УТВЕРЖДЕНО
приказом архивного управления
Курской области
от «15» мая 2025 г. № 01-03/39

Правила (политика) обработки персональных данных в архивном управлении Курской области

Курск

Оглавление

1. Общие положения

Настоящие Правила (политика) обработки персональных данных в архивном управлении Курской области (далее – Правила) разработаны на основании и во исполнение:

- Федерального закона РФ от 27.07.2006 №152-ФЗ «О персональных данных»;
- Постановления 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»;
- Постановления Правительства РФ от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановления Губернатора Курской области от 07 октября 2010 г. №385-пг «Об утверждении положения об архивном управлении Курской области»

и определяют **политику архивного управления Курской области в отношении обработки персональных данных**.

Настоящие Правила утверждаются [7] и вводятся в действие приказом начальника архивного управления Курской области (далее – начальника) и являются обязательными для исполнения всеми сотрудниками архивного управления Курской области (далее - архивуправление).

Настоящие Правила:

- устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных [7];
- определяют для каждой цели обработки персональных данных:
- содержание обрабатываемых персональных данных,
- категории субъектов, персональные данные которых обрабатываются,
- сроки их обработки и хранения,
- порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований;
- перечни персональных данных, обрабатываемых в связи с реализацией трудовых отношений, а также в связи с оказанием государственных услуг и осуществлением государственных функций [7];
- оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» [1];
- определяют соотношение вреда который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» и принимаемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» [1];
- устанавливают правила рассмотрения запросов субъектов персональных данных или их представителей [7];
- устанавливают правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора [7];
- устанавливают типовую форму согласия на обработку персональных данных сотрудников и иных субъектов персональных данных [7];
- устанавливают типовую форму разъяснения субъекту персональных данных

юридических последствий отказа предоставить свои персональные данные [7];

- устанавливают правила работы с обезличенными данными [7];
- определяют перечень должностей сотрудников, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных [7];
- определяют перечень информационных систем персональных данных [7];
- определяют перечень должностей сотрудников, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным [7];
- устанавливают порядок ознакомления сотрудников (наименование организации), непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных и (или) организуют обучение указанных сотрудников [7];
- устанавливают перечень и правила ведения иных локальных актов по вопросам обработки персональных данных [1], включая:
- порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных [7];
- должностная инструкция ответственного за организацию обработки персональных данных [7];
- типовое обязательство сотрудников, непосредственно осуществляющих обработку персональных данных, в случае расторжения с ними государственного контракта прекратить обработку персональных данных, ставших известными в связи с исполнением должностных обязанностей [7].

2. Требования по обработке персональных данных

2.1. Понятия и определения

В настоящих Правилах используются следующие основные понятия:

- **персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) [1];
- **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 [1];
- **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 [1];

- **автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники [1];
- **распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц [1];
- **предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц [1];
- **блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных) [1];
- **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 [1];
- **обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных [1];
- **информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств [1];
- **трансграничная передача персональных данных** – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу [1];
- **конфиденциальность персональных данных** – обязанность операторов и иных лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом [1]
- **специальные категории персональных данных** – персональные данные, в том числе, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, о судимости [1]
- **биометрические персональные данные** – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность [1]
- **использование персональных данных** – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц [1];
- **информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов [2];
- **информационно-телекоммуникационная сеть** – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники [2];
- **доступ к информации** – возможность получения информации и ее использования [2];
- **обладатель информации** – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам [2];

– **документированная информация** – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель [2];

– **средства вычислительной техники** - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем [3];

– **базой данных является** представленная в объективной форме совокупность самостоятельных материалов, систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ) [4];

– **к юридическим последствиям** относятся случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или иным образом затрагивающее его права, свободы и законные интересы [4].

Иные понятия в настоящих Правилах используются в значениях, определенных действующим законодательством Российской Федерации либо их значение дается по тексту.

2.2. Принципы обработки персональных данных

Обработка персональных данных должна осуществляться на основе следующих принципов:

- обработка персональных данных должна осуществляться на законной и справедливой основе [1];
- обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей [1];
- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных [1];
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой [1];
- обработке подлежат только персональные данные, которые отвечают целям их обработки [1];
- содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки [1];
- обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки [1];
- 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 [1];
- оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных [1];
- 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 [1];
- 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 [1];
- 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 [1, 7];

− обязанность лица, осуществляющего обработку персональных данных по поручению оператора, соблюдения принципов и правил обработки персональных данных [1];
− соблюдения принципов и правил обработки персональных данных при поручении такой обработки другому лицу [1];
− соблюдение конфиденциальности персональных данных [1];;
− обработки персональных данных (в том числе при обработке общедоступных персональных данных, специальных категорий персональных данных, биометрических персональных данных, при принятии решений на основании исключительно автоматизированной обработки персональных данных, при трансграничной передаче персональных данных) с письменного согласия субъектов персональных данных либо на ином законом основании [1];
− соблюдения законности при осуществлении трансграничной передачи персональных данных [1];
− соблюдением обязанностей, возлагаемых на оператора персональных данных, действующим законодательством и иными нормативными актами по обработке персональных данных [1];
− принятии мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных законодательством в области персональных данных [1];
− принятии необходимых правовых, организационных и технических мер или обеспечении их принятия 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 [1];
− недопустимости ограничения прав и свобод человека и гражданина по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных [1];
− недопустимости использования оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных [1];
− личной ответственности должностных лиц, осуществляющих обработку персональных данных;
− документального оформления всех принятых решений по обработке и обеспечению безопасности персональных данных.

Нарушение указанных принципов обработки персональных данных категорически запрещается!

2.3. Цели обработки персональных данных

Архивуправление, являясь оператором персональных данных, должен определять цели обработки персональных данных [1] в своих информационных системах персональных данных.

Цели обработки персональных данных в информационных системах персональных данных должны быть четко определены и соответствовать:
− заявленным в Положении об архивном управлении Курской области;
− перечням задач или функций структурных подразделений (должностных лиц) архивуправления, указанным в положениях о таких структурных подразделениях

(должностных обязанностях).

Цели обработки персональных данных определяют [1, 8]:
- содержание и объем обрабатываемых персональных данных,
- категории субъектов, персональные данные которых обрабатываются,
- сроки их обработки и хранения,
- порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

Цели обработки персональных данных должны быть [1]:
- конкретны;
- заранее определены;
- законны;
- заявлены.
-

Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой [1].

Совместимость целей определяется по наличию общей цели связанной с заявленным в Положении об архивном управлении Курской области основными полномочиями и правами архивуправления или по наличию общей цели, определяемой действующим законодательством Российской Федерации.

2.4. Способы и правила обработки персональных данных в информационных системах персональных данных в зависимости от применения средств автоматизации

Способы обработки персональных данных в информационных системах персональных данных:
- обработка персональных данных без использования средств автоматизации [1, 6];
- обработка персональных данных с использованием средств автоматизации [1];
- исключительно автоматизированная обработка персональных данных [1];

2.4.1. Правила обработки персональных данных без использования средств автоматизации

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков) [5].

Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель [5].

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых, заведомо не совместимы [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, должны быть приняты 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 [5].

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать:
- сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации,
- имя (наименование) и адрес оператора,
- фамилию, имя, отчество и адрес субъекта персональных данных,
- источник получения персональных данных,
- сроки обработки персональных данных,
- перечень действий с персональными данными, которые будут совершаться в процессе их обработки,
- общее описание используемых оператором способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, – при необходимости получения письменного согласия на обработку персональных данных;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых, заведомо не совместимы [5].

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 [5].

2.4.2. Правила обработки персональных данных средствами автоматизации

Обработка персональных данных средствами автоматизации в архивуправлении допускается только в следующих случаях:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных [1];
- обработка персональных данных необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на архивуправление функций, полномочий и обязанностей [1];
- обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта) [1];
- обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале

государственных и муниципальных услуг [1];

- 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 [1];
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно [1];
- обработка персональных данных необходима для осуществления прав и законных интересов архивного управления Курской области или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных [1];
- 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 (персональные данные, сделанные общедоступными субъектом персональных данных) [1];
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом [1].

Обработка персональных данных средствами автоматизации должна осуществляться на основании правил, инструкций, руководств, регламентов и иных документов, определяющих технологический процесс обработки информации, содержащих такие данные, определенный для выполнения конкретных операций с заранее определенными целями, с учетом требований настоящих Правил.

2.4.2.1. Обработка персональных данных с согласия субъекта персональных данных

В случае если обработка персональных данных субъекта персональных данных в информационной системе персональных данных осуществляется на основании согласия и не имеется оснований для обработки таких персональных данных без получения согласия, должны выполняться указанные в настоящем пункте правила.

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,
- сознательным [1].
-

Согласие на обработку персональных данных архивному управлению Курской области может быть дано субъектом персональных данных или его представителем только в письменной форме. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью [1].

Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством Российской Федерации [1].

В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором [1].

В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных [1].

В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни [1].

В случае получения согласия от законного представителя субъекта персональных данных или наследников субъекта персональных данных они обязаны представить документы, подтверждающие их полномочия.

Допускается включение согласия в типовые формы (бланки) материальных носителей персональных данных [5] и в договоры с субъектами персональных данных.

Письменные согласия субъектов персональных данных должны храниться в архивуправлении.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных путем направления обращения в архивное управление Курской области. При получении такого обращения выполняются действия предусмотренные пунктом 2.14.8 настоящих Правил.

Требования к содержанию согласия на обработку персональных данных приведено в пункте 2.15 настоящих Правил.

2.4.2.2. Обработка персональных данных без согласия субъекта персональных данных

Обработка персональных данных, осуществляемая без получения согласия на такую обработку от субъекта персональных данных может осуществляться только по основаниям, указанным в пункте 2.4.2, при этом обязанность предоставить доказательство наличия таких оснований [1] возлагается на архивуправление.

Порядок определения оснований обработки персональных данных без согласия на обработку персональных данных от субъекта персональных данных, их определения, оформления и предоставления приведен в пунктах 2.7, 2.9, 2.14 и 2.18 настоящих Правил.

2.4.3. Правила исключительно автоматизированной обработки персональных данных

При исключительно автоматизированной обработке персональных данных должны выполняться правила обработки персональных данных средствами автоматизации (пункт 2.4.2 настоящих Правил).

Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных [1].

В остальных случаях 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 запрещается [1].

При исключительно автоматизированной обработке персональных данных необходимо:

- разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных [1];

- разъяснить возможные юридические последствия такого решения [1];
- предоставить возможность заявить возражение против такого решения [1];
- рассмотреть возражение [1];
- уведомить субъекта персональных данных о результатах рассмотрения такого возражения [1] в порядке определенном в пункте 2.14.2 настоящих Правил в сроки, предусмотренные пунктом 2.14.1 настоящих Правил.

2.4.4. Правила смешенной обработки персональных данных

При смешанной обработке персональных данных необходимо выполнять правила объединяющие правила обработки персональных данных при их обработке каждым из используемых при смешанной обработке персональных данных способов (пункты 2.4.1-2.4.3 настоящих Правил).

2.4.5. Правила обработки персональных данных средствами автоматизации при поручении обработки персональных данных

2.4.5.1. Правила обработки персональных данных средствами автоматизации при поручении обработки персональных данных другому лицу

Архивуправление вправе поручить обработку персональных данных другому лицу (поручение оператора):
- с согласия субъекта персональных данных;
- если иное не предусмотрено федеральным законом;
- на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта;
- либо путем принятия соответствующего акта [1].

Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящими Правилами.

В поручении оператора:
- должен быть определен перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных [1];
- должны быть определены цели обработки персональных данных [1];
- должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных [1];
- должна быть установлена обязанность такого лица обеспечивать безопасность персональных данных при их обработке [1];
- должны быть указаны требования к защите обрабатываемых персональных данных [1] в соответствии с настоящими Правилами и техническим заданием на создание системы защиты персональных данных;
- установлена ответственность такого лица перед архивуправлением, в случаях нарушений установленных требований и законодательства Российской Федерации в области персональных данных;
- при необходимости получения согласий на обработку персональных данных от субъектов персональных данных, предусмотрен порядок сбора и передачи в архивуправление таких согласий субъектов персональных данных.

В случае если аархивуправление поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет [1] архивное управление Курской области.

В случае необходимости получения согласия на обработку персональных данных от субъекта персональных данных обязанность получения таких согласий возлагается на архивуправление.

2.4.5.2. Правила обработки персональных данных средствами автоматизации при поручении обработки персональных данных другим лицом

В случае поручения обработки персональных данных средствами автоматизации архивуправления другим лицом, такое лицо своим поручением оператору обязано:

- определить перечень действий (операций) с персональными данными, которые будут совершаться архивным управление Курской области при осуществлении обработки персональных данных [1];
- определить цели обработки персональных данных [1];
- указать требования к защите обрабатываемых персональных данных [1].

В случае не определения такой информации и требований другим лицом, архивуправление обязано добиться их определения и документального оформления.

В случае принятия поручения оператора от другого лица архивуправлением без указанной информации и требований, такая обработка не считается обработкой осуществляемой по поручению оператора, и архивуправление являться оператором персональных данных. При этом обработка персональных данных должна выполняться в соответствии с настоящими Правилами за исключением пункта 2.4.5.

Ааархивуправление обязано выполнить все требования установленные другим лицом в поручении оператора и за все нарушения в обработке персональных данных несет ответственность перед таким лицом [1].

Архивуправление при осуществлении обработки персональных данных по поручению оператора не обязано получать согласие субъекта персональных данных на обработку его персональных данных [1].

2.5. Особые правила обработки персональных данных в информационных системах персональных данных в зависимости от категории обрабатываемых персональных данных

В архивуправлении устанавливаются следующие особые правила обработки персональных данных в зависимости от категории обрабатываемых персональных данных:

- обработка специальных категорий персональных данных [1];
- обработка общедоступных персональных данных [1].

Особые правила обработки персональных данных в информационных системах персональных данных в зависимости от категории обрабатываемых персональных данных, являются дополнительными способам и правилам обработки персональных данных в информационных системах персональных данных в зависимости от применения средств автоматизации указанным в пункте 2.4 настоящих Правил.

2.5.1. Правила обработки специальных категорий персональных данных

К специальным категориям персональных данных относятся сведения касающиеся:

- расовой принадлежности;
- национальной принадлежности;
- политических взглядов;
- религиозных убеждений;
- философских убеждений;
- состоянии здоровья;

- интимной жизни;
- судимости [1].
-

В архивуправлении **категорически запрещается** обработка специальных категорий персональных данных касающихся:

- расовой принадлежности;
- национальной принадлежности;
- политических взглядов;
- религиозных убеждений;
- философских убеждений;
- интимной жизни.

В архивуправлении разрешается обработка специальных категорий персональных данных касающиеся состоянии здоровья и судимости в минимально необходимом объеме при обязательном соблюдении любого из следующих условий:

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных [1];
- обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях [1];
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно [1];
- обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия [1];
- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, о противодействии терроризму, о противодействии коррупции, об оперативно-разыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации [1];
- обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством [1];
- обработка персональных данных о судимости осуществляется в пределах полномочий, предоставленных архивуправлению в соответствии с законодательством Российской Федерации [1].

Обработка специальных категорий персональных данных в остальных случаях в архивуправлении не допускается [1].

Обработка специальных категорий персональных данных, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом [1].

2.5.2. Правила обработки биометрических персональных данных

К биометрическим персональным данным относятся (обязательно выполнение всех трех условий одновременно):

- сведения, которые характеризуют физиологические и биологические особенности человека;

− на основании которых можно установить его личность;

− и которые используются архивуправлении для установления личности субъекта персональных данных [1].

Обработка биометрических персональных данных в архивуправлении осуществляется исключительно без использования средств автоматизации.

В случае принятия решения об обработке биометрических персональных данных, такие данные могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных [1].

2.5.3. Правила обработки общедоступных персональных данных

Общедоступные персональные данные физических лиц, полученные из сторонних общедоступных источников персональных данных, в архивуправлении обрабатываются в исключительных случаях в сроки, не превышающие необходимых для их использования. При этом совместно с такими данными должны собираться реквизиты их источника и подтверждение согласия субъекта персональных данных на включение такой информации в общедоступные источники персональных данных, так как в случае обработки общедоступных персональных данных обязанность доказывания того, что обрабатываемые персональные данные являются общедоступными [1], возлагается на архивуправление. По достижении целей обработки общедоступных персональных данных они подлежат немедленному уничтожению.

С целью информационного обеспечения и осуществления взаимодействия как внутри архивуправления, так и со сторонними физическими и юридическими лицами в архивуправлении могут создаваться общедоступные источники персональных данных. Создание общедоступного источника персональных данных осуществляется по решению начальника. В решении о создании общедоступного источника персональных данных должны быть указаны:

− цель создания общедоступного источника персональных данных;

− ссылка на нормативный акт, устанавливающий необходимость создания общедоступного источника персональных данных (при наличии);

− перечень персональных данных, которые вносятся в общедоступный источник персональных данных;

− порядок включения персональных данных в общедоступный источник персональных данных;

− порядок уведомления пользователей общедоступного источника персональных данных об исключении из него персональных данных либо внесении в него изменений;

− порядок получения письменного согласия субъекта персональных данных на включение персональных данных в общедоступный источник персональных данных;

− ссылка на нормативный акт, устанавливающий порядок исключения персональных данных из общедоступного источника персональных данных.

В общедоступный источник персональных данных с письменного согласия субъекта персональных данных могут включаться: должность, фамилия, имя, отчество, абонентский номер рабочего телефона, место получения образования, достигнутые результаты и другая информация.

Включение в общедоступные источники персональных данных персональных данных субъекта персональных данных допускается только на основании его письменного согласия [1].

Исключение персональных данных из указанного общедоступного источника осуществляется при утрате необходимости в обработке таких данных, либо на основании заявления субъекта персональных данных в установленном настоящими Правилами (пункт 2.14.8) и действующим законодательством Российской Федерации порядке.

2.6. Особые правила обработки персональных данных в информационных системах персональных данных в зависимости от цели обработки персональных данных

В архивуправлении устанавливаются следующие особые правила обработки персональных данных в зависимости от цели обработки персональных данных:

- правила обработки персональных данных с целью однократного пропуска субъекта персональных данных на охраняемую территорию;
- правила обработки персональных данных при трансграничной передаче персональных данных;
- правила работы с обезличенными данными;
- правила обработки персональных данных в целях политической агитации.

