Тамбовское областное государственное бюджетное учреждение «Телевизионная и радиовещательная компания «Тамбовская губерния»

ПРИКАЗ

г. Тамбов

21 июля 2021 г. №35- о/д

Об утверждении документов, определяющих политику в отношении обработки и защиты персональных данных

В целях обеспечения защиты персональных данных Тамбовского областного бюджетного учреждения «Телевизионная и радиовещательная компания «Тамбовская губерния» (далее - ТОГБУ «ТРК «Тамбовская губерния»), в соответствии с требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

ПРИКАЗЫВАЮ:

1. Утвердить:

1.1. Положение о защите, хранении, обработке и передаче персональных данных работников ТОГБУ «ТРК «Тамбовская губерния» согласно приложению № 1;

1.2. Положение о порядке организации и проведения работ по обеспечению безопасности персональных данных в информационной системе ТОГБУ «ТРК «Тамбовская губерния» согласно приложению №2.

2. Начальникам отделов ТОГБУ «ТРК «Тамбовская губерния» обеспечить ознакомление сотрудников, имеющих доступ к персональным данным с настоящими положениями под роспись.

3. Разместить положения, утвержденные в п.1 настоящего приказа, на официальном сайте ТОГБУ «ТРК «Тамбовская губерния» по адресу https://togbutrktg.ru/.

4. Контроль за исполнением данного приказа возложить на заместителя генерального директора Рылееву Л.В.

Генеральный директор
ТОГБУ «ТРК «Тамбовская губерния» О.В. Муравьёва

С приказом ознакомлены: Л.В. Рылеева

ПРИЛОЖЕНИЕ № 1
УТВЕРЖДЕНО
приказом генерального директора
ТОГБУ «ТРК «Тамбовская губерния»
№35-о/д от «21» июля 2021г.

Положение о защите, хранении, обработке и передаче персональных данных работников ТОГБУ «ТРК «Тамбовская губерния»

1. Общие положения

1.1. Настоящее Положение об обработке персональных данных в ТОГБУ «ТРК «Тамбовская губерния» (далее - Положение) регламентируются Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и другими НПА.

1.2. Настоящее Положение определяет основные вопросы, связанные с обработкой персональных данных в ТОГБУ «ТРК «Тамбовская губерния» (далее - Оператор) 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.

1.3. Действие настоящего Положения не распространяется на отношения, возникающие при:

- организации хранения, комплектования, учета и использования содержащих персональные данные архивных документов в соответствии с законодательством об архивном деле в Российской Федерации:
- обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

1.4. Целью настоящего Положения 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.

2. Основные понятия

В настоящем положении используются следующие основные понятия:

- **персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

- 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;

- **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;

- **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

- **распространение персональных данных** — действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

- **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

- **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

- **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;

- **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

- **информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

- **трансграничная передача персональных данных** – передача персональных данных на территории иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

- **угрозы безопасности персональных данных** – 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;

- **уровень защищенности персональных данных** – комплексный показатель, характеризующий требования, исполнение которых обеспечивает

нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

3. Автоматизированная обработка персональных данных

3.1. Принципы обработки персональных данных

3.1.1. Обработка персональных данных осуществляется Оператором в соответствии со следующими принципами:

- обработка персональных данных должна осуществляться на законной и справедливой основе;
- обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей:
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, не совместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки;
- 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;
- 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.

3.2. Условия обработки персональных данных

3.2.1. Обработка персональных данных допускается в следующих случаях:

- обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных настоящим Положением;
- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;
- 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;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- 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;

- обработка персональных данных осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных;

- осуществляется обработка персональных данных, доступ неограниченного круга лиц, к которым предоставлен субъектом персональных данных либо по его просьбе;

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

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

3.2.3. Лицо, осуществляющее обработку персональных данных по поручению Оператора, несет ответственность перед Оператором.

3.3. Конфиденциальность персональных данных:

3.3.1. Оператор 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.

3.4. Общедоступные источники персональных данных:

3.4.1. 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.

3.5. Права субъектов персональных данных

3.5.1.Согласие субъекта персональных данных на обработку его персональных данных

3.5.1.1. 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.

3.5.1.2. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

- 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);

- наименование или фамилию, имя, отчество и адрес Оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Оператором способов обработки персональных данных;
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись субъекта персональных данных.

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

3.5.2. Право субъекта персональных данных на доступ к его персональным данным

3.5.2.1. 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.

3.5.2.2. Сведения 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.

3.5.2.3. Сведения 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.

3.5.2.4. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.

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

- подтверждение факта обработки персональных данных Оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Оператором способы обработки персональных данных;
- 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;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу.

3.5.2.6. Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» 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.

3.5.2.7. 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.

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

3.5.3.1. 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, Оператором не осуществляется.

3.5.4. Право на обжалование действий или бездействия Оператора

3.5.4.1. Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» 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.

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.

3.6. Обязанности Оператора

3.6.1. Оператор обязан принимать меры, необходимые и достаточные для

обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом «О персональных данных» или другими федеральными законами. К таким мерам могут, в частности, относиться:

- назначение Оператором ответственного за организацию обработки персональных данных;
- издание Оператором 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;
- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;
- 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;
- оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», соотношение указанного вреда и принимаемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;
- 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.

