2010 г., регистрационный N 18656).

5. Предметом государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных являются:

5.1. Документы, характер информации в которых предполагает или допускает включение в них персональных данных.

5.2. Информационные системы персональных данных.

5.3. Деятельность по обработке персональных данных.

#### Права и обязанности должностных лиц при осуществлении государственного контроля (надзора)

6. Должностные лица Службы или ее территориального органа при проведении проверок вправе в пределах своей компетенции:

6.1. Выдавать обязательные для выполнения предписания об устранении выявленных нарушений в области персональных данных.

6.2. Составлять протоколы об административном правонарушении или направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении дел об административных правонарушениях, а также о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью.

6.3. Обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных.

6.4. Использовать технику и оборудование, принадлежащие Службе или ее территориальному органу.

6.5. Запрашивать и получать необходимые документы (сведения) для достижения целей проведения проверки.

6.6. Получать доступ к информационным системам персональных данных в режиме просмотра и выборки необходимой информации.

6.7. 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 предусмотрен запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных.

6.8. Принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушениями требований законодательства Российской Федерации в области персональных данных.

6.9. Требовать от Оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных.

7. Должностные лица Службы или ее территориального органа при проведении проверки обязаны:

7.1. Своевременно и в полной мере исполнять предоставленные в соответствии с законодательством Российской Федерации полномочия по предупреждению, выявлению и пресечению нарушений требований в области персональных данных.

7.2. Соблюдать законодательство Российской Федерации, права и законные интересы Оператора, проверка которого проводится.

7.3. Проводить проверку на основании приказа руководителя Службы или ее территориального органа о ее проведении в соответствии с ее назначением.

7.4. Проводить проверку только во время исполнения служебных обязанностей, выездную проверку только при предъявлении служебных удостоверений, копии приказа руководителя Службы или ее территориального органа.

7.5. Не препятствовать руководителю или иному уполномоченному представителю Оператора присутствовать при проведении проверки и давать разъяснения по вопросам, относящимся к предмету проверки.

7.6. Предоставлять руководителю или иному уполномоченному представителю Оператора, присутствующим при проведении проверки, информацию и документы, относящиеся к предмету проверки.

7.7. Знакомить руководителя или иного уполномоченного представителя Оператора с результатами проверки.

7.8. Учитывать при определении мер, принимаемых по фактам выявленных нарушений, соответствие указанных мер тяжести нарушений, а также не допускать необоснованное ограничение прав и законных интересов Оператора.

7.9. Доказывать обоснованность своих действий при их обжаловании Оператором в порядке, установленном законодательством Российской Федерации.

7.10. Соблюдать установленные сроки проведения проверки.

7.11. Не требовать от Оператора документы и иные сведения, представление которых не предусмотрено законодательством Российской Федерации.

7.12. Перед началом проведения выездной проверки по просьбе руководителя или иного уполномоченного представителя Оператора ознакомить их с положениями Регламента, в соответствии с которым проводится проверка.

7.13. Осуществлять запись о проведенной проверке в журнале учета проверок.

#### Права и обязанности лиц, в отношении которых осуществляются мероприятия по контролю (надзору)

8. Оператор или его уполномоченный представитель при проведении проверки имеют право:

8.1. Непосредственно присутствовать при проведении проверки, давать объяснения по вопросам, относящимся к предмету проверки.

8.2. Получать от должностных лиц Службы или ее территориального органа информацию, которая относится к предмету проверки.

8.3. Знакомиться с результатами проверки и указывать в акте проверки о своем ознакомлении с результатами проверки, согласии или несогласии с ними, а также с отдельными действиями должностных лиц Службы или ее территориального органа.

8.4. Обжаловать действия (бездействие) должностных лиц Службы или ее территориального органа, повлекшие за собой нарушение прав Оператора при проведении проверки, в административном и (или) судебном порядке в соответствии с законодательством Российской Федерации.

9. Руководитель или иной уполномоченный представитель Оператора обязаны предоставить должностным лицам Службы или ее территориального органа возможность ознакомиться с документами, связанными с целями, задачами и предметом выездной проверки, в случае, если выездной проверке не предшествовало проведение документарной проверки, а также обеспечить доступ проводящих выездную проверку должностных лиц Службы или ее территориального органа на территорию, в используемые Оператором при осуществлении обработки персональных данных здания, строения, сооружения, помещения, к используемому Оператором оборудованию.

#### Описание результата исполнения государственной функции

10. Проверка Службы и ее территориального органа завершается:

10.1. Составлением и вручением Оператору акта проверки.

10.2. Выдачей Оператору предписаний об устранении выявленных нарушений требований законодательства Российской Федерации в области персональных данных.

10.3. Составлением протоколов об административных правонарушениях в отношении Оператора.

10.4. Подготовкой и направлением материалов проверки в органы прокуратуры, другие правоохранительные органы для решения вопроса о возбуждении дела об административном правонарушении, о возбуждении уголовного дела по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью.

### II. Требования к порядку исполнения государственной функции

#### Порядок информирования об исполнении государственной функции

11. Информация о порядке проведения проверок предоставляется:

11.1. Посредством размещения на официальном сайте Службы и ее территориальных органов в информационно-телекоммуникационной сети "Интернет", указанном в пункте 14 настоящего Регламента.

11.2. Непосредственно в центральном аппарате Службы и ее территориальных органах.

12. Место нахождения центрального аппарата Службы: 109074, Москва, Китайгородский проезд, д. 7, стр. 2.

13. Почтовый адрес для направления обращений: 109074, Москва, Китайгородский проезд, д. 7, стр. 2.

14. График работы Службы и ее территориальных органов: понедельник - четверг 9.00 - 18.00; пятница 9.00 - 16.45.

В предпраздничные дни продолжительность времени работы Службы и ее территориальных органов сокращается на 1 час.

Часы приема корреспонденции в экспедиции Службы: понедельник - пятница 10.00 - 13.00, 14.00 - 16.00.

Телефон Службы для получения справок по вопросам проведения проверок за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных: (495) 987-68-00, электронный адрес: rsoc\_in@rsoc.ru.

15. На официальных сайтах Службы в информационно-телекоммуникационной сети "Интернет": www.rsoc.ru, www.роскомнадзор.рф (далее - официальный сайт Службы), размещается следующая информация:

15.1. Нормативные правовые акты и методические документы, регулирующие деятельность Службы.

15.2. Текст настоящего Регламента с приложениями.

15.3. Местонахождение, график (режим) работы, номера телефонов, адрес центрального аппарата Службы, информация о ее территориальных органах и режиме их работы.

15.4. Публикации по вопросам защиты прав субъектов персональных данных.

15.5. Отчет о деятельности уполномоченного органа по защите прав субъектов персональных данных.

15.6. План проведения плановых проверок Службы.

16. Информация об основаниях и порядке проведения проверок предоставляется при личном обращении заинтересованных лиц в Службу, по письменным обращениям заявителей, размещается на официальном сайте Службы и ее территориальных органов, на Едином портале государственных и муниципальных услуг (функций) по адресу - www.gosuslugi.ru (далее - Единый портал), а также на информационных стендах Службы и ее территориальных органов.

17. При информировании об основаниях и порядке проведения проверок по письменным обращениям ответ на обращение направляется по почте в адрес заявителя в течение тридцати дней со дня регистрации письменного обращения. В случаях, предусмотренных законодательством Российской Федерации, руководитель Службы (заместитель руководителя Службы) либо уполномоченное на то лицо вправе продлить срок рассмотрения обращения не более чем на тридцать дней, уведомив о продлении срока заявителя.

При поступлении обращения в письменной форме на бумажном носителе или в электронной форме по существу рассматриваются обращения, содержащие следующую информацию:

* наименование (с указанием организационно-правовой формы), почтовый адрес - для юридического лица;
* фамилия, почтовый адрес - для физического лица.

Обращения по вопросам информирования и консультирования регистрируются в установленном порядке как обращения граждан в структурном подразделении Службы или ее территориального органа, отвечающего за вопросы делопроизводства.

18. В центральном аппарате Службы структурным подразделением, ответственным за организацию проведения проверок, является Управление по защите прав субъектов персональных данных.

19. В территориальном органе Службы структурным подразделением, ответственным за проведение проверок, является соответствующий отдел или должностное лицо (лица), назначенные руководителем территориального органа Службы.

#### Срок исполнения государственной функции

20. Срок проведения как плановой, так и внеплановой проверки не может превышать двадцать рабочих дней.

21. В случае возникновения необходимости срок проведения проверки может быть продлен, но на срок не более двадцати рабочих дней. При необходимости продления срока проверки проводящие проверку должностные лица Службы не позднее чем за два дня до даты окончания проверки готовят докладную записку с изложением причин продления срока и направляют ее руководителю Службы или руководителю территориального органа Службы, принявшему решение о проведении проверки.

22. Руководитель Службы или руководитель территориального органа Службы, принявший решение о проведении проверки, в течение одного рабочего дня назначает ответственного за подготовку приказа о продлении срока проверки.

23. Ответственный за подготовку приказа о продлении срока проверки в течение двух рабочих дней готовит проект приказа и передает его руководителю Службы или руководителю территориального органа Службы, принявшему решение о проведении проверки.

24. Руководитель Службы или руководитель территориального органа Службы, принявший решение о проведении проверки, подписывает приказ о продлении срока проверки.

25. При проведении проверок в отношении филиалов, представительств Оператора, осуществляющего деятельность на территории нескольких субъектов Российской Федерации, сроки проведения проверок устанавливаются территориальными органами Службы, участвующими в проверке, в рамках общего срока проверки, установленного ответственным территориальным органом Службы.

26. Решение о назначении одного из территориальных органов Службы ответственным за координацию проверки, взаимодействие с Оператором и оформление обобщенного акта по результатам проверок, проводимых участвовавшими в них территориальными органами Службы, принимает руководитель Службы или его заместитель, либо ответственным признается территориальный орган, на территории которого зарегистрирован Оператор.

### III. Состав, последовательность и сроки выполнения административных процедур (действий), требования к порядку их выполнения, в том числе особенности выполнения административных процедур (действий) в электронной форме

27. Регламент включает исполнение следующих административных процедур:

27.1. Принятие решения о проведении проверок.

27.2. Проведение проверки.

27.3. Оформление результатов и принятие мер по результатам проверки.

#### Принятие решения о проведении проверки

28. Служба и ее территориальные органы проводят проверки деятельности Оператора на предмет соответствия требованиям законодательства Российской Федерации в области персональных данных.

29. Службой и ее территориальными органами проводятся плановые и внеплановые проверки. Плановые и внеплановые проверки проводятся должностными лицами Службы и (или) ее территориальных органов в форме документарной или выездной проверки. Количественный состав участников проверки должен быть не менее двух должностных лиц, в том числе должностное лицо, отвечающее за вопросы правового обеспечения.

30. Плановые проверки проводятся на основании ежегодного плана проведения плановых проверок территориального органа Службы на текущий календарный год (далее - План).

31. План утверждается руководителем территориального органа Службы и размещается на официальном сайте территориального органа Службы.

32. Плановые проверки проводятся:

32.1. В отношении Операторов, включенных в Реестр операторов, осуществляющих обработку персональных данных (далее - Реестр).

32.2. В отношении Операторов, не включенных в Реестр, но осуществляющих обработку персональных данных.

33. Основанием для включения плановой проверки в План является начало осуществления Оператором деятельности по обработке персональных данных, а также истечение трех лет со дня:

33.1. Государственной регистрации Оператора в качестве юридического лица, индивидуального предпринимателя.

33.2. Окончания проведения последней плановой проверки Оператора.

34. О проведении плановой проверки Оператор уведомляется не позднее чем в течение трех рабочих дней до начала ее проведения посредством направления копии приказа руководителя, заместителя руководителя Службы или ее территориального органа почтовым отправлением с уведомлением о вручении или иным доступным способом.

35. Планирование проверок проводится в порядке и сроки, установленные приказом руководителя Службы.

36. Территориальные органы Службы в установленные приказом руководителя Службы сроки направляют на согласование в центральный аппарат свои предложения по плановым проверкам.

37. После прохождения процедуры согласования данные предложения вносятся в проект Плана территориального органа Службы на планируемый период, утверждаемый руководителем территориального органа Службы.

38. Внеплановые проверки проводятся по следующим основаниям:

38.1. Истечение срока исполнения Оператором ранее выданного предписания об устранении выявленного нарушения установленных требований законодательства Российской Федерации в области персональных данных.

38.2. Поступление в Службу или ее территориальные органы обращений и заявлений граждан, юридических лиц, индивидуальных предпринимателей, информации от органов государственной власти, органов местного самоуправления, из средств массовой информации, в том числе о следующих фактах:

38.2.1. Возникновение угрозы причинения вреда жизни, здоровью граждан.

38.2.2. Причинение вреда жизни, здоровью граждан.

38.3. Приказ руководителя Службы или руководителя территориального органа Службы, изданный в соответствии с поручениями Президента Российской Федерации, Правительства Российской Федерации.

38.4. Нарушение прав и законных интересов граждан действиями (бездействием) Операторов при обработке их персональных данных.

38.5. Нарушение Операторами требований законодательства Российской Федерации в области персональных данных, а также о несоответствии сведений, содержащихся в уведомлении об обработке персональных данных, фактической деятельности.

39. Обращения и заявления, не позволяющие установить лицо, обратившееся в Службу или ее территориальный орган, а также обращения и заявления, не содержащие сведений о фактах, указанных в пункте 30 настоящего Регламента, не могут служить основанием для проведения внеплановой проверки.

40. О проведении внеплановой выездной проверки Оператор уведомляется Службой или ее территориальным органом не менее чем за двадцать четыре часа до начала ее проведения любым доступным способом.

41. Если в результате деятельности Оператора причинен или причиняется вред жизни, здоровью граждан, предварительное уведомление Оператора о начале проведения внеплановой выездной проверки не требуется.

42. Проверки проводятся должностными лицами Службы и (или) ее территориального органа на основании приказов Службы и (или) ее территориальных органов.

Форма приказа утверждена Приказом Министерства экономического развития Российской Федерации от 30 апреля 2009 г. N 141 "О реализации положений Федерального закона "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля" (зарегистрирован Министерством юстиции Российской Федерации 13 мая 2009 г., регистрационный N 13915) (Российская газета, 2009, 14 мая; 2010, 16 июля; 2011, 18 ноября) (далее - Приказ Минэкономразвития России от 30.04.2009 N 141), с изменениями, внесенными Приказом Министерства экономического развития Российской Федерации от 24 мая 2010 г. N 199 "О внесении изменений в Приказ Минэкономразвития России от 30 апреля 2009 г. N 141 "О реализации положений Федерального закона "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля" (зарегистрирован Министерством юстиции Российской Федерации 6 июля 2010 г., регистрационный N 17702) и Приказом Министерства экономического развития Российской Федерации от 30 сентября 2011 г. N 532 "О внесении изменений в Приказ Минэкономразвития России от 30 апреля 2009 г. N 141 "О реализации положений Федерального закона "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля" (зарегистрирован Министерством юстиции Российской Федерации 10 ноября 2011 г., регистрационный N 22264).

42.1. Для оценки эффективности принимаемых Оператором технических мер по обеспечению безопасности персональных данных при их обработке в негосударственных информационных системах персональных данных Служба или ее территориальный орган в рамках проверки привлекают экспертов, экспертные организации, включенные в установленном порядке в реестр граждан и организаций, привлекаемых Службой в качестве экспертов, экспертных организаций к проведению мероприятий по контролю.

43. Решение о проведении проверки принимает руководитель Службы или руководитель территориального органа Службы.

44. В день принятия решения начальник ответственного структурного подразделения Службы или территориального органа Службы готовит проект приказа о проведении проверки и направляет его на подпись руководителю Службы или руководителю территориального органа Службы.

45. Руководитель Службы или руководитель территориального органа Службы в течение одного рабочего дня подписывает приказ о проведении проверки.

В случае отсутствия руководителя Службы или руководителя территориального органа Службы проект приказа о проведении проверки подписывается уполномоченным лицом, исполняющим его обязанности.

46. В приказе о проведении проверки указываются:

46.1. Наименование органа федерального государственного контроля (надзора).

46.2. Фамилии, имена, отчества должностных лиц, проводящих проверку.

46.3. Наименование (фамилия, имя, отчество) Оператора.

46.4. Цели, задачи, предмет проверки и срок ее проведения.

46.5. Правовые основания проведения проверки, в том числе подлежащие проверке обязательные требования законодательства Российской Федерации в области персональных данных.

46.6. Сроки проведения и перечень мероприятий по контролю, необходимых для достижения целей и задач проведения проверки.

46.7. Перечень административных регламентов проведения мероприятий по контролю.

46.8. Перечень документов, представление которых Оператором необходимо для достижения целей и задач проведения проверки.

46.9. Даты начала и окончания проведения проверки.

47. При проведении проверки в отношении Оператора, осуществляющего деятельность на территории нескольких субъектов Российской Федерации, приказ о назначении ответственного территориального органа подписывается руководителем или заместителем руководителя Службы и направляется в адрес соответствующего территориального органа Службы.

48. Приказ ответственного территориального органа Службы о проведении проверки готовится на основе изданного приказа Службы и направляется в территориальные органы Службы, участвующие в проверке.

49. Территориальными органами Службы, участвующими в проверке Оператора, но не являющихся ответственными, готовятся отдельные приказы о проведении мероприятия по контролю в отношении территориального структурного подразделения Оператора на основе приказа ответственного территориального органа Службы.