Особые правила обработки персональных данных в информационных системах персональных данных в зависимости от цели обработки персональных данных являются дополнительными способам и правилам обработки персональных данных в информационных системах персональных данных в зависимости от применения средств автоматизации указанным в пункте 2.4 настоящих Правил.

2.6.1. Правила обработки персональных данных с целью однократного пропуска субъекта персональных данных на охраняемую территорию

При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию архивуправления, должны соблюдаться следующие условия:

- необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актомархивуправления, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (по должностям), имеющих доступ к материальным носителям и перечень лиц, ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится архивуправление, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;
- копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;
- персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на охраняемую территорию [5].

2.6.2. Правила обработки персональных данных при трансграничной передаче персональных данных

Трансграничной передачей персональных данных называется передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Трансграничной передачи персональных данных архивуправлением не осуществляется.

В случае принятия архивуправлением решения о трансграничной передаче персональных данных, такие данные могут обрабатываться только в следующих случаях [1]:

- при наличии согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;
- предусмотренных международными договорами Российской Федерации;

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

Архивуправление до начала осуществления трансграничной передачи персональных данных обязано убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных.

2.6.3. Правила работы с обезличенными данными

Обезличиванием персональных данных называются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных [1].

Архивуправление не осуществляет обезличивания персональных данных, обрабатываемых в информационных системах персональных данных с использованием средств автоматизации. В случае принятия архивуправлением решения об обезличивании персональных данных, обрабатываемых в информационных системах персональных данных, такое обезличивание может осуществляться только при условии исполнения действующих требований и методов по обезличиванию персональных данных.

Порядок обезличивания в архивуправлении установлен пунктом 2.10.7 настоящих Правил.

2.6.4. Правила обработки персональных данных в целях политической агитации

Архивуправление не осуществляет обработки персональных данных в целях политической агитации.

В случае принятия архивным управлением Курской области решения об обработке персональных данных в целях политической агитации, такая обработка может осуществляться только при условии предварительного согласия субъекта персональных данных [1]. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта персональных данных, если архивуправление не докажет, что такое согласие было получено [1].

Архивуправление по требованию субъекта персональных данных обязан немедленно прекратить обработку его персональных данных, осуществляемую в целях политической агитации [1].

2.7. Необходимость обработки персональных данных

Необходимость обработки персональных данных определяется заранее определенной и документированной целью обработки персональных данных и может устанавливаться (требоваться) нормативно-правовым актом (например, федеральным законом) или определяется принятым в архивуправлении порядком выполнения определенных операций по обработке информации, в рамках заявленных в Положении основных полномочий и прав архивуправления, либо в рамках перечня задач или функций структурных подразделений (должностных лиц) архивуправления, указанных в положениях о таких структурных подразделениях (должностных обязанностях).

Принятый в архивуправлении порядок выполнения определенных операций по обработке информации, в рамках которых производится обработка персональных данных,

должен быть отражен в локальном нормативном акте архивуправления.

Необходимость обработки персональных данных в архивуправлении оформляются в порядке, установленном пунктом 2.18 настоящих Правил.

Обработка персональных данных без определения правового основания ее необходимости **категорически запрещается**.

2.8. Перечни персональных данных, используемые для решения задач и функций структурными подразделениями

Для решения тех или иных задач и функций структурными подразделениями архивуправления определяются наборы персональных данных, обработка которых вызвана заранее определенной и документированной целью обработки персональных данных.

Обработка персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных недопустима [1].

Перечни персональных данных, используемых для решения конкретных задач и функций структурными подразделениями в архивном управлении Курской области оформляются в порядке, установленном пунктом 2.18 настоящих Правил.

2.9. Правовое основание обработки персональных данных

Правовое основание обработки персональных данных включает в себя:

- определение законности целей обработки персональных данных;
- оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных;
- определение заданных характеристик безопасности персональных данных;
- определение сроков обработки, в том числе хранения персональных данных, осуществление контроля за соблюдением сроков обработки персональных данных и фактов достижения целей обработки персональных данных.

2.9.1. Определение законности целей обработки персональных данных

Заявляемые в качестве целей обработки персональных данных цели должны быть законны [1]. Законность целей обработки персональных данных в архивуправлении определяется их соответствием случаям, указанным в пункте 2.4.2 настоящих Правил.

Причем, кроме самого факта обработки персональных данных, должны рассматриваться, и соответственно иметь правовое основание, особые правила обработки определенных наборов персональных данных (таких как специальные категории персональных данных, биометрические персональные данные и др.), особые способы обработки персональных данных (обработка без использования средств автоматизации, исключительно автоматизированная обработка персональных данных и др.), а так же особые цели обработки персональных данных (однократный пропуск на охраняемую территорию, трансграничная передача персональных данных и др.).

При определении правовых оснований обработки персональных данных должны определяться реквизиты федерального закона, а также иных подзаконных актов, и документов органов государственной власти, которые требуют обработку персональных данных или иных документов, являющихся такими основаниями.

Обработка персональных данных без документально определенного и оформленного правового основания обработки персональных данных не допускается.

Правовые основания обработки персональных оформляются в порядке, установленном пунктом 2.18 настоящих Правил.

2.9.2. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности

персональных данных

Оценкой вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных является определение юридических или иным образом затрагивающих права и законные интересы последствий в отношении субъекта персональных данных, которые могут возникнуть в случае нарушения требований по обработке и обеспечению безопасности персональных данных.

К юридическим последствиям относятся случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или иным образом затрагивающее его права, свободы и законные интересы [4].

При обработке персональных данных должны определяться и документально оформляться все возможные юридические или иным образом затрагивающие права и законные интересы последствия в отношении субъекта персональных данных, которые могут возникнуть в случае нарушения требований по обработке и обеспечению безопасности персональных данных при выполнении заявленных в Положении об архивном управлении Курской области основных полномочий и прав архивного управления Курской области, либо в рамках перечня задач или функций структурных подразделений (должностных лиц) архивуправления, указанных в положениях о таких структурных подразделениях (должностных обязанностях) с учетом особых правил и способов обработки персональных данных.

Определение таких юридических последствий необходимо для недопущения нарушения и обеспечения 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, а также определения соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер.

Обработка персональных данных без оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных не допускается.

Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных документально оформляется в порядке, установленном пунктом 2.18 настоящих Правил.

2.9.3. Заданные характеристики безопасности персональных данных

Всеми лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных.

Конфиденциальность персональных данных это обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом [1].

Вне зависимости от необходимости обеспечения конфиденциальности персональных данных, при обработке персональных данных должно определяться наличие требований по обеспечению иных характеристик безопасности персональных данных, отличных от нее.

К таким характеристикам относятся [8]:

- требование по обеспечению целостности персональных данных;
- требование по обеспечению доступности персональных данных.

Обеспечение указанных характеристик безопасности персональных данных может устанавливаться:

- федеральным законом, а также иным подзаконным актом, документом органов государственной власти;

− локальным актом архивуправления.

При определении необходимости обеспечения характеристик безопасности персональных данных, отличных от конфиденциальности, локальным актом архивуправления, основным критерием должна служить оценка вреда, который может быть причинен субъектам персональных данных, с чьими персональными данными произошло нарушение таких характеристик безопасности персональных данных.

При принятии архивуправлением решения на обеспечение характеристик безопасности персональных данных, отличных от конфиденциальности, оно должно быть определено и документально оформлено в порядке, установленном пунктом 2.18 настоящих Правил.

Обработка персональных данных без документально определенного и оформленного решения по определению характеристик безопасности персональных данных не допускается.

2.9.4. Определение сроков обработки, в том числе хранения персональных данных, осуществление контроля за соблюдением сроков обработки персональных данных и фактов достижения целей обработки персональных данных

На основании определенных целей обработки персональных данных, способов обработки и образующихся в процессе такой обработки различных видов документов устанавливаются сроки такой обработки персональных данных, в том числе хранения.

Указанные сроки должны быть определены и документально оформлены в порядке, установленном пунктом 2.18 настоящих Правил.

Определение сроков хранения осуществляется в соответствии с требованиями архивного законодательства Российской Федерации, в том числе, в соответствии с перечнями типовых архивных документов с указанием сроков их хранения.

При использовании документов, содержащих персональные данные, в различных целях, определение сроков обработки, в том числе хранения, таких документов устанавливается по максимальному сроку. При этом в случае наличия персональных данных в таких документах, обработка которых более не требуется, производятся действия по уничтожению таких данных в порядке, определяемым пунктом 2.10.8 настоящих Правил.

Включение в состав Архивного фонда Российской Федерации документов, содержащих персональные данные, осуществляется на основании экспертизы ценности документов и оформляется договором между архивным управлением Курской области и государственным или муниципальным архивом. При этом объем передаваемых документов и условия передачи определяется условиями такого договора и действующим требованиями архивного законодательства Российской Федерации.

На документы, включенные в состав Архивного фонда Российской Федерации, действие настоящих Правил не распространяется.

Обработка персональных данных без документально определенных и оформленных сроков обработки, в том числе хранения персональных данных не допускается.

С целью выполнения требования по уничтожению либо обезличиванию персональных данных по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом [1] в архивуправлении создается комиссия, определяющая факт достижения целей обработки персональных данных и достижение предельных сроков хранения документов, содержащих персональные данные. Порядок работы данной комиссии устанавливается отдельным положением. Правила, устанавливаемые таким положением, не должны противоречить настоящим Правилам.

2.10. Действия (операции) с персональными данными

Обработкой персональных данных называется любое действие (операция) или

совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая:

- сбор персональных данных,
- запись персональных данных,
- систематизацию персональных данных,
- накопление персональных данных,
- хранение персональных данных,
- уточнение (обновление) персональных данных,
- уточнение (изменение) персональных данных,
- извлечение персональных данных,
- использование персональных данных,
- передачу (распространение) персональных данных,
- передачу (предоставление) персональных данных,
- передачу (доступ) персональных данных,
- обезличивание персональных данных,
- блокирование персональных данных,
- удаление персональных данных,
- уничтожение персональных данных [1].

Указанные действия (операции) с персональными данными в информационных системах персональных данных должны быть определены и документально оформлены в порядке, установленном пунктом 2.18 настоящих Правил. При документальном оформлении действий (операций) с персональными данными рекомендуется использовать только указанные термины.

Обработка персональных данных без определенных и документально оформленных действий (операций) совершаемых с персональными данными не допускается.

2.10.1. Осуществление сбора персональных данных

2.10.1.1. Способы сбора персональных данных и источники их получения

В архивуправлении применяются следующие способы получения персональных данных субъектов персональных данных:

- заполнение субъектом персональных данных соответствующих форм (в том числе для заключения договора);
- получение персональных данных от третьих лиц;
- получение данных на основании запроса третьим лицам;
- сбор данных из общедоступных источников.

Получение персональных данных в архивуправлении допускается только:

- непосредственно от субъекта персональных данных;
- из общедоступных источников;
- от третьих лиц по основаниям, указанным в пункте 2.4.2 настоящих Правил.

Получение персональных данных из иных источников не допускается.

В связи с необходимостью постоянного контроля за наличием персональных данных в общедоступных источниках персональных данных, получение и использование таких данных является не рекомендуемым и должно осуществляться только в исключительных случаях в сроки, не превышающие необходимых для принятия соответствующего решения.

2.10.1.2. Правила сбора персональных данных

При сборе персональных данных архивуправление обязано предоставить субъекту персональных данных по его просьбе информацию, предусмотренную пунктом 2.14.6.3 настоящих Правил.

Если предоставление персональных данных является обязательным в соответствии с

федеральным законом, архивуправление обязано разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные (пункт 2.9.1 настоящих Правил).

Если основания на обработку персональных данных без согласия отсутствуют, то необходимо получение согласия субъекта персональных данных на обработку его персональных данных в соответствии с пунктом 2.15 настоящих Правил. Обработка персональных данных без получения такого согласия категорически запрещается.

Сбор персональных данных должен осуществляться с учетом правил и особых правил обработки персональных данных, предусмотренных пунктами 2.4-2.9 настоящих Правил.

Если персональные данные получены не от субъекта персональных данных, архивуправление до начала обработки таких персональных данных обязано предоставить субъекту персональных данных (в соответствии с 2.14.2 настоящих Правил) следующую информацию [1]:

- наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные права субъекта персональных данных;
- источник получения персональных данных.

Архивуправление освобождается от обязанности предоставить субъекту персональных данных сведения, в случаях, если [1]:

- субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;
- персональные данные получены архивуправлением на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
- персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
- аархивуправление осуществляет обработку персональных данных для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта персональных данных;
- предоставление субъекту персональных данных сведений, которые архивуправление обязано предоставить субъекту персональных данных до начала обработки таких персональных данных если персональные данные получены не от субъекта персональных данных, нарушает права и законные интересы третьих лиц.

2.10.2. Осуществление систематизации, накопления, уточнения и использования персональных данных

Систематизация, накопление, уточнение, использование персональных данных могут осуществляться любыми законными способами в соответствии с правилами, инструкциями, руководствами, регламентами и иными документами, определяющими технологический процесс обработки информации.

В архивуправлении могут быть установлены особенности учета персональных данных в информационных системах персональных данных, в том числе использование различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей информационной системе персональных данных, конкретному субъекту персональных данных

Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в информационных системах персональных данных, конкретному субъекту персональных данных [1].

Не допускается использование оскорбляющих чувства граждан или унижающих

человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в информационных системах персональных данных, конкретному субъекту персональных данных [1].

Уточнение персональных данных должно производиться только на основании законно полученной в установленном порядке информации.

Решение об уточнении персональных данных субъекта персональных данных принимается лицом, ответственным за организацию обработки персональных данных в архивуправлении.

Использование персональных данных должно осуществляться исключительно в заявленных целях. Использование персональных данных в заранее не определенных и не оформленных установленным образом целях категорически не допускается.

2.10.3. Осуществление записи и извлечения персональных данных

Запись персональных данных в информационные системы персональных данных архивуправления может осуществляться с любых носителей информации или из других информационных систем персональных данных.

Извлечение персональных данных из информационных систем персональных данных может осуществляться с целью:

- вывода персональных данных на бумажный или иной носитель информации, не предназначенный для его обработки средствами вычислительной техники;
- вывода персональных данных на носители информации, предназначенные для их обработки средствами вычислительной техники.

При извлечении персональных данных должен проводится учет и обозначение (в соответствии с пунктом 2.10.9 настоящих Правил) носителей информации.

При осуществлении записи и извлечения персональных данных должны соблюдаться условия обработки персональных данных, конфиденциальность персональных данных и иные требования, указанные в настоящих Правилах.

2.10.4. Осуществление передачи персональных данных

Передача персональных данных в архивуправлении должна осуществляться с соблюдением настоящих Правил и действующего законодательства Российской Федерации.

В архивуправлении приняты следующие способы передачи персональных данных субъектов персональных данных:

- передача персональных данных на электронных носителях информации посредством нарочного;
- передача персональных данных на бумажных носителях посредством нарочного;
- передача персональных данных на электронных носителях посредством почтовой связи;
- передача персональных данных на бумажных носителях посредством почтовой связи;
- передача персональных данных по каналам электрической связи.

Перед осуществлением передачи персональных данных проверяется основание на осуществление такой передачи и наличие согласия на передачу персональных данных в согласии субъекта персональных данных на обработку персональных данных или наличие иных законных оснований, предусмотренных пунктом 2.4.2 настоящих Правил.

Передача персональных данных должна осуществляться на основании:

- договора с третьей стороной, которой осуществляется передача персональных данных;
- запроса, полученного от третьей стороны, которой осуществляется передача персональных данных;
- исполнения возложенных законодательством Российской Федерации на архивуправление функций, полномочий и обязанностей.

Передача персональных данных без согласия или иных законных оснований категорически запрещается.

Передача персональных данных должна осуществляться с учетом правил и особых правил обработки персональных данных, предусмотренных пунктами 2.4-2.9 настоящих Правил.

2.10.5. Осуществление хранения персональных данных

Хранение персональных данных в архивупралении допускается только в форме документов – зафиксированной на материальном носителе информации (содержащей персональные данные) с реквизитами, позволяющими ее идентифицировать и определить субъекта персональных данных. При этом предусматриваются следующие виды документов:

- изобразительный документ – документ, содержащий информацию, выраженную посредством изображения какого-либо объекта
- фотодокумент – изобразительный документ, созданный фотографическим способом;
- текстовой документ – документ, содержащий речевую информацию, зафиксированную любым типом письма или любой системой звукозаписи;
- письменный документ – текстовой документ, информация которого зафиксирована любым типом письма;
- рукописный документ – письменный документ, при создании которого знаки письма наносят от руки;
- машинописный документ – письменный документ, при создании которого знаки письма наносят техническими средствами;
- документ на машинном носителе – документ, созданный с использованием носителей и способов записи, обеспечивающих обработку его информации электронно-вычислительной машиной.

Хранение персональных данных в архивуправлении осуществляется 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 [1].

Хранение персональных данных в информационных системах персональных данных и вне таких систем архивуправлением осуществляется только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного [1]:

- доступа к ним,
- их уничтожения,
- изменения,
- блокирования,
- копирования,
- предоставления,
- распространения.

2.10.6. Осуществление блокирования персональных данных

Блокированием персональных данных называется временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных) [1].

Блокирование персональных данных конкретного субъекта персональных данных должно осуществляться во всех информационных системах персональных данных архивуправления, включая архивы баз данных, содержащих такие персональные данные, информационных систем персональных данных.

Блокирование персональных данных в архивуправлении осуществляется:

− 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 с момента такого обращения или получения указанного запроса на период проверки;

− в случае отсутствия возможности уничтожения персональных данных в установленные сроки до их уничтожения.

После устранения выявленной неправомерной обработки персональных данных архивуправление осуществляет снятие блокирования персональных данных.

Решение о блокировании и снятии блокирования персональных данных субъекта персональных данных принимается ответственным за организацию обработки персональных данных в архивуправлении.