3.6.2. 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.

3.6.3. Правительство Российской Федерации устанавливает перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами.

3.6.4. 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.

3.6.5. Обеспечение безопасности персональных данных достигается, в частности:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- 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;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учетом машинных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- 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;
- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

3.6.6. 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 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.

3.6.7. 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.

3.6.8. 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.

3.6.9. 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.

3.6.10. 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.

3.6.11. 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.

3.6.12. 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 Федеральным законом «О персональных данных» или другими федеральными законами.

3.6.13. 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 Федеральным законом «О персональных данных» или другими федеральными законами.

3.6.14. В случае отсутствия возможности уничтожения персональных данных в течение срока, 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.

3.6.15. Оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа организации, являющейся Оператором, и подотчетно ему.

3.6.16. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

- осуществлять внутренний контроль за соблюдением Оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения работников Оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- 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.

4. Обработка персональных данных, осуществляемая без использования средств автоматизации

4.1. Общие положения

4.1.1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, 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.

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

4.2.1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, обособляются 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).

4.2.2. 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 используется отдельный материальный носитель.

4.2.3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники Оператора или лица, осуществляющие такую обработку по договору с Оператором), 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 Оператора.

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

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) содержат 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;

- типовая форма предусматривает 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;

- типовая форма составляется 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;

- типовая форма исключает объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

4.2.5. 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, принимаются меры по обеспечению раздельной обработки персональных данных, в частности:

- 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;

- 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.

4.2.6. 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). Указанные правила применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

4.2.7. 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.

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

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

4.3.2. Обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей соблюдаются 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.

5. Сферы ответственности

5.1. Лица, ответственные за организацию обработки персональных данных в организациях

5.1.1. Оператор назначает лицо, ответственное за организацию обработки персональных данных.

5.1.2. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа организации, являющейся Оператором, и подотчетно ему.

5.1.3. Оператор предоставляет лицу, ответственному за организацию обработки персональных данных, необходимые сведения.

5.1.4. Лицо, ответственное за организацию обработки персональных данных, в частности, выполняет следующие функции:

- осуществляет внутренний контроль за соблюдением Оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводит до сведения работников Оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организовывает прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществляет контроль за приемом и обработкой таких обращений и запросов.

5.2. Ответственность за нарушение требований Федерального закона «О персональных данных»

5.2.1. Лица, виновные в нарушении требований Федерального закона «О персональных данных», несут предусмотренную законодательством Российской Федерации ответственность.

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

ПРИЛОЖЕНИЕ № 2
УТВЕРЖДЕНО
приказом генерального директора
ТОГБУ «ТРК «Тамбовская губерния»
№35-о/д от «21» июля 2021г.

Положение
о порядке организации и проведения работ по обеспечению безопасности персональных данных в информационной системе
ТОГБУ «ТРК «Тамбовская губерния»

1. Общие положения

1.1. Настоящее Положение о порядке организации и проведения работ по обеспечению безопасности персональных данных в информационной системе ТОГБУ «ТРК «Тамбовская губерния» (далее - Положение) устанавливает порядок организации и проведения работ по защите информации, содержащей персональные данные, на объектах информатизации ТОГБУ «ТРК «Тамбовская губерния» (далее – Учреждение) как в период их создания, так и в процессе повседневной эксплуатации.

1.2. Настоящее Положение определяет:

- перечень мероприятий по защите персональных данных;
- порядок резервирования и восстановления работоспособности технических средств и программного обеспечения баз данных и средств защиты информации;
- порядок контроля защиты персональных данных, обучения персонала практике работы в информационной системе (далее - ИС);
- правила антивирусной и парольной защиты, обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИС;
- порядок контроля соблюдения условий использования средств защиты информации;
- порядок проверки электронного журнала обращений к ресурсам информационной системы;
- порядок охраны и допуска посторонних лиц в помещения ИС.

1.3. Требования настоящего Положения являются обязательными для исполнения структурными подразделениями Учреждения, в которых обрабатываются персональные данные, а также структурными подразделениями Учреждения, организациями, учреждениями и предприятиями, выполняющими работы по защите персональных данных в Учреждение.

2. Термины и сокращения

В настоящем документе используются следующие термины и сокращения:

- **персональные данные (ПДн)** - любая информация, относящаяся к определённому 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;
- **информационная система (ИС)** - совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения различных задач;
- **информационная система персональных данных (ИСПДн)** - совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации;

- **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;

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

- **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;

- пользователь ИС - лицо (сотрудник Учреждения), участвующее в функционировании ИС или использующее результаты её функционирования;

- **криптосредства** - криптографические (шифровальные) средства для обеспечения безопасности персональных данных;

- **пользователь криптосредства** - пользователь ИС, использующий при обработке (передаче) персональных данных криптосредство;

- **инсайдер** - любое лицо, потенциально имеющее доступ к конфиденциальной информации (например, персональным данным) в силу служебного положения или родственных связей;

- **угрозы безопасности персональных данных** – 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;

- **несанкционированный доступ (несанкционированные действия) (НСД)** - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных;

- **объект информатизации** - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений и объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров;

