Правительство Республики Ингушетия

ГIалгIай Республика Правительство

ПОСТАНОВЛЕНИЕ

«13» апреля 2017 г. № 61

г. Магас

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в органах государственной власти Республики Ингушетия и подведомственных им организациях

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» в целях обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в органах государственной власти Республики Ингушетия и подведомственных им организациях, Правительство Республики Ингушетия **постановляет:**

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в органах государственной власти Республики Ингушетия и подведомственных им организациях, согласно приложению к настоящему постановлению.

2. Исполнительным органам государственной власти Республики Ингушетия и подведомственным им организациям при определении угроз безопасности персональных данных, актуальных при обработке персональных данных в используемых ими информационных системах персональных данных, руководствоваться настоящим постановлением.

3. Рекомендовать органам местного самоуправления муниципальных образований Республики Ингушетия и подведомственным им организациям

руководствоваться настоящим постановлением при определении угроз безопасности персональных данных, актуальных при обработке персональных данных в используемых ими информационных системах персональных данных.

4. Контроль за исполнением настоящего постановления возложить на заместителя Председателя Правительства Республики Ингушетия, координирующего и контролирующего деятельность Комитета промышленности, транспорта, связи и энергетики Республики Ингушетии.

5. Настоящее постановление вступает в силу со дня его официального опубликования.

Председатель Правительства
Республики Ингушетия **Р. Гагиев**

Аппарат Правительства Республики Ингушетия ПРОТОКОЛЬНАЯ ЧАСТЬ

Приложение
к постановлению Правительства
Республики Ингушетия
от «13» апреля 2017 г. № 61

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в органах государственной власти Республики Ингушетия и подведомственных им организациях

1. Общие положения

1.1. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в органах государственной власти Республики Ингушетия и подведомственных им организациях (далее – Актуальные угрозы безопасности ИСПДн РИ), разработаны в соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152).

1.2. Актуальные угрозы безопасности ИСПДн РИ содержат перечень актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее – ИСПДн) в органах государственной власти Республики Ингушетия и подведомственных им организациях (далее – государственные органы).

1.3. При разработке Актуальных угроз безопасности ИСПДн РИ использованы нормативные правовые акты, методические документы, модели угроз безопасности персональных данных, указанные в разделе 5 Актуальных угроз безопасности ИСПДн РИ.

1.4. Угрозы безопасности персональных данных, обрабатываемых в ИСПДн, приведенные в Актуальных угрозах безопасности ИСПДн РИ, подлежат адаптации в ходе разработки частных моделей угроз безопасности персональных данных.

При разработке частных моделей угроз безопасности персональных данных проводится анализ структурно-функциональных характеристик конкретной ИСПДн, применяемых в ней информационных технологий и особенностей её функционирования. По результатам анализа делается вывод об отнесении ИСПДн к одному из видов ИСПДн, приведенных в пункте 1.6 Актуальных угроз безопасности ИСПДн РИ.

В частной модели угроз безопасности персональных данных указываются:

- описание ИСПДн и её структурно-функциональных характеристик;

- описание угроз безопасности персональных данных с учетом совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Типовая форма частной модели угроз безопасности информации для государственных органов разрабатывается Комитетом промышленности, транспорта, связи и энергетики Республики Ингушетия с учетом требований приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и приказа Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (далее – Приказ ФСБ России № 378).

1.5. Актуальные угрозы безопасности персональных данных, обрабатываемых в ИСПДн, содержащиеся в Актуальных угрозах безопасности ИСПДн РИ, уточняются и дополняются по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности персональных данных в ИСПДн. Указанные изменения согласовываются с Федеральной службой по техническому и экспортному контролю (далее – ФСТЭК России) и Федеральной службой безопасности Российской Федерации (далее – ФСБ России) в установленном порядке.