2.10.7. Осуществление обезличивания персональных данных

Обезличивание персональных данных в архивуправлении при обработке персональных данных с использованием средств автоматизации осуществляется с помощью специализированного программного обеспечения на основании нормативно правовых актов, правил, инструкций, руководств, регламентов, инструкций на такое программное обеспечение и иных документов для достижения заранее определенных и заявленных целей.

Допускается обезличивание персональных данных при обработке персональных данных без использования средств автоматизации производить способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание) [5].

2.10.8. Осуществление удаления и уничтожения персональных данных

Уничтожение персональных данных это 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 [1].

Уничтожение персональных данных в архивуправлении производится только в следующих случаях:

− 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;

− персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки;

− в случае выявления неправомерной обработки персональных данных, если обеспечить правомерность обработки персональных данных невозможно;

− в случае достижения цели обработки персональных данных;

− в случае отзыва субъектом персональных данных согласия на обработку его персональных данных и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных.

По факту уничтожения персональных данных обязательно проверяется необходимость уведомления об этом и в случае наличия такого требования, осуществляется уведомление указанных в таком требовании лиц, в порядке, приведенном в пункте 2.14.2 настоящих Правил.

При уничтожении персональных данных необходимо:

− убедиться в необходимости уничтожения персональных данных;

− убедиться в том, что уничтожаются те персональные данные, которые

предназначены для уничтожения;

− уничтожить персональные данные подходящим способом, в соответствии с настоящими Правилами или способом, указанным в соответствующем требовании или распорядительном документе;

− проверить необходимость уведомления об уничтожении персональных данных;

− при необходимости, уведомить об уничтожении персональных данных требуемых лиц.

При уничтожении персональных данных применяются следующие способы:

− измельчение в бумагорезательной (бумагоуничтожительной) машине – для документов исполненных на бумаге;

− тщательное вымарывание (с проверкой тщательности вымарывания) – для сохранения возможности обработки иных данных, зафиксированных на материальном носителе, содержавшем персональные данные;

− измельчение в специальной бумагорезательной (бумагоуничтожительной) машине или физическое уничтожение (разрушение) носителей информации – для носителей информации на оптических дисках;

− физическое уничтожение частей носителей информации – разрушение или сильная деформация – для носителей информации на жестком магнитном диске (уничтожению подлежат внутренние диски и микросхемы); SSD-дисках, USB- и Flash-носителях (уничтожению подлежат модули и микросхемы долговременной памяти);

− стирание с помощью сертифицированных средств уничтожения информации – для записей в базах данных и отдельных документов на машинном носителе.

При уничтожении персональных данных необходимо учитывать их наличие в архивных базах данных и производить уничтожение во всех копиях базы данных, если иное не установлено действующим законодательством Российской Федерации.

При необходимости уничтожения части персональных данных допускается уничтожать материальный носитель одним из указанных в настоящем Положении способов, с предварительным копированием сведений, не подлежащих уничтожению, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению.

Уничтожение персональных данных производится лицами, обрабатывающими персональные данные в соответствующей информационной системе персональных данных, в которой производится уничтожение персональных данных, только в присутствии лица, ответственного за организацию обработки персональных данных в архивуправлении.

По факту уничтожения персональных данных составляется Акт уничтожения персональных данных, по форме, приведенной в Приложении 6, который подписывается лицами, производившими уничтожение, заверяется лицом, ответственным за организацию обработки персональных данных в архивуправлении, присутствовавшим при уничтожении и утверждается начальником.

Хранение актов уничтожения персональных данных осуществляется в течении срока исковой давности, если иное не установлено нормативно-правовыми актами Российской Федерации.

2.10.9. Способы обозначения документов содержащих персональные данные

С целью доведения до сотрудников архивуправления фактов работы с документами, содержащими персональные данные, все такие документы (в том числе машинные носители и документы в электронном виде) подлежат специальному обозначению (маркированию или визуальному выделению).

На документах в правом верхнем углу проставляется:

− в первой строке: **Содержит персональные данные**;

− во второй строке: архивуправление.

В третьей строке, при необходимости, дополнительно могут проставляться иные реквизиты документа, в том числе его регистрационный номер по журналам учета.

Ответственным за специальное обозначение документов является их исполнитель.

Специальное обозначение осуществляется при печати документов машинным способом или путем проставления штампа (клише) на ранее созданных документах и машинных носителях (в свободном месте на имеющихся наклейках или на специально наклеенном листе или корпусе носителя).

Специальное обозначение ранее созданных документов должно производиться при обращении к ним.

2.11. Круг субъектов, персональные данные которых подлежат обработке

Круг субъектов, персональные данные которых подлежат обработке в информационных системах персональных данных архивуправления, определяется целью обработки персональных данных в каждой информационной системе персональных данных.

2.12. Перечни должностей сотрудников, замещение которых предусматривает осуществление обработки персональных данных

Лицо, ответственное за организацию обработки персональных данных в архивуправлении готовит и уточняет:

− перечень должностей сотрудников архивуправления, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, в котором указываются должности сотрудников архивуправления, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным для каждой информационной системы персональных данных архивуправления [7];

− перечень должностей сотрудников архивуправления, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных [7].

Указанные перечни должностей сотрудников архивуправления подписываются лицом, ответственным за организацию обработки персональных данных в архивуправлении и утверждаются.

2.13. Права и обязанности при обработке персональных данных

2.13.1. Права и обязанности субъекта персональных данных

2.13.1.1. Права субъекта персональных данных

Субъект персональных данных, чьи персональные данные обрабатываются в архивуправлении, имеет право [1]:

− на получение сведений о подтверждении факта обработки персональных данных архивуправлением;

− на получение сведений о правовых основаниях и цели обработки персональных данных;

− на получение сведений о цели и применяемых архивуправлением способов обработки персональных данных;

− на получение сведений о наименовании и месте нахождения архивуправления, сведений о лицах (за исключением сведений о сотрудниках архивуправления), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с архивуправлением или на основании федерального закона;

− на получение сведений о обрабатываемых персональных данных, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной

порядок представления таких данных не предусмотрен федеральным законом;

- на получение сведений о сроках обработки персональных данных, в том числе сроках их хранения;
- на получение сведений о порядке осуществления субъектом персональных данных своих прав, предусмотренных законодательством в области персональных данных;
- на получение информации об осуществленной или о предполагаемой трансграничной передаче данных;
- на получение сведений о наименовании и адресе лица, осуществляющего обработку персональных данных по поручению архивуправления, если обработка поручена или будет поручена такому лицу;
- на получение иных сведений, предусмотренных законодательством в области персональных данных и другими федеральными законами;
- требовать от архивуправления 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;
- принимать предусмотренные законом меры по защите своих прав;
- требовать от архивуправления предоставления ему персональных данных в доступной форме;
- повторного обращения и запроса в целях получения сведений и ознакомления с его персональными данными;
- требовать разъяснения порядка принятия решения на основании исключительно автоматизированной обработки его персональных данных;
- заявить возражение против принятия решения 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;
- требовать разъяснения порядка принятия и возможные юридические последствия принятия решения 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, а также разъяснения порядка защиты субъектом персональных данных своих прав и законных интересов;
- обжаловать действия или бездействие архивуправления в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке, если субъект персональных данных считает, что архивуправление осуществляет обработку его персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы;
- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке;
- требовать предоставления безвозмездно субъекту персональных данных или его представителю возможности ознакомления с персональными данными, относящимися к этому субъекту персональных данных;
- принимать решение о предоставлении его персональных данных и давать согласие на их обработку свободно, своей волей и в своем интересе;
- отзывать согласие на обработку персональных данных.

Кроме указанных прав в вопросах обработки его персональных данных субъект персональных данных обладает другими правами, предоставляемыми ему действующим законодательством Российской Федерации.

2.13.1.2. Обязанности субъекта персональных данных

Субъект персональных данных, чьи персональные данные обрабатываются в архивуправлении, обязан [1]:

- предоставлять свои персональные данные в случаях, когда федеральными законами предусматриваются случаи обязательного предоставления субъектом персональных данных своих персональных данных;
- с целью соблюдения его законных прав и интересов подавать только достоверные персональные данные.

Кроме указанных обязанностей в вопросах обработки его персональных данных на субъекта персональных данных налагаются иные обязанности, предусмотренные действующим законодательством Российской Федерации.

2.13.2. Права и обязанности архивуправления при обработке персональных данных субъектов персональных данных

2.13.2.1. Права архивуправления при обработке персональных данных субъектов персональных данных

Архивуправление при обработке персональных данных субъектов персональных данных имеет право [1]:

- обрабатывать персональные данные в соответствии с пунктом 2.4.2 настоящих Правил;
- поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта;
- мотивированно отказать субъекту персональных данных в выполнении повторного запроса в целях получения сведений касающейся обработки его персональных данных, при нарушении субъектом персональных данных своих обязанностей по подаче такого запроса;
- ограничить право субъекта персональных данных на доступ к его персональным данным в соответствии с федеральными законами, в том числе, если обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- ограничить право субъекта персональных данных на доступ к его персональным данным в соответствии с федеральными законами, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;
- отказать субъекту персональных данных в выполнении запроса в целях получения сведений касающейся обработки его персональных данных в случае, если субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором или архивуправлением;
- отказать субъекту персональных данных в выполнении запроса в целях получения сведений касающейся обработки его персональных данных в случае, если персональные данные получены на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
- отказать субъекту персональных данных в выполнении запроса в целях получения сведений касающейся обработки его персональных данных в случае, если персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
- отказать субъекту персональных данных в выполнении запроса в целях получения

сведений касающейся обработки его персональных данных в случае, если оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта персональных данных;

- отказать субъекту персональных данных в выполнении запроса в целях получения сведений касающейся обработки его персональных данных в случае, если предоставление субъекту персональных данных таких сведений, нарушает права и законные интересы третьих лиц;
- самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных действующим законодательством в области персональных данных, если иное не предусмотрено указанным законом и другими федеральными законами;
- если обеспечить правомерность обработки персональных данных невозможно, осуществлять или обеспечивать осуществление блокирования или уничтожения персональных данных в сроки, указанные в пункте 2.14.1 настоящих Правил;
- в случае достижения цели обработки персональных данных осуществлять или обеспечивать осуществление уничтожения персональных данных в сроки, указанные в пункте 2.14.1 настоящих Правил;
- в случае достижения цели обработки персональных данных продолжить обработку персональных данных, если это предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между архивуправлением и субъектом персональных данных;
- в случае достижения цели обработки персональных данных продолжить обработку персональных данных, если обработка персональных данных осуществляется без согласия субъекта персональных данных на основаниях, предусмотренных пунктом 2.4.2 настоящих Правил или федеральными законами;
- в случае отзыва субъектом персональных данных согласия на обработку его персональных данных продолжить обработку персональных данных, если это предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между архивуправлением и субъектом персональных данных;
- в случае отзыва субъектом персональных данных согласия на обработку его персональных данных продолжить обработку персональных данных, если обработка персональных данных осуществляется без согласия субъекта персональных данных на основаниях, предусмотренных пунктом 2.4.2 настоящих Правил или федеральными законами;
- в случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пункте 2.14.1 настоящих Правил, осуществить блокирование таких персональных данных и обеспечить уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами;
- осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных, указанных в пункте 2.16 настоящих Правил

Кроме указанных прав в вопросах обработки персональных данных субъектов персональных данных архивуправление обладает другими правами, предоставляемыми ему действующим законодательством Российской Федерации.

2.13.2.2. Обязанности архивного управления Курской области при обработке персональных данных субъектов персональных данных

Архивуправление при обработке персональных данных субъектов персональных данных обязан:

− строго соблюдать принципы обработки персональных данных, указанные в пункте 2.2 настоящих Правил [1];
− строго соблюдать правила обработки персональных данных, указанные в пункте 2.4-2.6 настоящих Правил [1];
− в случае если, обработка персональных данных осуществляется по поручению оператора, строго соблюдать и выполнять требования поручения оператора [1];
− не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом [1];
− по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов исключить из общедоступных источников персональных данных сведения о субъекте персональных данных [1];
− обеспечить конкретность и информированность согласия на обработку персональных данных [1];
− получать согласие на обработку персональных данных в форме, указанной в пункте 2.15 настоящих Правил [1];
− в случае получения согласия на обработку персональных данных от представителя субъекта персональных данных проверять полномочия данного представителя на дачу согласия от имени субъекта персональных данных [1];
− предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований обработки персональных данных без получения согласия [1];
− строго соблюдать требования к содержанию согласия в письменной форме субъекта персональных данных на обработку его персональных данных в соответствии с пунктом 2.15 настоящих Правил [1];
− незамедлительно прекратить обработку специальных категорий персональных данных если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом [1];
− убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных [1];
− предоставить субъекту персональных данных сведения по запросу субъекта персональных данных 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 [1];
− мотивировать и представить доказательства обоснованности отказа в выполнении повторного запроса субъекта персональных данных [1];
− доказывать, что от субъекта персональных данных было получено предварительное согласие на обработку персональных данных в целях политической агитации [1];
− немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных в целях политической агитации [1];
− разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов [1];
− рассмотреть возражение против принятия решения на основании исключительно автоматизированной обработки его персональных данных в течение срока указанного в пункте 2.14.1 настоящих Правил и уведомить субъекта персональных данных о результатах рассмотрения такого возражения [1];

- предоставить субъекту персональных данных по его просьбе информацию, касающуюся обработки его персональных данных [1];
- разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные, если предоставление персональных данных является обязательным в соответствии с федеральным законом
- до начала обработки персональных данных, полученных не от субъекта персональных данных, предоставить субъекту персональных данных информацию о своем наименовании и адресе, цели обработки персональных данных и ее правовом основании, предполагаемых пользователей персональных данных, установленные права субъекта персональных данных, источник получения персональных данных [1];
- принимать меры, необходимые и достаточные для обеспечения выполнения своих обязанностей в области персональных данных, если иное не предусмотрено федеральными законами [1];
- 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 [1];
- по запросу уполномоченного органа по защите прав субъектов персональных данных представить документы и локальные акты, определяющие политику в отношении обработки персональных данных и сведения о реализуемых требованиях к защите персональных данных [1];
- 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 [1];
- сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо при получении запроса субъекта персональных данных или его представителя [1];
- в случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя дать в письменной форме мотивированный ответ [1];
- предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных
- внести в персональные данные необходимые изменения или уничтожить такие персональные данные в случае предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными [1];
- строго соблюдать сроки по уведомлениям, блокированию и уничтожению персональных данных в соответствии с пунктом 2.14.1 настоящих Правил [1];
- 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 [1];
- сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию [1];
- в случае выявления неправомерной обработки персональных данных при

обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки [1];

- 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 [1];
- уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и снять блокирование персональных данных в случае подтверждения факта неточности персональных данных на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов [1];
- прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора в случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора [1];
- уничтожить персональные данные или обеспечить их уничтожение в случае, если обеспечить правомерность обработки персональных данных невозможно [1];
- 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 об устранении допущенных нарушений или об уничтожении персональных данных [1];
- 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 случае достижения цели обработки персональных данных, если обработка персональных данных осуществляется без согласия субъекта персональных данных на основаниях, предусмотренных пунктом 2.4.2 настоящих Правил или федеральными законами [1];
- 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 случае отзыва субъектом персональных данных согласия на обработку его персональных данных, если обработка персональных данных осуществляется без согласия субъекта персональных данных на

основаниях, предусмотренных пунктом 2.4.2 настоящих Правил или федеральными законами [1];

− уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных в соответствии с пунктом 2.16 настоящих Правил [1];

− уведомить уполномоченный орган по защите прав субъектов персональных данных в случае изменения сведений, указанных в уведомлении о своем намерении осуществлять обработку персональных данных [1];

− назначить лицо, ответственное за организацию обработки персональных данных [1];

− предоставлять лицу, ответственному за организацию обработки персональных данных, необходимые сведения, указанные в пункте 2.14.3 настоящих Правил [1];

− неукоснительно соблюдать все требования настоящих Правил;

− ознакомить сотрудников архивуправления, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучить таких сотрудников [1];

Кроме указанных обязанностей в вопросах обработки персональных данных субъектов персональных данных на архивуправление налагаются иные обязанности, предусмотренные действующим законодательством Российской Федерации.

2.13.2.3. Меры, направленные на обеспечение выполнения оператором своих обязанностей

Архивуправление принимает меры, необходимые и достаточные для обеспечения выполнения своих обязанностей, предусмотренных законодательством Российской Федерации в области персональных данных [1]. Архивуправление определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения указанных обязанностей, в том числе:

− назначает ответственного за организацию обработки персональных данных в архивуправлении из числа сотрудников данного органа (пункт 2.14.3 настоящих Правил) [1, 8];

− разрабатывает и утверждает должностную инструкцию ответственного за организацию обработки персональных данных в государственном или муниципальном органе (пункт 2.14.3 настоящих Правил) [1, 8];

− создает комиссию, в целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям (пункт 4 настоящих Правил) [7];

− издает и утверждает приказом начальника архивуправления правила обработки персональных данных (настоящие Правила) [1, 8], включающие в себя:

− процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (пункт 2.13.2.4 настоящих Правил) [1, 8];

− порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований (пункт 2.10.8 настоящих Правил) [1, 8];

− правила рассмотрения запросов субъектов персональных данных или их представителей (пункты 2.14.5-2.14.6 настоящих Правил) [1, 8];

− правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям законодательства Российской Федерации в в области персональных данных и локальным актам архивуправления (пункт 4 настоящих Правил)

[1, 8];

- правила работы с обезличенными данными (пункт 2.10.7 настоящих Правил) [7];
- типовую форму согласия на обработку персональных данных субъектов персональных данных (пункт 2.16, Приложение 3 настоящих Правил) [7];
- типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные (пункт 2.14.4 и Приложение 5 настоящих Правил) [7];
- оценку вреда, который может быть причинен субъектам персональных данных в случае в случае нарушения требований по обработке и обеспечению безопасности персональных данных (пункты 2.9.2 и 2.18 настоящих Правил) [1];
- издает и утверждает приказом начальника документ, определяющий соотношение вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных, и принимаемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством Российской Федерации в области персональных данных [1];
- издает и утверждает приказом архивуправления перечень информационных систем персональных данных (пункт 2.20 и Приложение 2 настоящих Правил) [7];
- издает и утверждает приказом архивуправления правила обработки персональных данных, определяющие для каждой информационной системы персональных данных:
- цели обработки персональных данных содержание обрабатываемых персональных данных (пункты 2.3 и 2.18 настоящих Правил) [1, 8];
- категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения (пункт 2.18 настоящих Правил) [1, 8];
- перечни персональных данных, обрабатываемых в государственном или муниципальном органе в связи с реализацией трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций (пункты 2.8 и 2.18 настоящих Правил) [7];
- перечень должностей сотрудников государственного или муниципального органа, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (пункт 2.21 настоящих Правил) [7];
- перечень должностей сотрудников государственного или муниципального органа, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных (пункт 2.21 настоящих Правил) [7];
- типовое обязательство служащего государственного или муниципального органа, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним государственного или муниципального контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей (пункт 2.21 и Приложение 8 настоящих Правил) [7];
- порядок доступа сотрудников государственного или муниципального органа в помещения, в которых ведется обработка персональных данных (пункт 2.22 настоящих Правил) [7];
- принимают правовые, организационные и технические меры по обеспечению безопасности персональных данных при их обработке, предусмотренные законодательством Российской Федерации в области персональных данных (пункт 3 настоящих Правил) [1, 8];
- осуществляют ознакомление сотрудников государственного или муниципального органа, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных и (или) организуют обучение указанных сотрудников (пункты 2.21 и 3.8 настоящих Правил) [1, 8];

− уведомляют уполномоченный орган по защите прав субъектов персональных данных об обработке (намерении осуществлять обработку) персональных данных (пункт 2.16 настоящих Правил) [1, 8].