50. При проведении проверки в отношении Оператора, осуществляющего деятельность на территории нескольких субъектов Российской Федерации, в приказе ответственного территориального органа Службы дополнительно указываются:

50.1. Перечень территориальных органов Службы, участвующих в проверке.

50.2. Срок представления территориальными органами Службы актов проверок.

51. Ответственные за проведение проверки должностные лица Службы или ее территориального органа в соответствии с возложенными обязанностями уведомляют Оператора о проведении проверки в сроки, установленные пунктами 34, 40 настоящего Регламента.

52. При проведении проверки должностными лицами Службы или ее территориального органа составляется план (программа) проверки.

53. План (программа) проверки утверждается руководителем или заместителем руководителя Службы либо руководителем или заместителем руководителя территориального органа Службы не менее чем за три рабочих дня до начала проверки.

54. При необходимости и исходя из конкретных обстоятельств проведения проверки, в План (программу) проверки вносятся изменения. Внесение изменений производится на основании служебной записки руководителю Службы или руководителю территориального органа Службы. План (программа) проверки с внесенными изменениями утверждается руководителем или заместителем руководителя Службы либо руководителем или заместителем руководителя территориального органа Службы.

55. Согласование проведения внеплановых выездных проверок Службы или ее территориальных органов производится по месту осуществления деятельности Операторов, относящихся в соответствии с законодательством Российской Федерации к субъектам малого или среднего предпринимательства с прокурорами (заместителями прокуроров) субъектов Российской Федерации по основаниям, предусмотренным подпунктами 38.2.1, 38.2.2 настоящего Регламента.

56. Форма заявления о согласовании с органом прокуратуры проведения внеплановой выездной проверки Операторов, относящихся в соответствии с законодательством Российской Федерации к субъектам малого или среднего предпринимательства, утверждена Приказом Минэкономразвития России от 30.04.2009 N 141.

57. Заявление о согласовании проведения внеплановой выездной проверки Операторов, относящихся в соответствии с законодательством Российской Федерации к субъектам малого или среднего предпринимательства, и прилагаемые к нему документы направляются Службой или ее территориальным органом в органы прокуратуры заказным почтовым отправлением с уведомлением о вручении либо в форме электронного документа, подписанного электронной подписью в целях оценки законности проведения внеплановой выездной проверки.

58. Решение уполномоченных должностных лиц органов прокуратуры о согласовании проведения внеплановой выездной проверки или об отказе в согласовании ее проведения может быть обжаловано вышестоящему прокурору или в суд.

59. Блок-схема административной процедуры принятия решения о проведении проверки представлена в Приложении N 2 к Регламенту.

#### Проведение проверки

60. Копия приказа о проведении проверки, заверенная печатью Службы или ее территориального органа, предъявляется должностным лицом, проводящим проверку, руководителю или иному уполномоченному представителю Оператора одновременно со служебным удостоверением.

61. На втором экземпляре копии приказа о проведении проверки, остающейся у должностного лица Службы или территориального органа, руководитель или иной уполномоченный представитель Оператора проставляет отметку о получении копии приказа о проведении проверки с указанием должности, фамилии, имени и отчества, а также даты и времени его получения.

62. Проверка проводится должностными лицами Службы или ее территориального органа, которые указаны в приказе о ее проведении.

63. При необходимости изменения состава должностных лиц Службы или ее территориального органа, проводящих проверку, Служба или ее территориальный орган издает соответствующий приказ.

64. Служба или ее территориальный орган не вправе осуществлять плановую или внеплановую выездную проверку в случае отсутствия при ее проведении руководителя или иного уполномоченного представителя Оператора, за исключением случая проведения такой проверки по основанию, предусмотренному подпунктами 38.2.2 настоящего Регламента.

65. Руководитель, иной уполномоченный представитель Оператора должен обеспечить необходимые условия для проведения проверки и обязан по требованию должностных лиц Службы или ее территориального органа, проводящих проверку, организовать доступ к оборудованию, в помещения, где осуществляется обработка персональных данных, предоставить необходимую информацию и документацию для достижения целей проверки.

66. В случае необоснованного препятствования проведению проверки, уклонения от участия в проведении проверки руководитель или иной уполномоченный представитель Оператора несут ответственность в соответствии с законодательством Российской Федерации.

67. В ходе проведения проверки Служба или ее территориальный орган осуществляют следующие мероприятия по контролю:

67.1. Рассмотрение документов Оператора, в том числе:

67.1.1. Уведомление об обработке персональных данных.

67.1.2. Документов, необходимых для проверки фактов, содержащих признаки нарушения законодательства Российской Федерации в области персональных данных, изложенных в обращениях граждан и информации, поступившей в Службу или ее территориальный орган.

67.1.3. Документов, подтверждающих выполнение Оператором предписаний об устранении ранее выявленных нарушений законодательства Российской Федерации в области персональных данных.

67.1.4. Письменного согласия субъекта персональных данных на обработку его персональных данных.

67.1.5. Документов, подтверждающих соблюдение требований законодательства Российской Федерации при обработке специальных категорий и биометрических персональных данных.

67.1.6. Документов, подтверждающих уничтожение Оператором персональных данных субъектов персональных данных по достижении цели обработки.

67.1.7. Локальных актов Оператора, регламентирующих порядок и условия обработки персональных данных.

67.2. Исследование (обследование) информационной системы персональных данных, в части, касающейся персональных данных субъектов персональных данных, обрабатываемых в ней.

68. Плановые и внеплановые проверки проводятся в форме документарной или выездной проверки. Форма проведения проверки определяется Службой или ее территориальным органом самостоятельно, с учетом оснований, предусмотренных пунктами 33, 38 настоящего Регламента.

70. Документарная проверка проводится по месту нахождения Службы или ее территориального органа.

70.1. Предметом документарной проверки являются сведения, содержащиеся в документах Оператора, устанавливающих их организационно-правовую форму, права и обязанности, документы, используемые при осуществлении деятельности по обработке персональных данных и связанные с исполнением обязательных требований, установленных нормативными правовыми актами в области персональных данных, исполнением предписаний Службы или ее территориального органа.

70.2. В процессе проведения документарной проверки должностными лицами Службы или ее территориального органа в первую очередь рассматриваются документы Оператора, имеющиеся в распоряжении Службы или ее территориального органа, в том числе уведомление об обработке персональных данных, акты предыдущих проверок в области персональных данных, материалы рассмотрения дел об административных правонарушениях и иные документы о результатах, проведенных в отношении Оператора проверок за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.

70.3. Уведомление о проведении документарной проверки направляется в адрес Оператора не позднее чем в течение трех рабочих дней до начала ее проведения.

70.4. В случае, если достоверность сведений, содержащихся в документах, имеющихся в распоряжении Службы или ее территориального органа, вызывает обоснованные сомнения либо эти сведения не позволяют оценить исполнение Оператором требований, установленных нормативными правовыми актами, Служба или ее территориальный орган направляют в адрес Оператора мотивированный запрос с требованием представить иные необходимые для рассмотрения в ходе проведения документарной проверки документы. К запросу прилагается заверенная печатью копия приказа руководителя, заместителя руководителя Службы или ее территориального органа о проведении документарной проверки.

70.5. В течение десяти рабочих дней со дня получения мотивированного запроса Оператор обязан представить в Службу или ее территориальный орган указанные в запросе документы.

70.6. Указанные документы представляются в виде копий, заверенных печатью (при ее наличии) и подписью руководителя или иного уполномоченного представителя Оператора.

70.7. Не допускается требовать нотариального удостоверения копий документов, представляемых в Службу или ее территориальный орган, если иное не предусмотрено законодательством Российской Федерации.

70.8. В случае если в ходе документарной проверки выявлены ошибки и (или) противоречия в представленных Оператором документах либо несоответствие сведений, содержащихся в этих документах, сведениям, содержащимся в имеющихся у Службы или ее территориального органа документах и (или) полученным в ходе проведения государственного контроля (надзора), информация об этом направляется Оператору с требованием представить в течение десяти рабочих дней необходимые пояснения в письменной форме.

70.9. Оператор вправе представить дополнительно документы, подтверждающие достоверность ранее представленных документов.

70.10. Должностные лица Службы или ее территориального органа, проводящие документарную проверку, обязаны рассмотреть представленные руководителем или иным уполномоченным представителем Оператора пояснения и документы, подтверждающие достоверность ранее представленных документов. В случае если после рассмотрения представленных пояснений и документов либо при отсутствии пояснений Служба или ее территориальный орган установят признаки нарушения обязательных требований, установленных нормативными правовыми актами в области персональных данных, должностные лица Службы или ее территориального органа вправе провести выездную проверку.

71. Решение о проведении выездной проверки также может быть принято в случаях, если Оператор не представил запрашиваемые документы в установленные законодательством Российской Федерации сроки.

72. В день принятия решения о проведении выездной проверки ответственное должностное лицо Службы или территориального органа Службы готовит проект приказа о внесении изменений в приказ о проведении документарной проверки в части изменения вида проверки, продления сроков ее проведения и направляет его на подпись руководителю Службы или руководителю территориального органа Службы.

73. Выездная проверка (как плановая, так и внеплановая) проводится по месту нахождения Оператора и (или) по месту фактического осуществления его деятельности.

73.1. Предметом выездной проверки являются содержащиеся в документах Оператора сведения и принимаемые им меры по исполнению обязательных требований, установленных нормативными правовыми актами в области персональных данных.

73.2. Выездная проверка проводится в случае, если при документарной проверке не представляется возможным:

73.2.1. Удостовериться в полноте и достоверности сведений, содержащихся в уведомлении об обработке персональных данных, и иных имеющихся в распоряжении Службы или ее территориального органа документов Оператора.

73.2.2. Оценить соответствие деятельности Оператора требованиям, установленным нормативными правовыми актами в области персональных данных, без проведения соответствующей проверки.

73.2.3. Выездная проверка начинается с предъявления служебного удостоверения должностными лицами Службы или ее территориального органа, обязательного ознакомления руководителя или иного уполномоченного представителя Оператора с приказом о назначении выездной проверки и с полномочиями должностных лиц Службы или ее территориального органа, проводящих проверку, а также с целями, задачами, основаниями проведения выездной проверки, видами и объемом мероприятий по контролю, со сроками и с условиями ее проведения.

74. При проведении проверки должностные лица Службы и (или) ее территориальных органов не вправе:

74.1. Проверять выполнение обязательных требований и требований, установленных нормативными правовыми актами в области персональных данных, если такие требования не относятся к полномочиям Службы.

74.2. Осуществлять плановую или внеплановую выездную проверку в случае отсутствия при ее проведении руководителя, иного уполномоченного представителя Оператора, за исключением случая проведения такой проверки по основанию, предусмотренному подпунктами 38.2.2 настоящего Регламента.

74.3. Требовать представления документов, информации, если они не относятся к предмету проверки, а также изымать оригиналы таких документов.

74.4. Распространять информацию, полученную в результате проведения проверки и составляющую государственную, коммерческую, служебную, иную охраняемую законом тайну, за исключением случаев, предусмотренных законодательством Российской Федерации.

74.5. Превышать установленные сроки проведения проверки.

74.6. Осуществлять выдачу Операторам предписаний или предложений о проведении за их счет проверок.

75. Блок-схема административной процедуры проведения проверок представлена в Приложении N 2 к Регламенту.

#### Оформление результатов и принятие мер по результатам проверки

76. По результатам проверки должностными лицами Службы или ее территориального органа, проводившими проверку, составляется акт проверки, который оформляется непосредственно после ее завершения.

77. Форма акта утверждена Приказом Минэкономразвития России от 30.04.2009 N 141.

78. В акте проверки указываются:

78.1. Дата, время и место составления акта проверки.

78.2. Наименование Службы (ее территориального органа).

78.3. Дата и номер приказа руководителя Службы (руководителя территориального органа Службы).

78.4. Фамилии, имена, отчества должностных лиц, проводивших проверку.

78.5. Наименование (фамилия, имя, отчество) Оператора, иного уполномоченного представителя Оператора, присутствовавших при проведении проверки.

78.6. Дата, время, продолжительность и место проведения проверки.

78.7. Сведения о результатах проверки, в том числе о выявленных нарушениях обязательных требований законодательства Российской Федерации в области персональных данных, об их характере и о лицах, допустивших указанные нарушения.

78.8. Сведения об ознакомлении или отказе в ознакомлении с актом проверки руководителя, иного уполномоченного представителя Оператора, присутствовавших при проведении проверки, о наличии их подписей или об отказе от совершения подписи, а также сведения о внесении в журнал учета проверок записи о проведенной проверке либо о невозможности внесения такой записи в связи с отсутствием у Оператора указанного журнала.

78.9. Подписи должностных лиц, проводивших проверку.

79. Акт должен содержать одно из следующих заключений:

79.1. Об отсутствии в деятельности Оператора нарушений требований законодательства Российской Федерации в области персональных данных.

79.2. О выявленных в деятельности Оператора нарушениях требований законодательства Российской Федерации в области персональных данных, с указанием конкретных статей и (или) пунктов нормативных правовых актов.

80. По результатам проведения проверки Оператора, осуществляющего деятельность на территории одного субъекта Российской Федерации, должностными лицами Службы или ее территориального органа акт составляется в двух экземплярах. Один экземпляр акта с копиями приложений вручается руководителю или иному уполномоченному представителю Оператора под расписку об ознакомлении либо об отказе в ознакомлении с актом проверки или направляется заказным почтовым отправлением с уведомлением о вручении, которое приобщается к экземпляру акта, хранящемуся в деле Службы или ее территориального органа.

81. По результатам проведения проверки Оператора, осуществляющего деятельность на территории нескольких субъектов Российской Федерации, должностными лицами ответственного территориального органа Службы, проводившими проверку, составляется и подписывается обобщенный акт в двух экземплярах. Один экземпляр акта с копиями приложений вручается руководителю или иному уполномоченному представителю Оператора под расписку об ознакомлении либо об отказе в ознакомлении с актом проверки или направляется заказным почтовым отправлением с уведомлением о вручении, которое приобщается к экземпляру акта, хранящемуся в деле ответственного территориального органа Службы.

Территориальные органы Службы, проводящие проверку под руководством ответственного территориального органа Службы, составляют и подписывают заключение об итогах мероприятия по контролю в двух экземплярах. Один экземпляр заключения об итогах мероприятия по контролю с копиями приложений направляется в ответственный территориальный орган Службы для составления акта проверки с уведомлением о вручении, которое приобщается ко второму экземпляру заключения об итогах мероприятия по контролю, хранящемуся в деле территориального органа Службы, проводившего мероприятие по контролю.

82. В случае отсутствия руководителя или иного уполномоченного представителя Оператора, а также в случае отказа Оператора дать расписку об ознакомлении либо об отказе в ознакомлении с актом проверки, в акте делается соответствующая запись, подтверждаемая подписями должностных лиц Службы или ее территориального органа, проводивших проверку. Данный акт с копиями приложений направляется заказным почтовым отправлением с уведомлением о вручении, которое приобщается к экземпляру акта, хранящемуся в деле Службы или ее территориального органа.

83. При наличии разногласий по содержанию акта окончательное решение принимает должностное лицо Службы или ее территориального органа, исполняющее функции руководителя проверки. Должностные лица Службы или ее территориального органа, проводящие проверку, а также представители Оператора, не согласные с принятым решением, вправе изложить в письменной форме свое особое мнение, которое прилагается к акту.

Акт подписывают все должностные лица Службы или ее территориального органа, проводившие проверку, после чего в него запрещается вносить изменения и дополнения. К акту прилагаются протоколы, справки, объяснительные работников Оператора, на которых возложены обязанности по обработке персональных данных, и другие документы, подтверждающие выявление (устранение) нарушения.

84. После завершения внеплановой выездной проверки, согласованной ранее с органами прокуратуры, Служба или ее территориальный орган направляют в орган прокуратуры, принявший решение о согласовании проведения проверки, копию акта проверки в течение пяти рабочих дней со дня его составления.

85. В случае выявления по результатам проверки нарушения требований законодательства Российской Федерации в области персональных данных, Оператору, вместе с актом, выдается предписание об устранении выявленных нарушений.

86. В предписании об устранении выявленных нарушений указываются:

86.1. Наименование органа федерального государственного контроля (надзора).

86.2. Дата выдачи предписания об устранении выявленных нарушений.

86.3. Номер предписания об устранении выявленных нарушений.

86.4. Наименование Оператора.

86.5. Регистрационный номер Оператора в Реестре (при наличии).

86.6. Наименование вида деятельности.

86.7. Дата и номер акта проверки.

86.8. Содержание нарушения.

86.9. Основание выдачи предписания.

86.10. Срок устранения нарушения.

86.11. Срок информирования органа федерального государственного контроля (надзора) об устранении выявленного нарушения.

86.12. Подписи должностных лиц, проводивших проверку.

87. В случае выявления, по результатам проверки Оператора, осуществляющего деятельность на территории нескольких субъектов Российской Федерации, нарушений требований законодательства Российской Федерации в области персональных данных, предписания выдаются ответственным территориальным органом Службы.