1.6. В государственных органах создаются и эксплуатируются информационные системы, в которых могут обрабатываться персональные данные. В зависимости от предназначения такие информационные системы подразделяются на:

- ИСПДн обеспечения типовой деятельности – информационные системы, предназначенные для автоматизации обеспечивающей деятельности государственных органов в рамках исполнения ими типовых полномочий, предусмотренных нормативными правовыми актами, за исключением специфических полномочий, автоматизация или информационная поддержка которых предусмотрена информационными системами специальной деятельности. К ИСПДн обеспечения типовой деятельности можно отнести локальные ИСПДн:

ИСПДн управления персоналом, ИСПДн управления финансами, ИСПДн документооборота, ИСПДн информационного обеспечения деятельности и другие;

- ИСПДн обеспечения специальной деятельности – государственные информационные системы Республики Ингушетия, предназначенные для автоматизации либо информационной поддержки предоставления государственных услуг и исполнения государственных функций, предусмотренных в нормативных правовых актах Республики Ингушетия в качестве полномочий конкретного государственного органа, а также исполняемых им функций. К ИСПДн обеспечения специальной деятельности относятся: ИСПДн региональной системы межведомственного электронного взаимодействия Республики Ингушетия, ИСПДн государственной информационной системы Республики Ингушетия «Народный контроль», ИСПДн единой региональной автоматизированной информационной системы поддержки деятельности многофункциональных центров предоставления государственных и муниципальных услуг в Республике Ингушетия, ИСПДн по направлениям деятельности государственных органов, исполняемым функциям, предоставлению услуг (например, государственные информационные системы Республики Ингушетия в социальной сфере, сферах здравоохранения, образования, ЖКХ и других).

2. ИСПДн обеспечения типовой деятельности

2.1. ИСПДн обеспечения типовой деятельности органов государственной власти характеризуются тем, что в качестве объектов информатизации выступают автономные автоматизированные рабочие места или рабочие места локальных вычислительных сетей, имеющих или не имеющих подключения к сетям общего пользования и (или) сетям международного информационного обмена.

Ввод персональных данных осуществляется как с бумажных носителей, так и с электронных носителей информации. Персональные данные субъектов могут выводиться из ИСПДн с целью передачи персональных данных третьим лицам в предусмотренных Федеральным законом № 152 случаях как в электронном, так и в бумажном виде.

Информационный обмен по сетям связи общего пользования и (или) сетям международного информационного обмена осуществляется с использованием сертифицированных средств криптографической защиты информации (далее – СКЗИ).

Контролируемой зоной ИСПДн являются здания и отдельные помещения. В пределах контролируемой зоны находятся рабочие места пользователей, серверы системы, сетевое и телекоммуникационное оборудование ИСПДн. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное

оборудование, используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

2.2. ИСПДн управления персоналом предназначены для персонального кадрового учета, управления кадровым резервом, проведения аттестации, повышения квалификации и для других целей, связанных с управлением персоналом.

В ИСПДн управления персоналом обрабатывается обязательный перечень информации, имеющей характер персональных данных сотрудников государственного органа, граждан, подавших сведения для участия в конкурсе на замещение вакантных должностей государственной гражданской службы и для включения в кадровый резерв, а также граждан, претендующих на замещение иных должностей в государственном органе (фамилия, имя, отчество; дата и место рождения; адрес; паспортные данные; сведения для заполнения личного дела; личные карточки работников формы № Т-2; сведения из трудовой книжки; дополнительный перечень информации, имеющей характер персональных данных сотрудников).

2.3. ИСПДн управления финансами предназначены для обработки персональных данных, необходимых для бухгалтерского и управленческого финансового учета, предоставления информации в пенсионные и налоговые органы, систему обязательного медицинского страхования.

В ИСПДн управления финансами обрабатываются фамилия, имя, отчество, дата и место рождения, паспортные данные, адрес, номер телефона, идентификационный номер налогоплательщика (далее – ИНН), страховой номер индивидуального лицевого счета, табельный номер, должность, номер приказа и дата приема на работу (увольнения), номер лицевого счёта для перечисления денежного содержания и иных выплат работнику; фамилия, имя, отчество, паспортные данные, адрес, должность, номер телефона (либо иной вид связи), ИНН, платежные реквизиты граждан, являющихся стороной гражданско-правовых договоров.

2.4. ИСПДн документооборота предназначены для автоматизации делопроизводства, служебной переписки, архивной деятельности, учета корреспонденции, обращений граждан, обеспечения доступа к электронным документам.

В ИСПДн документооборота обрабатываются фамилия, имя, отчество, должность, контактные данные (адрес, электронный адрес, номер телефона), информация в документах, имеющая характер персональных данных.

2.5. ИСПДн информационного обеспечения предназначены для автоматизации деятельности органов государственной власти.

В ИСПДн информационного обеспечения деятельности обрабатываются персональные данные, содержащиеся в адресных и телефонных справочниках, иных базах данных, содержащих персональные данные.