Указанные документы, являются документами, определяющими политику в отношении обработки персональных данных в архивуправлении и подлежат опубликованию на официальном сайте архивуправления в течение 10 дней после их утверждения [1, 8]. К указанным документам обеспечивается неограниченный доступ [1].

2.13.2.4. Процедуры, направленные на предотвращение и выявление нарушений законодательства в отношении обработки персональных данных и устранение таких последствий

К процедурам, направленным на предотвращение и выявление нарушений законодательства в отношении обработки персональных данных и устранение таких последствий относятся:

− реализация мер, направленных на обеспечение выполнения оператором своих обязанностей (пункт 2.13.2.3 настоящих Правил);

− выполнение предусмотренных законодательством в области персональных данных обязанностей, возложенных на архивуправление [1];

− личная ответственность сотрудников архивуправления, осуществляющих обработку либо осуществление доступа к персональным данным;

− организация рассмотрения запросов субъектов персональных данных или их представителей и ответов на такие запросы [1, 8];

− организация внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным действующим законодательством в области персональных данных и локальными актами архивуправления [1, 8];

− сокращение объема обрабатываемых данных;

− сокращение должностей сотрудников, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

− стандартизация операций осуществляемых с персональными данными;

− определение порядка доступа сотрудников архивуправления в помещения, в которых ведется обработка персональных данных [7];

− проведение необходимых мероприятий по обеспечению безопасности персональных данных и носителей их содержащих [1, 8];

− проведение периодических проверок условий обработки персональных данных [1, 8];

− повышение осведомленности сотрудников, занимающих должности, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, путем их ознакомления, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами архивуправления по вопросам обработки персональных данных и (или) организация обучения указанных сотрудников [1, 8];

− блокирование, внесение изменений и уничтожение персональных данных в предусмотренных действующим законодательством в области персональных данных случаях [1];

− оповещение субъектов персональных данных в предусмотренных действующим законодательством в области персональных данных случаях [1];

− разъяснение прав субъектам персональных данных в вопросах обработки и обеспечения безопасности их персональных данных [1];

− оказание содействия правоохранительным органам, в случаях нарушений

законодательства в отношении обработки персональных;

− публикация на официальном сайте архивуправления документов, определяющих политику в отношении обработки персональных данных [1, 8].

Указанный перечень процедур, направленных на предотвращение и выявление нарушений законодательства в отношении обработки персональных данных и устранение таких последствий является открытым и может дополняться мероприятиями в конкретных случаях.

2.14. Порядок взаимодействия с субъектами персональных данных и иными лицами

Настоящие Правила при определении порядка взаимодействия архивуправления с субъектами персональных данных устанавливают:

− сроки выполнения действий по защите прав субъектов персональных данных;

− требования по уведомлениям/предоставлению информации субъектов персональных данных и в иных случаях;

− требования к лицам, ответственным за организацию обработки персональных данных;

− порядок разъяснения субъектам персональных данных особенностей обработки персональных данных и порядка защиты их прав;

− порядок реагирования на обращения субъектов персональных данных;

− порядок действий при обращениях субъектов персональных данных;

− требования к форме запроса на предоставления персональных данных и сведений об операторе субъектом персональных данных;

− порядок и основание отказа субъекту персональных данных в предоставлении сведений о его персональных данных;

− порядок, форма предоставления персональных данных и сведений об операторе и объем предоставляемой информации;

− действия в случае выявления фактов нарушения законодательства, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных;

− порядок реализации права субъекта персональных данных на обжалование действий или бездействия архивупраления;

− порядок действий при достижении целей обработки персональных данных и отзыве согласия на обработку персональных данных;

− порядок действий при отзыве согласия субъекта персональных данных на обработку его персональных данных.

2.14.1. Установленные сроки выполнения действий по защите прав субъектов персональных данных

В архивуправлении устанавливаются следующие сроки по защите прав субъектов персональных данных:

− в случае если **сведения**, а также **обрабатываемые персональные данные были предоставлены** для ознакомления субъекту персональных данных **по** его **запросу**, субъект персональных данных вправе обратиться повторно в архивуправление или направить ему повторный запрос в целях получения таких сведений, и ознакомления с такими персональными данными **не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса**, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных [1];

− в случае **отказа в предоставлении информации** о наличии персональных данных о соответствующем субъекте персональных данных **или персональных данных** субъекту персональных данных или его представителю при их обращении либо при получении запроса

субъекта персональных данных или его представителя архивного управления Курской области **обязан дать в письменной форме мотивированный ответ**, содержащий ссылку на положение федерального закона, являющееся основанием для такого отказа, **в срок, не превышающий тридцати дней со дня обращения субъекта** персональных данных или его представителя **либо с даты получения запроса** субъекта персональных данных или его представителя [1];

- **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**, архивное управление Курской области обязано внести в них необходимые изменения [1];
- **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, архивное управление Курской области обязано уничтожить такие персональные данные [1];
- **в случае выявления неправомерной обработки** персональных данных, осуществляемой архивуправлением или лицом, действующим по его поручению, архивуправление **в срок, не превышающий трех рабочих дней с даты этого выявления**, обязано прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по его поручению [1];
- **в случае если обеспечить правомерность обработки персональных данных невозможно**, архивуправление **в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки** персональных данных, обязано уничтожить такие персональные данные или обеспечить их уничтожение [1];
- **в случае достижения цели обработки** персональных данных архивуправление обязано прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по его поручению) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по его поручению) **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 архивуправлением и субъектом персональных данных, **либо если** архивуправление **не вправе осуществлять обработку персональных данных без согласия** субъекта персональных данных на основаниях, предусмотренных федеральными законами [1];
- **в случае отзыва** субъектом персональных данных **согласия на обработку** его персональных данных архивуправление обязано прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по его поручению) 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 его поручению) **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** архивуправление **не вправе осуществлять обработку персональных данных без согласия** субъекта персональных данных на основаниях, предусмотренных федеральными законами [1];
- **в случае отсутствия возможности уничтожения** персональных данных в течение

указанных сроков, архивуправление осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по его поручению) и обеспечивает уничтожение персональных данных **в срок не более чем шесть месяцев, если иной срок не установлен** федеральными законами [1];

− архивуправление обязано рассмотреть возражение субъекта персональных данных **о принятии на основании исключительно автоматизированной обработки** персональных данных решений, порождающих юридические последствия в отношении него или иным образом затрагивающих его права и законные интересы, **в течение тридцати дней со дня его получения** и уведомить субъекта персональных данных о результатах рассмотрения такого возражения [1];

− архивуправление обязано сообщить в установленном порядке, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также **предоставить** возможность ознакомления с этими персональными данными **при обращении** субъекта персональных данных или его представителя **либо в течение тридцати дней с даты получения запроса субъекта** персональных данных или его представителя [1];

− архивуправление обязано сообщить в уполномоченный орган по защите прав субъектов персональных данных **по запросу** этого органа необходимую информацию **в течение тридцати дней с даты получения такого запроса** [1];

– в случае подтверждения факта неточности персональных данных архивуправление 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 его поручению) **в течение семи рабочих дней со дня представления таких сведений** и снять блокирование персональных данных [1].

Установленные сроки обязательны к исполнению всеми должностными лицами архивуправления;

− в **случае изменения сведений**, указных в уведомлении об обработке персональных данных, а также в **случае прекращения обработки** персональных данных архивуправление обязано уведомить об этом уполномоченный орган по защите прав субъектов персональных данных **в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки** персональных данных.

2.14.2. Требования по уведомлениям (предоставлению информации, разъяснениям) субъектов персональных данных и в иных случаях

Архивуправление обязано осуществлять уведомления и предоставлять информацию в следующих случаях:

− архивуправление обязано **разъяснить** субъекту персональных данных **порядок принятия решения на основании исключительно автоматизированной обработки** его персональных данных и **возможные юридические последствия** такого решения, **предоставить возможность заявить возражение** против такого решения, а также **разъяснить порядок защиты** субъектом персональных данных **своих прав и законных интересов** [1];

− архивуправление обязано рассмотреть **возражение** субъекта персональных данных **о принятии на основании исключительно автоматизированной обработки** персональных данных решений, порождающих юридические последствия в отношении него или иным образом затрагивающих его права и законные интересы, в течение тридцати дней со дня его получения и **уведомить субъекта персональных данных о результатах рассмотрения такого возражения** [1];

– **если предоставление персональных данных** является **обязательным в соответствии с федеральным законом**, архивуправление обязано **разъяснить** субъекту персональных данных **юридические последствия отказа предоставить его персональные данные**;

− архивуправление обязано **предоставить** безвозмездно субъекту персональных данных или его представителю **возможность ознакомления с персональными данными**, относящимися к этому субъекту персональных данных;

− архивуправление обязано **уведомить** субъекта персональных данных или его представителя **о внесенных изменениях и предпринятых мерах** в случаях когда персональные данные являются неполными, неточными или неактуальными и персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки и **принять разумные меры для уведомления третьих лиц**, которым персональные данные этого субъекта были переданы;

− об **устранении допущенных нарушений или об уничтожении** персональных данных **в случае выявления неправомерной обработки** персональных данных ааархивуправление **обязано 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**;

− архивуправление **до начала обработки** персональных данных **обязан уведомить уполномоченный орган по защите прав субъектов персональных данных** о своем намерении осуществлять обработку персональных данных;

– **в случае изменения** сведений, а также **в случае прекращения обработки** персональных данных архивуправление обязано **уведомить об этом уполномоченный орган по защите прав субъектов персональных данных**;

− обязанность **предоставить доказательство получения согласия** субъекта персональных данных на обработку его персональных данных или **доказательство наличия иных законных оснований** возлагается на оператора;

− персональные данные **могут быть получены** архивуправление **от лица, не являющегося** субъектом персональных данных, **при условии предоставления им подтверждения наличия законных оснований** обработки, в том числе передачи таких персональных данных;

− архивуправлением **должны быть предоставлены** субъекту персональных данных запрашиваемые им сведения 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;

− сведения, запрашиваемые субъектом персональных данных, **предоставляются** субъекту персональных данных или его представителю **при обращении либо при получении запроса** субъекта персональных данных или его представителя;

− обязанность **представления доказательств обоснованности** мотивированного **отказа** в выполнении повторного запроса субъекта персональных данных лежит на архивуправлении;

− архивуправление обязано **разъяснить** субъекту персональных **данных порядок принятия решения на основании исключительно автоматизированной обработки** его персональных данных и **возможные юридические последствия** такого решения, **предоставить возможность заявить возражение** против такого решения, а также **разъяснить порядок защиты** субъектом персональных данных своих **прав и законных интересов**;

– **при сборе** персональных данных архивуправление обязано по просьбе субъекта

персональных данных **предоставить** информацию, касающуюся обработки его персональных данных;

- если персональные данные получены не от субъекта персональных данных, архивуправление, до начала обработки таких персональных данных обязано предоставить субъекту персональных данных информацию, касающуюся обработки его персональных данных;
- архивуправление **по запросу** уполномоченного органа по защите прав субъектов персональных данных обязано **представить** документы и локальные акты, и (или) иным образом **подтвердить принятие мер**, направленных на обеспечение выполнения оператором обязанностей, предусмотренных действующим законодательством в области персональных данных;
- архивупраление обязано **сообщить** субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также **предоставить** возможность ознакомления с этими персональными данными **при обращении** субъекта персональных данных или его представителя;
- архивуправление обязано **предоставить** безвозмездно субъекту персональных данных или его представителю **возможность ознакомления** с персональными данными, относящимися к этому субъекту персональных данных;
- архивуправление обязано **уведомить** субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах **в случае выявления того, что персональные данные являются неполными, неточными или неактуальными или являются незаконно полученными или не являются необходимыми для заявленной цели** обработки и **принять** разумные **меры для уведомления третьих лиц**, которым персональные данные этого субъекта были переданы;
- архивуправление обязано **сообщить** в уполномоченный орган по защите прав субъектов персональных данных **по запросу этого органа** необходимую информацию;
- архивуправление обязано **предоставлять** лицу, ответственному за организацию обработки персональных данных в архивном управлении Курской области сведения, предусмотренные действующим законодательством в области персональных данных.

Архивуправление освобождается от обязанности предоставить субъекту персональных данных сведения об обрабатываемых персональных данных, относящихся к субъекту персональных данных, в случаях, если:

- субъект персональных данных уведомлен об осуществлении обработки его персональных данных архивуправлением;
- персональные данные получены архивуправлением на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
- персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
- архивуправление осуществляет обработку персональных данных для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта персональных данных;
- предоставление субъекту персональных данных нарушает права и законные интересы третьих лиц.

Уведомление в указанных случаях готовиться лицом, ответственным за организацию обработки персональных данных в архивуправление. Подготовленное уведомление утверждается начальником архивуправления. Отправка уведомления осуществляется лицом, ответственным за организацию обработки персональных данных в архивуправлении в установленные настоящими Правилами (пункт 2.14.1) сроки.

Форма уведомлений о совершенных операциях над персональными данными

приведена в Приложении 4.

Требования к уведомлению уполномоченного органа по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных и об изменении поданных сведений устанавливаются настоящими Правилами (пункт 2.16).

2.14.3. Лица, ответственные за организацию обработки персональных данных

Заместитель начальника архивуправления назначается, ответственным лицом за организацию обработки персональных данных в архивуправлении.

Архивуправление предоставляет лицу, ответственному за организацию обработки персональных данных сведения об обработке персональных данных в архивуправлении, в соответствии с требованиями действующего законодательства в области персональных данных [1].

Архивуправление разрабатывает должностную инструкцию ответственного за организацию обработки персональных данных в архивуправлении [7].

Основными обязанностями лица, ответственного за организацию обработки персональных данных в архивуправлении:

− осуществление внутреннего контроля за соблюдением архивуправлением и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных [1];

− доведение до сведения сотрудников архивуправления положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных [1];

− организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов [1].

2.14.4. Порядок разъяснения субъектам персональных данных особенностей обработки персональных данных и порядка защиты их прав

Сотрудники архивуправления обязаны разъяснять субъектам персональных данных особенности обработки персональных данных и порядок защиты их прав в следующих случаях:

− при принятии решения на основании исключительно автоматизированной обработки его персональных данных – разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных, возможные юридические последствия такого решения, а также порядок защиты субъектом персональных данных своих прав и законных интересов [1];

− если предоставление персональных данных является обязательным в соответствии с федеральным законом – разъяснить субъекту персональных данных юридические последствия отказа предоставить свои персональные данные [1].

Разъяснение субъектам персональных данных особенностей обработки персональных данных и порядка защиты их прав осуществляется сотрудниками архивуправления, осуществляющими непосредственные операции по обработке персональных данных или лицом, ответственным за организацию обработки персональных данных в архивуправлении.

Разъяснения осуществляются на основании настоящих Правил, правил обработки персональных данных в конкретных информационных системах персональных данных в архивуправлении и действующего законодательства Российской Федерации в области персональных данных.

Для разъяснения субъектам персональных данных особенностей обработки персональных данных и порядка защиты их прав используются официальный сайт архивуправления, стенды, раздаточный материал.

2.14.5. Порядок реагирования на обращения субъектов персональных данных

Все обращения субъектов персональных данных принимаются в письменном виде и подлежат учету, наряду с остальными входящими документами.

С целью соблюдения сроков по реагированию на обращения субъектов персональных данных они должны незамедлительно передаваться лицу, ответственному за организацию обработки персональных данных в архивуправлении.

Ответы на обращения, не отвечающие требованиям, предъявляемым к ним действующим законодательством в области персональных данных, не производятся [1].

Передача ответов субъекту персональных данных осуществляется требуемым им способом, или, если такой способ не указан, посредством отправки заказного письма с уведомлением.

Передача ответов на обращения субъектов персональных данных осуществляется в установленном в архивуправлении для исходящей корреспонденции порядке с соблюдением указанных в пункте 2.14.1 настоящих Правил сроков.

2.14.6. Порядок действий при обращениях субъектов персональных данных

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, при личном обращении в архивуправлении, либо путем направления запроса, в том числе в форме электронного документа, подписанного электронной подписью в соответствии с законодательством Российской Федерации [1].

2.14.6.1. Требования к форме запроса на предоставления персональных данных и сведений об операторе субъектом персональных данных

Письменный запрос субъекта персональных данных на получение информации, касающейся обработки его персональных данных архивуправления должен содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя [1];
- сведения о дате выдачи указанного документа и выдавшем его органе [1];
- сведения, подтверждающие участие субъекта персональных данных в отношениях с архивуправлением (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных архивуправлением [1];
- подпись субъекта персональных данных или его представителя [1].

Письменные запросы, не отвечающие указанным требованиям, обработке не подлежат.