88. В случае выявления в ходе или по результатам проверки административного правонарушения, предусмотренного Кодексом Российской Федерации об административных правонарушениях, в том числе невыполнения в установленный срок ранее выданного предписания об устранении выявленного нарушения обязательных требований законодательства Российской Федерации в области персональных данных, должностные лица Службы или ее территориального органа составляют такой протокол в порядке, установленном законодательством Российской Федерации, или направляют материалы в органы прокуратуры, другие правоохранительные органы для разрешения вопроса о возбуждении дела об административном правонарушении, а также о возбуждении уголовного дела, при наличии оснований для возбуждения уголовных дел по признакам преступлений, выявленных в ходе проверки и связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью.

89. По окончании проверки должностное лицо Службы или ее территориального органа в журнале Оператора по учету проверок производит запись о проведенной проверке.

Форма журнала учета проверок установлена Приказом Минэкономразвития России от 30.04.2009 N 141. Журнал учета проверок должен быть прошит, пронумерован и удостоверен печатью Оператора.

При отсутствии журнала учета проверок в акте проверки делается соответствующая запись.

90. Блок-схема административной процедуры оформления результатов и принятия мер по результатам проверок представлена в Приложении N 2 к Регламенту.

### IV. Порядок и формы контроля за исполнением государственной функции

#### Порядок осуществления текущего контроля за соблюдением и исполнением должностными лицами Службы и ее территориальных органов положений регламента и иных нормативных правовых актов, устанавливающих требования к исполнению государственной функции, а также за принятием ими решений

91. Текущий контроль за соблюдением последовательности действий, определенных административными процедурами по исполнению государственной функции, осуществляется руководителями структурных подразделений, ответственных за организацию работы по исполнению государственной функции.

92. Текущий контроль осуществляется путем проведения указанными руководителями:

92.1. Проверок соблюдения и исполнения должностными лицами положений Регламента, иных нормативных правовых актов Российской Федерации;

92.2. Визирования документов, подлежащих направлению вышестоящему должностному лицу, руководителю структурного подразделения, руководителю Службы (или руководителю территориального органа Службы).   
При осуществлении текущего контроля также используется Единая информационная система Службы (ЕИС).

93. Предметом контроля является выявление и устранение нарушений порядка рассмотрения обращений заявителей, оценка полноты рассмотрения обращений, объективность и тщательность проверки сведений, обоснованность и законность предлагаемых для принятия решений по таким обращениям.

94. При выявлении в ходе текущего контроля нарушений Регламента или требований законодательства Российской Федерации руководители структурных подразделений, ответственных за организацию работы по исполнению государственной функции, принимают меры по устранению таких нарушений и направляют уполномоченному должностному лицу Службы или территориального органа Службы предложения о применении или неприменении мер дисциплинарной ответственности лиц, допустивших соответствующие нарушения.

#### Порядок и периодичность осуществления плановых и внеплановых проверок полноты и качества исполнения государственной функции, в том числе порядок и формы контроля за полнотой и качеством исполнения государственной функции

.95. Контроль за полнотой и качеством исполнения государственной функции осуществляется в формах:

* проведения проверок соблюдения и исполнения специалистами положений Регламента;
* визирования документов руководителями структурных подразделений;
* направления запросов в уполномоченные органы с просьбой о предоставлении сведений о рассмотрении соответствующих обращений;
* рассмотрения жалоб на действия (бездействия) должностных лиц структурных подразделений, ответственных за организацию работы по исполнению государственной функции.

96. Проверки полноты и качества исполнения государственной функции могут быть плановыми и внеплановыми.

97. Плановые проверки проводятся в соответствии с установленными планами работы.

98. Внеплановые проверки организуются и проводятся в случаях:

* получения информации от граждан, юридических лиц, органов государственной власти или местного самоуправления о соответствующих нарушениях;
* обращений граждан, юридических лиц и индивидуальных предпринимателей с жалобами на нарушения их прав и законных интересов действиями (бездействием) должностными лицами Службы или ее территориального органа.

99. Проверки проводятся руководителями и должностными лицами структурных подразделений, ответственных за организацию работы по исполнению такой государственной функции, а также руководителем Службы.

100. Руководитель Службы (руководители территориальных органов Службы) организует и осуществляет общий контроль за исполнением государственной функции ответственными подразделениями.

#### Ответственность должностных лиц Службы и ее территориальных органов за решения и действия (бездействие), принимаемые (осуществляемые) ими в ходе исполнения государственной функции

101. Ответственность за исполнение государственной функции по настоящему Регламенту возлагается на руководителей структурных подразделений Службы и территориальных органов Службы и непосредственно руководителя Службы и руководителей территориальных органов Службы.

102. Персональная ответственность за выполнение государственной функции закрепляется в должностных регламентах специалистов Службы, ответственных за осуществление государственной функции.

#### Положения, характеризующие требования к порядку и формам контроля за исполнением государственной функции, в том числе со стороны граждан, их объединений и организаций

103. Контроль за предоставлением государственной услуги со стороны граждан, их объединений и организаций осуществляется в форме направления обращений в федеральные органы исполнительной власти в установленном порядке.

### V. Досудебный (внесудебный) порядок обжалования решений и действий (бездействия) Службы или ее территориального органа, а также ее должностных лиц

104. Заявитель вправе обратиться в Службу или ее территориальный орган устно в ходе личного приема или письменно с обращением (жалобой, заявлением) на решения, действия (бездействие) должностных лиц Службы или ее территориальных органов в ходе проведения проверок на основании настоящего Регламента в соответствии с действующим законодательством Российской Федерации.

105. Заявитель вправе обжаловать действия (бездействие) должностных лиц:

105.1. Территориального органа Службы - руководителю территориального органа Службы.

105.2. Службы или руководителя территориального органа Службы - руководителю Службы.

105.3. Руководителя Службы - Министру связи и массовых коммуникаций Российской Федерации.

106. Личный прием должностными лицами Службы проводится в установленные для приема дни и время.

107. В ходе личного приема заявителю может быть отказано в дальнейшем рассмотрении обращения, если ему ранее неоднократно давались ответы по существу поставленных в обращении вопросов.

108. Письменное обращение (жалоба, заявление) рассматривается Службой или ее территориальным органом в течение 30 дней с момента его регистрации. В случаях, предусмотренных законодательством Российской Федерации, руководитель Службы или ее территориального органа либо иное уполномоченное лицо вправе продлить срок рассмотрения обращения не более чем на 30 дней, уведомив заявителя о продлении срока.

109. Служба и ее территориальные органы:

109.1. Обеспечивают объективное, всестороннее и своевременное рассмотрение обращения.

109.2. Запрашивают необходимые для рассмотрения обращения документы и материалы в других государственных органах, органах местного самоуправления и у иных должностных лиц, за исключением судов, органов дознания и органов предварительного следствия.

109.3. Принимают меры, направленные на восстановление или защиту нарушенных прав, свобод и законных интересов заявителя.

109.4. Дают письменный ответ по существу поставленных в обращении вопросов, за исключением случаев, установленных законодательством Российской Федерации.

109.5. Уведомляют заявителя о направлении его обращения на рассмотрение в другой государственный орган, орган местного самоуправления или иному должностному лицу в соответствии с их компетенцией.

110. Рассмотрение обращения и подготовка ответа осуществляется в порядке, установленном Федеральным законом от 2 мая 2006 г. N 59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации" (Собрание законодательства Российской Федерации, 2006, N 19, ст. 2060; 2010, N 27, ст. 3410; N 31, ст. 4196).

В исключительных случаях, при наличии оснований, руководитель Службы или ее территориального органа, заместитель руководителя Службы или ее территориального органа продлевает срок рассмотрения обращения не более чем на 30 дней, уведомив о продлении срока заявителя, направившего жалобу.

В случае если в письменной жалобе не указаны фамилия заявителя, направившего жалобу, и почтовый адрес, по которому должен быть направлен ответ, ответ на жалобу не дается.

Служба или ее территориальный орган при получении письменной жалобы, в которой содержатся нецензурные либо оскорбительные выражения, угрозы имуществу государственного органа, угрозы имуществу, жизни, здоровью должностного лица, а также членов его семьи, вправе оставить жалобу без ответа по существу поставленных в ней вопросов и сообщить заявителю, направившему жалобу, о недопустимости злоупотребления правом.

В случае если текст жалобы не поддается прочтению, она не рассматривается, о чем сообщается заявителю, направившему жалобу, если его фамилия и почтовый адрес поддаются прочтению.

В случае если в жалобе содержится вопрос, на который многократно давались письменные ответы по существу в связи с ранее направляемыми жалобами, и при этом в жалобе не приводятся новые доводы или обстоятельства, руководитель Службы или ее территориального органа, заместитель руководителя Службы или ее территориального органа вправе принять решение о безосновательности очередной жалобы и прекращении переписки с заявителем по данному вопросу при условии, что указанная жалоба и ранее направляемые жалобы направлялись в один и тот же государственный орган. О данном решении уведомляется заявитель, направивший жалобу.

111. По результатам рассмотрения обращения принимается одно из следующих решений:

* об отказе в удовлетворении жалобы;
* о частичном удовлетворении жалобы;
* об удовлетворении жалобы, отмене принятого решения должностных лиц, государственных служащих (в том числе результатов проверки) либо о возложении на должных лиц обязанностей по восстановлению прав и (или) интересов лица, направившего жалобу.

Ответ на жалобу подписывается руководителем Службы (руководителем территориального органа Службы) либо иным уполномоченным должностным лицом.  
Ответ на жалобу, поступившую в Службу (территориальный орган Службы), направляется по почтовому адресу или адресу электронной почты, указанным в обращении.

112. Заявители могут сообщить о нарушении своих прав и законных интересов, противоправных решениях, действиях (бездействии) должностных лиц Службы или ее территориального органа, нарушении положений настоящего Регламента, некорректном поведении или нарушении служебной этики:

* по номеру телефона, указанному на официальном сайте Службы или ее территориального органа./li>

В таких сообщениях должна содержаться следующая информация:

* фамилия, имя, отчество (последнее - при наличии) гражданина (представителя юридического лица), которым подается сообщение, его место жительства или пребывания (место нахождения юридического лица);
* фамилия, имя, отчество должностного лица Службы или ее территориального органа, решение, действия (бездействие) которого нарушает права и законные интересы гражданина (юридического лица);
* суть нарушенных прав и законных интересов, противоправного решения, действия (бездействия).

Приложение N 1  
к Административному регламенту  
исполнения Федеральной службой  
по надзору в сфере связи, информационных  
технологий и массовых коммуникаций  
государственной функции по осуществлению  
государственного контроля (надзора)  
за соответствием обработки персональных  
данных требованиям законодательства  
Российской Федерации в области  
персональных данных

**Реквизиты Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций**

|  |  |  |  |
| --- | --- | --- | --- |
| **Местонахождение:** | Китайгородский проезд, д.7, стр.2, г. Москва, 109074 | | |
| **Официальный сайт Роскомнадзора в сети Интернет:** | | www.rsoc.ru | |
| **График работы отдела документооборота, архива, контроля и работы с обращениями граждан (приём документов):** | | понедельник – пятница | с 10.00 до 12.00 с 14.00 до 16.00 |
| суббота, воскресенье | выходной |