- **система защиты информации** - проводимые мероприятия по защите информации и средства защиты информации (в том числе криптографические, средства защиты от несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства и системы), а также используемые информационные технологии;

- **аттестация объектов информатизации** – комплекс организационных и технических мероприятий, в результате которых подтверждается соответствие системы защиты информации объекта информатизации требованиям безопасности информации;

- **контролируемая зона (КЗ)** — пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание сторонних лиц, а также транспортных, технических и иных материальных средств;

- **основные технические средства и системы (ОТСС)** – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации;

- **вспомогательные технические средства и системы (ВТСС)** - технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях;

- **технический канал утечки информации** — совокупность носителей информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

3. Нормативно-методическая документация

При организации и проведении работ по обеспечению безопасности ПДн необходимо руководствоваться следующими нормативными и методическими документами:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановление Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
- приказ ФСТЭК от 11 февраля 2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- постановление Правительства Российской Федерации от 1.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСТЭК от 5.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;
- Указ Президента от 6.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;
- нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР- К)» (утв. приказом Гостехкомиссии России от 30 августа 2002 № 282);
- приказ ФСБ России от 10.07.2014 № 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»;
- руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением председателя Гостехкомиссии России от 30.03.1992).

4. Порядок организации и проведения работ по обеспечению безопасности персональных данных при их обработке в ИС

- Под организацией обеспечения безопасности персональных данных при их обработке в ИС понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности персональных данных.

Обеспечение безопасности персональных данных осуществляется путём выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой системы защиты персональных данных, направленных на минимизацию ущерба от возможной реализации угроз безопасности персональных данных.

5. Организационные мероприятия

Организационные мероприятия по защите персональных данных включают в себя:

- Определение перечня персональных данных, обрабатываемых в ИС
- Устанавливается наличие и состав персональных данных, которые обрабатываются в Управлении.
- Определение целей обработки персональных данных
- Обработка персональных данных осуществляется Учреждением в следующих целях:
- организация кадрового учета Учреждения для обеспечения соблюдения требований действующих нормативно-правовых актов;
- учет представителей юридических лиц и индивидуальных предпринимателей, участвующих в процессе лицензирования деятельности в сфере телевидения и радиовещания.
- Определение сроков обработки и хранения персональных данных
- Хранение персональных данных должно осуществляться не дольше, чем этого требуют цели их обработки, по достижении которых персональные данные подлежат уничтожению.

По результатам анализа информации, обрабатываемой в Управлении, и реализации мероприятий, указанных в п.п. 4.1.1-4.1.3:

- определяется уровень защищенности персональных данных, обрабатываемых в информационной системе Учреждения, в соответствии с требованиями постановления Правительства Российской Федерации от 1.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- осуществляется классификация ИС в соответствии с требованиями приказа ФСТЭК от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся вгосударственных информационных системах»;
- осуществляется классификация автоматизированных систем, обрабатывающих персональные данные, в соответствии с требованиями СТР- К и руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением председателя Гостехкомиссии России от 30.03.1992).
- Определение ответственных за обеспечение безопасности персональных данных

- Ответственный за организацию обработки ПДн, ответственный за обеспечение безопасности ПДн и администратор безопасности ИС определяются приказом начальника Учреждения.

- Ответственный за организацию обработки ПДн определяет цели, содержание и порядок обработки ПДн в Управлении, а также организовывает и контролирует осуществление мероприятий по обеспечению безопасности ПДн при их обработке в ИС, координирует работу ответственного за обеспечение безопасности ПДн и администратора безопасности ИС в Управлении.

- Ответственный за обеспечение безопасности ПДн разрабатывает и осуществляет мероприятия по обеспечению безопасности ПДн при их обработке в ИС.

Задачи, функции, обязанности, права и ответственность администратора безопасности ИС определяются данным Положением, а также инструкцией администратора безопасности ИС.

- Определение круга лиц, допущенных к обработке персональных данных

- Руководителями структурных подразделений Учреждения составляется перечень сотрудников, доступ которых к обрабатываемым в ИС персональным данным необходим для выполнения ими служебных (трудовых) обязанностей. Перечень лиц, допущенных к обработке персональных данных, утверждается начальником Учреждения.

- К обработке персональных данных допускаются сотрудники Учреждения, подготовленные к работе с информацией, требующей защиты (пользователи ИС).

- Ответственным за обеспечение безопасности ПДн разрабатывается разрешительная система доступа данных пользователей к информационным ресурсам ИС.

- Права доступа администратору безопасности ИС и пользователям ИС оформляются в виде «Матрицы разграничения доступа к защищаемым ресурсам автоматизированной системы...».

- Организация доступа в помещения, где осуществляется обработка персональных данных

- Необходимо исключить возможность несанкционированного доступа и пребывания в помещениях, где обрабатываются персональные данные, а также к техническим средствам обработки персональных данных, хищения и нарушения работоспособности технических средств обработки персональных данных, хищения носителей информации.

- Порядок охраны помещений ИС, доступа в эти помещения определяется «Порядком доступа в помещения ТОГБУ «ТРК «Тамбовская губерния», в которых ведется обработка персональных данных».