При личном обращении в архивуправление субъект персональных данных обязан предъявить документ, удостоверяющий его личность, а его представитель – документ, удостоверяющий личность представителя и документы, подтверждающие полномочия этого представителя, и сообщить сведения, подтверждающие участие субъекта персональных данных в отношениях с архивуправлением (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных архивуправлением.

Данные предоставляемые субъектом персональных данных при личном обращении в архивуправление фиксируется в Журнале учета лиц (организаций), получивших доступ к персональным данным, и (или) лиц (организаций), которым такая информация была предоставлена или передана (Приложение 7 к настоящим Правилам).

2.14.6.2. Порядок и основание отказа субъекту персональных данных в предоставлении сведений о его персональных данных

Право субъекта персональных данных на доступ к своим персональным данным ограничивается в следующих случаях если:

- обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма [1];
- доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц [1].

В случае отказа в предоставлении субъекту персональных данных при обращении информации, касающейся обработки его персональных данных архивуправлением, либо при получении запроса субъекта персональных данных о такой информации, лицо, ответственное за организацию обработки персональных данных в архивуправлении, составляет в письменной форме мотивированный ответ, содержащий ссылку на пункты или статьи федерального закона, являющегося основанием для такого отказа.

2.14.6.3. Порядок, форма предоставления персональных данных и сведений об операторе и объем предоставляемой информации

Предоставление доступа к своим персональным данным в случае непосредственного обращения субъекта персональных данных осуществляется только по адресу: г. Курск, ул. Ленина, д. 57, архивное управление Курской области. Доступ субъекта персональных данных в этом случае осуществляется в порядке, установленном в пункте 2.14.6.1 настоящих Правил.

Субъект персональных данных имеет право на получение при обращении или при подаче запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных архивуправлением [1];
- правовые основания и цели обработки персональных данных [1];
- цели и применяемые архивуправлением способы обработки персональных данных [1];
- наименование и место нахождения архивуправления, сведения о лицах (в том числе о сотрудниках архивуправления в объеме, предусмотренном пунктом 2.12 настоящих Правил), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с архивуправлением или на основании федерального закона [1];
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом [1];
- сроки обработки персональных данных, в том числе сроки их хранения [1];
- порядок осуществления субъектом персональных данных прав, предусмотренных законодательством в области персональных данных [1];
- информацию об осуществленной или о предполагаемой трансграничной передаче данных [1];
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению архивуправления, если обработка поручена или будет поручена такому лицу [1];
- иные сведения, предусмотренные законодательством в области персональных данных или другими федеральными законами [1].

Ответ на обращения и запросы субъектов персональных данных готовится лицом, ответственным за организацию обработки персональных данных в архивуправлении, по существу такого обращения в двух экземплярах. Запрашиваемые сведения

предоставляются в соответствии с настоящими Правилами, правилами обработки персональных данных в конкретных информационных системах персональных данных архивуправления и действующего законодательства Российской Федерации в области персональных данных.

Сведения о наличии персональных данных должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных [1].

Форму предоставления данных определяет лицо, ответственное за организацию обработки персональных данных в архивуправлении, если она не оговорена в таком обращении или запросе. Форма ответа на обращение или запрос субъекта персональных данных не должна противоречить установленным в архивуправлении требованиям по защите информации и обеспечению безопасности персональных данных.

Хранение информации об обращении или запрос субъекта персональных данных, а так же второй экземпляр ответа на такое обращение или запрос, хранятся установленным в архивуправлении порядке.

2.14.6.4. Действия в случае выявления фактов нарушения законодательства, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных

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 архивуправление осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки [1].

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 архивуправление осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает 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 [1].

В случае подтверждения факта неточности персональных данных архивуправление на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов уточняет персональные данные либо обеспечивает их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и снимает блокирование персональных данных [1].

В случае выявления неправомерной обработки персональных данных, осуществляемой архивуправлением или лицом, действующим по поручению оператора, архивуправление прекращает неправомерную обработку персональных данных или обеспечивает прекращение неправомерной обработки персональных данных лицом, действующим по поручению архивуправления [1].

В случае если обеспечить правомерность обработки персональных данных невозможно, архивуправление уничтожает такие персональные данные или обеспечивает их уничтожение [1].

Об устранении допущенных нарушений или об уничтожении персональных данных архивуправление уведомляет субъект 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 [1].

При совершении указанных действий должны соблюдаться сроки, установленные в пункте 2.14.1 настоящих Правил.

При обнаружении нарушений правил обработки или обеспечения безопасности персональных данных лицо, ответственное за организацию обработки персональных данных в архивуправлении Курской области незамедлительно принимает меры по устранению таких нарушений и минимизации их последствий. При этом должен проводиться анализ таких нарушений и приниматься меры по их недопущению в дальнейшем.

В случае если произошло нарушение прав субъекта персональных данных и данное нарушение может повлиять на нарушение прав такого субъекта в дальнейшем, архивуправление организует оповещение этого субъекта о возможных последствиях выявленных нарушений и принятых по ним мерам. Порядок такого оповещения устанавливается в каждой конкретной ситуации лицом, ответственным за организацию обработки персональных данных в архивуправлении.

2.14.6.5. Право на обжалование действий или бездействия оператора

Если субъект персональных данных считает, что архивуправление осуществляет обработку его персональных данных с нарушением требований законодательства в области персональных данных или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие архивуправления в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке [1].

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 [1].

2.14.7. Порядок действий при достижении целей обработки персональных данных и отзыве согласия на обработку персональных данных

В случае достижения цели обработки персональных данных ааархивуправление обязано прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручениюархивуправления) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению архивуправления) [1].

При совершении указанных действий должны соблюдаться сроки, установленные в пункте 2.14.1 настоящих Правил.

2.14.8. Порядок действий при отзыве согласия субъекта персональных данных на обработку его персональных данных

В случае отзыва субъектом персональных данных согласия на обработку его персональных данных архивуправление обязано прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению архивуправления) 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 архивуправления) [1].

При совершении указанных действий должны соблюдаться сроки, установленные в пункте 2.14.1 настоящих Правил.

2.15. Согласие субъекта персональных данных на обработку его персональных данных

Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе [1].

Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным [1].

В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются архивуправлением.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных [1].

Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, при которых такое согласие не требуется, возлагается на архивуправление [1].

В архивуправлении обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных.

Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью [1].

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 [1];
- 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) [1];
- наименование адрес архивуправления или иного оператора, получающего согласие субъекта персональных данных [1];
- цель обработки персональных данных [1];
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных [1];
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению архивуправления, если обработка будет поручена такому лицу [1];
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых в архивуправлении способов обработки персональных данных [1];
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом [1];
- дата предоставления согласия;
- подпись субъекта персональных данных [1].

В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных [1].

В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни [1].

Персональные данные могут быть получены архивуправлением от лица, не являющегося субъектом персональных данных, при условии предоставления подтверждения наличия оснований, что обработка персональных данных может осуществляться без получения согласия [1].

Согласие субъекта персональных данных оформляется в двух экземплярах – один из которых передается субъекту персональных данных, а второй – архивуправлению.

При документальном оформлении действий (операций) с персональными данными необходимо обратить особое внимание на использование термина «распространение» персональных данных, так как это действия, направленные на раскрытие персональных данных **неопределенному кругу лиц**, что при обработке персональных данных чаще всего является запрещенным. **Указанный термин «распространение» необходимо указывать только при обработке общедоступных данных.**

2.16. Уведомление об обработке (о намерении осуществлять обработку) персональных данных

Архивуправление уведомляет уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных [1].

При этом должны соблюдаться установленные настоящими Правилами (2.14.1) сроки подачи уведомлений.

Архивуправление вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

- обрабатываемых в соответствии с трудовым законодательством [1];
- полученных архивуправлением в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются архивуправлением исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных [1];
- относящихся к членам (участникам) общественного объединения и обрабатываемых соответствующими общественным объединением, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных [1];
- сделанных субъектом персональных данных общедоступными [1];
- включающих в себя только фамилии, имена и отчества субъектов персональных данных [1];
- необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится архивуправление или в иных аналогичных целях [1];
- обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных [1].

Уведомление готовится лицом, ответственным за организацию обработки персональных данных в архивуправлении, подписывается начальником и направляется в виде документа на бумажном носителе или в форме электронного документа.

Уведомление должно содержать следующие сведения [1]:

- наименование (фамилия, имя, отчество), адрес оператора;
- цель обработки персональных данных;
- категории персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- правовое основание обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;
- описание мер направленных на обеспечение выполнения обязанностей, предусмотренных законодательством в области персональных данных и по обеспечению безопасности персональных данных при их обработке;
- фамилия, имя, отчество физического лица, ответственного за организацию обработки персональных данных в архивуправлении и номер его контактного телефона, почтовый адрес и адрес электронной почты;
- дата начала обработки персональных данных;
- срок или условие прекращения обработки персональных данных;
- сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
- сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных.

Письменная форма уведомления устанавливается уполномоченным органом по защите прав субъектов персональных данных.

Уполномоченный орган по защите прав субъектов персональных данных в течение тридцати дней с даты поступления уведомления об обработке персональных данных вносит сведения в реестр операторов [1].

Сведения, содержащиеся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными [1].

На архивуправление не могут возлагаться расходы в связи с рассмотрением уведомления об обработке персональных данных уполномоченным органом по защите прав субъектов персональных данных, а также в связи с внесением сведений в реестр операторов [1].

В случае предоставления неполных или недостоверных сведений, уполномоченный орган по защите прав субъектов персональных данных вправе требовать от архивуправления уточнения предоставленных сведений до их внесения в реестр операторов [1].

В случае изменения сведений, а также в случае прекращения обработки персональных данных архивуправление обязано уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в сроки, указанные в пункте 2.14.1 настоящих правил.

В случае изменения сведений, содержащихся в уведомлении об обработке персональных данных, структурное подразделение архивуправления, являющееся инициатором таких изменений в обработке персональных данных, готовит изменения в уведомление и передает такие изменения лицу, ответственному за организацию обработки персональных данных в архивуправлении. Дальнейшие действия по подготовке изменений в уведомление для передачи в уполномоченный орган по защите прав субъектов персональных данных осуществляются аналогично действиям при первоначальной подаче уведомления.

2.17. Информационные системы персональных данных

К информационным системам персональных данных относятся совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств [1]. В архивуправлении устанавливаются:

- критерии определения информационных систем персональных данных;
- наименование информационной системы персональных данных;
- цели создания или эксплуатации информационной системы персональных данных;
- параметры, характеризующие информационную систему персональных данных.

2.17.1. Критерии определения информационных систем персональных данных

Все информационные системы архивуправления, в которых производится обработка персональных данных, являются информационными системами персональных данных. Информационная система персональных данных состоит из совокупности [1]:

- базы данных, в состав которой входят персональные данные;
- информационных технологий, позволяющих осуществлять обработку, содержащихся в базе данных персональных данных;
- технических средств, позволяющих осуществлять обработку, содержащихся в базе данных персональных данных.

Обработка персональных данных может осуществляться как с использованием средств автоматизации, так и без использования таких средств.

Обработка персональных данных с помощью средств вычислительной техники является автоматизированной обработкой персональных данных [1].

Под средствами вычислительной техники понимается совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем [3].

Частным случаем автоматизированной обработки персональных данных является исключительно автоматизированная обработка персональных данных, при осуществлении которой решения, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, принимаются на основании исключительно автоматизированной обработки его персональных данных [1].

Обязательным условием создания информационной системы персональных данных является наличие **обособленной** базы данных, содержащей персональные данные, при изоляции которой от других информационных систем персональных данных, возможна обработка содержащихся в ней персональных данных с помощью информационных технологий и технических средств, входящих в состав этой информационной системы персональных данных.

Допускается использование одних и тех же информационных технологий и технических средств, для обработки различных баз данных, содержащих персональные данные, при этом разделение на различные информационные системы персональных данных производится по критерию уникальности баз данных, содержащих персональные данные.

2.17.2. Наименование информационной системы персональных данных

С целью идентификации каждой информационной системе персональных данных в архивуправлении присваивается наименование, которое должно отражать основное назначение данной информационной системы либо наименование программных средств обработки персональных данных в данной информационной системе персональных данных.

2.17.3. Цели создания или эксплуатации информационной системы персональных данных

Для каждой информационной системы персональных данных определяются цели ее создания и эксплуатации. При этом определяется предполагаемое назначение информационной системы персональных данных, в соответствии с оказываемыми услугами, реализуемыми информационной системой персональных данных внутренними задачами или с определенными требованиями, предъявляемыми действующим в Российской Федерации

законодательством.

2.17.4. Параметры, характеризующие информационную систему персональных данных

Для каждой информационной системы персональных данных архивного управления Курской области определяются следующие параметры, характеризующие такую информационную систему персональных данных:

- наименование информационной системы персональных данных;
- цели создания или эксплуатации информационной системы персональных данных;
- цель обработки персональных данных в информационной системе персональных данных;
- перечень персональных данных о субъекте персональных данных, обрабатываемых в информационной системе персональных данных;
- правовое основание обработки персональных данных в информационной системе персональных данных;
- оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных;
- действия (операции) с персональными данными;
- источники получения персональных данных;
- способы передачи персональных данных и их получатели;
- определение сроков обработки, в том числе хранения персональных данных в информационной системы персональных данных;
- заданные характеристики безопасности обрабатываемых в информационной системе персональных данных;
- места обработки персональных данных;
- характеристики средств автоматизации обработки персональных данных.

2.18. Правила обработки персональных данных в информационных системах персональных данных

В архивуправлении разрабатываются Правила обработки персональных данных для каждой информационной системы персональных данных архивуправления. Правила обработки персональных данных в каждой информационной системы персональных данных содержат:

- наименование информационной системы персональных данных;
- цели создания или эксплуатации информационной системы персональных данных;
- цель обработки персональных данных в информационной системе персональных данных;
- перечень персональных данных о субъекте персональных данных, обрабатываемых в информационной системе персональных данных;
- правовое основание обработки персональных данных в информационной системе персональных данных;
- оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных;
- источники получения персональных данных;
- способы передачи персональных данных и их получатели;
- определение сроков обработки, в том числе хранения персональных данных в информационной системы персональных данных;
- заданные характеристики безопасности обрабатываемых в информационной

системе персональных данных;

- места обработки персональных данных;
- характеристики средств автоматизации обработки персональных данных.

Форма Правил обработки персональных данных в информационной системе архивуправления и порядок их заполнения устанавливается настоящими Правилами (Приложение 1). При заполнении таких правил категорически запрещается указание недостоверных или неполных сведений. Такие правила утверждаются начальником и хранятся у лица, ответственного за организацию обработки персональных данных в архивуправлении.

2.19. Порядок создания, модернизации и ликвидации информационных систем персональных данных

В архивуправлении устанавливаются правила:

- создания информационных систем персональных данных;
- модернизации информационных систем персональных данных;
- ликвидации информационных систем персональных данных.

2.19.1. Порядок создания информационных систем персональных данных

При возникновении необходимости в автоматизированной обработке персональных данных в архивуправлении создается информационная система персональных данных. Запрещается создание информационной системы персональных данных, не соответствующей хотя бы одному из принципов, указанных в пункте 2.2 настоящих Правил.

Подразделение (должностное лицо) архивуправлеения, выступающее инициатором обработки персональных данных, при условии, что такая обработка не осуществляется в рамках обработки персональных данных в существующих информационных системах персональных данных, готовит проект Правил обработки персональных данных для такой информационной системы персональных данных архивуправления по установленному настоящими Правилами образцу (Приложение 1).

Проект Правил обработки персональных данных для такой информационной системы персональных данных архивуправления в обязательном порядке согласовывается с лицом, ответственным за организацию обработки персональных данных в архивуправлении.

Утвержденные Правила обработки персональных данных для такой информационной системы персональных данных архивуправления являются основанием для создания информационной системы персональных данных в архивуправлении.

По факту создания информационной системы персональных данных вносятся изменения в Перечень информационных систем персональных данных архивуправления (пункт 2.20 настоящих Правил) и выполняются мероприятия по внесению изменений в уведомление по обработке персональных данных (пункт 2.16 настоящих Правил).

2.19.2. Порядок модернизации информационных систем персональных данных

При возникновении необходимости внесения изменений в обработку персональных данных, в рамках существующих информационных систем персональных данных, осуществляется модернизация существующей информационной системы персональных данных.

В случае возникновении необходимости внесения изменений в обработку персональных данных в существующих информационных систем персональных данных, подразделение (должностное лицо) архивуправления, выступающее ответственным за осуществление такой обработки, готовит изменения в существующие Правила обработки персональных данных такой информационной системы персональных данных архивуправления. Такие изменения в обязательном порядке согласовываются с лицом, ответственным за организацию обработки персональных данных в архивуправлении и

утверждаются начальником.

Утвержденные Правила обработки персональных данных информационной системы персональных данных архивуправления с внесенными изменениями являются основанием для модернизации (изменения) информационной системы персональных данных.

По факту модернизации информационной системы персональных данных выполняются мероприятия по внесению изменений в уведомление по обработке персональных данных (пункт 2.16 настоящих Правил).

2.19.3. Порядок ликвидации информационных систем персональных данных

При возникновении необходимости в ликвидации информационной системы персональных данных, осуществляется комплекс мероприятий по уничтожению или передаче персональных данных в другие информационные системы персональных данных.

В случае возникновения необходимости в ликвидации информационной системы персональных данных, подразделение (должностное лицо) аархивуправления, выступающее ответственным за ее ликвидацию, готовит План ликвидации информационной системы персональных данных, в котором определяет совершаемые при этом действия с персональными данными и их последовательность.

План ликвидации информационной системы персональных данных в обязательном порядке согласовывается с лицом, ответственным за организацию обработки персональных данных в архивуправлении и утверждаются начальником.

Утвержденный План ликвидации информационной системы персональных данных является основанием ликвидации информационной системы персональных данных.

По факту ликвидации информационной системы персональных данных вносятся изменения в Перечень информационных систем персональных данных архивуправления (пункт 2.20 настоящих Правил) и выполняются мероприятия по внесению изменений в уведомление по обработке персональных данных (пункт 2.16 настоящих Правил).