### Территориальные органы Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№№** | **Наименование** | **Почтовый адрес и** **телефон** | **Официальный сайт (http://)** | **Электронный адрес** **(http://)** |
| 1. | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Алтайскому краю | ул. Интернациональная, д. 72, г. Барнаул, 656049  (3852) 63-04-10  (3852) 35-46-84 | [22.rsoc.ru](http://22.rsoc.ru/) | [rsockanc22@rsoc.ru](mailto:rsockanc22@rsoc.ru) |
| 2 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Амурской области | ул. Ленина, д. 113,  г. Благовещенск, Амурской области, 675000 (616-2) 33-73-63  (616-2) 37-16-98 | [28.rsoc.ru](http://28.rsoc.ru/) | [rsockanc28@rsoc.ru](mailto:rsockanc28@rsoc.ru) |
| 3. | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Архангельской области и Ненецкому автономному округу | Троицкий пр., д. 45, г. Архангельск, 163000 (8182) 28-62-31  (8182) 20-18-43 | [29.rsoc.ru](http://29.rsoc.ru/) | [rsockanc29@rsoc.ru](mailto:rsockanc29@rsoc.ru) |
| 4 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Астраханской области | ул. Студенческая, д. 3, г. Астрахань, 414004 (8512) 49-67-82 | [30.rsoc.ru](http://30.rsoc.ru/) | [rsockanc30@rsoc.ru](mailto:rsockanc30@rsoc.ru) |
| 5 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Белгородской области | ул. Гагарина, д. 6 «А»,  г. Белгород, 308007 (4722) 31-53-77 | [31.rsoc.ru](http://31.rsoc.ru/) | [rsockanc31@rsoc.ru](mailto:rsockanc31@rsoc.ru) |
| 6 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Брянской области | ул. К. Маркса, д. 9, г. Брянск, 241050 (4832) 74-10-85 | [32.rsoc.ru](http://32.rsoc.ru/) | [rsockanc32@rsoc.ru](mailto:rsockanc32@rsoc.ru) |
| 7 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Владимирской области | ул. 1-я Пионерская, д. 92, г. Владимир, 600017 (4922) 23-03-53 (4922) 43-17-17 | [33.rsoc.ru](http://33.rsoc.ru/) | [rsockanc33@rsoc.ru](mailto:rsockanc33@rsoc.ru) |
| 8 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Волгоградской области | ул. Мира, д. 9,  г. Волгоград, 400131; почтовый 400066,  а/я 60 (8442) 33-43-34  (8442) 33-36-55 | [34.rsoc.ru](http://34.rsoc.ru/) | [rsockanc34@rsoc.ru](mailto:rsockanc34@rsoc.ru) |
| 9 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Вологодской области | ул. Некрасова, д. 34 А, г. Вологда, 160019 (8172) 54-89-20  (8172) 54-84-94 | [35.rsoc.ru](http://35.rsoc.ru/) | [rsockanc35@rsoc.ru](mailto:rsockanc35@rsoc.ru) |
| 10 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Воронежской области | ул. Куцыгина, д. 29 А,  г. Воронеж, 394006 а/я 274  (4732) 36-43-43 | [36.rsoc.ru](http://36.rsoc.ru/) | [rsockanc36@rsoc.ru](mailto:rsockanc36@rsoc.ru) |
| 11 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Забайкальскому краю | ул. Подгорбунского, д. 9, г. Чита, 672027  (3022) 32-30-47  (3022) 26-55-10  (3022) 26-19-83 | [75.rsoc.ru](http://75.rsoc.ru/) | [rsockanc75@rsoc.ru](mailto:rsockanc75@rsoc.ru) |
| 12 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Ивановской области | пр-т Ленина, д. 17 оф. 335, г. Иваново, 153000 (4932) 41-00-55  (4932) 41-00-49 | [37.rsoc.ru](http://37.rsoc.ru/) | [rsockanc37@rsoc.ru](mailto:rsockanc37@rsoc.ru) |
| 13 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Иркутской области | ул. Халтурина, д. 7,  г. Иркутск, 664011 (3952) 25-50-93  (3952) 34-19-91 | [38.rsoc.ru](http://38.rsoc.ru/) | [rsockanc38@rsoc.ru](mailto:rsockanc38@rsoc.ru) |
| 14 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Кабардино-Балкарской Республике | пр. Шогенцукова, д. 14, г. Нальчик, КБР, 360000 (8662) 42-22-21  (8662) 42-40-80 | [07.rsoc.ru](http://07.rsoc.ru/) | [rsockanc07@rsoc.ru](mailto:rsockanc07@rsoc.ru) |
| 15 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Калининградской области | ул. Коммунальная, д. 4  г. Калининград, 236000  (4012) 45-15-50  (4012) 93-00-82 | [39.rsoc.ru](http://39.rsoc.ru/) | [rsockanc39@rsoc.ru](mailto:rsockanc39@rsoc.ru) |
| 16 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Калужской области | ул. Дзержинского, д. 1/46, г. Калуга, 248600 (4842) 59-00-59 | [40.rsoc.ru](http://40.rsoc.ru/) | [rsockanc40@rsoc.ru](mailto:rsockanc40@rsoc.ru) |
| 17 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Камчатскому краю | пр-кт. Победы д. 47, г. Петропавловск - Камчатский, 683023 (4152) 49-00-37 (4152) 49-01-20 | [41.rsoc.ru](http://41.rsoc.ru/) | [rsockanc41@rsoc.ru](mailto:rsockanc41@rsoc.ru) |
| 18 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Карачаево-Черкесской Республике | ул. Кавказская,  д. 19, г. Черкесск, Карачаево-Черкесская республика, 369000 (7822) 26-42-92 | [09.rsoc.ru](http://09.rsoc.ru/) | [rsockanc09@rsoc.ru](mailto:rsockanc09@rsoc.ru) |
| 19 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Кемеровской области | ул. Сарыгина, д. 7,  г. Кемерово, 650025 (3842) 36-90-03  (3842) 36-49-24 | [42.rsoc.ru](http://42.rsoc.ru/) | [rsockanc42@rsoc.ru](mailto:rsockanc42@rsoc.ru) |
| 20 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Кировской области | ул. Комсомольская,  д. 43, г. Киров, 610001 (8332) 63-39-00  (8332) 54-37-28 | [43.rsoc.ru](http://43.rsoc.ru/) | [rsockanc43@rsoc.ru](mailto:rsockanc43@rsoc.ru) |
| 21 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Костромской области | мкр. Паново, д. 36,  г. Кострома, 156010 (4942) 43-33-23  (4942) 33-65-61 | [44.rsoc.ru](http://44.rsoc.ru/) | [rsockanc44@rsoc.ru](mailto:rsockanc44@rsoc.ru) |
| 22 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Краснодарскому краю и Республике Адыгея (Адыгея) | ул. Маяковского, д. 158,  г. Краснодар, 350001 (861) 233-37-14  (861) 239-31-36 | [23.rsoc.ru](http://23.rsoc.ru/) | [rsockanc23@rsoc.ru](mailto:rsockanc23@rsoc.ru) |
| 23 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Красноярскому краю | ул. Новосибирская, д. 64-А, г. Красноярск, 660028 (3912) 44-19-09  (3912) 65-39-84 | [24.rsoc.ru](http://24.rsoc.ru/) | [rsockanc24@rsoc.ru](mailto:rsockanc24@rsoc.ru) |
| 24 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Курганской области | ул. Климова, д. 60, г. Курган, 640000 (3522) 41-76-26  (3522) 41-77-37 | [45.rsoc.ru](http://45.rsoc.ru/) | [rsockanc45@rsoc.ru](mailto:rsockanc45@rsoc.ru) |
| 25 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Курской области | Красная площадь, д. 8, г. Курск, 305000 (4712) 56-26-33  (4712) 56-12-03 | [46.rsoc.ru](http://46.rsoc.ru/) | [rsockanc46@rsoc.ru](mailto:rsockanc46@rsoc.ru) |
| 26 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Липецкой области | пер. Попова, д. 5,  г. Липецк, 398016 (4742) 35-66-00  (4742) 34-14-58 | [48.rsoc.ru](http://48.rsoc.ru/) | [rsockanc48@rsoc.ru](mailto:rsockanc48@rsoc.ru) |
| 27 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Магаданской области и Чукотскому автономному округу | ул. Пролетарская, д. 68, г. Магадан, 685030 (413-2) 62-27-18  (413-2) 62-54-36 | [49.rsoc.ru](http://49.rsoc.ru/) | [rsockanc49@rsoc.ru](mailto:rsockanc49@rsoc.ru) |
| 28 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Москве и Московской области | Старокаширское шоссе, д. 2, корп. 10, ГСП-7, Москва, 115998 (495) 957-08-20 (495) 957-08-48 | [77.rsoc.ru](http://77.rsoc.ru/) | [rsockanc77@rsoc.ru](mailto:rsockanc77@rsoc.ru) |
| 29 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Мурманской области | пер. Русанова, д. 10,  г. Мурманск, 183038 (8152) 45-54-30  (8152) 55-01-00 | [51.rsoc.ru](http://51.rsoc.ru/) | [rsockanc51@rsoc.ru](mailto:rsockanc51@rsoc.ru) |
| 30 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Нижегородской области | Зеленский съезд, д. 4, ГСП-5, г. Нижний Новгород, 603001 (831) 430-33-17 (831) 430-83-39 | [52.rsoc.ru](http://52.rsoc.ru/) | [rsockanc52@rsoc.ru](mailto:rsockanc52@rsoc.ru) |
| 31 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Новгородской области | ул. Славная, д. 48 А, г. Великий Новгород, 173000 (8162) 67-16-74  (8162) 66-32-01 (8162) 67-16-70 | [53.rsoc.ru](http://53.rsoc.ru/) | [rsockanc53@rsoc.ru](mailto:rsockanc53@rsoc.ru) |
| 32 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Новосибирской области | ул. Советская, д. 33, г. Новосибирск, 630099 (383) 227-14-41 (383) 219-11-76 | [54.rsoc.ru](http://54.rsoc.ru/) | [rsockanc54@rsoc.ru](mailto:rsockanc54@rsoc.ru) |
| 33 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Омской области | ул. Куйбышева,  д. 79, г. Омск, 644001 (3812) 37-12-08 | [55.rsoc.ru](http://55.rsoc.ru/) | [rsockanc55@rsoc.ru](mailto:rsockanc55@rsoc.ru) |
| 34 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Оренбургской области | Телевизионный пер., д. 3/1, г. Оренбург, 460024 (3532) 56-00-72 (3532) 56-00-94 | [56.rsoc.ru](http://56.rsoc.ru/) | [rsockanc56@rsoc.ru](mailto:rsockanc56@rsoc.ru) |
| 35 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Орловской области | ул. Красина, д. 7,  г. Орел, 302001 (486 2) 43-04-24 | [57.rsoc.ru](http://57.rsoc.ru/) | [rsockanc57@rsoc.ru](mailto:rsockanc57@rsoc.ru) |
| 36 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Пензенской области | ул. Карпинского, д. 12, г. Пенза, 440011 (841-2) 48-79-79 | [58.rsoc.ru](http://58.rsoc.ru/) | [rsockanc58@rsoc.ru](mailto:rsockanc58@rsoc.ru) |
| 37 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Пермскому краю | ул. Ленина, д. 68, г. Пермь, 614096 (342) 236-16-33 (342) 236-26-49 | [59.rsoc.ru](http://59.rsoc.ru/) | [rsockanc59@rsoc.ru](mailto:rsockanc59@rsoc.ru) |
| 38 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Приморскому краю | ул. Беломорская, д. 18,  г. Владивосток, 690022  (4232) 37-43-53 (4232) 37-50-46 | [25.rsoc.ru](http://25.rsoc.ru/) | [rsockanc25@rsoc.ru](mailto:rsockanc25@rsoc.ru) |
| 39 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Псковской области | ул. Советская, д. 49, г. Псков, 180004 (811-2) 66-84-93 (811-2) 66-01-19 | [60.rsoc.ru](http://60.rsoc.ru/) | [rsockanc60@rsoc.ru](mailto:rsockanc60@rsoc.ru) |
| 40 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Республике Алтай | Коммунистический пр., д. 61, г. Горно -Алтайск, Республика Алтай, 649006  (388 22) 230-80 (388 22) 231-81 | [04.rsoc.ru](http://04.rsoc.ru/) | [rsockanc04@rsoc.ru](mailto:rsockanc04@rsoc.ru) |
| 41 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Республике Башкортостан | ул. 50 лет Октября, д. 20, корп. 1, г. Уфа, 450005 (347) 251-50-51 (347) 251-50-40 | [02.rsoc.ru](http://02.rsoc.ru/) | [rsockanc02@rsoc.ru](mailto:rsockanc02@rsoc.ru) |
| 42 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Республике Бурятия | ул. Красноармейская, д. 20, г. Улан-Удэ, 670034 (301-2) 44-88-22 (301-2) 44-25-16 (301-2) 44-69-99 | [03.rsoc.ru](http://03.rsoc.ru/) | [rsockanc03@rsoc.ru](mailto:rsockanc03@rsoc.ru) |
| 43 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Республике Дагестан | ул. С. Стальского, д. 2, г. Махачкала, Республика Дагестан, 367000 (8722) 68-26-00 (8722) 67-91-90 | [05.rsoc.ru](http://05.rsoc.ru/) | [rsockanc05@rsoc.ru](mailto:rsockanc05@rsoc.ru) |
| 44 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Республике Ингушетия | ул. Московская, д. 20, г. Назрань, Республика Ингушетия, 386102 (87322) 22-26-50 (87322) 22-25-56 | [06.rsoc.ru](http://06.rsoc.ru/) | [rsockanc06@rsoc.ru](mailto:rsockanc06@rsoc.ru) |
| 45 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Республике Калмыкия | ул. Ленина, д. 329,  г. Элиста, Республика Калмыкия, 358000  (847) 244-03-68 | [08.rsoc.ru](http://08.rsoc.ru/) | [rsockanc08@rsoc.ru](mailto:rsockanc08@rsoc.ru) |
| 46 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Республике Карелия | Первомайский пр., д. 30-А, г. Петрозаводск, Республика Карелия, 185910 (8142) 71-70-70 (8142) 71-70-89 | [10.rsoc.ru](http://10.rsoc.ru/) | [rsockanc10@rsoc.ru](mailto:rsockanc10@rsoc.ru) |
| 47 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Республике Коми | ул. Коммунистическая, д. 17, г. Сыктывкар, Республика Коми, 167981 (8212) 21-68-00 | [11.rsoc.ru](http://11.rsoc.ru/) | [rsockanc11@rsoc.ru](mailto:rsockanc11@rsoc.ru) |
| 48 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Республике Марий Эл | пр. Гагарина, д. 8,  г. Йошкар-Ола, Республика Марий Эл, 424006 (8362) 63-04-23 (8362) 45-10-39 | [12.rsoc.ru](http://12.rsoc.ru/) | [rsockanc12@rsoc.ru](mailto:rsockanc12@rsoc.ru) |
| 49 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Республике Мордовия | ул. Коммунистическая, д. 89, ком. 607, г. Саранск, 430000 (834) 247-55-48 (834) 232-75-21 | [13.rsoc.ru](http://13.rsoc.ru/) | [Rsockanc13@rsoc.ru](mailto:Rsockanc13@rsoc.ru) |
| 50 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Республике Саха (Якутия) | ул. Курашова, д. 22, г. Якутск, 677000 (4112) 42-43-84 (4112) 34-14-28 | [14.rsoc.ru](http://14.rsoc.ru/) | [rsockanc14@rsoc.ru](mailto:rsockanc14@rsoc.ru) |
| 51 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Республике Северная Осетия – Алания | ул. Маркуса, д. 22,  г. Владикавказ, Республика Северная Осетия-Алания, 362027 (8672) 54-32-32 (8672) 54-54-54 | [15.rsoc.ru](http://15.rsoc.ru/) | [rsockanc15@rsoc.ru](mailto:rsockanc15@rsoc.ru) |
| 52 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Республике Татарстан (Татарстан) | ул. Гарифьянова, 28 А, г. Казань, 420138, а/я 25 (843) 224-21-21 (843) 228-59-05 | [16.rsoc.ru](http://16.rsoc.ru/) | [rsockanc16@rsoc.ru](mailto:rsockanc16@rsoc.ru) |
| 53 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Республике Тыва | ул. Дружба, д. 156,  г. Кызыл, 667000, а/я 53 (39422) 2-09-90 (39422) 2-09-91 | [17.rsoc.ru](http://17.rsoc.ru/) | [rsockanc17@rsoc.ru](mailto:rsockanc17@rsoc.ru) |
| 54 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Республике Хакасия | ул. Щетинкина, д. 20,  г. Абакан, Республика Хакасия, 655017 (3902) 23-98-18 | [19.rsoc.ru](http://19.rsoc.ru/) | [rsockanc19@rsoc.ru](mailto:rsockanc19@rsoc.ru) |
| 55 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Ростовской области | ул. Металлургическая, д. 113/46, г. Ростов-на -Дону, 344029 (863) 218-65-73 (863) 211-12-12 | [61.rsoc.ru](http://61.rsoc.ru/) | [rsockanc61@rsoc.ru](mailto:rsockanc61@rsoc.ru) |
| 56 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Рязанской области | ул. Ленинского Комсомола, д. 15,  г. Рязань, 390005 (4912) 76-35-30 (4912) 21-52-03 | [62.rsoc.ru](http://62.rsoc.ru/) | [rsockanc62@rsoc.ru](mailto:rsockanc62@rsoc.ru) |
| 57 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Самарской области | ул. Аэродромная, д. 45 г. Самара, 443070 (846) 332-53-26 (846) 270-44-00 | [63.rsoc.ru](http://63.rsoc.ru/) | [rsockanc63@rsoc.ru](mailto:rsockanc63@rsoc.ru) |
| 58 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Санкт-Петербургу и Ленинградской области | ул. Галерная, д. 27, Санкт-Петербург, BOX 1048, 190000 (812) 571-72-17 (812) 571-27-31 | [78.rsoc.ru](http://78.rsoc.ru/) | [rsockanc78@rsoc.ru](mailto:rsockanc78@rsoc.ru) |
| 59 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Саратовской области | ул. Жуковского, д. 19, г. Саратов, 410010 (845-2) 64-91-57 (845-2) 64-93-38 | [64.rsoc.ru](http://64.rsoc.ru/) | [rsockanc64@rsoc.ru](mailto:rsockanc64@rsoc.ru) |
| 60 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Сахалинской области | ул. Дзержинского, д. 38, г. Южно – Сахалинск, 693020,  а/я 43 (4242) 74-46-44 (4242) 77-19-15 | [65.rsoc.ru](http://65.rsoc.ru/) | [rsockanc65@rsoc.ru](mailto:rsockanc65@rsoc.ru) |
| 61 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Свердловской области | пр. Ленина, д. 39,  г. Екатеринбург, 620000, а/я 337 (343) 359-01-00 (343) 359-01-59 | [66.rsoc.ru](http://66.rsoc.ru/) | [rsockanc66@rsoc.ru](mailto:rsockanc66@rsoc.ru) |
| 62 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Смоленской области | ул. Нахимова, д. 21,  г. Смоленск, 214025 (4812) 35-39-53 (4812) 35-50-20 | [67.rsoc.ru](http://67.rsoc.ru/) | [rsockanc67@rsoc.ru](mailto:rsockanc67@rsoc.ru) |
| 63 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Ставропольскому краю | ул. Тухачевского, д. 8, г. Ставрополь, 355040 (8652) 72-35-36 (8652) 73-15-35 | [26.rsoc.ru](http://26.rsoc.ru/) | [rsockanc26@rsoc.ru](mailto:rsockanc26@rsoc.ru) |
| 64 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Тамбовской области | ул. Советская, д. 182,  г. Тамбов, 392000 (4752) 56-06-57 (4752) 56-16-55 | [68.rsoc.ru](http://68.rsoc.ru/) | [rsockanc68@rsoc.ru](mailto:rsockanc68@rsoc.ru) |
| 65 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Тверской области | ул. Трехсвятская, д. 6, г. Тверь, 170000 (4822) 35-81-31 (4822) 35-81-90 | [69.rsoc.ru](http://69.rsoc.ru/) | [rsockanc69@rsoc.ru](mailto:rsockanc69@rsoc.ru) |
| 66 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Томской области | ул. Енисейская, д. 23/1,  г. Томск, 634041 (3822) 31-01-11 | [70.rsoc.ru](http://70.rsoc.ru/) | [rsockanc70@rsoc.ru](mailto:rsockanc70@rsoc.ru) |
| 67 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Тульской области | ул. Смидович, д. 1-А,  г. Тула, 300600 (4872) 33-13-85 (4872) 33-26-26 | [71.rsoc.ru](http://71.rsoc.ru/) | [rsockanc71@rsoc.ru](mailto:rsockanc71@rsoc.ru) |
| 68 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Тюменской области, Ханты-Мансийскому автономному округу – Югре и  и Ямало-Ненецкому автономному округу | ул. Республики, д. 12,  г. Тюмень, 625003 (3452) 46-86-39 (3452) 24-12-36 | [72.rsoc.ru](http://72.rsoc.ru/) | [rsockanc72@rsoc.ru](mailto:rsockanc72@rsoc.ru) |
| 69 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Удмуртской Республике | ул. 5-я Подлесная, д. 12 А, г. Ижевск, 426069  (3412) 58-66-44 (3412) 51-19-87 | [18.rsoc.ru](http://18.rsoc.ru/) | [rsockanc18@rsoc.ru](mailto:rsockanc18@rsoc.ru) |
| 70 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Ульяновской области | ул. К. Маркса, д. 33/2,  г. Ульяновск, 432071  (8422) 44-65-55 (8422) 41-17-79 | [73.rsoc.ru](http://73.rsoc.ru/) | [rsockanc73@rsoc.ru](mailto:rsockanc73@rsoc.ru) |
| 71 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Хабаровскому краю и Еврейской автономной области | ул. Ленина, д. 4,  г. Хабаровск, 680000 (4212) 41-72-70 (4212) 41-72-88 | [27.rsoc.ru](http://27.rsoc.ru/) | [rsockanc27@rsoc.ru](mailto:rsockanc27@rsoc.ru) |
| 72 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Челябинской области | ул. Цвиллинга, д. 22,  г. Челябинск, 454000 (351) 263-91-09 | [74.rsoc.ru](http://74.rsoc.ru/) | [rsockanc74@rsoc.ru](mailto:rsockanc74@rsoc.ru) |
| 73 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Чеченской Республике | пр. Исаева, д. 36,  г. Грозный, 364024 (8712) 22-31-24 | [20.rsoc.ru](http://20.rsoc.ru/) | [rsockanc20@rsoc.ru](mailto:rsockanc20@rsoc.ru) |
| 74 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Чувашской Республике – Чувашии | ул. Гладкова, д. 7 Б,  г. Чебоксары, 428020  (8352) 66-73-25 | [21.rsoc.ru](http://21.rsoc.ru/) | [rsockanc21@rsoc.ru](mailto:rsockanc21@rsoc.ru) |
| 75 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Ярославской области | ул. Кирова, д. 7,  г. Ярославль, 150000 (4852) 30-49-20 (4852) 30-54-08 | [76.rsoc.ru](http://76.rsoc.ru/) | [rsockanc76@rsoc.ru](mailto:rsockanc76@rsoc.ru) |

Приложение N 2  
к Административному регламенту  
исполнения Федеральной службой  
по надзору в сфере связи, информационных  
технологий и массовых коммуникаций  
государственной функции по осуществлению  
государственного контроля (надзора)  
за соответствием обработки персональных  
данных требованиям законодательства  
Российской Федерации в области  
персональных данных

**Блок-схема административной процедуры принятия решенияо проведении проверок**

**Блок-схема административной процедуры проведения проверок**

**Блок-схема административной процедуры оформления результатов и принятия мер по результатам проверок**

# ПРИКАЗ МИНИСТЕРСТВА СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РФ ОТ 21 ДЕКАБРЯ 2011 Г. N 346 «ОБ УТВЕРЖДЕНИИ АДМИНИСТРАТИВНОГО РЕГЛАМЕНТА ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ ПО ПРЕДОСТАВЛЕНИЮ ГОСУДАРСТВЕННОЙ УСЛУГИ «ВВЕДЕНИЕ РЕЕСТРА ОПЕРАТОРОВ, ОСУЩЕСТВЛЯЮЩИХ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ»

Зарегистрировано в Минюсте РФ 29 марта 2012 г. N 23650

**МИНИСТЕРСТВО СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ  
  
ПРИКАЗ  
от 21 декабря 2011 г. N 346  
  
ОБ УТВЕРЖДЕНИИ АДМИНИСТРАТИВНОГО РЕГЛАМЕНТА ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ ПО ПРЕДОСТАВЛЕНИЮ ГОСУДАРСТВЕННОЙ УСЛУГИ «ВЕДЕНИЕ РЕЕСТРА ОПЕРАТОРОВ, ОСУЩЕСТВЛЯЮЩИХ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ»**

В целях реализации пункта 3 части 5 статьи 23 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2009, № 48, ст. 5716; № 52, ст. 6439; 2010, № 27, ст. 3407; № 31, ст. 4173, ст. 4196; № 49, ст. 6409; № 52, ст. 6974; 2011, № 23, ст. 3263; № 31, ст. 4701), Федерального закона от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (Собрание законодательства Российской Федерации, 2010, № 31, ст. 4179; 2011, № 15, ст. 2038; № 27, ст. 3880; № 29, ст. 4291; № 30, ст. 4587), в соответствии с пунктом 5.2.4 Положения о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, утвержденного постановлением Правительства Российской Федерации от 16 марта 2009 г. № 228 (Собрание законодательства Российской Федерации, 2009, № 12, ст. 1431 ; 2010, № 13, ст. 1502; № 26, ст. 3350; 2011, № 3, ст. 542; № 6, ст. 888; № 14, ст. 1935; № 21, ст. 2965; № 40, ст. 548; № 44, ст. 6272), постановлением Правительства Российской Федерации от 16 мая 2011 г. № 373 «О разработке и утверждении административных регламентов исполнения государственных функций и административных регламентов предоставления государственных услуг» (Собрание законодательства Российской Федерации, 2011, № 22, ст. 3169; № 35, ст. 5092)

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемый Административный регламент Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги «Ведение реестра операторов, осуществляющих обработку персональных данных».