3. ИСПДн обеспечения специальной деятельности

3.1. ИСПДн обеспечения специальной деятельности государственных органов характеризуются тем, что в качестве объектов информатизации выступают распределенные информационные системы и локальные информационные системы, подключенные к сетям общего пользования и (или) сетям международного информационного обмена.

Ввод персональных данных осуществляется как с бумажных носителей, так и с электронных носителей информации. Персональные данные субъектов персональных данных обрабатываются с целью получения государственных и муниципальных услуг и могут выводиться из ИСПДн как в электронном, так и в бумажном виде.

Информационный обмен по сетям связи общего пользования и (или) сетям международного информационного обмена осуществляется с использованием сертифицированных СКЗИ.

Контролируемой зоной ИСПДн являются здания и отдельные помещения. В пределах контролируемой зоны находятся рабочие места пользователей, серверы системы, сетевое и телекоммуникационное оборудование ИСПДн. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

3.2. ИСПДн региональной системы межведомственного электронного взаимодействия Республики Ингушетия в соответствии с постановлением Правительства Республики Ингушетия от 4 июня 2014 г. № 105 «О региональной системе межведомственного электронного взаимодействия Республики Ингушетия» предназначена для технологического обеспечения на территории Республики Ингушетия исполнения государственных и муниципальных функций в электронной форме, предоставления государственных и муниципальных услуг в электронной форме, информационного взаимодействия в электронной форме при предоставлении государственных и муниципальных услуг и исполнении государственных и муниципальных функций.

С использованием ИСПДн обрабатываются (передаются) персональные данные заявителей, необходимые для предоставления государственных и муниципальных услуг и получаемые в рамках межведомственного

информационного взаимодействия, в том числе из базовых государственных информационных ресурсов, в соответствии с действующим законодательством.

3.3. ИСПДн государственной информационной системы Республики Ингушетия «Народный контроль» в соответствии с Указом Главы Республики Ингушетия от 1 декабря 2012 г. № 242 «О государственной информационной системе Республики Ингушетия «Народный контроль» и постановлением Правительства Республики Ингушетия от 27 декабря 2012 г. № 287 «О порядке эксплуатации государственной информационной системы Республики Ингушетия «Народный контроль» предназначена для обеспечения информационного взаимодействия между гражданами, исполнительными органами государственной власти Республики Ингушетия и органами местного самоуправления Республики Ингушетия с использованием информационно-телекоммуникационной системы «Интернет» и обеспечения учета мнения граждан при совершенствовании деятельности исполнительных органов государственной власти и органов местного самоуправления Республики Ингушетия.

С использованием ИСПДн обрабатываются (передаются) персональные данные заявителей, необходимые для обеспечения информационного взаимодействия между гражданами, исполнительными органами государственной власти Республики Ингушетия и органами местного самоуправления Республики Ингушетия и совершенствования деятельности исполнительных органов государственной власти и органов местного самоуправления Республики Ингушетия с учетом мнения граждан.

3.4. ИСПДн единой региональной автоматизированной информационной системы поддержки деятельности многофункциональных центров предоставления государственных и муниципальных услуг в Республике Ингушетия предназначена для обеспечения деятельности многофункциональных центров на территории Республики Ингушетия.

В ИСПДн обрабатываются персональные данные, предоставляемые заявителями при запросе, получаемые из базовых государственных информационных ресурсов, от органов и учреждений, используемые для подготовки ответов на запрос заявителя в соответствии с административными регламентами предоставления государственных и муниципальных услуг, утвержденными нормативными правовыми актами соответствующего органа.

3.5. ИСПДн по направлениям деятельности государственных органов, исполняемым функциям предназначены для обеспечения деятельности государственных органов и исполнения функций, не отраженных в пунктах 3.2 – 3.4 Актуальных угроз безопасности ИСПДн РИ.

В ИСПДн обрабатываются персональные данные, необходимые для выполнения деятельности государственных органов, исполнения функций и предоставления услуг, определенных в нормативных правовых актах.

4. Актуальные угрозы безопасности информационных систем персональных данных

4.1. Угрозы безопасности персональных данных рассмотрены в приказах и методических документах ФСТЭК России и Приказе ФСБ России № 378.

Учитывая особенности обработки персональных данных в государственных органах, а также категорию и объем обрабатываемых в ИСПДн персональных данных, основными характеристиками безопасности являются конфиденциальность, целостность и доступность.