5.1. Обучение сотрудников

- Не реже одного раза в год необходимо проводить обучение пользователей ИС правилам обработки персональных данных в соответствии с действующим законодательством, а также правилам работы со средствами защиты информации, применяемыми в ИС, в соответствии с документацией (инструкции, руководства и т.п.), прилагаемой к таким средствам защиты информации.

- Обучение может проводиться в форме совещаний, обучающих занятий, семинаров, инструктажей, методической помощи и практических занятий на месте. Обучение может проводиться в ходе периодических (плановых) и внеплановых проверок условий обработки персональных данных в ИС на местах.

Первичные инструктажи проводятся с пользователями ИС:

- после проведения аттестационных испытаний ИС и получения Аттестата соответствия по требованиям безопасности ИС;

- при поступлении на работу сотрудника в структурное подразделение Учреждения, в котором происходит обработка персональных данных в ИС.

Ответственным за организацию обучения и оказание методической помощи пользователям ИС в Управлении является ответственный за обеспечение безопасности ПДн.

Для проведения обучающих мероприятий могут привлекаться администратор безопасности ИС, специалисты по программному и техническому обеспечению, а также специалисты органов по аттестации объектов ИС.

К работе в ИС допускаются только сотрудники, прошедшие первичный инструктаж обеспечения безопасности персональных данных в ИС и показавшие твёрдые теоретические знания и практические навыки.

В целях изучения практических вопросов обеспечения безопасности в реально действующих информационных системах и ознакомления с новыми решениями в области информационной безопасности ответственный за обеспечение безопасности ПДн, администратор безопасности ИС и другие специалисты, обеспечивающие безопасность персональных данных, должны периодически проходить курсы повышения квалификации (переподготовки) в области информационной безопасности.

Кроме того, данные сотрудники должны самостоятельно изучать необходимые для работы документы, а также современные средства защиты информации.

Установление персональной ответственности за нарушения правил обработки персональных данных

В должностные инструкции пользователей ИС должны быть внесены дополнения в части персональной ответственности за нарушение правил обработки персональных данных.

Учёт применяемых технических средств защиты персональных данных

При выборе технических (аппаратных, программных и программно-аппаратных) средств защиты следует использовать сертифицированные средства защиты информации. Перечень используемых средств защиты с указанием их заводского номера, сведений о сертификате соответствия, месте и дате установки приводится в Техническом паспорте автоматизированной системы.

5.2. Учёт носителей персональных данных

В обязательном порядке должен быть организован учёт всех защищаемых носителей персональных данных с помощью их маркировки и с занесением учётных данных в Журнал учета машинных носителей информации.

Запрещается несанкционированное использование съёмных носителей информации, содержащей персональные данные, и использование незарегистрированных носителей информации, содержащей персональные данные.

Разработка организационно-распорядительных документов по обеспечению безопасности персональных данных

В рамках реализации мер по обеспечению безопасности персональных данных должны быть разработаны следующие документы:

- Акт определения уровня защищенности ПДн (в соответствии с постановлением Правительства Российской Федерации от 1.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»);

- Акт классификации для каждой ИС (в соответствии с приказом ФСТЭК от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»);

- Акт классификации для каждой АС, в составе которой находится ИС (в соответствии с руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением председателя Гостехкомиссии России от 30.03.1992));

- Уведомление об обработке персональных данных;

- Перечень лиц, допущенных к обработке персональных данных (Список постоянных пользователей) для каждой ИС и установленные им права доступа к информационным ресурсам (матрица доступа пользователей к защищаемым информационным ресурсам);

- Технический паспорт на каждую ИС;

- Инструкция администратора безопасности информационной системы;

- Инструкция по работе пользователей ИС;

- Инструкция по организации антивирусной защиты и проведению антивирусного контроля;

- Инструкция по организации парольной защиты;

- Инструкция по архивированию и резервированию персональных данных в ИС;

- Инструкция по ликвидации последствий нештатных ситуаций в ИС;

- Инструкция о порядке предоставления доступа к защищаемым ресурсам ИС;

- Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств ИС;

- Инструкция о порядке охраны и допуска в помещения ИС;

- Инструкция по применению криптосредств для защиты конфиденциальной информации;

- Журнал регистрации, учёта и выдачи носителей информации, содержащей персональные данные.

Ответственность за организацию разработки организационно-распорядительных документов возлагается на ответственного за организацию обработки ПДн.

Подача Уведомления об обработке персональных данных в Уполномоченный орган по защите прав субъектов персональных данных

Ответственность за своевременную подачу Уведомления об обработке персональных данных в Уполномоченный орган по защите прав субъекта персональных данных возлагается на ответственного за обеспечение безопасности ПДн.

5.3. Технические мероприятия

Технические меры защиты персональных данных предполагают использование программно-аппаратных средств защиты информации (далее - СЗИ). При обработке персональных данных с использованием средств автоматизации применение СЗИ является обязательным условием, а их количество и степень защиты определяется в процессе предпроектного обследования информационных ресурсов Учреждения.

5.3.1. Требования к техническим и программным средствам

Технические и программные средства, используемые для обработки персональных данных в ИС, должны удовлетворять установленным в соответствии

с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Средства защиты информации, применяемые в ИС, в установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

5.3.2. Необходимость создания системы защиты персональных данных.