2. Направить настоящий приказ на государственную регистрацию в Министерство юстиции Российской Федерации.

3. Признать утратившим силу приказ Министерства связи и массовых коммуникаций Российской Федерации от 30 января 2010 г. № 18 «Об утверждении Административного регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по исполнению государственной функции «Ведение реестра операторов, осуществляющих обработку персональных данных»» (зарегистрирован в Министерстве юстиции Российской Федерации 24.03.2010, регистрационный № 16717).

Министр И.О. Щёголев

УТВЕРЖДЕН  
приказом Министерства связи   
и массовых коммуникаций   
Российской Федерации  
от 21.12.2011 № 346

## АДМИНИСТРАТИВНЫЙ РЕГЛАМЕНТ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ ПО ПРЕДОСТАВЛЕНИЮ ГОСУДАРСТВЕННОЙ УСЛУГИ «ВЕДЕНИЕ РЕЕСТРА ОПЕРАТОРОВ, ОСУЩЕСТВЛЯЮЩИХ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ»

### I. Общие положения

#### Предмет регулирования регламента

1. Административный регламент Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги «Ведение реестра операторов, осуществляющих обработку персональных данных» (далее - Административный регламент) устанавливает сроки и последовательность административных процедур и административных действий Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее - Роскомнадзор) и её территориальных органов с операторами, осуществляющими обработку персональных данных (далее - Оператор), при предоставлении государственной услуги «Ведение реестра операторов, осуществляющих обработку персональных данных» (далее - реестр).

2. Предоставление государственной услуги осуществляется путем:

2.1. Внесения сведений об Операторе в Реестр;

2.2. Изменения сведений об Операторе в Реестре;

2.3. Исключения сведений об Операторе из Реестра;

2.4. Предоставления выписки из Реестра.

#### Круг заявителей

3. Заявителем при предоставлении государственной услуги в соответствии с пунктами 2.1. - 2.3. Административного регламента является Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных.

Заявителем при предоставлении государственной услуги в соответствии с пунктом 2.4. является любое заинтересованное лицо.

4. При подаче заявлений в электронной форме с использованием федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)» по адресу - www.gosuslugi.ru (далее – Единый портал), заявитель подтверждает свое согласие на передачу информации в информационно-телекоммуникационной сети «Интернет» в порядке, установленном законодательством Российской Федерации.

Требования к порядку информирования о предоставлении государственной услуги

5. Информация о правилах предоставления государственной услуги предоставляется:

5.1. Непосредственно в центральном аппарате Роскомнадзора и в его территориальных органах. Справочно-информационный центр центрального аппарата Роскомнадзора: (495) 987–68-00.

5.2. Посредством размещения на официальном сайте Роскомнадзора в информационно-телекоммуникационной сети «Интернет» по адресу - www.rsос.гu (далее – официальный сайт).

6. Местонахождение центрального аппарата Роскомнадзора: г. Москва, Китайгородский проезд, д. 7, стр. 2.

Почтовый адрес для направления обращений: Китайгородский проезд, д. 7, стр. 2, Москва, 109074. Адрес электронной почты: rsoc\_in@rsoc.ru. Почтовые адреса, адреса электронной почты территориальных органов Роскомнадзора, а также адреса официальных сайтов территориальных органов Роскомнадзора, приведены в приложении № 1 к Административному регламенту.

7. Вся информация, касающаяся процедур ведения Реестра, размещается на официальном сайте и Едином портале:x

7.1. Форма уведомления об обработке персональных данных (далее - Уведомление).

7.2. Форма информационного письма о внесении изменений в сведения об Операторе в Реестре (далее - информационное письмо).

7.3. Форма заявления о предоставлении выписки из Реестра.

7.4. Форма заявления об исключении сведений об Операторе из Реестра.

8. На официальном сайте также размещается информация:

8.1. Местонахождение центрального аппарата Роскомнадзора и его территориальных органов, график (режим) работы, номера телефонов, адреса официальных сайтов.

8.2. Административный регламент.

8.3. Нормативные правовые акты, регулирующие предоставление государственной услуги.

8.4. Информация о безвозмездности предоставления государственной услуги.

9. Информация о правилах предоставления государственной услуги предоставляется по обращениям заявителей, а также размещается в информационно - телекоммуникационных сетях общего пользования (в том числе в сети «Интернет»), на информационных стендах территориальных органов Роскомнадзора.

10. При информировании о правилах предоставления государственной услуги по письменным обращениям ответ на обращение направляется по почте или на адрес электронный почты заявителя в течение 30 дней со дня регистрации письменного обращения.

В исключительных случаях, при наличии оснований, руководитель Роскомнадзора (руководитель территориального органа Роскомнадзора), заместитель руководителя Роскомнадзора (заместитель руководителя территориального органа Роскомнадзора) продлевает срок рассмотрения обращения не более чем на 30 дней, уведомив о продлении срока заявителя.

При поступлении обращения в письменной форме на бумажном носителе или в электронной форме по существу рассматриваются обращения, содержащие следующую информацию:

* наименование (с указанием организационно-правовой формы), почтовый адрес или адрес электронной почты - для юридического лица;
* фамилия, почтовый адрес или адрес электронной почты - для физического лица.

11. Обращения по вопросам информирования и консультирования регистрируются в установленном порядке как обращения граждан в отделе документооборота, архива, контроля и работы с обращениями граждан Роскомнадзора и его территориальных органов и рассматриваются в срок не более 30 дней.

12. В случае, если в письменном обращении не указаны фамилия заявителя, направившего обращение (наименование с указанием организационно-правовой формы), почтовый адрес или адрес электронной почты, по которому должен быть направлен ответ, ответ на обращение не дается. Если в указанном обращении содержатся сведения о подготавливаемом, совершаемом или совершенном противоправном деянии, а также о лице, его подготавливающем, совершающем или совершившем, обращение подлежит направлению в государственный орган в соответствии с его компетенцией.

Роскомнадзор и его территориальный орган при получении письменного обращения, в котором содержатся нецензурные либо оскорбительные выражения, угрозы жизни, здоровью и имуществу должностного лица, а также членов его семьи, вправе оставить обращение без ответа по существу поставленных в нем вопросов и сообщить заявителю, направившему обращение, о недопустимости злоупотребления правом.

В случае если текст письменного обращения не поддается прочтению, ответ на обращение не дается, и оно не подлежит направлению на рассмотрение в государственный орган, орган местного самоуправления или должностному лицу в соответствии с их компетенцией, о чем в течение семи дней со дня регистрации обращения сообщается заявителю, направившему обращение, если его фамилия (наименование с указанием организационно-правовой формы), почтовый адрес или адрес электронной почты поддаются прочтению.

В случае если в письменном обращении содержится вопрос, на который заявителю многократно давались письменные ответы по существу в связи с ранее направляемыми обращениями, и при этом в обращении не приводятся новые доводы или обстоятельства, руководитель Роскомнадзора (руководитель территориального органа Роскомнадзора) либо уполномоченное на то должностное лицо вправе принять решение о безосновательности очередного обращения и прекращении переписки с заявителем по данному вопросу при условии, что указанное обращение и ранее направляемые обращения направлялись в Роскомнадзор (его территориальный орган). О данном решении уведомляется заявитель, направивший обращение.

### II. Стандарт предоставления государственной услуги

#### Наименование государственной услуги

13. Наименование государственной услуги, предоставляемой Роскомнадзором и его территориальными органами: «Ведение реестра операторов, осуществляющих обработку персональных данных».

#### Наименование федерального органа исполнительной власти, предоставляющего государственную услугу

14. Предоставление государственной услуги осуществляется Роскомнадзором и его территориальными органами, перечень которых приведен в приложении № 1 к Административному регламенту.

Сотрудники Роскомнадзора и его территориальных органов не вправе требовать от заявителя осуществления действий, в том числе согласований, необходимых для получения государственной услуги и связанных с обращением в иные государственные органы, органы местного самоуправления, организации.

#### Описание результата предоставления государственной услуги

15. Предоставление государственной услуги по ведению Реестра завершается:

15.1. Внесением сведений об Операторе в Реестр.

15.2. Изменением сведений об Операторе в Реестре.

15.3. Исключением сведений об Операторе из Реестра.

15.4. Размещением общедоступных сведений об Операторе на официальном сайте Роскомнадзора.

15.5. Предоставлением выписки из Реестра.

#### Срок предоставления государственной услуги

16. Общий срок внесения сведений об Операторе в Реестр - 15 дней с момента регистрации Уведомления.

17. Общий срок внесения изменений в сведения об Операторе в Реестр - 15 дней с момента регистрации информационного письма.

18. Общий срок исключения сведений об Операторе из Реестра - 15 дней с момента регистрации заявления.

19. Предоставление выписки из Реестра - не позднее 5 дней с даты поступления соответствующего запроса.

20. Срок размещения общедоступных сведений, содержащихся в Реестре, на официальном сайте Роскомнадзора - не позднее 3 дней с даты подписания приказа о внесении сведений об Операторе в Реестр (внесении изменений и исключении сведений об Операторе из Реестра).

#### Перечень нормативных правовых актов, регулирующих отношения, возникающие в связи с предоставлением государственной услуги, с указанием их реквизитов и источников официального опубликования

21. Предоставление государственной услуги осуществляется в соответствии со следующими нормативными правовыми актами:

21.1. Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2009, № 48, ст. 5716; № 52, ст. 6439; 2010, № 27, ст. 3407; № 31, ст. 4173, ст. 4196; № 49, ст. 6409; № 52, ст. 6974; 2011, № 23, ст. 3263; № 31, ст. 4701) (далее – Федеральный закон).

21.2. Федеральным законом от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» (Собрание законодательства Российской Федерации, 2006, № 19, ст. 2060; 2010, № 27, ст. 3410; № 31, ст. 4196).

21.3. Федеральным законом от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» (Собрание законодательства Российской Федерации, 2009, № 7, ст. 776; 2011, № 29, ст. 4291).

21.4. Федеральным законом от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (Собрание законодательства Российской Федерации, 2010, № 31, ст. 4179; 2011, № 15, ст. 2038; № 27, ст. 3880; № 29, ст. 4291; № 30, ст. 4587).

21.5. Постановлением Правительства Российской Федерации от 16 марта 2009 г. № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» (Собрание законодательства Российской Федерации, 2009, № 12, ст. 1431; 2010, № 13, ст. 1502; № 26, ст. 3350; 2011, № 3, ст. 542; № 6, ст. 888; № 14, ст. 1935; № 21, ст. 2965; № 40, ст. 5548; № 44, ст. 6272).

#### Исчерпывающий перечень документов, необходимых в соответствии с нормативными правовыми актами для предоставления государственной услуги, подлежащих представлению заявителем

22. Документом для рассмотрения вопроса о внесении сведений об Операторе в Реестр является Уведомление, предусмотренное частью 3 статьи 22 Федерального закона. Форма Уведомления приведена в приложении № 2 к Административному регламенту.

23. Документом для рассмотрения вопроса о внесении изменений в сведения об Операторе в Реестре является информационное письмо Оператора. Форма информационного письма приведена в приложении № 3 к Административному регламенту.

24. Документом для рассмотрения вопроса о предоставлении выписки из Реестра является заявление Оператора или иного заинтересованного лица о предоставлении выписки из Реестра. Форма заявления приведена в приложении № 4 к Административному регламенту.

25. Документом для рассмотрения вопроса об исключении сведений об Операторе из Реестра является заявление Оператора об исключении сведений о нем из Реестра. Форма заявления приведена в приложении № 5 к Административному регламенту.

#### Исчерпывающий перечень документов, необходимых в соответствии с нормативными правовыми актами для предоставления государственной услуги, которые находятся в распоряжении Роскомнадзора

26. Документы, находящиеся в Роскомнадзоре или иных государственных органах, необходимые для предоставления государственной услуги, отсутствуют.

#### Исчерпывающий перечень оснований для отказа в приеме документов, необходимых для предоставления государственной услуги

27. Основания для отказа в приеме документов, необходимых для предоставления государственной услуги, отсутствуют.

#### Исчерпывающий перечень оснований для приостановления или отказа в предоставлении государственной услуги

28. Основанием для приостановления предоставления государственной услуги является представление Оператором неполных или недостоверных сведений, предусмотренных частью 3 статьи 22 Федерального закона.

#### Перечень услуг, которые являются необходимыми и обязательными для предоставления государственной услуги

29. Необходимые и обязательные услуги для предоставления государственной услуги отсутствуют.

#### Порядок, размер и основания взимания государственной пошлины или иной платы, взимаемой за предоставление государственной услуги

30. Плата за предоставление государственной услуги не взимается.

#### Максимальный срок ожидания в очереди при подаче запроса о предоставлении государственной услуги

31. Предоставление государственной услуги осуществляется без непосредственного взаимодействия с заявителем.

#### Срок и порядок регистрации запроса заявителя о предоставлении государственной услуги

32. Уведомление (информационное письмо, заявление) о предоставлении государственной услуги регистрируется в срок, не позднее дня, следующего за днем его поступления в Роскомнадзор (территориальный орган Роскомнадзора).

33. При поступлении Уведомления (информационного письма, заявления) на бумажном носителе, сотрудник Роскомнадзора (территориального органа Роскомнадзора), ответственный за делопроизводство, проводит их регистрацию в системе электронного документооборота Роскомнадзора с присвоением входящего номера и даты.

34. При поступлении Уведомления (информационного письма, заявления) в электронном виде регистрация осуществляется сотрудником Роскомнадзора (территориального органа Роскомнадзора), ответственным за работу в области персональных данных, путем присвоения регистрационного номера и даты в информационной системе Роскомнадзора (далее - ЕИС), при этом на странице личного кабинета на Едином портале Оператор получает сообщение об изменении статуса Уведомления (информационного письма, заявления).

#### Требования к помещениям, в которых предоставляется государственная услуга, к месту ожидания и приема заявлений, размещению и оформлению визуальной, текстовой и мультимедийной информации о порядке предоставления такой услуги

35. Предоставление государственной услуги осуществляется без непосредственного взаимодействия с заявителем.

36. Рабочие места сотрудников Роскомнадзора (его территориальных органов), участвующих в предоставлении государственной услуги, должны быть оборудованы:

* рабочими столами и стульями (не менее 1 комплекта на одного сотрудника);
* компьютерами (1 компьютер с установленными справочно-правовыми системами на каждого сотрудника);
* оргтехникой, позволяющей своевременно и в полном объеме организовать предоставление государственной услуги;
* стульями для посетителей.

Структурным подразделениям Роскомнадзора и его территориальных органов, ответственным за предоставление государственной услуги по ведению Реестра, должен быть предоставлен доступ к информационно-телекоммуникационной сети «Интернет», в том числе доступ к Единому порталу, и должны выделяться расходные материалы, бумага и канцтовары в количестве, достаточном для предоставления государственной услуги.

#### Показатели доступности и качества государственных услуг

37. Взаимодействие Роскомнадзора и его территориальных органов при обращении заявителя за предоставлением государственной услуги в соответствии с Административным регламентом обеспечивается при однократном обращении:

37.1. Лично или через своего законного представителя.

