Приложение 6 к распоряжению
Думы Далматовского муниципального округа
Курганской области
от 13.08.2024 г. № 54
«О мерах, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных»

ПОЛОЖЕНИЕ
об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Думы Далматовского муниципального округа Курганской области

1.Общие положения

Положение об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Думы Далматовского муниципального округа Курганской области (далее – Положение) разработано в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119 (далее – ПП-1119), Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» в целях обеспечения соблюдения законных прав и интересов работников Думы Далматовского муниципального округа Курганской области (далее – Дума, Оператор), граждан и иных лиц, персональные данные которых обрабатываются Оператором, а также установления ответственности за нарушение порядка обработки персональных данных.

2.Назначение и область применения

Настоящее Положение определяет порядок организации работ, а также средства и меры по обеспечению безопасности персональных данных при их обработке в информационных системах Оператора.

Настоящее Положение должно быть доведено до каждого работника Оператора, осуществляющего обработку персональных данных, под расписку.

3.Основные термины, определения, сокращения

В настоящем Положении использованы следующие термины и определения:

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Безопасность информации – состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, то есть сохранение втайне от субъектов, не имеющих полномочий на ознакомление с ней, целостность и доступность информации при ее обработке техническими средствами.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Бумажный носитель персональных данных – материальный носитель графической и буквенно-цифровой информации, отраженной (зафиксированной) на бумаге.

Доступ к информации (доступ) – ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

Доступность информации – состояние информации, характеризуемое способностью автоматизированной системы обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

Инцидент - событие или группа событий, которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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

Машинный носитель информации – сменный носитель данных, предназначенный для записи и считывания данных, представленных в стандартных кодах.

Обезличивание персональных данных - действия, в результате которых невозможно определить без использования дополнительной информации принадлежность персональных данных конкретному субъекту персональных данных.

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.

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.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому или иностранному юридическому лицу.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных и (или) результате которых уничтожаются материальные носители персональных данных.

В настоящем Положении использованы следующие сокращения и понятия:

ИС – информационная система;

ИСПДН - информационная система персональных данных;

Оператор - Дума Далматовского муниципального округа Курганской области;

Ответственный - ответственный за организацию обработки персональных данных;

ПДн - персональные данные;

Роскомнадзор - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций;

4.Организация обработки и защиты персональных данных

Для организации обработки и защиты персональных данных в Думе Далматовского муниципального округа Курганской области назначаются следующие ответственные лица:

1) ответственный за организацию обработки персональных данных (далее – Ответственный);

2) администраторы информационных систем, обрабатывающих персональные данные;

3) администратор информационной безопасности;

4) ответственный за регистрацию и предоставление ответов.

Организацию обработки персональных данных субъектов, контроль соблюдения мер их защиты в структурных подразделениях Оператора, сотрудники которых имеют доступ к персональным данным, осуществляют их непосредственные руководители.

Работники, доступ которых к обрабатываемым в информационных системах персональным данным, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании утвержденного Перечня должностей работников после ознакомления с организационно-распорядительными документами Оператора по вопросам обработки и защиты персональных данных и инструктажа специалистом по кадрам. Эти работники являются пользователями информационных систем персональных данных (далее – Пользователи).

Пользователи обязаны соблюдать режим конфиденциальности и безопасности персональных данных при их обработке в информационных системах на всех этапах их жизненного цикла.

4.1 Ответственный за организацию обработки ПДн

Ответственный за организацию обработки ПДн обязан:

– планировать и организовывать проведение работ по приведению процессов обработки персональных данных Оператора в соответствие требованиям федерального законодательства в области персональных данных;

– осуществлять внутренний контроль за соблюдением работниками Оператора законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;

– обеспечивать разработку (доработку) и утверждение организационно-распорядительной и иной документации Оператора по вопросам обработки и защиты персональных данных;

– организовывать ведение актуального перечня должностей работников, допущенных к работе с персональными данными для выполнения служебных обязанностей;

– организовать первоначальное ознакомление работников Оператора с требованиями нормативных правовых актов Российской Федерации и локальных актов Оператора по вопросам обработки и защиты персональных данных;

– организовывать и контролировать прием, обработку обращений и запросов субъектов персональных данных (их представителей), а также запросов и предписаний Уполномоченного органа по защите прав субъектов персональных данных (далее – Роскомнадзор);

– разрабатывать дополнения к трудовым договорам (и/или должностным инструкциям) для работников, задействованных в обеспечении безопасности и обработки ПДн;

– организовывать подачу уведомления в Роскомнадзор при возникновении изменений в сведениях об Операторе;

– представлять интересы Оператора при осуществлении государственного контроля и надзора за обработкой персональных данных Уполномоченным органом по защите прав субъектов персональных данных;

– производить оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных" с составлением акта оценки вреда (форма представлена в документе «Типовые формы документов, используемые для организации обработки персональных данных в Думе Далматовского муниципального округа Курганской области».