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

Целостность – состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность информации при попытках несанкционированных воздействий на нее в процессе обработки или хранения.

Доступность – состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

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 безопасности персональных данных, актуальные при обработке персональных данных в ИСПДн, подразделяются на угрозы первого, второго, третьего типа.

Для определения актуальных угроз безопасности из общего перечня угроз безопасности выбираются только те угрозы, которые являются актуальными для ИСПДн в соответствии с Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной ФСТЭК России 14 февраля 2008 года.

Основная часть угроз безопасности персональных данных в ИСПДн государственных органов относится к 3 типу, уровень защищенности ИСПДн

государственных органов не выше 3 уровня защищенности (за исключением информационных систем, обрабатывающих специальные категории персональных данных регионального масштаба).

Основной целью применения в ИСПДн государственных органов СКЗИ является защита персональных данных при информационном обмене по сетям связи общего пользования и (или) сетям международного информационного обмена.

Основными видами угроз безопасности персональным данным в ИСПДн являются:

- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к информационным ресурсам ИСПДн, включая пользователей ИСПДн;

- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;

- угрозы, возникновение которых напрямую зависит от свойств техники и программного обеспечения, используемого в ИСПДн;

- угрозы, возникающие в результате внедрения аппаратных закладок и вредоносных программ;

- угрозы, направленные на нарушение нормальной работы технических средств и средств связи, используемых в ИСПДн;

- угрозы, связанные с недостаточной квалификацией обслуживающего ИСПДн персонала.

При определении актуальных угроз безопасности персональных данных используются следующие положения:

- при создании государственных информационных систем Республики Ингушетия государственные органы руководствуются Положением о координации мероприятий в сфере информатизации в Республике Ингушетия, утвержденным постановлением Правительства Республики Ингушетия от 3 марта 2015 г. № 41 «О координации мероприятий в сфере информатизации в Республике Ингушетия»;

- единый подход к созданию, развитию (модернизации) и эксплуатации государственных информационных систем Республики Ингушетия, основанный на согласовании технологий обработки информации с органом исполнительной власти Республики Ингушетия, уполномоченным на осуществление деятельности в сфере информационных технологий;

- реализация единого порядка согласования технических заданий и технических проектов на создание информационных систем и входящих в их состав систем защиты информации с использованием некриптографических средств защиты информации (далее – СЗИ) и (или) с использованием СКЗИ.

4.2. Актуальные угрозы безопасности ИСПДн обеспечения типовой деятельности.

4.2.1. ИСПДн обеспечения типовой деятельности отличаются следующими особенностями:

- использование стандартных (унифицированных) технических средств обработки информации;

- использование типового программного обеспечения;

- наличие незначительного количества автоматизированных рабочих мест, участвующих в обработке персональных данных;

- дублирование информации, содержащей персональные данные, на бумажных носителях и внешних накопителях информации;

- незначительные негативные последствия для субъектов персональных данных при реализации угроз безопасности ИСПДн;

- эксплуатация ИСПДн (как правило) сотрудниками государственных органов без привлечения на постоянной основе сторонних организаций;

- жесткая регламентация процедуры взаимодействия со сторонними организациями (банки, пенсионные, страховые и налоговые органы, органы статистики).

4.2.2. Актуальными угрозами безопасности ИСПДн обеспечения типовой деятельности в государственных органах, учитывая положения, изложенные в настоящем разделе, признаются:

- угрозы непреднамеренного или преднамеренного вывода из строя технических средств и СЗИ;

- угрозы несанкционированного отключения СЗИ;

- угрозы, связанные с недостаточной квалификацией обслуживающего ИСПДн персонала;

- угрозы надежности технических средств и коммуникационного оборудования;

- угрозы легитимности программного обеспечения;

- угрозы достаточности и качества применяемых СЗИ и средств антивирусной защиты;

- угрозы создания способов, подготовки и проведения атак без привлечения специалистов в области разработки и анализа СКЗИ;

- угрозы создания способов, подготовки и проведения атак на различных этапах жизненного цикла СКЗИ;

- угрозы проведения атак с нахождением за пределами контролируемой зоны;

- угрозы получения из находящихся в свободном доступе источников, включая сети общего пользования и сети международного информационного обмена, информации об информационной системе, в которой используется СКЗИ;

- угрозы применения находящихся в свободном доступе или используемых за пределами контролируемой зоны аппаратных средств (далее – АС) и программного обеспечения (далее – ПО), включая аппаратные и программные компоненты СКЗИ и среду функционирования СКЗИ (далее – СФ), специально разработанных АС и ПО;

- угрозы проведения на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети;

- угрозы использования на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ штатных средств;

- угрозы проведения атаки при нахождении в пределах контролируемой зоны.