37.2. В письменной форме почтовым отправлением.

37.3. В электронной форме с Единого портала и официального сайта.

38. Основными требованиями к качеству рассмотрения обращений заявителей в Роскомнадзоре являются:

38.1. Достоверность предоставляемой заявителям информации о ходе рассмотрения обращения.

38.2. Полнота информирования заявителей о ходе рассмотрения обращения.

38.3. Наглядность форм предоставляемой информации об административных процедурах.

38.4. Удобство и доступность получения информации заявителями о порядке предоставления государственной услуги.

38.5. Оперативность вынесения решения в отношении рассматриваемого обращения.

#### Иные требования, в том числе учитывающие особенности предоставления государственной услуги в многофункциональных центрах предоставления государственных услуг и особенности предоставления государственной услуги в электронной форме

39. Обеспечение возможности получения заявителями информации о предоставляемой государственной услуге на официальном сайте и на Едином портале.

40. Обеспечение возможности получения заявителями на официальном сайте и на Едином портале форм заявлений, необходимых для получения государственной услуги в электронном виде.

41. Обеспечение возможности получения информации о ходе предоставления государственной услуги на официальном сайте и на Едином портале.

42. Роскомнадзор при предоставлении государственной услуги взаимодействие с многофункциональными центрами не осуществляет.

43. Согласно части 3 статьи 22 Федерального закона Уведомление, направленное в электронной форме, должно быть подписано электронной цифровой подписью.

### III. Состав, последовательность и сроки выполнения административных процедур (действий), требования к порядку их выполнения, в том числе особенности выполнения административных процедур (действий) в электронной форме

44. Ведение Реестра осуществляет Роскомнадзор и его территориальные органы и предусматривает выполнение следующих административных процедур:

44.1. Внесение сведений об Операторе в Реестр.

44.2. Изменение сведений об Операторе в Реестре.

44.3. Исключение сведений об Операторе из Реестра.

44.4. Предоставление выписки из Реестра.

45. Ведение Реестра осуществляется в электронной форме с применением ЕИС.

В Реестр вносятся сведения об Операторах, подавших Уведомление в соответствии с требованиями части 3 статьи 22 Федерального закона.

46. В Реестр вносятся следующие сведения:

46.1. Регистрационный номер.

46.2. Наименование (фамилия, имя, отчество), адрес Оператора.

46.3. Адреса филиалов (представительств) Оператора (при наличии).

46.4. Дата направления Уведомления.

46.5. Цель обработки персональных данных.

46.6. Категории персональных данных.

46.7. Категории субъектов, персональные данные которых обрабатываются.

46.8. Правовое основание обработки персональных данных.

46.9. Перечень действий с персональными данными, общее описание используемых Оператором способов обработки персональных данных.

46.10. Описание мер, предусмотренных статьями 18.1 и 19 Федерального закона, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств.

46.11. 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.

46.12. Сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки.

46.13. Сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

46.14. Дата начала обработки персональных данных.

46.15. Срок или условие прекращения обработки персональных данных.

46.16. Дата и основание внесения сведений об Операторе в Реестр.

46.17. Дата и основание внесения изменения в сведения об Операторе в Реестр.

46.18. Дата и основание исключения сведений об Операторе из Реестра.

#### Состав документов, которые находятся в распоряжении Роскомнадзора и которые должны быть представлены в иные органы и организации

47. Документы, находящиеся в распоряжении Роскомнадзора и которые должны быть представлены в иные органы и организации, отсутствуют.

#### Состав документов, которые необходимы Роскомнадзору, но находятся в иных органах и организациях

48. Основным и единственным документом для рассмотрения вопроса о внесении сведений об Операторе в Реестр является Уведомление, предусмотренное частью 3 статьи 22 Федерального закона.

#### Порядок осуществления в электронной форме, в том числе с использованием Единого портала, отдельных административных процедур

49. Информация о правилах предоставления государственной услуги предоставляется по обращениям заявителей, а также размещена на официальном сайте и Едином портале.

50. Предоставление государственной услуги в соответствии с Административным регламентом обеспечивается при однократном обращении:

50.1. Лично или через своего законного представителя.

50.2. В электронной форме с Единого портала и официального сайта.

51.Информация о ходе предоставления государственной услуги предоставляется на Едином портале, официальном сайте Роскомнадзора и через справочно-информационный центр центрального аппарата Роскомнадзора.

52. Сведения, содержащиеся в Реестре, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, размещаются на официальном сайте Роскомнадзора не позднее 3 дней с даты подписания приказа о внесении сведений об Операторе в Реестр. При необходимости заявитель вправе обратиться за получением выписки из Реестра.

#### Внесение сведений об Операторе в Реестр

53. Основанием для рассмотрения вопроса о внесении сведений об Операторе в Реестр является направление Оператором Уведомления непосредственно в Роскомнадзор (территориальный орган Роскомнадзора) или поступление Уведомления в ЕИС с Единого портала с присвоением ему входящего номера.

54. Уведомление должно содержать следующие сведения:

54.1. Наименование (фамилия, имя, отчество), адрес Оператора.

54.2. Цель обработки персональных данных.

54.3. Категории персональных данных.

54.4. Категории субъектов, персональные данные которых обрабатываются.

54.5. Правовое основание обработки персональных данных.

54.6. Перечень действий с персональными данными, общее описание используемых Оператором способов обработки персональных данных.

54.7. Описание мер, предусмотренных статьями 18.1 и 19 Федерального закона, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств.

54.8. 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.

54.9. Сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки.

54.10. Сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

54.11. Дату начала обработки персональных данных.

54.12. Срок или условие прекращения обработки персональных данных.

55. При поступлении Уведомления на бумажном носителе, сотрудник Роскомнадзора (территориального органа Роскомнадзора), ответственный за делопроизводство, проводит регистрацию Уведомления и направляет его заместителю руководителя Роскомнадзора (руководителю территориального органа Роскомнадзора) для определения ответственного исполнителя или принятия решения об отказе о внесении сведений об Операторе в Реестр, в случае предоставления неполных или недостоверных сведений.

56. Сотрудник Роскомнадзора (территориального органа Роскомнадзора) ответственный за работу в области персональных данных, вносит Уведомление в подсистему «Персональные данные» ЕИС в срок не позднее дня, следующего за днем его регистрации.

57. Сотрудник Роскомнадзора (территориального органа Роскомнадзора), ответственный за работу в области персональных данных, не позднее 5 дней с момента присвоения Уведомлению регистрационного номера рассматривает его и при соответствии требованиям части 3 статьи 22 Федерального закона переводит Уведомление в статус «На включение в приказ» для включения в проект приказа о внесении сведений об Операторе в Реестр.

58. В случае предоставления Оператором неполных или недостоверных сведений, предусмотренных с частью 3 статьи 22 Федерального закона, сотрудник Роскомнадзора (территориального органа Роскомнадзора) направляет Оператору письмо с уведомлением о его вручении, содержащее запрос с указанием перечня недостающих сведений для внесения в Реестр. После подписания письма и присвоения ему регистрационного номера файл со сканированным письмом вносится в ЕИС в срок не позднее дня, следующего за днем его регистрации.

59. Оператор обязан сообщить в территориальный орган Роскомнадзора по его запросу уточненные сведения, необходимые для осуществления деятельности указанного органа, в течение 30 дней с даты получения такого запроса.

60. После получения от Оператора уточненных сведений, соответствующих требованиям части 3 статьи 22 Федерального закона, сотрудник Роскомнадзора (территориального органа Роскомнадзора), ответственный за работу в области персональных данных, вносит уточненные сведения в ЕИС и переводит Уведомление в статус «На включение в приказ» для включения в проект приказа о внесении сведений об Операторе в Реестр.

61. Если в течение 30 дней с даты получения запроса Оператор не представил уточненные сведения, то по истечении указанного срока Уведомление с неполными или недостоверными сведениями возвращается Оператору без внесения сведений о нем в Реестр.

62. При поступлении Уведомления от Оператора с Единого портала в ЕИС, сотрудник Роскомнадзора (территориального органа Роскомнадзора), ответственный за работу в области персональных данных, проверяет Уведомление в подсистеме «Персональные данные» ЕИС на соответствие предоставленных сведений требованиям Федерального закона.

63. Уведомлению, соответствующему требованиям Федерального закона, присваивается регистрационный номер в срок не позднее дня, следующего за днем его поступления, при этом на странице личного кабинета на Едином портале Оператор получает сообщение об изменении статуса Уведомления.

64. Сотрудник Роскомнадзора (территориального органа Роскомнадзора), ответственный за работу в области персональных данных, не позднее 5 дней с момента присвоения Уведомлению регистрационного номера рассматривает его и, при соответствии требованиям части 3 статьи 22 Федерального закона, переводит в статус «На включение в приказ» для включения в проект приказа о внесении сведений об Операторе в Реестр. На странице личного кабинета на Едином портале Оператор получает сообщение об изменении статуса Уведомления.

65. В случае предоставления Оператором Уведомления с неполными или недостоверными сведениями, сотрудник Роскомнадзора по согласованию с начальником отдела ведения реестра операторов, осуществляющих обработку персональных данных (территориального органа Роскомнадзора по согласованию с начальником отдела, на которого возложены функции защиты прав субъектов персональных данных), информирует Оператора о перечне недостающих сведений до их внесения в Реестр. Информирование происходит путем изменения статуса Уведомления на странице личного кабинета Единого портала и по электронной почте.

66. Оператор обязан представить новое Уведомление в электронной форме в течение 30 дней с даты получения извещения о необходимости доработки ранее представленного Уведомления.

67. После получения от Оператора нового Уведомления, соответствующего требованиям Федерального закона, ему присваивается регистрационный номер в срок не позднее дня, следующего за днем его поступления. Не позднее 5 дней, с момента присвоения Уведомлению регистрационного номера, сотрудник Роскомнадзора (территориального органа Роскомнадзора) рассматривает его и переводит в статус «На включение в приказ» для включения в проект приказа о внесении сведений об Операторе в Реестр. На Едином портале Оператор получает сообщение об изменении статуса Уведомления.

68. Сотрудник Роскомнадзора (территориального органа Роскомнадзора) в срок, не превышающий 5 дней с момента перевода Уведомления в статус «На включение в приказ», готовит проект приказа о внесении сведений об Операторе в Реестр.

69. В течение 5 дней с момента подготовки проекта приказа о внесении сведений об Операторе в Реестр руководитель Роскомнадзора (руководитель территориального органа Роскомнадзора) издает приказ о внесении сведений об Операторе в Реестр. На основании данного приказа в Реестр вносится запись об Операторе. Указанной записи присваивается регистрационный номер.

70. Информация о внесении сведений об Операторе в Реестр размещается на официальном сайте Роскомнадзора в срок не позднее 3 дней с даты подписания приказа о внесении сведений об Операторе в Реестр.

Блок-схемы административной процедуры внесения сведений об Операторе в Реестр представлены в приложении № 6 к Административному регламенту.

#### Изменение сведений об Операторе в Реестре

71. Основанием для рассмотрения вопроса о внесении изменений в сведения, содержащиеся в Реестре, является направление Оператором в Роскомнадзор (территориальный орган Роскомнадзора) или поступление в ЕИС с Единого портала информационного письма с указанием основания изменения сведений. В случае изменения сведений, указанных в части 3 статьи 22 Федерального закона, Оператор обязан уведомить об изменениях Роскомнадзор (территориальный орган Роскомнадзора) в течение 10 рабочих дней с даты возникновения таких изменений.

72. При поступлении информационного письма на бумажном носителе, сотрудник Роскомнадзора (территориального органа Роскомнадзора), ответственный за делопроизводство, проводит регистрацию информационного письма с измененными сведениями.

73. Сотрудник Роскомнадзора (территориального органа Роскомнадзора), ответственный за работу в области персональных данных, вносит файл со сканированным информационным письмом, содержащий измененные сведения в ЕИС, в срок, не позднее дня, следующего за днем его регистрации.

74. Сотрудник Роскомнадзора (территориального органа Роскомнадзора), ответственный за работу в области персональных данных, не позднее 5 дней со дня присвоения информационному письму с измененными сведениями регистрационного номера рассматривает и переводит указанное информационное письмо с измененными сведениями в статус «На включение в приказ» для включения в проект приказа о внесении изменений в сведения об Операторе в Реестре.

75. Сотрудник Роскомнадзора (территориального органа Роскомнадзора) в срок, не превышающий 5 дней с момента перевода информационного письма с измененными сведениями в статус «На включение в приказ», готовит проект приказа об изменении сведений об Операторе в Реестре.

76. При поступлении информационного письма от Оператора с Единого портала в ЕИС, сотрудник Роскомнадзора (территориального органа Роскомнадзора), ответственный за работу в области персональных данных, проверяет содержание информационного письма в подсистеме «Персональные данные» ЕИС.

77. Информационному письму присваивается регистрационный номер, при этом на странице личного кабинета на Едином портале Оператор получает сообщение об изменении статуса Уведомления.

78. Сотрудник Роскомнадзора (территориального органа Роскомнадзора), ответственный за работу в области персональных данных, не позднее 5 дней со дня присвоения информационному письму с измененными сведениями регистрационного номера, рассматривает его и переводит в статус «На включение в приказ» для включения в проект приказа о внесении изменений в сведения об Операторе в Реестре.

79. Сотрудник Роскомнадзора (территориального органа Роскомнадзора) в срок, не превышающий 5 дней с момента перевода информационного письма с измененными сведениями в статус «На включение в приказ» готовит проект приказа об изменении сведений об Операторе в Реестре.

На странице личного кабинета Оператор получает сообщение об изменении статуса Уведомления.

80. В течение 5 дней подготовленный проект приказа о внесении изменений в сведения об Операторе в Реестр согласовывается в структурных подразделениях Роскомнадзора (в отделах территориальных органов Роскомнадзора) и подписывается руководителем Роскомнадзора (руководителем территориального органа Роскомнадзора).

На основании данного приказа в Реестр вносится запись о внесении изменений в сведения об Операторе. На странице личного кабинета Оператор получает сообщение о внесении изменений в сведения о нем в Реестре.

Ранее присвоенный регистрационный номер записи об Операторе в Реестре не изменяется.

81. Информация о внесении изменений в сведения об Операторе в Реестр размещается на официальном сайте Роскомнадзора в срок, не позднее 3 дней с даты подписания приказа о внесении изменений в сведения об Операторе в Реестр.

Блок-схемы административной процедуры внесения изменений в сведения об Операторе в Реестр представлены в приложении № 6 к Административному регламенту.

#### Исключение сведений об Операторе из Реестра

82. Вопрос об исключении сведений об Операторе из Реестра рассматривается в следующих случаях:

82.1. Поступление в Роскомнадзор или территориальные органы Роскомнадзора заявления от Оператора, сведения о котором внесены в Реестр, об исключении сведений о нем из Реестра с приложением обоснований.

82.2. Принятие Роскомнадзором (территориальным органом Роскомнадзора) мер по приостановлению или прекращению Оператором обработки персональных данных, осуществляемой с нарушением требований Федерального закона.

82.3. Поступление в Роскомнадзор (территориальный орган Роскомнадзора) информации от других органов государственной власти, юридических или физических лиц о прекращении Оператором обработки персональных данных.

82.4. Выявление в Реестре недостоверной информации, указанной Оператором в Уведомлении.

82.5. Выявление в Реестре сведений об Операторе, внесенных повторно.

83. Операторы исключаются из Реестра при наступлении одного из следующих условий:

83.1. Ликвидация Оператора.

83.2. Прекращение деятельности Оператора в результате его реорганизации.

83.3. Прекращение Оператором деятельности по обработке персональных данных.

83.4. Аннулирование лицензий на осуществление лицензируемой деятельности Оператора, если условием лицензии на осуществление такой деятельности является запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных.

83.5. Наступление срока или условия прекращения обработки персональных данных, указанных в Уведомлении.

83.6. Вступившее в законную силу решение суда о прекращении Оператором деятельности по обработке персональных данных.

84. При поступлении заявления от Оператора об исключении сведений о нем из Реестра на бумажном носителе, сотрудник Роскомнадзора (территориального органа Роскомнадзора), ответственный за делопроизводство, проводит регистрацию данного заявления и направляет его заместителю руководителя Роскомнадзора (руководителю территориального органа Роскомнадзора).

85. Сотрудник Роскомнадзора (территориального органа Роскомнадзора), ответственный за работу в области персональных данных, создает заявление об исключении сведений об Операторе из Реестра в ЕИС, вносит файл со сканированным заявлением с резолюцией заместителя руководителя Роскомнадзора (руководителя территориального органа Роскомнадзора) и прилагаемыми документами, подтверждающими необходимость исключения Оператора из Реестра в ЕИС в срок не позднее дня, следующего за днем регистрации заявления.

86. Сотрудник Роскомнадзора (территориального органа Роскомнадзора), ответственный за работу в области персональных данных, в течение 5 дней со дня присвоения заявлению регистрационного номера, проводит проверку сведений, содержащихся в заявлении, на соответствие прилагаемым документам. При соответствии заявления прилагаемым документам в срок, не превышающий 5 дней с момента поступления заявления об исключении, сотрудник Роскомнадзора (территориального органа Роскомнадзора), ответственный за работу в области персональных данных, переводит его в статус «На включение в приказ».