2.20. Перечень информационных систем персональных данных

Перечень информационных систем персональных данных архивуправления готовится лицом, ответственным за организацию обработки персональных данных в архивуправлении и утверждаются начальником.

Перечень информационных систем персональных данных архивуправления храниться у лица, ответственного за организацию обработки персональных данных в архивуправлении.

Форма Перечня информационных систем персональных данных аархивуправления устанавливается настоящими Правилами (Приложение 2).

В Перечне информационных систем персональных данных архивуправления должна содержаться следующая информация:

- наименование информационной системы персональных данных;
- перечень структурных подразделений, осуществляющих эксплуатацию информационной системы персональных данных;
- перечень сотрудников архивуправления, осуществляющих обработку персональных данных;
- перечень средств вычислительной техники, участвующей в обработке персональных данных;
- структурное подразделение, ответственное за эксплуатацию информационной системы персональных данных.

С Перечнем информационных систем персональных данных в архивуправлении под роспись должны быть ознакомлены все руководители структурных подразделений архивуправления.

2.21. Требования к сотрудникам, осуществляющим доступ к персональным данным или их обработку

Архивуправление осуществляет ознакомление своих сотрудников, непосредственно осуществляющих обработку персональных данных или осуществляющих доступ к ним, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами архивуправления по вопросам обработки персональных данных [7], включая настоящие Правила:

- при оформлении договора, в том числе трудового;
- после каждого перерыва в исполнении своих обязанностей на срок более 28 рабочих дней;
- при первоначальном допуске к обработке персональных данных в информационной системе персональных данных;
- при назначении на новую должность, связанную с обработкой персональных данных или доступом к ним;
- после внесения изменений в действующее законодательство Российской Федерации о персональных данных, локальные акты архивуправления по вопросам обработки персональных данных, включая настоящие Правила.

Сотрудники архивуправления непосредственно осуществляющие обработку персональных данных или осуществляющие доступ к ним обязаны:

- неукоснительно следовать принципам обработки персональных данных (пункт 2.2 настоящих Правил);
- знать и строго соблюдать положения действующего законодательства Российской Федерации в области персональных данных;
- знать и строго соблюдать положения локальных актов архивуправления в области обработки и обеспечения безопасности персональных данных;
- знать и строго соблюдать инструкции, руководства и иные эксплуатационные документы на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;
- соблюдать конфиденциальность персональных данных, то есть не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;
- не допускать нарушений требований и правил обработки и обеспечения безопасности персональных данных;
- обо всех подозрениях и ставших известными случаях нарушений требований и правил обработки и обеспечения безопасности персональных данных сообщать лицу, ответственному за обработку персональных данных в архивуправлении.

Сотрудники архивуправления несут личную ответственность за соблюдение указанных обязанностей в предусмотренном действующим законодательством Российской Федерации объеме.

2.22. Порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных

Доступ сотрудников архивуправления в помещения, в которых ведется обработка персональных данных, осуществляется по Спискам сотрудников архивуправления допущенных в помещения, в которых ведется обработка персональных данных. Такие списки готовятся и уточняются лицом, ответственным за организацию обработки персональных данных в архивуправлении и утверждаются начальником.

Допуск в помещения, в которых ведется обработка персональных данных, иных лиц, осуществляется сотрудниками, указанными в Списках сотрудников архивуправления допущенных в помещения, в которых ведется обработка персональных данных.

Пребывание таких посторонних лиц в кабинетах, в которых ведется обработка персональных данных, допускается только в присутствии сотрудников, указанных в Списках сотрудников архивуправления допущенных в помещения, в которых ведется обработка персональных данных.

3. Конфиденциальность персональных данных

Запрет раскрытия третьим лицам и распространения персональных данных без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом архивуправлением и иными лицами, получившим доступ к персональным данным называется конфиденциальностью персональных данных.

3.1. Режим ограниченного доступа к персональным данным

С целью реализации требований действующего законодательства Российской Федерации в области персональных данных по обеспечению конфиденциальности персональных данных в архивуправлении вводится режим ограниченного доступа к персональным данным.

Создание режима ограниченного доступа к персональным данным включает в себя:

- создание и уточнение Перечня информационных систем персональных данных в архивуправлении;
- создание и уточнение настоящих Правил в части касающейся обеспечения конфиденциальности персональных данных и обеспечения безопасности персональных данных;
- создание и уточнение Перечня помещений, предназначенных для обработки персональных данных;
- разработка инструкций для сотрудников по организации режима обеспечения безопасности помещений (предназначенных для обработки персональных данных);
- перечень должностей сотрудников архивуправлеения, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
- определение технических средств обработки персональных данных, путем разработки, оформления и уточнения Технического паспорта (или Технических паспортов) информационных систем персональных данных архивуправления;
- разработки, оформления и уточнения Перечня информационных ресурсов, содержащих персональные данные (мест расположения баз данных или иных документов и массивов содержащих персональные данные);
- дополнение в гражданско-правовые договоры с контрагентами по вопросам обязательства по обеспечению охраны конфиденциальности информации и ответственности за обеспечение охраны ее конфиденциальности;
- внесение изменений в должностные обязанности (дополнения в трудовой договор сотрудников), предусматривающие регулирование отношений по использованию информации, ограниченного доступа;
- получение расписок в ознакомлении сотрудников архивуправления, доступ которых к информации ограниченного доступа, обладателями которой являются архивуправление, его контрагенты и клиенты, необходим для выполнения им своих трудовых обязанностей, с перечнем информации ограниченного доступа, установленным режимом ограничения доступа к информации и мерами ответственности за его нарушение;
- передаче (возврате) сотрудниками архивуправления при прекращении или расторжении трудового договора, имеющихся в пользовании такого сотрудника материальных носителей информации, содержащих персональные данные;
- проведение начальных и периодических занятий и иных мероприятий по

повышению уровня знаний сотрудников архивуправления, допущенных к обработке персональных данных по вопросам обработки и обеспечения безопасности персональных данных;

- создание и ведение Журнала регистрации машинных носителей информации;
- создание и ведение Журнала учета сейфов, металлических шкафов, спецхранилищ и ключей от них;
- создание и ведение Перечней лиц, имеющих доступ в помещения, в которых обрабатываются персональные данные;
- создание и ведение Журнала (-ов) приема (сдачи) под охрану помещений, в которых осуществляется обработка персональных данных;
- проектирование и реализация системы защиты персональных данных;
- документирование и реализация разрешительной системы доступа (матриц доступа) к информационным (программным) ресурсам в автоматизированных системах информационных систем персональных данных архивуправления;
- разработка инструкций о действиях сотрудников архивуправления в отношении носителей персональных данных при возникновении чрезвычайных ситуаций (стихийных бедствий, техногенных катастроф, наводнений, пожаров, нарушениях правопорядка и др.);
- разработка инструкций для сотрудников архивуправления по вопросам обеспечения безопасности персональных данных.

Организация и контроль за выполнением указанных мероприятий возлагается на лицо, ответственное за организацию обработки персональных данных в архивуправлении. Разрабатываемые документы подлежат утверждению начальником.

3.2. Порядок учета и маркирования материальных носителей информации, образующихся в процессе обработки персональных данных

С целью реализации режима ограниченного доступа к персональным данным в архивуправлении и недопущению бесконтрольного использования машинных носителей, содержащих персональные данные вводится их поэкземплярный учет.

Организация и контроль за выполнением учета машинных носителей, содержащих персональные данные, возлагается на лицо, ответственное за организацию обработки персональных данных в архивуправлении.

Учет машинных носителей, содержащих персональные данные, осуществляется по Журналу учета машинных носителей информации.

4. Обеспечение безопасности персональных данных при их обработке

В соответствии с требованиями действующего законодательства в области персональных данных при обработке персональных данных архивуправление обязано принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Безопасность персональных данных достигается путем исключения 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.

Для обеспечения безопасности персональных данных при их обработке в информационных системах осуществляется защита информации, содержащейся в информационных системах, технических средств (в том числе средств вычислительной техники, машинных носителей информации, средств и систем связи и передачи данных, технических средств обработки буквенно-цифровой, графической, видео- и речевой информации), общесистемного, прикладного, специального программного обеспечения,

информационных технологий, а также средств защиты информации.

Работы по обеспечению безопасности персональных данных при их обработке в информационных системах в архивуправления являются неотъемлемой частью работ по созданию информационных систем.

4.1. Принципы обеспечения безопасности персональных данных при их обработке

Обеспечение безопасности персональных данных в архивуправлении должно осуществляться на основе следующих принципов:

- соблюдение конфиденциальности персональных данных и иных характеристик их безопасности;
- реализация права на доступ к персональным данным лиц, доступ которых к таким данным разрешается в рамках действующего законодательства Российской Федерации и локальными нормативными актами архивуправления;
- обеспечение защиты информации, содержащей персональные данные, от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- проведение мероприятий, направленных на предотвращение несанкционированной передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности персональных данных;
- применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия.

Категорически запрещается нарушать указанные принципы по обеспечению безопасности персональных данных.

4.2. Требования по уровню обеспечения безопасности

С целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных, классификация информационной системы проводится в зависимости от значимости обрабатываемой в ней информации и масштаба информационной системы (федеральный, региональный, объектовый). Проведение классификации информационных систем включает в себя следующие этапы:

- сбор и анализ исходных данных по информационной системе;
- присвоение информационной системе соответствующего класса и его документальное оформление.

Устанавливаются четыре класса защищенности информационной системы, определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс – четвертый, самый высокий – первый.

При проведении классификации информационной системы учитываются следующие исходные данные:

- уровень значимости обрабатываемых в информационной системе персональных данных;
- масштаб информационной системы (федеральный, региональный, объектовый);
- заданные характеристики безопасности персональных данных, обрабатываемых в

информационной системе;

− степень возможного ущерба для оператора от нарушения конфиденциальности, целостности и доступности персональных данных.

Класс защищенности определяется для информационной системы в целом и, при необходимости, для ее отдельных сегментов (составных частей). В случае выделения в составе информационной системы подсистем, каждая из которых является информационной системой, информационной системе в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем.

Классификация информационных систем проводится на этапе создания информационных систем или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем).

Класс защищенности информационной системы подлежит пересмотру при изменении масштаба информационной системы или значимости обрабатываемой в ней информации. Результаты классификации информационной системы оформляются актом классификации.

4.3. Состав мероприятий по обеспечению безопасности персональных данных

Мероприятия по обеспечению безопасности персональных данных должны носить комплексный характер и включать в себя правовые, организационные и технические меры, описанные в настоящих Правилах.

Порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются настоящими Правилами.

4.3.1. Состав мероприятий по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

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

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

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

Ответственным за организацию и контроль за обеспечение безопасности персональных данных в архивуправлении при обработке персональных данных, осуществляемой без использования средств автоматизации, является лицо, ответственное за организацию обработки персональных данных в архивуправлении.

4.3.2. Состав мероприятий по обеспечению безопасности персональных данных при их обработке, осуществляемой с использованием средств автоматизации

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в архивуправлении включают в себя:

− определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

− применение 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;

− применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

− оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
− учет машинных носителей персональных данных;
− обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;
− восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
− установление 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;
− контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы осуществляется архивуправлением в соответствии с эксплуатационной документацией на систему защиты информации и организационно-распорядительными документами по защите информации и в том числе включает:
− управление (администрирование) системой защиты информации информационной системы;
− выявление инцидентов и реагирование на них;
− управление конфигурацией аттестованной информационной системы и ее системы защиты информации;
− контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в информационной системе.

В ходе управления (администрирования) системой защиты информации информационной системы осуществляются:
− заведение и удаление учетных записей пользователей, управление полномочиями пользователей информационной системы и поддержание правил разграничения доступа в информационной системе;
− управление средствами защиты информации в информационной системе, в том числе параметрами настройки программного обеспечения, включая программное обеспечение средств защиты информации, управление учетными записями пользователей, восстановление работоспособности средств защиты информации, генерацию, смену и восстановление паролей;
− установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых разработчиками (производителями) средств защиты информации или по их поручению;
− централизованное управление системой защиты информации информационной системы (при необходимости);
− регистрация и анализ событий в информационной системе, связанных с защитой информации (далее - события безопасности);
− информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации информационной системы и отдельных средств защиты информации, а также их обучение;
− сопровождение функционирования системы защиты информации информационной системы в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации.

В ходе выявления инцидентов и реагирования на них осуществляются:
− определение лиц, ответственных за выявление инцидентов и реагирование на них;
− обнаружение и идентификация инцидентов, в том числе отказов в обслуживании,

сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

− своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;

− анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

− планирование и принятие мер по устранению инцидентов, в том числе по восстановлению информационной системы и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

− планирование и принятие мер по предотвращению повторного возникновения инцидентов.

В ходе управления конфигурацией аттестованной информационной системы и ее системы защиты информации осуществляются:

− поддержание конфигурации информационной системы и ее системы защиты информации (структуры системы защиты информации информационной системы, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации информационной системы и ее системы защиты информации);

− определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации;

− управление изменениями базовой конфигурации информационной системы и ее системы защиты информации, в том числе определение типов возможных изменений базовой конфигурации информационной системы и ее системы защиты информации, санкционирование внесения изменений в базовую конфигурацию информационной системы и ее системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации, сохранение данных об изменениях базовой конфигурации информационной системы и ее системы защиты информации, контроль действий по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации;

− анализ потенциального воздействия планируемых изменений в базовой конфигурации информационной системы и ее системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность информационной системы;

− определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию информационной системы и ее системы защиты информации;

− внесение информации (данных) об изменениях в базовой конфигурации информационной системы и ее системы защиты информации в эксплуатационную документацию на систему защиты информации информационной системы;

− принятие решения по результатам управления конфигурацией о повторной аттестации информационной системы или проведении дополнительных аттестационных испытаний.

В ходе контроля (мониторинга) за обеспечением уровня защищенности информации,

содержащейся в информационной системе, осуществляются:

- контроль за событиями безопасности и действиями пользователей в информационной системе;
- контроль (анализ) защищенности информации, содержащейся в информационной системе;
- анализ и оценка функционирования системы защиты информации информационной системы, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации информационной системы;
- периодический анализ изменения угроз безопасности информации в информационной системе, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;
- документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;
- принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) системы защиты информации информационной системы, повторной аттестации информационной системы или проведении дополнительных аттестационных испытаний.

4.4. Система защиты персональных данных

Организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность информационной системы и информации;
- доступность информации;
- защиту среды виртуализации;
- защиту технических средств;
- защиту информационной системы, ее средств, систем связи и передачи данных.

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного

обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

Меры по защите машинных носителей информации (средства обработки (хранения) информации, съемные машинные носители информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных носителей информации.

Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.

Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

Меры по обеспечению доступности информации должны обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в информационной системе, в штатном режиме функционирования информационной системы.

Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной

системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

Меры защиты информации выбираются и реализуются в информационной системе в рамках ее системы защиты информации с учетом угроз безопасности информации применительно ко всем объектам и субъектам доступа на аппаратном, системном, прикладном и сетевом уровнях, в том числе в среде виртуализации и облачных вычислений. Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы приведены в Приложении 9.

Разработка системы защиты персональных данных, частных моделей угроз, моделей нарушителя осуществляется специализированной организацией на основании специального разрешения (лицензии) на осуществление данного вида деятельности.

4.4.1. Модели угроз и нарушителя

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем.

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

Модель угроз решает следующие задачи:

- анализ защищенности информационной системы персональных данных от угроз безопасности персональных данных в ходе учреждении и выполнения работ по обеспечению безопасности персональных данных;
- разработка системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационной системы персональных данных;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональных данных и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущение воздействия на технические средства информационной системы персональных данных, в результате которого может быть нарушено их функционирование;
- контроль обеспечения уровня защищенности персональных данных.

Модель угроз безопасности информации должна содержать описание информационной системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Модель угроз содержит единые исходные данные по угрозам безопасности

персональных данных, обрабатываемых в информационной системе персональных данных, связанным:

- с перехватом (съемом) персональных данных по техническим каналам с целью их копирования или неправомерного распространения;
- с несанкционированным, в том числе случайным, доступом в информационной системы персональных данных с целью изменения, копирования, неправомерного распространения персональных данных или деструктивных воздействий на элементы информационной системы персональных данных и обрабатываемых в них персональных данных с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования персональных данных.

Состав и содержание угроз безопасности персональным данным определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным.

Совокупность таких условий и факторов формируется с учетом характеристик информационной системы персональных данных, свойств среды распространения информативных сигналов, содержащих защищаемую информацию, и возможностей и источников угроз.

При обеспечении безопасности персональных данных с использованием криптографических средств защиты информации производится нейтрализация атак, готовящимися и проводимыми нарушителями, причем возможности проведения атак обусловлены их возможностями. С учетом этого все возможные атаки определяются моделью нарушителя.

Модель нарушителя тесно связана с частной моделью угроз и, по сути, является ее частью. Смысловые отношения между ними следующие:

- в модели угроз содержится максимально полное описание угроз безопасности объекта;
- модель нарушителя содержит описание предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

4.4.2. Средства защиты информации

Средства защиты информации, применяемые в информационных системах персональных данных, в установленном порядке проходят процедуру оценки соответствия.

Технические меры защиты информации реализуются посредством применения средств защиты информации, имеющих необходимые функции безопасности.

В этом случае в информационных системах 1 и 2 класса защищенности применяются:

- средства вычислительной техники не ниже 5 класса;
- системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса;
- межсетевые экраны не ниже 3 класса в случае взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 4 класса в случае отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена.

В информационных системах 3 класса защищенности применяются:

- средства вычислительной техники не ниже 5 класса;
- системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса в случае взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 5

класса в случае отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

− межсетевые экраны не ниже 3 класса в случае взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 4 класса в случае отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена.

В информационных системах 4 класса защищенности применяются:

− средства вычислительной техники не ниже 5 класса;

− системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса;

− межсетевые экраны не ниже 4 класса.

В информационных системах 1 и 2 классов защищенности применяются средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей.

Технические и программные средства обработки персональных данных должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Эксплуатация средств защиты информации должна осуществляться строго в соответствии с эксплуатационной документацией на такие средства. Сотрудники архивуправления, эксплуатирующие средства защиты информации должны быть ознакомлены с такой документацией под роспись.