Ответственный имеет право:

– вносить предложения по совершенствованию уровня защищенности персональных данных;

– требовать соблюдения установленных правил и порядка выполнения работ с персональными данными, а также прекращения обработки персональных данных в случае их нарушения;

– инициировать проведение служебных расследований по фактам нарушения установленных правил обработки персональных данных, несанкционированного доступа к защищаемой информации и техническим средствам информационных систем;

– давать отдельным работникам поручения по вопросам, входящим в компетенцию Ответственного;

– вступать во взаимоотношения со сторонними организациями для решения вопросов, входящих в компетенцию Ответственного.

4.2 Администраторы информационных систем

Обеспечение обработки персональных данных в информационных системах возлагается на администраторов информационных систем, обрабатывающих персональные данные (администраторов ИСПДн).

На администраторов информационных систем, обрабатывающих персональные данные, возлагаются следующие обязанности:

- предоставление, изменение и прекращение доступа пользователей к персональным данным в ИСПДн в соответствии с утвержденным Перечнем должностей работников;
- управление учетными записями пользователей в ИСПДн;
- поддержание штатной работы ИСПДн;
- инсталляция, конфигурирование и администрирование программно-аппаратных средств информационных систем, кроме средств защиты информации;
- уточнение, блокирование, уничтожение персональных данных в случаях, определенных организационно-распорядительными документами по вопросам персональных данных и федеральным законодательством;
- периодическое резервное копирование персональных данных;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- участие в обработке инцидентов безопасности персональных данных;
- предоставление информации для формирования ответов на обращения, запросы и предписания субъектов персональных данных и Роскомнадзора в установленные сроки.

Администраторы информационных систем, обрабатывающих персональные данные, имеют право:

- требовать от пользователей выполнения установленных правил обработки персональных данных;
- вносить предложения по совершенствованию системы защиты персональных данных;
- решать поставленные задачи в соответствии с полномочиями доступа к ресурсам информационной системы персональных данных.

4.3 Администратор информационной безопасности

Обеспечение защиты персональных данных в информационных системах возлагается на администратора информационной безопасности, который выполняет следующие функции:

- учет машинных носителей персональных данных в соответствии с п.10 настоящего Положения;
- инсталляция, конфигурирование и администрирование программно-аппаратных средств защиты информации в соответствии с техническим проектом;
- учет технических средств защиты информации;
- обновление средств защиты информации, контроль правильности их функционирования;
- предоставление информации для формирования ответов на обращения, запросы и предписания субъектов персональных данных и Роскомнадзора в установленные сроки.

Администратор информационной безопасности имеет право:

- требовать от пользователей и администраторов информационных систем выполнения установленных правил обработки персональных данных;
- вносить предложения по совершенствованию системы защиты персональных данных;
- решать поставленные задачи в соответствии с полномочиями доступа к ресурсам информационной системы персональных данных и средствам защиты информации.

4.4 Ответственный за регистрацию обращений и предоставление ответов

Для регистрации и отправки ответов обращений и запросов субъектов персональных данных или их представителей, а также запросов и предписаний Уполномоченного органа по защите прав субъектов персональных данных назначается ответственный за регистрацию обращений и предоставление ответов.

Ответственный за регистрацию обращений и предоставление ответов:

- регистрирует обращения субъектов в Журнале учета обращений;
- информирует ответственного за организацию обработки персональных данных о

получении обращений и запросов;

– ведет Журнал учета проверок, проводимых Уполномоченным органом по защите прав субъектов персональных данных, и отправляет ответы (мотивированные отказы) на запросы, обращения и предписания.

Процедура обработки обращений субъектов персональных данных и запросов Уполномоченного органа по защите прав субъектов персональных данных установлена в локальных нормативных актах Оператора.

Ответственный имеет право:

– запрашивать необходимую информацию у работников Оператора;

– выдавать администратору ИСПДн распоряжения о блокировании, уточнении, уничтожении персональных данных;

– созывать Комиссию для решения вопросов по возражениям субъектов ПДн против принятия решений на основании исключительно автоматизированной обработки персональных данных.

5.Обеспечение безопасности персональных данных при их автоматизированной обработке

5.1.Требования к системе защиты персональных данных

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты, реализованной организационными и техническими мерами.

Система защиты персональных данных Оператора должна обеспечивать:

– нейтрализацию актуальных угроз безопасности персональных данных;

– проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) 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 обеспечения уровня защищенности персональных данных.