87. В случае выявления несоответствий заявления прилагаемым документам сотрудник Роскомнадзора (территориального органа Роскомнадзора), ответственный за работу в области персональных данных, направляет Оператору письмо с уведомлением о его вручении, содержащее запрос с указанием перечня недостающих сведений. После подписания этого письма и присвоения ему регистрационного номера, файл со сканированным письмом вносится в ЕИС.

88. Оператор обязан сообщить в Роскомнадзор (территориальный орган Роскомнадзора) по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение 30 дней с даты получения такого запроса.

89. После получения от Оператора письма с уточненными сведениями сотрудник Роскомнадзора (территориального органа Роскомнадзора), ответственный за работу в области персональных данных, вносит файл со сканированным письмом с уточненными сведениями в ЕИС в срок не позднее дня, следующего за днем его регистрации, и переводит заявление в статус «На включение в приказ».

90. Сотрудник Роскомнадзора (территориального органа Роскомнадзора) в срок, не превышающий 5 дней с момента перевода Уведомления в статус «На включение в приказ», готовит проект приказа о внесении сведений об исключении Оператора из Реестра.

91. В случае возникновения одного из условий, предусмотренных в пункте 83 Административного регламента и подтвержденных соответствующими документами, руководитель Роскомнадзора (территориального органа Роскомнадзора) в течение 5 дней с момента подготовки проекта приказа издает приказ об исключении сведений об Операторе из Реестра.

92. Оператор может оформить заявление об исключении из Реестра на Едином портале и направить в ЕИС Роскомнадзора. К заявлению прилагаются отсканированные документы, обосновывающие исключение Оператора из Реестра. При поступлении заявления Оператора в электронном виде регистрация осуществляется путем присвоения регистрационного номера в ЕИС, при этом на странице личного кабинета на Едином портале Оператор получает сообщение об изменении статуса заявления.

93. Сотрудник Роскомнадзора (территориального органа Роскомнадзора), ответственный за работу в области персональных данных, обязан ежедневно проверять поступление заявлений от Операторов.

94. Сотрудник Роскомнадзора (территориального органа Роскомнадзора), ответственный за работу в области персональных данных, проверяет в ЕИС заявление и прилагаемые документы, подтверждающие необходимость исключения Оператора из Реестра в срок не позднее дня, следующего за днем регистрации заявления. На странице личного кабинета Оператор получает сообщение об изменении статуса заявления.

95. Сотрудник Роскомнадзора (территориального органа Роскомнадзора), ответственный за работу в области персональных данных, в течение 5 дней со дня присвоения заявлению регистрационного номера, проводит проверку сведений, содержащихся в заявлении, на соответствие прилагаемым документам. При соответствии заявления прилагаемым документам оно переводится в статус «На включение в приказ» для включения в проект приказа об исключении сведений об Операторе из Реестра.

96. В случае выявления несоответствий заявления прилагаемым документам, сотрудник Роскомнадзора по согласованию с начальником отдела ведения реестра операторов, осуществляющих обработку персональных данных (территориального органа Роскомнадзора по согласованию с начальником отдела, на которого возложены функции защиты прав субъектов персональных данных), уведомляет заявителя о необходимости его доработки. На странице личного кабинета Оператор получает сообщение о направлении письма и изменении статуса заявления.

97. Оператор обязан сообщить в Роскомнадзор (территориальный орган Роскомнадзора) по его запросу информацию, необходимую для осуществления деятельности Роскомнадзора, в течение 30 дней с даты получения такого запроса.

98. После получения от Оператора письма с уточненными сведениями сотрудник Роскомнадзора (территориального органа Роскомнадзора), ответственный за работу в области персональных данных, вносит файл со сканированным письмом с уточненными сведениями в ЕИС в срок не позднее дня, следующего за днем его регистрации, и переводит заявление в статус «На включение в приказ» для включения в проект приказа об исключении сведений об Операторе из Реестра.

99. Сотрудник Роскомнадзора (территориального органа Роскомнадзора) в срок, не превышающий 5 дней с момента перевода заявления в статус «На включение в приказ», готовит проект приказа об исключении сведений об Операторе из Реестра.

100. В случае возникновения одного из условий, предусмотренных в пункте 83 Административного регламента, руководитель Роскомнадзора (территориального органа Роскомнадзора) в течение 5 дней с момента подготовки проекта приказа издает приказ об исключении сведений об Операторе из Реестра.

На основании данного приказа в Реестр вносится запись об исключении сведений об Операторе из Реестра. После исключения сведений об Операторе из Реестра регистрационный номер соответствующей записи в дальнейшем не используется. На странице личного кабинета Оператор получает сообщение об исключении из Реестра.

101. В случае исключения сведений об Операторе из Реестра по основаниям, не связанным с обращением Оператора об исключении сведений о нем из Реестра, необходимо уведомить Оператора об исключении сведений о нем из Реестра в срок, не превышающий 5 дней со дня исключения сведений о нем из Реестра. На странице личного кабинета Оператор получает сообщение об исключении сведений о нем из Реестра.

Блок-схемы административной процедуры исключения сведений об Операторе из Реестра представлены в приложении № 6 к Административному регламенту.

#### Предоставление выписки из Реестра

102. Заявители вправе получить выписку из Реестра на основании письменного заявления в Роскомнадзор (соответствующий территориальный орган Роскомнадзора) или заявления в электронной форме с Единого портала.

103. Выписка из Реестра предоставляется при наличии в заявлении следующих сведений:

103.1. Наименования юридического лица; фамилии, имени, отчества (последнее - при наличии) физического лица.

103.2. Почтового адреса юридического лица, физического лица.

104. При поступлении письменного заявления от Оператора сотрудником Роскомнадзора (территориального органа Роскомнадзора), ответственным за делопроизводство, проводится регистрация данного запроса и направляется заместителю руководителя Роскомнадзора (руководителю территориального органа Роскомнадзора).

105. При соответствии заявления требованиям пункта 103 Административного регламента, сотрудник Роскомнадзора (территориального органа Роскомнадзора) в срок, не превышающий 5 дней с даты поступления запроса, готовит выписку из Реестра. Заявителю по почте с уведомлением о вручении направляется выписка, подписанная уполномоченным лицом, либо письмо с указанием причины отказа.

106. Оператор может оформить заявление на выписку из Реестра на Едином портале и направить в ЕИС Роскомнадзора. При поступлении заявления Оператора в электронном виде регистрация осуществляется путем присвоения регистрационного номера в ЕИС.

107. Сотрудник Роскомнадзора (территориального органа Роскомнадзора), ответственный за работу в области персональных данных, обязан ежедневно проверять поступление заявлений от Операторов.

108. Сотрудник Роскомнадзора (территориального органа Роскомнадзора) в срок, не превышающий 5 дней с даты поступления запроса, готовит выписку из Реестра. Заявителю по почте с уведомлением о вручении направляется выписка, подписанная заместителем руководителя Роскомнадзора (руководителем территориального органа Роскомнадзора), либо письмо с указанием причины отказа.

На странице личного кабинета Оператор получает сообщение о предоставлении выписки или информацию о причине отказа в предоставлении выписки.

Блок-схемы административной процедуры предоставления выписки из Реестра представлены в приложении № 6 к Административному регламенту.

### IV. Формы контроля за исполнением Административного регламента

109. Текущий контроль за соблюдением последовательности действий (административных процедур) по предоставлению государственной услуги осуществляется:

109.1. В центральном аппарате Роскомнадзора – курирующим заместителем руководителя, начальником Управления по защите прав субъектов персональных данных, начальником отдела (заместителем начальника отдела) ведения Реестра (далее – должностные лица центрального аппарата).

109.2. В территориальном органе Роскомнадзора – курирующим заместителем руководителя, начальником отдела (заместителем начальника отдела) на которого возложены функции защиты прав субъектов персональных данных (далее - должностные лица территориального органа).

110. Ответственность должностных лиц центрального аппарата и территориальных органов Роскомнадзора:

110.1. Должностные лица центрального аппарата и территориальных органов Роскомнадзора, ответственные за рассмотрение письменных обращений заявителей по вопросам информирования о правилах исполнения государственной услуги, несут ответственность за соблюдение сроков и порядка приема и рассмотрения письменных обращений заявителей по вопросам информирования о правилах предоставления государственной услуги, установленных пунктом 10 Административного регламента.

110.2. Должностные лица центрального аппарата и территориальных органов Роскомнадзора, ответственные за рассмотрение Уведомлений, несут ответственность за соблюдение сроков и порядка приема и рассмотрения Уведомления, установленных пунктами 57, 59, 61, 64, 67-70 Административного регламента.

110.3. Должностные лица центрального аппарата и территориальных органов Роскомнадзора, ответственные за рассмотрение информационного письма с указанием основания изменения сведений об Операторе в Реестре, несут ответственность за соблюдение сроков и порядка приема и рассмотрения информационного письма с указанием основания изменения сведений об Операторе в Реестре, установленных пунктами 72-81 Административного регламента.

110.4 Должностные лица центрального аппарата и территориальных органов Роскомнадзора, ответственные за рассмотрение Уведомлений, заявлений от Оператора, сведения о котором внесены в Реестр, об исключении сведений о нем из Реестра с приложением обоснований, несут ответственность за соблюдение сроков и порядка приема и рассмотрения заявления (обращения) от Оператора, сведения о котором внесены в Реестр, об исключении сведений о нем из Реестра с приложением обоснований, установленных пунктами 82, 85-87, 89-91, 94, 95, 98-101 Административного регламента.

110.5. Должностные лица центрального аппарата и территориальных органов Роскомнадзора, ответственные за рассмотрение запроса, поступившего в Роскомнадзор (территориальный орган Роскомнадзора) о получении выписки из Реестра, несут ответственность за соблюдение сроков, порядка приема и рассмотрения запроса, установленных пунктами 106, 107, 110-114 Административного регламента.

111. Ответственность должностных лиц центрального аппарата и территориальных органов Роскомнадзора устанавливается в их должностных регламентах в соответствии с требованиями законодательных и иных нормативных правовых актов Российской Федерации.

112. Должностные лица центрального аппарата и территориальных органов Роскомнадзора, осуществляющие текущий контроль за предоставлением государственной услуги, определяются соответствующими приказами.

113. Порядок осуществления контроля:

113.1. Текущий контроль осуществляется путем визирования документов, подлежащих направлению вышестоящему должностному лицу центрального аппарата или территориального органа Роскомнадзора, проведения проверок соблюдения и исполнения сотрудниками положений Административного регламента и иных нормативных правовых актов Российской Федерации.

113.2. Плановый и внеплановый контроль осуществляется путем проведения должностными лицами центрального аппарата и территориальных органов Роскомнадзора, ответственными за организацию работы по предоставлению государственной услуги, проверок соблюдения и исполнения сотрудниками положений Административного регламента. Периодичность осуществления планового и внепланового контроля устанавливается руководителем Роскомнадзора (руководителем территориального органа Роскомнадзора).

113.3. Контроль за полнотой и качеством предоставления государственной услуги включает в себя проведение проверок, выявление и устранение нарушений.

113.4. Для проведения проверки полноты и качества предоставления государственной услуги формируется комиссия, в состав которой включаются должностные лица центрального аппарата и территориальных органов Роскомнадзора. Деятельность комиссии осуществляется в соответствии с приказами Роскомнадзора.

113.5. При проверке комиссия рассматривает вопросы, связанные с предоставлением государственной услуги.

113.6. Результаты деятельности комиссии оформляются в виде справки, в которой отмечаются выявленные недостатки и предложения по их устранению. Справка подписывается председателем и членами комиссии.

113.7. В случае выявления нарушений прав лиц, обратившихся в Роскомнадзор, осуществляется привлечение виновных должностных лиц к ответственности в соответствии с законодательством Российской Федерации. При этом принимаются меры, направленные на восстановление и защиту прав физических и юридических лиц.

114. В целях обеспечения контроля за предоставлением государственной услуги со стороны граждан, их объединений и организаций сведения, содержащиеся в Реестре, размещаются на официальном сайте.

### V. Досудебный (внесудебный) порядок обжалования решений и действий (бездействия) Роскомнадзора, а также его должностных лиц

115. Решения и действия (бездействие), осуществляемые в ходе предоставления Роскомнадзором государственной услуги могут обжаловаться лицами (гражданами, юридическими лицами), чьи права или законные интересы были нарушены обжалуемыми действиями (бездействием) (далее – заявители).

116. Заявители имеют право на обжалование решений и действий (бездействия) Роскомнадзора, должностных лиц Роскомнадзора и территориальных органов Роскомнадзора в досудебном (внесудебном) порядке.

117. Заявитель может обратиться с жалобой в том числе в следующих случаях:

* нарушение срока регистрации запроса заявителя о предоставлении Роскомнадзором государственной услуги;
* нарушение срока предоставления Роскомнадзором государственной услуги;
* требование у заявителя Роскомнадзором документов, не предусмотренных нормативными правовыми актами Российской Федерации;
* отказ Роскомнадзором в приеме документов, предоставление которых предусмотрено нормативными правовыми актами Российской Федерации;
* отказ Роскомнадзором в предоставлении государственной услуги, если основания не предусмотрены федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации;
* затребование Роскомнадзором с заявителя при предоставлении государственной услуги платы, не предусмотренной нормативными правовыми актами Российской Федерации;
* отказ Роскомнадзора, должностного лица Роскомнадзора в исправлении допущенных опечаток и ошибок в выданных в результате предоставления государственной услуги документах либо нарушение установленного срока таких исправлений.

118. Жалоба подается в письменной форме на бумажном носителе, в электронной форме в Роскомнадзор. Жалоба на решения, принятые руководителем Роскомнадзора, в Министерство связи и массовых коммуникаций Российской Федерации.

119. Жалоба может быть направлена по почте, через многофункциональный центр, с использованием информационно-телекоммуникационной сети «Интернет», официального сайта, Единого портала, а также может быть принята при личном приеме заявителя.

120. Жалоба должна содержать:

* наименование органа, предоставляющего государственную услугу, должностного лица органа, предоставляющего государственную услугу, либо государственного служащего, решения и действия (бездействие) которых обжалуются;
* фамилию, имя, отчество (последнее - при наличии), сведения о месте жительства заявителя - физического лица либо наименование, сведения о месте нахождения заявителя - юридического лица, а также номер (номера) контактного телефона, адрес (адреса) электронной почты (при наличии) и почтовый адрес, по которым должен быть направлен ответ заявителю;
* сведения об обжалуемых решениях и действиях (бездействии) органа, предоставляющего государственную услугу, должностного лица органа, предоставляющего государственную услугу, либо государственного служащего;
* доводы, на основании которых заявитель не согласен с решением и действием (бездействием) органа, предоставляющего государственную услугу, должностного лица органа, предоставляющего государственную услугу, либо государственного служащего. Заявителем могут быть представлены документы (при наличии), подтверждающие доводы заявителя, либо их копии.

121. Жалоба, поступившая в Роскомнадзор подлежит рассмотрению должностным лицом Роскомнадзора, наделенным полномочиями по рассмотрению жалоб, в течение пятнадцати рабочих дней со дня ее регистрации, а в случае обжалования отказа Роскомнадзора, должностного лица Роскомнадзора в приеме документов у заявителя либо в исправлении допущенных опечаток и ошибок или в случае обжалования нарушения установленного срока таких исправлений - в течение пяти рабочих дней со дня ее регистрации.

122. По результатам рассмотрения жалобы Роскомнадзор принимается одно из следующих решений:

* удовлетворяет жалобу, в том числе в форме отмены принятого решения, исправления допущенных Роскомнадзором опечаток и ошибок в выданных в результате предоставления государственной услуги документах, возврата заявителю денежных средств, взимание которых не предусмотрено нормативными правовыми актами Российской Федерации;
* отказывает в удовлетворении жалобы.

123. Не позднее дня, следующего за днем принятия решения, указанного в пункте 122, заявителю в письменной форме и по желанию заявителя в электронной форме направляется мотивированный ответ о результатах рассмотрения жалобы.

124. В случае установления в ходе или по результатам рассмотрения жалобы признаков состава административного правонарушения или преступления должностное лицо Роскомнадзора, наделенное полномочиями по рассмотрению жалоб, незамедлительно направляет имеющиеся материалы в органы прокуратуры.