4.5. Требования к помещениям, в которых производится обработка персональных данных

Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Помещения, в которых располагаются технические средства информационных систем персональных данных или хранятся носители персональных данных, соответствуют требованиям пожарной безопасности, установленными действующим законодательством Российской Федерации.

В архивуправлении производится оснащение помещений, в которых располагаются технические средства информационных систем персональных данных или хранятся носители персональных данных, входными дверьми с замками, осуществляется обеспечение постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода, а также оборудование помещений устройствами, сигнализирующими о несанкционированном вскрытии помещений.

Доступ в помещения, в которых располагаются технические средства информационных систем персональных данных или хранятся носители персональных данных, в рабочее и нерабочее время, а также в нештатных ситуациях, должен осуществляться в соответствии с инструкцией по организации режима обеспечения безопасности помещений по утверждённым перечням лиц, имеющих право доступа в соответствующие помещения.

Кроме указанных мер по специальному оборудованию и охране помещений, в которых устанавливаются криптографические средства защиты информации или осуществляется их хранение, реализуются дополнительные требования, определяемые методическими документами ФСБ России.

4.6. Порядок оценки соответствия требованиям по безопасности персональных данных

Порядок оценки соответствия информационных систем персональных данных требованиям безопасности информации осуществляется в порядке, определяемом действующим законодательством Российской Федерации и Программой такой оценки. Программу проведения оценочных испытаний разрабатывает организация, проводящая такую оценку. Программа согласовывается с архивуправлением.

Программа оценки соответствия информационных систем персональных данных требованиям безопасности информации содержит:

- перечень работ и их продолжительность;
- методики испытаний (или используются типовые методики);
- количественный и профессиональный состав оценочной комиссии;
- необходимость использования контрольной аппаратуры и тестовых средств.

Порядок, содержание, условия и методы испытаний для оценки характеристик и показателей, соответствия их установленным требованиям, а также применяемые в этих целях контрольная аппаратура и тестовые средства определяются в методиках испытаний различных видов объектов информатизации.

По результатам оценки соответствия информационных систем персональных данных требованиям безопасности информации оформляются протоколы и заключение о соответствии таким требованиям. На основании заключения, в случае получения положительного решения о соответствии информационной системы персональных данных предъявляемым требованиям по обеспечению безопасности персональных данных, оформляется документ, подтверждающий выполнение требований по безопасности информации.

5. Контроль и надзор за соблюдением требований по обработке и обеспечению безопасности персональных данных

Контроль и надзор за соблюдением требований по обработке и обеспечению безопасности персональных данных в архивуправлении состоит из следующих направлений:

- внешний контроль и надзор за соблюдением требований по обработке и обеспечению безопасности персональных данных;
- внутренний контроль и надзор за соблюдением требований по обработке и обеспечению безопасности персональных данных.

Внутренний контроль и надзор за соблюдением требований по обработке и обеспечению безопасности персональных данных в архивуправлении состоит из:

- контроля и надзора за исполнением требований по обработке и обеспечению безопасности персональных данных;
- оценки соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер.

5.1. Порядок внешнего контроля над соблюдением требований по обработке и обеспечению безопасности данных

Внешний контроль и надзор за выполнением требований законодательства в области персональных данных осуществляется федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере информационных технологий и связи, 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 [1].

Внешний контроль и надзор за выполнением требований законодательства в области персональных данных осуществляется в соответствии с действующим законодательством Российской Федерации в области защиты прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля, подзаконных нормативных актов Правительства Российской Федерации, ведомственных нормативных актов и административных регламентов.

Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям настоящего Федерального закона, является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи [1].

Уполномоченный орган по защите прав субъектов персональных данных имеет право [1]:

- запрашивать у архивуправления информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;
- осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных архивуправления, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;
- требовать от архивуправления уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
- принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства в области персональных данных;
- обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных, в том числе в защиту прав неопределенного круга лиц, и представлять интересы субъектов персональных данных в суде;
- направлять в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, применительно к сфере их деятельности, необходимые сведения;
- направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью;
- привлекать к административной ответственности лиц, виновных в нарушении настоящего Федерального закона.

В отношении персональных данных, ставших известными уполномоченному органу по защите прав субъектов персональных данных в ходе осуществления им своей деятельности, должна обеспечиваться конфиденциальность персональных данных [1].

Решения уполномоченного органа по защите прав субъектов персональных данных могут быть обжалованы в судебном порядке [1].

Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных [1].

5.2. Порядок внутреннего контроля за соблюдением требований по обработке и обеспечению безопасности данных

В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в архивуправлении организуется проведение периодических проверок условий обработки персональных данных [7]. Проверки осуществляются ответственным за организацию обработки персональных данных в архивуправлении либо комиссией, образуемой начальником [7] не реже одного раза в год.

При осуществлении внутреннего контроля соответствия обработки персональных данных установленным требованиям в архивуправлении производится проверка:

- соблюдения принципов обработки персональных данных в архивуправлении;
- соответствия локальных актов в области персональных данных архивного управления Курской области действующему законодательству Российской Федерации;
- выполнения сотрудниками архивуправления требований и правил (в том числе особых) обработки персональных данных в информационных системах персональных данных архивуправления;
- перечней персональных данных, используемых для решения задач и функций структурными подразделениями архивного управления Курской области и необходимости обработки персональных данных в информационных системах персональных данных архивуправления;
- актуальности содержащихся в Правилах обработки персональных данных в каждой информационной системе персональных данных архивуправления информации о законности целей обработки персональных данных и оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных
- правильность осуществления сбора, систематизации, сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения персональных данных в каждой информационной системе персональных данных архивуправления;
- актуальность перечня должностей сотрудников архивуправления, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
- актуальность перечня должностей сотрудников архивуправления, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;
- соблюдение прав субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных архивуправления;
- соблюдение обязанностей архивуправлением, предусмотренных действующим законодательством в области персональных данных;
- порядка взаимодействия с субъектами персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных архивного управления Курской области, в том числе соблюдения сроков предусмотренных действующим законодательством в области персональных данных, соблюдения требований по уведомлениям, порядка разъяснения субъектам персональных данных необходимой информации, порядка реагирования на обращения субъектов персональных данных, порядка действий при достижении целей обработки персональных данных и отзыве согласий субъектами персональных данных;
- наличие необходимых согласий субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных архивуправления;

− актуальность сведений, содержащихся в уведомлении архивуправления об обработке персональных данных;
− актуальность перечня информационных систем персональных данных в архивуправлении;
− наличие и актуальность сведений, содержащихся в Правилах обработки персональных данных для каждой информационной системы персональных данных архивуправления;
− знания и соблюдение сотрудниками архивуправления положений действующего законодательства Российской Федерации в области персональных данных;
− знания и соблюдение сотрудниками архивуправления положений локальных актов архивного управления Курской области обработки и обеспечения безопасности персональных данных;
− знания и соблюдение сотрудниками архивуправления инструкций, руководств и иные эксплуатационных документов на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;
− соблюдение сотрудниками архивуправления конфиденциальности персональных данных;
− актуальность локальных актов архивуправления в области обеспечения безопасности персональных данных, в том числе в Технических паспортах информационных систем персональных данных;
− соблюдение сотрудниками архивуправления требований по обеспечению безопасности персональных данных;
− наличие локальных актов архивуправления, технической и эксплуатационной документации технических и программных средств информационных систем персональных данных архивуправления;
− иных вопросов.

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, начальнику докладывает ответственный за организацию обработки персональных данных в архивуправлении, либо председатель комиссии [7].

5.3. Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер по обработке и обеспечению безопасности персональных данных

Во время осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в архивуправлении производится оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер по обработке и обеспечению безопасности персональных данных в архивуправлении [1].

При оценке соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных, для каждой информационной системы персональных данных архивуправления производится экспертное сравнение заявленной архивуправлением в своих локальных актах оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных (пункт 2.9.2 настоящих Правил) и применяемых архивуправлением мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области персональных данных и изложенных в настоящих Правилах.

По итогам сравнений принимается решение о достаточности применяемых

архивуправлением мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области персональных данных и возможности или необходимости принятия дополнительных мер или изменения установленного в архивуправлении порядка обработки и обеспечения безопасности персональных данных.

Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер по обработке и обеспечению безопасности персональных данных в архивуправлении оформляется в виде отдельного документа, подписывается лицом, ответственным за организацию обработки персональных данных в архивуправлении либо председателем комиссии, образуемой начальником, и утверждается архивуправлением.

По результатам принятых решений, лицом, ответственным за организацию обработки персональных данных в архивуправлении организуется работа по их реализации.

6. Ответственность за нарушение требований в области персональных данных

Лица, виновные в нарушении требований действующего законодательства в области персональных данных, несут предусмотренную законодательством Российской Федерации ответственность. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также требований к защите 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 [1].

7. Мероприятия при возникновении обстоятельств непреодолимой силы (форс-мажор)

В случае появления обстоятельств непреодолимой силы, возникших в результате событий чрезвычайного характера, которые архивное управление Курской области не мог предвидеть и предотвратить разумными мерами, должностные лица архивного управления Курской области обязаны принять все возможные меры по недопущению нарушения прав субъектов персональных данных.

К обстоятельствам непреодолимой силы относятся события, на которые архивное управление Курской области не мог оказывать влияние и за возникновение которых он не несет ответственности: землетрясение, наводнение, пожар, забастовки, насильственные или военные действия любого характера, решения органов государственной власти препятствующие исполнению требований законодательства в области персональных данных.

Надлежащим доказательством наличия указанных выше обстоятельств будут служить официальные документы архивуправления и органов государственной власти Российской Федерации.

Архивуправление в случае возникновении указанных выше обстоятельств и нарушении прав субъектов персональных данных, связанных с такими обстоятельствами, извещает субъектов персональных данных всеми доступными способами.

8. Мероприятия по обработке персональных данных при проведении процедур ликвидации или реорганизации

При архивуправлении все носители персональных данных подлежат уничтожению установленным настоящими Правилами способами, за исключением носителей, подлежащих в соответствии с действующим законодательством Российской Федерации передаче в организацию-учредитель архивуправления.

При реорганизации архивуправления в форме слияния, присоединения и

преобразования решение о необходимости уничтожения персональных данных или передачи их образуемому учреждению принимается в соответствии с действующим законодательством Российской Федерации.

9. Ознакомление субъектов персональных данных с документами, определяющими политику в отношении обработки персональных данных

Настоящие Правила, а также иные документы, определяющие политику в отношении обработки персональных данных в архивуправлении, на официальном сайте архивуправления http://archive.rkursk.ru в течение 10 дней после их утверждения [7].

Ответственным за публикацию настоящих Правил, а также иных документов, определяющих политику в отношении обработки персональных данных в архивуправлении, а так же изменений к ним, является лицо, ответственное за организацию обработки персональных данных в архивуправлении.

Лицом, ответственным за организацию обработки персональных данных в архивуправлении обеспечивается неограниченный доступ к настоящим Правилам, а также иным документам, определяющим политику в отношении обработки персональных данных в архивуправлении любых заинтересованных лиц [1] при личном приеме либо по запросу, совершаемому в соответствии с действующим законодательством Российской Федерации.

10. Ссылки на нормативные акты, используемые в настоящих Правилах

В настоящих Правилах использованы ссылки на следующие нормативные акты:

[1] – Федеральный закон РФ № 152-ФЗ от 27.07.2006 г. «О персональных данных» .

[2] – Федеральный закон РФ № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации»

[3] – Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (Выписка) (утв. ФСТЭК РФ 15.02.2008)

[4] – Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ

[5] – Постановление Правительства РФ от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

[6] – «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993)

[7] – 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»

[8] – Приказ ФСТЭК РФ №17 от 11.02.2013 года «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

11. Приложения

- **Приложение 1.** Форма Правил обработки персональных данных в информационной системе персональных данных архивного управления Курской области
- **Приложение 2.** Форма перечня информационных систем персональных данных
- **Приложение 3.** Типовая форма согласия на обработку персональных данных государственного служащего (работника) архивного управления Курской области, а также иных субъектов персональных данных
- **Приложение 4.** Форма уведомлений о совершенных операциях над персональными данными

- **Приложение 5.** Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные
- **Приложение 6.** Форма акта уничтожения персональных данных
- **Приложение 7.** Форма Журнала учета лиц (организаций), получивших доступ к персональным данным, и (или) лиц (организаций), которым такая информация была предоставлена или передана
- **Приложение 8.** Типовое обязательство государственного служащего (работника), непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (трудового договора) прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей
- **Приложение 9.** Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы

Приложение 1

Форма Правил обработки персональных данных в информационной системе персональных данных архивного управления Курской области

Утверждаю

Начальник архивного управления
Курской области

_____ [Инициалы и фамилия]

«_____» _____ 20___ г.

**Правила обработки персональных данных
в информационной системы персональных данных
[наименование информационной системы персональных данных]
архивного управления Курской области**

Разработал

[Наименование должности]

_____ [Инициалы и фамилия]

«_____» _____ 20__ г.

Курск

1. Наименование информационной системы персональных данных

Полное наименование информационной системы персональных данных (далее – ИСПДн): информационная система персональных данных (далее – ИСПДн) *[полное наименование ИСПДн].*

Примечание: в данном разделе указывается наименование информационной системы персональных данных (далее – ИСПДн), которое должно отражать основное назначение данной информационной системы либо наименование программных средств обработки персональных данных в данной ИСПДн.

2. Цели создания или эксплуатации информационной системы персональных данных

Цель создание и эксплуатации ИСПДн *[наименование ИСПДн] – [описание (перечисление) целей создания ИСПДн].*

Примечание: в данном разделе определяются цели создания и эксплуатации ИСПДн. При этом указываются предполагаемое назначение ИСПДн, в соответствии с предлагаемыми потребителям услугами, осуществляемыми ИСПДн внутренними задачами или с определенными требованиями, предъявляемыми действующим в Российской Федерации законодательством.

3. Цель обработки персональных данных в информационной системе персональных данных

Персональные данные в информационной системе персональных данных архивуправления *[наименование ИСПДн]* обрабатываются со следующими целями: *[описание (перечисление) целей обработки персональных данных в ИСПДн]*

Примечание: в данном разделе определяются цели обработки персональных данных в ИСПДн. При этом указываются виды деятельности в соответствии с действующим в Российской Федерации законодательством, требующие обработки персональных данных.

4. Перечень персональных данных о субъекте персональных данных, обрабатываемых в информационной системе персональных данных

В информационной системе персональных данных архивуправления *[наименование ИСПДн]* обрабатываются следующие персональные данные: *[описание (перечисление) обрабатываемых в ИСПДн персональных данных]*

Примечание: в данном разделе указываются все наборы персональных данных принадлежащих субъекту персональных данных, обрабатываемых в информационной системе персональных данных, включая внутренние идентификаторы, принятые в архивном управлении Курской области.

5. Правовое основание обработки персональных данных в информационной системе персональных данных

Персональные данные в информационной системе персональных данных архивуправления *[наименование ИСПДн*] обрабатываются на основании следующих нормативных документов: *[перечисление нормативных актов]*

Примечание: в данном разделе указываются вид, издавший орган, номер, дата принятия и наименование нормативно-правовых актов, в том числе локальных, определяющих правовое основание обработки персональных данных.

6. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных

К юридическим последствиям, порождаемым в результате действий (операций) с персональными данными, в отношении субъекта персональных данных либо иным образом затрагивающих права и свободы субъекта персональных данных в информационной системе персональных данных архивуправления *[наименование ИСПДн]* относятся случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или иным образом затрагивающее его права, свободы и законные интересы, в том числе *[перечисление возможных юридических последствий в отношении субъекта персональных данных]*

Примечание: в данном разделе указываются возможные юридические последствия в отношении субъекта персональных данных.

7. Источники получения персональных данных

Персональные данные в информационной системе персональных данных архивуправления *[наименование ИСПДн]* получаются *[перечисление источников персональных данных]*

Примечание: в данном разделе указываются источники получения персональных данных для информационной системы персональных данных.

8. Действия (операции) с персональными данными

В информационной системе персональных данных архивуправления *[наименование ИСПДн]* осуществляются следующие операции с персональными данными: *[перечисление действий (операций) с персональными данными]*

Примечание: в данном разделе указываются действия (операции) с персональными данными, осуществляемые в информационной системе персональных данных.

9. Способы передачи персональных данных и их получатели

Персональные данные из информационной системы персональных данных архивуправления *[наименование ИСПДн]* передаются в *[перечисляются лица, которым осуществляется передача персональных данных, способ такой передачи и программные средства, с помощью которой она осуществляется]*

Примечание: в данном разделе перечисляются лица, которым осуществляется передача персональных данных, способ такой передачи и программные средства, с помощью которой она осуществляется.

10. Определение сроков обработки, в том числе хранения персональных данных в информационной системе персональных данных

Сроки обработки персональных данных субъектов персональных данных в рамках информационной системы персональных данных архивуправления *[наименование ИСПДн]* определяются *[вид, издавший орган, номер, дата принятия и наименование нормативно-правовых актов, в том числе локальных, определяющих сроки обработки, в том числе хранения персональных данных]*

Примечание: в данном разделе указываются вид, издавший орган, номер, дата принятия и наименование нормативно-правовых актов, в том числе локальных, определяющих сроки обработки, в том числе хранения персональных данных.

11. Заданные характеристики безопасности обрабатываемых в информационной системе персональных данных

В информационной системе персональных данных архивуправления *[наименование ИСПДн]* необходимо обеспечение конфиденциальности, *[при необходимости, указываются характеристики безопасности персональных данных, отличные от конфиденциальности]* содержащихся в ней персональных данных.

Примечание: в данном разделе при необходимости, указываются характеристики безопасности персональных данных, отличные от конфиденциальности, такие как защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий.

12. Места обработки персональных данных

Обработка персональных данных о субъектах персональных данных в информационной системе персональных данных архивуправления *[наименование ИСПДн]* осуществляется техническими средствами по адресу: г.Курск, ул.Ленина, д. 57.

Примечание: в данном разделе указываются все адреса по которым осуществляется обработка персональных данных в информационной системе персональных данных

13. Характеристики средств автоматизации обработки персональных данных

Обработка персональных данных в информационной системе персональных данных архивуправления [наименование ИСПДн] производится с помощью специально программного обеспечения [указываются наименование специального программного обеспечения, с помощью которого осуществляется обработка персональных данных в рамках информационной системы персональных данных]

Примечание: в данном разделе указываются наименование специального программного обеспечения, с помощью которого осуществляется обработка персональных данных в рамках информационной системы персональных данных.