Создание системы защиты персональных данных (далее - СЗПДн) является необходимым условием обеспечения безопасности персональных данных в том случае, если существующие организационные и технические меры обеспечения безопасности не соответствуют требованиями к обеспечению безопасности персональных данных для ИС соответствующего класса и/или не покрывают всех угроз безопасности персональных данных для данной ИС.

Целью создания СЗПДн является обеспечение защиты информации, содержащей персональные данные, от утечки по техническим каналам и от несанкционированного доступа. Защита осуществляется путём выполнения комплекса организационных и технических мероприятий в соответствии с требованиями государственных стандартов, руководящих и нормативно-методических документов ФСТЭК России, реализуемых в рамках создаваемой СЗПДн.

СЗПДн должна включать:

- организационные меры и технические средства защиты информации;
- средства предотвращения несанкционированного доступа к информации;
- средства предотвращения утечки информации по техническим каналам;
- средства предотвращения программно-технических воздействий на технические средства обработки персональных данных;
- используемые в ИС информационные технологии.

Результатом создания СЗПДн является подтверждение соответствия ИС требованиям безопасности персональных данных - аттестация объекта информатизации (ИС) по требованиям безопасности информации.

Аттестация объекта информатизации по требованиям безопасности информации представляет собой комплекс организационно-технических мероприятий, в результате которых подтверждается, что на аттестационном объекте выполнены требования по безопасности информации, заданные в нормативно-технической документации, утверждённые государственными органами обеспечения безопасности информации и контролируемые при аттестации.

Аттестация проводится органом по аттестации в установленном законодательством порядке.

Результатом аттестации объекта информатизации (ИС) является получение «Аттестата соответствия автоматизированной системы ТОГБУ «ТРК «Тамбовская губерния» требованиям безопасности информации» (далее - Аттестат соответствия).

Владелец аттестованного объекта информатизации несёт ответственность за выполнение установленных условий функционирования объекта информатизации, технологии обработки защищаемой информации и требований по безопасности информации.

5.4. Контроль обеспечения безопасности (защиты) персональных данных при создании СЗПДн

Задачами контроля обеспечения безопасности (защиты) персональных данных являются:

- контроль выполнения требований безопасности персональных данных в ИС;

- координация действий подразделений Учреждения по организации и обеспечению безопасности персональных данных;

- предупреждение, выявление и пресечение выявленных нарушений.

Общее руководство работами по обеспечению безопасности персональных данных осуществляет заместитель генерального директора

Ответственный за обеспечение безопасности ПДн (администратор безопасности ИС) выполняет:

- анализ состояния и определение требований к защищённости различных ИС;

- выбор методов и средств обеспечения защиты персональных данных;

- разработку необходимых нормативно-методических и организационно-распорядительных документов по вопросам обеспечения безопасности персональных данных;

- администрирование и контроль применения средств защиты информации, а также поддержку функционирования средств, технологий и процессов при обработке персональных данных;

- разработку требований по обеспечению безопасности персональных данных (создание/модернизацию СЗПДн);

- организацию проведения работ по защите персональных данных;

- контроль выполнения требований по обеспечению безопасности персональных данных и эффективности предусмотренных мер защиты.

Обязанности пользователей ИС определяются их должностными инструкциями, Инструкцией администратора безопасности ИС, Инструкцией пользователей ИС и другими организационно-распорядительными документами, разрабатываемыми в соответствии с настоящим Положением.

Пользователи ИС не имеют права использовать в неслужебных целях информационные ресурсы ИС, обязаны соблюдать конфиденциальность (не разглашать, не допускать распространения) ставшей им известной в связи с исполнением должностных обязанностей информации ограниченного доступа (персональных данных).

6. Привлечение сторонних организаций

Разработка и осуществление мероприятий СЗПДн может проводиться как специалистами по защите информации Учреждения, так и специализированными организациями, имеющими лицензии ФСТЭК России на соответствующий вид деятельности.

В случае разработки СЗПДн или её отдельных компонентов специализированными организациями разработка и внедрение СЗПДн осуществляется при взаимодействии разработчика с ответственным за организацию обработки ПДн Учреждения и ответственным за обеспечение безопасности ПДн Учреждения, которые осуществляют методическое руководство и участвуют в:

- разработке конкретных требований по защите ПДн;

- аналитическом обосновании необходимости создания СЗПДн;

- согласовании выбора средств вычислительной техники и связи, технических и программных средств защиты;

- организации работ по выявлению возможных каналов утечки информации или воздействий на неё и предупреждению утечки и нарушения целостности персональных данных;

- аттестации ИС.

7. Контроль защиты персональных данных

Контроль защиты персональных данных в ИС - это комплекс организационных и технических мероприятий, которые осуществляются в целях предупреждения и пресечения возможности получения с помощью технических средств защищаемой информации (персональных данных), выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности ИС.

Периодический контроль защиты персональных данных осуществляется ежегодно ответственным за организацию обработки ПДн в рамках своих полномочий, а также специалистами органа по аттестации ИС в установленном законодательством порядке.