4.3. Актуальные угрозы безопасности ИСПДн обеспечения специальной деятельности.

4.3.1. ИСПДн обеспечения специальной деятельности отличаются следующими особенностями:

- использование широкой номенклатуры (зачастую уникальных) технических средств получения, отображения и обработки информации;

- использование специального (адаптированного под конкретную задачу) программного обеспечения;

- наличие значительного количества автоматизированных рабочих мест, участвующих в обработке персональных данных;

- построение ИСПДн на базе распределенной по территории республики вычислительной сети со сложной архитектурой;

- наличие выходов в сети общего пользования и (или) сети международного информационного обмена, локальные вычислительные сети сторонних организаций;

- использование разнообразной телекоммуникационной среды, принадлежащей различным операторам связи;

- широкое применение СЗИ, сертифицированных СКЗИ при информационном обмене по сетям связи общего пользования и (или) сетям международного информационного обмена;

- использование аутсорсинга при создании и эксплуатации ИСПДн и ее элементов;

- сложность дублирования больших массивов информации, содержащей персональные данные, на бумажных носителях и внешних накопителях информации;

- значительные негативные последствия при реализации угроз безопасности ИСПДн;

- риск недостаточной квалификации пользователей и обслуживающего ИСПДн и СЗИ персонала;

- проблемы взаимодействия различных ИСПДн, вызванные несовершенством действующего законодательства и ведомственных инструкций.

4.3.2. Актуальными угрозами безопасности ИСПДн обеспечения специальной деятельности в государственных органах, учитывая положения, изложенные в настоящем разделе, признаются:

- угрозы непреднамеренного или преднамеренного вывода из строя технических средств и СЗИ;

- угрозы несанкционированного отключения СЗИ;

- угрозы, связанные с недостаточной квалификацией обслуживающего ИСПДн персонала;

- угрозы надежности технических средств и коммуникационного оборудования;

- угрозы легитимности программного обеспечения;

- угрозы достаточности и качества применяемых СЗИ и средств антивирусной защиты;

- угрозы совершения атак на монитор виртуальных машин из физической сети;

- угрозы совершения атаки с виртуальной машины на другую виртуальную машину;

- угрозы совершения атаки на систему управления виртуальной инфраструктурой;

- угрозы создания способов, подготовки и проведения атак без привлечения специалистов в области разработки и анализа СКЗИ;

- угрозы создания способов, подготовки и проведения атак на различных этапах жизненного цикла СКЗИ;

- угрозы проведения атак с нахождением за пределами контролируемой зоны;

- угрозы получения из находящихся в свободном доступе источников, включая сеть «Интернет», информации об информационной системе, в которой используется СКЗИ;

- угрозы применения находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ, специально разработанных АС и ПО;

- угрозы проведения на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети;

- угрозы использования на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ штатных средств;

- угрозы проведения атаки при нахождении в пределах контролируемой зоны.

5. Нормативные правовые акты и методические документы, использованные при разработке Актуальных угроз безопасности ИСПДн РИ

1. Федеральный закон № 152-ФЗ;

2. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

3. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

4. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

5. Приказ ФСБ России № 378;

6. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК России 14 февраля 2008 г.

7. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК России 15 февраля 2008 г.;

8. Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и

занятости, утвержденные Министерством здравоохранения и социального развития Российской Федерации 23 декабря 2009 г.;

9. Указ Главы Республики Ингушетия от 1 декабря 2012 г. № 242 «О государственной информационной системе Республики Ингушетия «Народный контроль»;

10. Постановление Правительства Республики Ингушетия от 27 декабря 2012 г. № 287 «О порядке эксплуатации государственной информационной системы Республики Ингушетия «Народный контроль»;

11. Постановление Правительства Республики Ингушетия от 4 июня 2014 г. № 105 «О региональной системе межведомственного электронного взаимодействия Республики Ингушетия»;

12. Постановление Правительства Республики Ингушетия от 3 марта 2015 г. № 41 «О координации мероприятий в сфере информатизации в Республике Ингушетия».