14. Лист ознакомления

№ п/п	Должность	Фамилия и инициалы	Подпись
1.			
2.			
3.			

Примечание: в данном разделе указывается должности, инициалы и фамилии сотрудников, осуществляющих обработку персональных данных в информационной системе персональных данных и подписи указанных лиц в ознакомлении с настоящим документом.

Приложение 2

Форма перечня информационных систем персональных данных

На «10» апреля 2025 г. в архивном управлении Курской области находятся в эксплуатации следующие информационные системы персональных данных:

№ п/п	Наименование информационной системы персональных данных	Программное обеспечение обработки персональных данных	Инвентарный номер ПЭВМ	Фамилия и инициалы пользователя	Номер помещения	Наименование подразделения
1.	Управление финансами архивного управления Курской области	1С Предприятие, Бюджет-Смарт	№114302020587 №11432215145	Большанина Н.В. Копалова И.Н.	№9	отдел бюджетного планирования и программного обеспечения
2.	Ведение кадрового учета, юридической работы и внутреннего документооборота архивного управления Курской области (кабинет №14)	МойОфис	№11013420179	Анышева Е.А.	№14	отдел кадровой, правовой, мобилизационной работы и секретного делопроизводства
3.	Управление кадрами архивного управления Курской области	МойОфис	№110134201711	Прокопович Е.Л.	№16а	отдел кадровой, правовой, мобилизационной работы и секретного делопроизводства
4.	Автоматизированная система по приёму заявителей и электронного документооборота архивного управления Курской области	МойОфис, АИС «Дело»	№11432215143	Калугина О.А.	№6	отдел кадровой, правовой, мобилизационной работы и секретного делопроизводства
Итого, информационных систем персональных данных: 4						

Лист ознакомления руководителей структурных подразделений

№ п/п	Наименование структурного подразделения	Должность руководителя структурного подразделения	Фамилия и инициалы	Подпись
1.	отдел бюджетного планирования и программного обеспечения	начальник отдела	Большанина Н.В.	
2.	отдел кадровой, правовой, мобилизационной работы и секретного делопроизводства	начальник отдела	Анышева Е.А.	
3.	отдел по организации деятельности государственных, муниципальных архивов Курской области и государственному контролю в сфере архивного дела	заместитель начальника архивного управления Курской области – начальник отдела	Карманова Л.Б.	

Приложение 3

Типовая форма согласия
на обработку персональных данных государственного служащего (работника) архивного управления Курской области, а также иных субъектов персональных данных

Согласие **на обработку персональных данных**
(информация о субъекте персональных данных)
Я, _____ *(фамилия)* *(имя)* *(отчество)*
(основной документ, удостоверяющий личность) *(номер основного документа, удостоверяющего его личность)*
(сведения о дате выдачи указанного документа) *(сведения о выдавшем указанный документ органе)* **зарегистрированный по адресу:** _____ *(адрес)*
принимаю решение о предоставлении своих персональных данных в составе:
- фамилия, имя, отчество (при наличии) (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);
- число, месяц, год рождения;
- место рождения;
- сведения о гражданстве (в том числе предыдущие гражданства, иные гражданства);
- вид, серия, номер документа, удостоверяющего личность, дата выдачи, наименование органа, выдавшего его;
- адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания;
- номер контактного телефона или сведения о других способах связи;
- реквизиты страхового свидетельства обязательного пенсионного страхования;
- идентификационный номер налогоплательщика;
- реквизиты страхового медицинского полиса обязательного медицинского страхования;
- реквизиты свидетельств о государственной регистрации актов гражданского состояния;
- сведения о семейном положении, составе семьи и о близких родственниках (в том числе бывших);
- сведения о трудовой деятельности;
- сведения о воинском учете и реквизиты документов воинского учета;
- сведения об образовании (когда и какие образовательные, научные и иные организации окончил, номера документов об образовании, направление подготовки или специальность по документу об образовании, квалификация);
- сведения об ученой степени;

- сведения о владении иностранными языками, уровень владения;
- сведения об отсутствии у гражданина заболевания, препятствующего поступлению на государственную гражданскую службу или ее прохождению;
- фотография;
- сведения о прохождении гражданской службы (работы), в том числе: дата, основания поступления на гражданскую службу (работу) и назначения на должность гражданской службы, дата, основания назначения, перевода, перемещения на иную должность гражданской службы (работы), наименование замещаемых должностей гражданской службы с указанием структурных подразделений, размера денежного содержания (заработной платы), результатов аттестации на соответствие замещаемой должности гражданской службы, а также сведения о прежнем месте работы;
- сведения, содержащиеся в служебном контракте (трудовом договоре), дополнительных соглашениях к служебному контракту (трудовому договору);
- сведения о пребывании за границей;
сведения о классном чине гражданской службы Российской Федерации (воинском или специальном звании, классном чине гражданской службы субъекта Российской Федерации или классном чине муниципальной службы);
- сведения о наличии или отсутствии судимости;
- сведения об оформленных допусках к государственной тайне;
- сведения о государственных наградах, иных наградах и знаках отличия;
- сведения о профессиональной переподготовке и (или) повышении квалификации;
- сведения о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;
- сведения о доходах, расходах, об имуществе и обязательствах имущественного характера;
- номер расчетного счета;
- номер банковской карты;
- персональные данные, содержащиеся в выписке из домовой книги, копиях финансового лицевого счета, свидетельства о браке, свидетельства о рождении ребенка (детей), трудовой книжки, документов о наличии в собственности гражданского служащего и (или) членов его семьи жилых помещений;
- иные персональные данные, предусмотренные законодательством Российской Федерации.
и своей волей и в своем интересе даю согласие на их обработку уполномоченными должностными лицами архивного управления Курской области, расположенного по адресу: г. Курск, ул. Ленина, д.57, включающую:
1. сбор
2. запись
3. систематизацию
4. накопление
5. хранение
6. уточнение (обновление)
7. уточнение (изменение)
8. извлечение
9. использование
10. передачу (предоставление)
11. передачу (доступ)
12. обезличивание
13. блокирование
14. удаление

15. уничтожение

(в случае обработки общедоступных персональных данных)

16. передачу (распространение)

способами, определяемыми локальными актами архивного управления Курской области, регламентирующими работу в информационных системах персональных данных и программных продуктах таких систем, включая их обработку в информационных системах персональных данных: ГИС «Ведение бухгалтерского учета архивного управления Курской области», ГИС «Ведение кадрового учета, юридической работы и внутреннего документооборота архивного управления Курской области (кабинет 14)», ГИС «Ведение кадрового учета, юридической работы и внутреннего документооборота архивного управления Курской области (кабинет 16а)»

с целью:
обеспечения соблюдения в отношении меня законодательства Российской Федерации в сфере отношений, связанных с поступлением на государственную гражданскую службу субъекта Российской Федерации, ее прохождением и прекращением (трудовых и непосредственно связанных с ними отношений), для реализации полномочий, возложенных на архивное управление Курской области действующим законодательством

на срок: с даты подписания настоящего согласия в течение всего срока прохождения государственной гражданской службы субъекта Российской Федерации (срока работы) в архивном управлении Курской области

Я извещен (а) о том, что согласие на обработку персональных данных может быть отозвано на основании заявления субъекта персональных данных.

Порядок отзыва согласия:

Отзыв согласия подается в письменном виде лицом, указанным в согласии на обработку персональных данных, лично.

Отзыв должен содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных;
- сведения о дате выдачи указанного документа и выдавшем его органе;
- собственноручную подпись субъекта персональных данных;
- сведения о согласии на обработку персональных данных (дата и адрес, по которому давалось согласие).

Отзыв согласия осуществляется месту нахождения архивного управления Курской области.

В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных прекращение обработки персональных данных и уничтожение персональных данных будет произведено по окончании календарного года, в течение которого поступил отзыв.

В случае отзыва согласия на обработку персональных данных архивное управление вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных".

Порядок защиты субъектом персональных данных своих прав и законных интересов осуществляется в соответствии с требованиями Федерального закона №152 от 27 июля 2006 г. «О персональных данных

Я извещен (а) о том, что:

- после увольнения с государственной гражданской службы (прекращения трудовых отношений) персональные данные будут храниться в архивном управлении Курской области в течение предусмотренного законодательством Российской Федерации срока хранения документов;
- персональные данные, предоставляемые в отношении третьих лиц, будут обрабатываться только в целях осуществления и выполнения возложенных законодательством Российской Федерации на архивное управление Курской области функций, полномочий и обязанностей.
Я подтверждаю, что предоставленные мною персональные данные являются полными, актуальными и достоверными.
Я обязуюсь своевременно извещать об изменении предоставленных персональных данных.
« ____ » _____ 20 _____ г. _____ *(личная подпись)* *(инициалы, фамилия)*

Приложение 4

Форма уведомлений о совершенных операциях над персональными данными

на официальном бланке

Уважаемый (-ая), [Имя Отчество]!

В соответствии с требованиями Федерального закона Российской Федерации №152-ФЗ от 27 июля 2006 года «О персональных данных» уведомляем Вас

- о результатах рассмотрения возражения о принятии решения при обработке Ваших персональных данных на основании исключительно автоматизированной обработки **[ответ по существу]**
- о внесенных изменениях и предпринятых мерах по уничтожению или блокированию соответствующих персональных данных на основании предоставленных субъектом персональных данных сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет архивное управление Курской области являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки **[ответ по существу]**
- об устранении выявленных неправомерных действий с персональными данными или об уничтожении персональных данных, в случае невозможности устранения допущенных нарушений **[ответ по существу]**
- о прекращении обработки персональных данных и уничтожении соответствующих персональных данных в случае достижения цели обработки персональных данных **[ответ по существу]**
- о прекращении обработки персональных данных и уничтожении соответствующих персональных данных в случае отзыва субъектом персональных данных согласия на обработку своих персональных **[ответ по существу]**
- о получении Ваших персональных данных архивным управлением Курской области, располагается по адресу (указать адрес) с целью **[цель обработки персональных данных]** на основании **[правовое основание]**. Обработка Ваших персональных данных будет осуществляться только специально допущенными сотрудниками архивного управления Курской области. В соответствии с действующим законодательством РФ в области персональных данных Вы имеете право: давать своей волей и в своем интересе и отзывать согласие на обработку своих персональных данных в предусмотренных действующим законодательством Российской Федерации случаях; на получение сведений об архивном управлении Курской области (в объеме необходимом для защиты своих прав и законных интересов по вопросам обработки своих персональных данных), о месте нахождения архивного управления Курской области, о наличии у архивного управления Курской области своих персональных данных, а также на ознакомление с такими персональными данными; подавать запрос на доступ к своим персональным данным; требовать безвозмездного предоставления возможности ознакомления со своими персональными данными, а также внесения в них необходимых изменений, их уничтожения или блокирования при предоставлении сведений, подтверждающих, что такие персональные данные являются неполными, устаревшими,

недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки; получать уведомления по вопросам обработки персональных данных в установленных действующим законодательством Российской Федерации случаях и сроки; требовать от архивного управления Курской области разъяснения порядка защиты субъектом персональных данных своих прав и законных интересов; обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке; на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Наименование
должности **подпись** **Ф.И.О.**

Ф.И.О. сотрудника
телефон

Приложение 5

Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

на официальном бланке

Уважаемый (-ая), [Имя Отчество]!

В соответствии с требованиями Федерального закона Российской Федерации №152-ФЗ от 27 июля 2006 года «О персональных данных» уведомляем Вас, что обязанность предоставления Вами персональных данных установлена **[пункт]** федерального закона **[реквизиты и наименование федерального закона]**, а также следующими нормативными актами **[указываются реквизиты и наименования таких нормативных актов]**. В случае отказа Вами предоставить свои персональные данные, архивное управление Курской области не сможет на законных основаниях осуществлять такую обработку, что приведет к следующим для Вас юридическим последствиям **[перечисляются юридические последствия для субъекта персональных данных, то есть случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или случаи иным образом затрагивающее его права, свободы и законные интересы]**.

В соответствии с действующим законодательством РФ в области персональных данных Вы имеете право: на получение сведений об архивном управлении Курской области (в объеме необходимом для защиты своих прав и законных интересов по вопросам обработки своих персональных данных), о месте нахождения архивного управления Курской области, о наличии у архивного управления Курской области своих персональных данных, а также на ознакомление с такими персональными данными; подавать запрос на доступ к своим персональным данным; требовать безвозмездного предоставления возможности ознакомления со своими персональными данными, а также внесения в них необходимых изменений, их уничтожения или блокирования при предоставлении сведений, подтверждающих, что такие персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки; получать уведомления по вопросам обработки персональных данных в установленных действующим законодательством Российской Федерации случаях и сроки; требовать от архивного управления Курской области разъяснения порядка защиты субъектом персональных данных своих прав и законных интересов; обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке; на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Наименование
должности **подпись** **Ф.И.О.**

Ф.И.О. сотрудника
телефон

Приложение 6

Форма акта уничтожения персональных данных

Акт
уничтожения персональных данных

№ _____ «___» _____202__ г.

Комиссия в составе:
председателя комиссии:

членов комиссии:

уничтожила персональные данные:

№ п/п	Дата уничтожения	ФИО	Основание на уничтожение
1.			
2.			
3.			
4.			
5.			

Председатель комиссии

Члены комиссии

Приложение 7

Форма Журнала учета лиц (организаций), получивших доступ к персональным данным, и (или) лиц (организаций), которым такая информация была предоставлена или передана

№ п/п	Дата ознакомления	Основание на ознакомление	Лицо (организация) получившее доступ к персональным данным	С какими данными ознакомлены
1.				
2.				
3.				

Приложение 8

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

Я, **[фамилия имя отчество полностью]**, являясь сотрудником архивного управления Курской области и непосредственно осуществляя обработку персональных данных, в соответствии с требованиями по соблюдению конфиденциальности обрабатываемых мною персональных данных субъектов персональных данных обязуюсь в случае расторжения со мной служебного контракта (трудового договора), прекратить обработку персональных данных, ставших мне известными в связи с исполнением должностных обязанностей.

Я ознакомлен с предусмотренной действующим законодательством Российской Федерации ответственностью за нарушения неприкосновенности частной жизни и установленного Федеральным законом «О персональных данных» порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

[дата] **[подпись]**

Приложение 9

Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Классы защищенности информационной системы			
		4	3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+	+
ИАФ.7	Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа				
II. Управление доступом субъектов доступа к объектам доступа (УПД)					
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+	+	+
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+	+
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами			+	+

УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы		+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы		+	+	+
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	+	+
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации				
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему				
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы				+
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		+	+	+
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	+	+	+	+
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки				
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+	+	+	+
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	+	+	+
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+	+	+
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+	+	+	+
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники			+	+
III. Ограничение программной среды (ОПС)					
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения				+

ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения			+	+
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	+	+	+	+
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов				
IV. Защита машинных носителей информации (ЗНИ)					
ЗНИ.1	Учет машинных носителей информации	+	+	+	+
ЗНИ.2	Управление доступом к машинным носителям информации	+	+	+	+
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны				
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах				
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации			+	+
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации				
ЗНИ.7	Контроль подключения машинных носителей информации				
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)	+	+	+	+
V. Регистрация событий безопасности (РСБ)					
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+	+
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+	+
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+	+
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти	+	+	+	+
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	+	+	+	+

РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	+	+	+	+
РСБ.7	Защита информации о событиях безопасности	+	+	+	+
РСБ.8	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе				
VI. Антивирусная защита (АВЗ)					
АВЗ.1	Реализация антивирусной защиты	+	+	+	+
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	+
VII. Обнаружение вторжений (СОВ)					
СОВ.1	Обнаружение вторжений			+	+
СОВ.2	Обновление базы решающих правил			+	+
VIII. Контроль (анализ) защищенности информации (АНЗ)					
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		+	+	+
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+	+
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		+	+	+
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+	+
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе		+	+	+
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)					
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации			+	+
ОЦЛ.2	Контроль целостности информации, содержащейся в базах данных информационной системы				
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций	+	+	+	+
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)			+	+

ОЦЛ.5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы				
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему				+
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему				
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях				
X. Обеспечение доступности информации (ОДТ)					
ОДТ.1	Использование отказоустойчивых технических средств				+
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы				+
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование			+	+
ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители информации			+	+
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала			+	+
ОДТ.6	Кластеризация информационной системы и (или) ее сегментов				
ОДТ.7	Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации			+	+
XI. Защита среды виртуализации (ЗСВ)					
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+	+	+	+
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+	+	+
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		+	+	+

ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры			+	+
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией				
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных			+	+
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций			+	+
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры			+	+
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре		+	+	+
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей			+	+
XII. Защита технических средств (ЗТС)					
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам				
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования	+	+	+	+
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены	+	+	+	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+	+
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)				+
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)					

ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы			+	+
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	+	+	+	+
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)				
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств	+	+	+	+
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными информационными системами				
ЗИС.7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода			+	+
ЗИС.8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи			+	+
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации			+	+
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения				

	сетевых имен по сетевым адресам				
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов			+	+
ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю			+	+
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя			+	+
ЗИС.14	Использование устройств терминального доступа для обработки информации				
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации			+	+
ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов				
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы			+	+
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения				
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти				
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе		+	+	+
ЗИС.21	Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы				+
ЗИС.22	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы			+	+
ЗИС.23	Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями			+	+
ЗИС.24	Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого			+	+

	соединения				
ЗИС.25	Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды)				
ЗИС.26	Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем				
ЗИС.27	Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации				
ЗИС.28	Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы				
ЗИС.29	Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы				
ЗИС.30	Защита мобильных технических средств, применяемых в информационной системе		+	+	+

"+" - мера защиты информации включена в базовый набор мер для соответствующего класса защищенности информационной системы.

Меры защиты информации, не обозначенные знаком "+", применяются при адаптации базового набора мер и уточнении адаптированного базового набора мер, а также при разработке компенсирующих мер защиты информации в информационной системе соответствующего класса защищенности.