7.1. Задачи и содержание контроля

Основными задачами контроля являются:

- проверка организации выполнения мероприятий по защите персональных данных в ИС, учёта требований по защите персональных данных в разрабатываемых плановых и распорядительных документах;
- уточнение зон перехвата обрабатываемой в ИС информации, возможных каналов утечки персональных данных, несанкционированного доступа к ним и программно-технических воздействий на них;
- проверка выполнения установленных норм и требований по защите персональных данных от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите персональных данных;
- проверка выполнения требований по защите ИС от несанкционированного доступа;
- проверка выполнения требований по антивирусной защите ИС;
- проверка знаний сотрудников по вопросам защиты персональных данных и их соответствия требованиям уровня подготовки для конкретного рабочего места;
- оперативное принятие мер по пресечению нарушений требований (норм) защиты персональных данных в ИС;
- разработка предложений по устранению (ослаблению) технических каналов утечки информации, содержащей персональные данные.

Контроль защиты персональных данных проводится с учётом реальных условий по потенциальным техническим каналам утечки информации, содержащей персональные данные, и осуществляется по объектовому принципу, при котором на объекте одновременно проверяются все вопросы защиты персональных данных.

В ходе контроля проверяются:

- соответствие принятых мер по обеспечению безопасности персональных данных требованиям законодательства по безопасности персональных данных;
- своевременность и полнота выполнения требований настоящего Положения и других руководящих документов по защите персональных данных;
- полнота выявления демаскирующих признаков охраняемых сведений
- об объектах защиты и возможных технических каналов утечки персональных
- данных, несанкционированного доступа к информации и программно-
- технических воздействий на персональные данные;
- эффективность применения организационных и технических мероприятий по защите персональных данных.

Кроме того, могут проводиться необходимые измерения и расчёты приглашенными для этих целей специалистами органа по аттестации ИС.

Основными типами контроля являются:

- визуально-оптический контроль;
- контроль эффективности защиты ПДн от утечки по техническим каналам (инструментальный контроль с использованием контрольно- измерительной аппаратуры);
- контроль несанкционированного доступа к персональным данным.

7.2. Виды контроля

Контроль защиты персональных данных осуществляется путём проведения обследования, периодических (плановых) и внеплановых проверок объектов информатизации, обрабатывающих персональные данные. Проверки ИС проводятся силами ответственного за организацию обработки ПДн, ответственного за обеспечение безопасности ПДн в ИС и администратора безопасности ИС Учреждения в рамках их полномочий, с привлечением специалистов органа по аттестации.

Обследование ИС проводится не реже одного раза в год рабочей группой в составе ответственного за организацию обработки ПДн,

ответственного за обеспечение безопасности ПДн в ИС, администратора безопасности ИС и специалистов подразделения, в ведении которого находится ИС.

Обследование ИС проводится с целью определения соответствия помещений, технических средств требованиям по защите персональных данных.

В ходе обследования проверяется:

- соответствие категории, обследуемой ИС условиям, сложившимся на момент проверки;
- соблюдение организационно-режимных требований к помещениям;
- соответствие выполняемых в ИС мероприятий по защите персональных данных мероприятиям, изложенным в техническом паспорте ИС;
- выполнение требований по защите ИС от несанкционированного доступа;
- выполнение требований по антивирусной защите.

Внеплановые проверки объектов информатизации могут проводиться как по результатам обследования, так и в случае возникновения нештатных ситуаций в ИС.

Периодические плановые проверки проводятся по истечении одного года с даты выдачи Аттестата соответствия или Акта (Заключения) о результатах предыдущей периодической проверки.

В ходе периодических (плановых) и внеплановых проверок ИС проверяется:

- соответствие состава и структуры программно-технических средств, обрабатывающих персональных данных, задокументированному составу и структуре, разрешённым для обработки такой информации;
- путём опроса персонала: доведение до конкретных исполнителей руководящих документов, технологических инструкций, предписаний, актов, заключений; уровень владения персоналом технологией безопасной обработки персональных данных, описанной в этих инструкциях;
- наличие документов, подтверждающих возможность применения технических и программных средств вычислительной техники, средств защиты для обработки персональных данных (сертификатов соответствия и других документов);
- выполнение требований по условиям размещения автоматизированных рабочих мест (далее - АРМ) в рабочих помещениях, которые исключали бы

возможность несанкционированного просмотра информации с экранов мониторов, с распечаток принтеров и с других устройств ввода-вывода информации лицами, не имеющими права доступа к ПДн;

- соответствие уровня полномочий по доступу к персональным данным различных пользователей ИС разрешённым полномочиям;

- знание инструкций по обеспечению безопасности персональных данных пользователями ИС;

- прохождение инструктажа пользователей ИС по вопросам обеспечения безопасности персональных данных и выполнение требований обеспечения безопасности персональных данных пользователями ИС.

Результатом контроля является специальный документ (Акт или Заключение/Акт (протокол) оценки эффективности принятых мер по обеспечению безопасности ПДн), который содержит выводы о состоянии обеспечения безопасности персональных данных и рекомендации по её совершенствованию.

7.3. Результаты контроля

Полученные в ходе контроля результаты обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер защиты персональных данных и выявления нарушений. При обнаружении нарушений норм и требований по защите персональных данных ответственный за обеспечение безопасности ПДн в ИС уведомляет руководителя подразделения, эксплуатирующего ИС, в которой допущены нарушения, для принятия им решения о прекращении обработки персональных данных и проведения, соответствующих организационных и технических мер по устранению нарушения. Результаты контроля защиты персональных данных оформляются актами и заносятся в Журнал по учету мероприятий по внутреннему контролю обработки персональных данных и обеспечения защиты персональных данных в ИС.