Приложение № 1  
к Административному регламенту  
Федеральной службы по надзору в сфере   
связи, информационных технологий и  
массовых коммуникаций по предоставлению   
государственной услуги «Ведение реестра   
операторов, осуществляющих обработку   
персональных данных»

### Реквизиты Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций

|  |  |  |  |
| --- | --- | --- | --- |
| **Местонахождение:** | Китайгородский проезд, д.7, стр.2, г. Москва, 109074 | | |
| **Официальный сайт Роскомнадзора в сети Интернет:** | | www.rsoc.ru | |
| **График работы отдела документооборота, архива, контроля и работы с обращениями граждан (приём документов):** | | понедельник – пятница | с 10.00 до 12.00 с 14.00 до 16.00 |
| суббота, воскресенье | выходной |

### Территориальные органы Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№№** | **Наименование** | **Почтовый адрес и** **телефон** | **Официальный сайт (http://)** | **Электронный адрес** **(http://)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| 63 | Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Ставропольскому краю | ул. Тухачевского, д. 8, г. Ставрополь, 355040 (8652) 72-35-36 (8652) 73-15-35 | [26.rsoc.ru](http://26.rsoc.ru/) | [rsockanc26@rsoc.ru](mailto:rsockanc26@rsoc.ru) |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Приложение № 2  
к Административному регламенту   
Федеральной службы по надзору в сфере   
связи, информационных технологий и   
массовых коммуникаций по предоставлению  
государственной услуги «Ведение реестра  
операторов, осуществляющих обработку   
персональных данных»

Уведомление об обработке (о намерении осуществлять обработку) персональных данных 

(полное и сокращенное наименования, фамилия, имя отчество оператора)

руководствуясь:

(адрес местонахождения и почтовый адрес оператора)

с целью:

(цель обработки персональных данных)

осуществляет обработку:

(категории персональных данных)

принадлежащих:

(категории субъектов, персональные данные которых обрабатываются)

Обработка вышеуказанных персональных данных будет осуществляться путем:

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

Для обеспечения безопасности персональных данных принимаются следующие меры:

«О персональных данных» в т.ч. сведения о наличии шифровальных (криптографических)

средств и наименования этих средств; 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)

Сведения о наличии или об отсутствии трансграничной передачи персональных данных:

(при наличии трансграничной передачи персональных данных в процессе их обработки, указывается перечень

иностранных государств, на территорию которых осуществляется трансграничная передача персональных данных

Сведения об обеспечении безопасности персональных данных:

(сведения об обеспечении безопасности персональных данных в соответствии с требованиями

к защите персональных данных, установленными Правительством Российской Федерации)

Дата начала обработки персональных данных

(число, месяц, год)

Срок или условие прекращение обработки персональных данных:

(число, месяц, год или основание (условие), наступление которого повлечет прекращение обработки

персональных данных)

(должность)(подпись)расшифровка подписи

«\_\_\_»\_\_\_\_\_\_\_\_\_\_20\_\_г.

Приложение № 3  
к Административному регламенту   
Федеральной службы по надзору в сфере   
связи, информационных технологий и   
массовых коммуникаций по предоставлению  
государственной услуги «Ведение реестра  
операторов, осуществляющих обработку   
персональных данных»

Информационное письмо о внесении изменений в сведения об операторе в реестре операторов, осуществляющих обработку персональных данных

(полное и сокращенное наименование, фамилия, имя отчество оператора)

(адрес местонахождения и почтовый адрес оператора)

(регистрационный номер записи в реестре)

Основания изменений:

руководствуясь:

(правовое основание обработки персональных данных)

с целью:

(цель обработки персональных данных)

осуществляет обработку:

(категории персональных данных)

осуществляет обработку:

(категории субъектов, персональные данные которых обрабатываются)

Обработка вышеуказанных персональных данных будет осуществляться путем:

(перечень действий с персональными данными, общее описание используемых оператором способов обработки

персональных данных)

Для обеспечения безопасности персональных данных принимаются следующие меры:

(описание мер, предусмотренных ст.ст. 18.1. и 19 Федерального закона № 152-ФЗ от 27.07.2006

«О персональных данных», в т.ч. сведения о наличии шифровальных (криптографических)

средств и наименования этих средств; 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)

Сведения о наличии или об отсутствии трансграничной передачи персональных данных

при наличии трансграничной передачи персональных данных в процессе их обработки, с указанием перечня

иностранных государств, на территорию которых осуществляется трансграничная передача персональных данных)

Сведения об обеспечении безопасности персональных данных

(сведения об обеспечении безопасности персональных данных в соответствии с требованиями

к защите персональных данных, установленными Правительством Российской Федерации)

Дата начала обработки персональных данных

(число, месяц, год)

Срок или условие прекращение обработки персональных данных:

(должность)(подпись)расшифровка подписи

«\_\_\_»\_\_\_\_\_\_\_\_\_\_20\_\_г.

Приложение № 4  
к Административному регламенту   
Федеральной службы по надзору в сфере   
связи, информационных технологий и   
массовых коммуникаций по предоставлению  
государственной услуги «Ведение реестра  
операторов, осуществляющих обработку   
персональных данных»

Заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных

(полное наименование (фамилия, имя отчество) заявителя

(адрес местонахождения, почтовый адрес заявителя)

(ИНН заявителя)

Сведения о запрашиваемом операторе:

(ИНН, регистрационный номер записи в реестре)

(должность)(подпись)расшифровка подписи

«\_\_\_»\_\_\_\_\_\_\_\_\_\_20\_\_г.

Приложение № 5  
к Административному регламенту   
Федеральной службы по надзору в сфере   
связи, информационных технологий и   
массовых коммуникаций по предоставлению  
государственной услуги «Ведение реестра  
операторов, осуществляющих обработку   
персональных данных»

Заявление об исключении сведений об операторе из реестра операторов, осуществляющих обработку персональных данных

(полное наименование (фамилия, имя отчество) оператора)

(адрес местонахождения, почтовый адрес оператора

Сведения об операторе:

(ИНН, ОГРН, регистрационный номер записи в реестре)

Основание исключения из реестра:

(ликвидация оператора, реорганизация оператора, прекращение деятельности по обработке пд, аннулирование

лицензии, наступление срока или условия прекращения обработки персональных данных)

(должность)(подпись)расшифровка подписи

«\_\_\_»\_\_\_\_\_\_\_\_\_\_20\_\_г.

Приложение № 6  
к Административному регламенту   
Федеральной службы по надзору в сфере   
связи, информационных технологий и   
массовых коммуникаций по предоставлению  
государственной услуги «Ведение реестра  
операторов, осуществляющих обработку   
персональных данных»

# ПРИКАЗ РОСКОМНАДЗОРА ОТ 19 АВГУСТА 2011 Г. №706 "ОБ УТВЕРЖДЕНИИ РЕКОМЕНДАЦИЙ ПО ЗАПОЛНЕНИЮ ОБРАЗЦА ФОРМЫ УВЕДОМЛЕНИЯ ОБ ОБРАБОТКЕ (О НАМЕРЕНИИ ОСУЩЕСТВЛЯТЬ ОБРАБОТКУ) ПЕРСОНАЛЬНЫХ ДАННЫХ"

**МИНКОМСВЯЗЬ РОССИИ   
ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ,  
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ  
(РОСКОМНАДЗОР)  
  
ПРИКАЗ**

19 августа 2011 г. Москва № 706

## ОБ УТВЕРЖДЕНИИ РЕКОМЕНДАЦИЙ ПО ЗАПОЛНЕНИЮ ОБРАЗЦА ФОРМЫ УВЕДОМЛЕНИЯ ОБ ОБРАБОТКЕ (О НАМЕРЕНИИ ОСУЩЕСТВЛЯТЬ ОБРАБОТКУ) ПЕРСОНАЛЬНЫХ ДАННЫХ

В целях реализации частей 1, 3 статьи 22, также части 4 статьи 25 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2009, № 48, ст. 5716, № 52, ст. 6439; 2010, № 27, ст. 3407; № 31, ст. 4173, ст. 4196; № 49, ст. 6409; № 52, ст. 6974; 2011, № 23, ст. 3263; № 31, ст. 4701), п р и к а з ы в а ю:

1. Утвердить прилагаемые Рекомендации по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных.
2. Признать утратившими силу пункты 1, 2 приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 16 июля 2010 г. № 482 «Об утверждении образца формы уведомления об обработке персональных данных».
3. Контроль за исполнением настоящего приказа возложить на заместителя руководителя Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций Р.В. Шередина.

Врио руководителя К. В. Протопопов

УТВЕРЖДЕНЫ  
приказом Роскомнадзора  
от «19» августа 2011 г. № 706

## РЕКОМЕНДАЦИИ ПО ЗАПОЛНЕНИЮ ОБРАЗЦА ФОРМЫ УВЕДОМЛЕНИЯ ОБ ОБРАБОТКЕ (О НАМЕРЕНИИ ОСУЩЕСТВЛЯТЬ ОБРАБОТКУ) ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Настоящие Рекомендации разработаны в целях установления единых принципов и порядка заполнения уведомления об обработке (о намерении осуществлять обработку) персональных данных (далее - Уведомление).

2. Уведомление оформляется на бланке Оператора (по форме, прилагаемой к настоящим Рекомендациям), осуществляющего обработку персональных данных (далее - Оператор), и направляется в территориальный орган Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее - территориальный орган Роскомнадзора).

3. Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом.

4. В поле «наименование (фамилия, имя, отчество), адрес Оператора» указывается:

4.1. Для юридических лиц (Операторов):

полное наименование с указанием организационно-правовой формы и сокращенное наименование юридического лица (Оператора), осуществляющего обработку персональных данных;  
наименование филиала (ов) (представительства (в) юридического лица (Оператора), осуществляющего обработку персональных данных; 1

1Для юридических лиц с филиальной структурой указывается список субъектов Российской Федерации (с указанием кода субъекта - согласно справочнику «Коды регионов», утвержденному приказом ФНС России от 13.10.2006 года № САЭ-3-04/706@ «Об утверждении формы сведений о доходах физических лиц» (зарегистрированным Министерством юстиции Российской Федерации 17.11.2000 г., регистрационный номер 8507), на территории которых находятся филиалы (представительства) юридического лица и (или) где оператором производится обработка персональных данных. Уведомление направляется юридическим лицом в соответствующее территориальное управление Роскомнадзора по месту своего нахождения с указанием всех имеющихся филиалов (представительств).

адрес Оператора2;  
индивидуальный номер налогоплательщика (ИНН).

4.2. Для физических лиц:  
фамилия, имя, отчество физического лица (Оператора);  
адрес Оператора3;  
данные документа, удостоверяющего личность, дата его выдачи, наименование органа, выдавшего документ;  
индивидуальный номер налогоплательщика (ИНН).

4.3. Для государственных, муниципальных органов (Операторов):  
полное и сокращенное наименование государственного, муниципального органа;  
наименование территориального(ых) органа(ов), осуществляющего(их) обработку персональных данных;  
адрес Оператора 4;  
индивидуальный номер налогоплательщика (ИНН).  
При указании наименования (фамилии, имени, отчества), адреса Оператора, а также направления деятельности рекомендуется использовать также ссылки на код(ы) классификаторов (ОКВЭД, ОКПО, ОКОГУ, ОКОП, ОКФС).

2Указывается место нахождения юридического лица в соответствии с учредительными документами и свидетельством о постановке юридического лица на учет в налоговом органе, почтовый адрес юридического лица, контактная информация.

Для организаций, учреждений, имеющих филиалы (представительства), указываются юридический и почтовый адреса (как юридического лица, так и его филиалов и представительств), где осуществляется непосредственная обработка персональных данных (все действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных). При этом, необходимо уточнить - обработка персональных данных осуществляется только юридическим лицом (формирование центральной информационной системы) и (или) филиалами (представительствами).

3Указывается место нахождения физического лица в соответствии со свидетельством о постановке на учет физического лица в налоговом органе, почтовый адрес физического лица, контактная информация.

4Указывается место нахождения государственного, муниципального органа в соответствии с учредительными документами и свидетельством о постановке юридического лица на учет в налоговом органе, почтовый адрес государственного, муниципального органа, контактная информация.

5. В поле «цель обработки персональных данных» указываются цели обработки персональных данных (а также их соответствие полномочиям Оператора) (Примечание № 1).

**Примечание № 1.***Под «целью обработки персональных данных» понимаются, как цели, указанные в учредительных документах Оператора, так и цели, фактически осуществляемой Оператором деятельности по обработке персональных данных.*

6. В поле «категории персональных данных» указываются все категории персональных данных, подлежащих обработке:

6.1. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (фамилия, имя, отчество, год, месяц, дата рождения, место рождения, адрес, семейное положение, социальное положение, имущественное положение, образование, профессия, доходы, другая информация, относящаяся к субъекту персональных данных).

6.2. Специальные категории персональных данных (расовая принадлежность, национальная принадлежность, политические взгляды, религиозные и философские убеждения, состояния здоровья, интимной жизни).

6.3. Биометрические персональные данные (сведения, которые характеризуют физиологические и биологические особенности человека, на основе которых можно установить его личность (биометрические персональные данные) и которые используются Оператором для установления личности субъекта персональных данных).

7. В поле «категории субъектов, персональные данные которых обрабатываются» указываются категории субъектов (физических лиц) и виды отношений с субъектами (физическими лицами), персональные данные которых обрабатываются (например: работники (субъекты), состоящие в трудовых отношениях с юридическим лицом (Оператором), физические лица (абонент, пассажир, заемщик, вкладчик, страхователь, заказчик и др.) (субъекты), состоящие в договорных и иных гражданско-правовых отношениях с юридическим лицом (Оператором) и др.).

8. В поле «правовое основание обработки персональных данных» указываются:

Федеральный закон, постановление Правительства Российской Федерации, иной нормативно-правовой акт, закрепляющий основание и порядок обработки персональных данных (Примечание № 2);

**Примечание № 2.***Указываются не только соответствующие статьи Федерального закона «О персональных данных», но и статьи иного нормативно-правового акта, регулирующие осуществляемый вид деятельности и касающиеся обработки персональных данных (например: ст.ст. 85-90 Трудового кодекса Российской Федерации, ст. 85.1 Воздушного кодекса Российской Федерации, ст. 12 Федерального закона «Об актах гражданского состояния» и др.).*

Номер, дату выдачи и наименование лицензии на осуществляемый вид деятельности, с указанием лицензионных условий, закрепляющих запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных (Примечание № 3).

**Примечание № 3.***Номер лицензии и пункт лицензионных условий, закрепляющий запрет на передачу персональных данных (или информации, касающейся физических лиц), отражается только при наличии лицензии и (или) соответствующего пункта лицензионных условий.*

9. В поле «перечень действий с персональными данными, общее описание используемых Оператором способов обработки персональных данных», указываются действия, совершаемые Оператором с персональными данными, а также описание используемых Оператором способов обработки персональных данных:

* неавтоматизированная обработка персональных данных;
* исключительно автоматизированная обработка персональных данных с передачей полученной информации по сети или без таковой;
* смешанная обработка персональных данных (Примечание № 4).

**Примечание № 4.***При автоматизированной обработке персональных данных либо смешанной обработке, необходимо указать, передается ли полученная в ходе обработки персональных данных информация по внутренней сети юридического лица (информация доступна лишь для строго определенных сотрудников юридического лица) либо информация передается с использованием сети общего пользования Интернет либо без передачи полученной информации.*

10. В поле «описание мер, предусмотренных статьями 18.1 и 19 Федерального закона «О персональных данных», указываются:

1. описание мер, предусмотренных ст.ст. 18.1 и 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
2. фамилия, имя, отчество физического лица или сотрудника юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;
3. класс информационной системы персональных данных Оператора (пункт 14 приказа ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»;
4. организационные и технические меры, применяемые для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных.

В случае использования Оператором, осуществляющим обработку персональных данных, шифровальных (криптографических) средств указываются следующие сведения:

1. наименование, регистрационные номера и производителей используемых криптографических средств;
2. уровень криптографической защиты персональных данных;
3. уровень специальной защиты от утечки по каналам побочных излучений и наводок;
4. уровень защиты от несанкционированного доступа.

Предоставление данной информации осуществляется в соответствии с Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденных руководством 8 Центра Федеральной службы безопасности Российской Федерации 21 февраля 2008 г. № 149/5-144.

11. В поле «сведения о наличии или об отсутствии трансграничной передачи персональных данных» указываются сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки с указанием перечня иностранных государств, на территорию которых осуществляется трансграничная передача персональных данных.

12. В поле «сведения об обеспечении безопасности персональных данных» указываются сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

13. В поле «дата начала обработки персональных данных» указывается конкретная дата (число, месяц, год) начала любого действия (операции) 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 (фактическая дата начала обработки персональных данных).

14. В поле «срок или условие прекращения обработки персональных данных» указывается конкретная дата (число, месяц, год) или основание (условие), наступление которого повлечет прекращение обработки персональных данных.

Приложение  
к Рекомендациям по заполнению  
образца формы уведомления об обработке  
(о намерении осуществлять обработку) персональных данных

Руководителю Управления Федеральной службы   
по надзору в сфере связи, информационных  
технологий и массовых коммуникаций   
по \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
(наименование территориального органа Роскомнадзора)

УВЕДОМЛЕНИЕ  
об обработке (о намерении осуществлять обработку) персональных данных

(полное и сокращенное наименования, фамилия, имя отчество)

(адрес местонахождения и почтовый адрес Оператора)

руководствуясь:

(правовое основание обработки персональных данных)

с целью:

(цель обработки персональных данных)

осуществляет обработку:

(категории персональных данных)

принадлежащих:

(категории субъектов, персональные данные которых обрабатываются)

Обработка вышеуказанных персональных данных будет осуществляться путем:

(перечень действий с персональными данными, общее описание используемых Оператором способов обработки персональных данных)

Для обеспечения безопасности персональных данных принимаются следующие меры:

(описание мер, предусмотренных ст.ст. 18.1. и 19 Федерального закона от 27.07.2006 № 152-ФЗ

«О персональных данных», в т.ч. сведения о наличии шифровальных (криптографических) средств и наименования этих средств; 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)

Сведения о наличии или об отсутствии трансграничной передачи персональных данных

при наличии трансграничной передачи персональных данных в процессе их обработки, указывается перечень иностранных государств, на территорию которых осуществляется трансграничная передача персональных данных)

Сведения об обеспечении безопасности персональных данных

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

Дата начала обработки персональных данных \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (число, месяц, год)

Срок или условие прекращение обработки персональных данных

(должность) (подпись) расшифровка подписи

«\_\_\_»\_\_\_\_\_\_\_\_\_\_20\_\_г.