Невыполнение предписанных мероприятий по защите персональных данных считается предпосылкой к утечке информации (далее - предпосылка).

По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по решению ответственного за обеспечение безопасности ПДн проводится расследование.

Для проведения расследования назначается комиссия с привлечением специалистов по защите информации. Комиссия обязана установить:

- факт, имела ли место утечка персональных данных;
- обстоятельства, ей сопутствующие;
- лиц, виновных в нарушении предписанных мероприятий по защите персональных данных;
- причины и условия, способствовавшие нарушению.

По результатам расследования комиссия вырабатывает рекомендации по устранению нарушений и недостатков, и их последствий, а также предложения заместителю генерального директора о привлечении к ответственности виновных лиц.

8. Переаттестация объекта информатизации (ИС) по требованиям безопасности информации

Переаттестация объекта информатизации (ИС) по требованиям безопасности информации проводится:

- по истечении срока действия «Аттестата соответствия»:
- при изменении мер технической защиты информации, условий технической защиты или применяемых технологий обработки и передачи информации (далее - изменения в ИС).

В случае изменений в ИС владелец аттестованного объекта обязан известить об этом орган по аттестации, проводивший аттестацию объекта информатизации, в следующем порядке:

1. Руководитель подразделения, эксплуатирующего ИС, уведомляет о необходимости внесения изменений в ИС ответственного за обеспечение безопасности ПДн.

2. Ответственный за обеспечение безопасности ПДн согласовывает изменения в ИС с органом по аттестации.

Внесение изменений в ИС разрешается по заключению органа по аттестации:

- при условии проведения переаттестации;
- при внесении отметок об изменениях в ИС в технический паспорт на ИС и другие нормативно-методические документы на ИС.

8.1.Резервное копирование и восстановление информации:

Резервное копирование персональных данных применяется для оперативного восстановления данных в случае их утери, искажения, нарушения целостности и т.п. в результате ошибочных действий пользователей ИС, сбоя работоспособности основных технических средств и систем (далее - ОТСС), входящих с состав ИС, средств защиты информации, общесистемного или специального программного обеспечения (далее - ПО), а также вследствие других причин.

Резервное копирование общесистемного, специального ПО и программных средств защиты информации осуществляется в случаеотсутствия дистрибутивов на указанное ПО.

Порядок резервного копирования и восстановления информации определяется «Инструкцией по порядку резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах ТОГБУ «ТРК «Тамбовская губерния».

8.2.Восстановление работоспособности ОТСС, общесистемного, специального ПО и средств защиты информации в ИС

Ответственность за организацию проведения мероприятий по восстановлению работоспособности ОТСС, общесистемного и специального ПО, а также средств защиты информации в ИС возлагается на администратора безопасности ИС, которые он выполняет самостоятельно в рамках своих полномочий или с привлечением специализированных организаций (органы по аттестации в случае проведения работ в аттестованных по требованиям безопасности информации ИС) в соответствии с «Инструкцией по порядку резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах Учреждения».

9. Защита от вредоносных программ

Все ИС должны быть защищены от последствий воздействия вредоносных программ средствами антивирусной защиты.

Средства антивирусной защиты, применяемые в ИС, должны быть сертифицированы по безопасности информации для защиты персональных данных установленного ИС класса.

Ответственность за эксплуатацию средств антивирусной защиты возлагается на:

- пользователей ИС в части периодического антивирусного контроля носителей информации с персональными данными;

- администратора безопасности ИС в части установки и администрирования средств антивирусной защиты в ИС, а также контроля их использования пользователями ИС.

Порядок защиты от вредоносных программ определяется.
«Инструкцией по организации антивирусной защиты и проведению антивирусного контроля на ПЭВМ, входящих в состав информационных систем ТОГБУ «ТРК «Тамбовская губерния».

10. Регистрация пользователей ИС и назначение им прав доступа

Регистрацию пользователей ИС и назначение им прав доступа, определённых ответственным за организацию обработки ПДн, а также блокировку учётных записей осуществляет администратор безопасности ИС.

После включения сотрудника Учреждения в состав постоянных пользователей ИС ему присваивается уникальный идентификатор (имя) пользователя, и он регистрируется как пользователь ИС.

При регистрации пользователя ИС проводится проверка соответствия уровня доступа его должностным обязанностям.

Назначенные пользователю ИС права доступа должны быть отражены в «Матрице разграничения доступа к защищаемым ресурсам автоматизированной системы...», определенной в «Положении о разрешительной системе доступа к информационным ресурсам, программным и техническим средствам автоматизированной системы...».

При изменении должностных обязанностей (увольнении) пользователя ИС его права доступа корректируются (удаляются). Администратором безопасности ИС производится корректировка Матрицы разграничения доступа к защищаемым ресурсам и Перечня лиц, допущенных к обработке ПДн в ИС.

Неиспользуемые учётные записи блокируются (удаляются).

В сочетании с парольной защитой идентификатор пользователя используется для аутентификации пользователя в ИС.

11. Парольная защита

Парольная защита является одним из способов защиты информации от несанкционированного доступа. На компьютерах, обрабатывающих персональные данные, наличие парольной защиты (пароля пользователя) обязательно.

Порядок использования паролей пользователей в ИС определяется «Инструкцией по организации парольной защиты на ПЭВМ, входящих в состав информационных систем ТОГБУ «ТРК «Тамбовская губерния».

11.1 .Применение средств криптографической защиты

Необходимость применения средств криптографической защиты (далее - криптосредств) при обработке персональных данных может возникнуть в следующих случаях:

- при передаче персональных данных в среду (носители информации, каналы связи и т.п.), в которой они могут оказаться доступными для несанкционированного доступа;

- в ИС, являющихся многопользовательскими, в которых введено разграничение прав доступа пользователей и возможно наличие инсайдера, если безопасность хранения и обработки не может быть гарантирована другими средствами.

В случае необходимости применения криптосредств при обработке персональных данных безопасность обработки персональных данных обеспечивается:

- соблюдением пользователями криптосредств конфиденциальности при обращении со сведениями, которые им доверены или стали известны при выполнении своих служебных обязанностей, 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;

-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.

Администрирование криптосредств осуществляется ответственным пользователем криптографических средств в информационной системе Учреждения. Функции, права и обязанности ответственного пользователя криптографических средств в информационной системе Учреждения определены в «Инструкции ответственного пользователя криптографических средств в информационной системе Учреждения».

Порядок обеспечения функционирования и безопасности криптосредств, а также права и обязанности сотрудников, эксплуатирующих криптосредства, определяются «Инструкцией по применению криптографических средств для защиты конфиденциальной информации в информационных системах Учреждения».

12. Обновление общесистемного и прикладного программного обеспечения, техническое обслуживание ИС

Все изменения конфигураций технических и программных средств ПЭВМ должны производиться только на основании заявок ответственного за эксплуатацию конкретной подсистемы ИС (пользователя конкретного АРМ).

Право внесения изменений в конфигурацию аппаратно-программных средств, защищенных АРМ предоставляется:

в отношении системных и прикладных программных средств - ответственному за обеспечение безопасности ПДн с привлечением администратора безопасности ИС, по согласованию с органом по аттестации;

- в отношении аппаратных средств, а также в отношении программно-аппаратных средств защиты информации - уполномоченным сотрудникам органа по аттестации ИС.

Изменение конфигурации аппаратно-программных средств ПЭВМ кем-либо, кроме вышеперечисленных уполномоченных сотрудников и подразделений, **запрещено.**

Установка, модификация и техническое обслуживание программного обеспечения и аппаратных средств ИС должны проводиться в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем Учреждения».

13. Порядок контроля соблюдения условий использования средств защиты информации

Средства защиты информации являются важным компонентом обеспечения безопасности персональных данных.

Порядок работы со средствами защиты информации определён в инструкциях (руководствах) по настройке и использованию, прилагаемых к средствам защиты информации, обязательных для исполнения всеми пользователями ИС и администратором безопасности ИС.

Право проверки соблюдения условий использования средств защиты информации имеет администратор безопасности ИС.

Пользователю ИС категорически запрещается:

- производить обработку персональных данных с отключенными средствами защиты информации;
- изменять настройки средств защиты информации.

Контроль за соблюдением условий использования средств защиты информации, обеспечение правильного функционирования и поддержание работоспособности средств защиты информации осуществляет ответственный за безопасность функционирования средств защиты информации, за исключением криптографических, используемых в информационной системе Учреждения (далее - Ответственный за безопасность функционирования СЗИ), назначаемый приказом генерального директора. Функции, права и обязанности Ответственного за безопасность функционирования СЗИ определены в «Инструкции ответственного за безопасность функционирования средств защиты информации, за исключением криптографических, используемых в информационной системе Учреждения.

Ответственному за безопасность функционирования СЗИ запрещается менять настройки программно-аппаратных средств защиты информации, предустановленные сотрудником органа по аттестации при настройке системы защиты информации в ходе аттестации ИС.

14. Порядок проверки электронных журналов обращений к ресурсам ИС

Проверка электронных журналов обращений проводится с целью выявления несанкционированного доступа (далее - НСД) к защищаемой информации в ИС.

Право проверки электронного журнала обращений имеют:

- ответственный за организацию обработки ПДн;
- администратор безопасности ИС;
- генеральный директора Учреждения.

На технических средствах ИС, на которых установлены специализированные средства защиты информации типа «Secret Net», «Dallas Lock» и другие, проверка электронного журнала производится в соответствии с прилагаемым к указанным СЗИ Руководством.

Проверке подлежат все электронные журналы ИС.

Проверка должна проводиться не реже, чем один раз в неделю с целью своевременного выявления фактов нарушения требований настоящего Положения.

Факты проверок электронных журналов отражаются в Журнале проверок электронных журналов. После каждой проверки ответственный за обеспечение безопасности ПДн в ИС делает соответствующую отметку в журнале и ставит свою подпись.

15. Заключительные положения

Требования настоящего Положения обязательны для всех сотрудников,

обрабатывающих персональные данные, и ответственных за обеспечение безопасности персональных данных.

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