5.2. Порядок создания системы защиты персональных данных

Для создания (модернизации) системы защиты персональных данных, как правило, проводятся следующие мероприятия и работы:

– обследование порядка обработки персональных данных в информационных системах;

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

– установление уровня защищенности персональных данных;

– определение состава и содержания мер по обеспечению безопасности персональных данных;

– проектирование системы защиты персональных данных;

– закупка и внедрение средств защиты информации;

– оценка соответствия информационной системы персональных данных требованиям безопасности информации;

– ввод системы защиты персональных данных в эксплуатацию.

Разработка и осуществление мероприятий по созданию системы защиты персональных данных может осуществляться Оператором силами собственных специалистов или сторонней организацией на договорной основе, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

5.2.1. Обследование обработки персональных данных в информационных системах

Обследование обработки персональных данных в информационных системах проводится с целью определения (актуализации) состава, структуры информационных систем, принятых мер безопасности, содержания и объема обрабатываемых персональных данных, а также взаимодействия информационных систем с иными системами и телекоммуникационными сетями общего пользования. На основании обследования вырабатываются рекомендации по совершенствованию существующей системы защиты персональных данных.

5.2.2. Определение угроз безопасности

Актуальные угрозы безопасности персональных данных при их обработке в информационных системах персональных данных определяются исходя из наличия вероятного нарушителя, возможных способов и средств реализации угроз. На их основе в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», на основании нормативно-методических документов ФСТЭК России и ФСБ России по вопросам защиты персональных данных формируется Модель угроз и нарушителя.

Моделью угроз и нарушителя необходимо руководствоваться на всех этапах жизненного цикла информационных систем персональных данных Оператора:

- при проектировании;
- при вводе в эксплуатацию;
- в режиме эксплуатации;
- при модернизации;
- при проведении регламентных и ремонтно-профилактических работ.

5.2.3. Установление уровня защищенности персональных данных

Для информационной системы персональных данных в соответствии с ПП-1119 с учетом актуальных угроз безопасности специально назначенной комиссией устанавливается уровень защищенности персональных данных. Результаты установления уровня защищенности персональных данных при их обработке в информационных системах Оператора оформляются Актом (форма – Приложение № 1 к настоящему Положению).

5.2.4. Определение состава и содержания мер по обеспечению безопасности ПДн

Выбор мер по защите персональных данных в информационной системе осуществляется на основе уровня ее защищенности с учетом структуры информационной системы, применяемых технических средств и информационных технологий, а также актуальных угроз безопасности персональных данных.

Система защиты персональных данных в соответствии с требованиями приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Приказ № 21) должна быть, как правило, реализована следующими группами мер (подсистемами):

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;
- регистрация событий безопасности;
- антивирусная защита;
- контроль (анализ) защищенности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- управление конфигурацией информационной системы и системы защиты персональных данных.

Состав и содержание мер защиты персональных данных, необходимых для реализации в информационной системе персональных данных, отражаются в техническом (частном техническом) задании на создание системы защиты персональных данных.

5.2.5. Проектирование системы защиты персональных данных

Проектирование системы защиты заключается в выработке вариантов технических решений по реализации установленных мер обеспечения безопасности персональных данных с учетом существующих способов и средств защиты информации.

По результатам проектирования оформляется технический проект системы защиты.

5.2.6. Закупка и внедрение средств защиты

Закупка средств защиты информации в соответствии с техническим проектом осуществляется за счет бюджета Оператора.

Все работы по установке, монтажу и испытанию средств защиты информации должны производиться Оператором самостоятельно либо сторонней организацией, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

В процессе пуско-наладочных работ средства защиты информации устанавливаются, настраиваются и испытываются на готовность к использованию в информационных системах персональных данных Оператора. При положительных результатах средства защиты вводятся в

эксплуатацию с составлением Акта (форма – Приложение № 2 к настоящему Положению). Установка, проверка и ввод средств защиты информации в эксплуатацию производится в соответствии с эксплуатационной и технической документацией на эти средства защиты комиссией организации – исполнителя работ.

5.2.7. Оценка эффективности принятых мер

Оценка эффективности принятых мер безопасности информации в информационной системе персональных данных проводится в форме добровольной аттестации или в форме оценки соответствия. Результатом оценки эффективности принятых мер является Аттестат соответствия (Заключение о соответствии) информационной системы персональных данных требованиям безопасности информации.

5.2.8. Ввод системы защиты в эксплуатацию

На основании Аттестата соответствия (Заключения о соответствии) требованиям безопасности информации Оператором издается приказ о вводе системы защиты в промышленную эксплуатацию и о разрешении обработки в информационной системе конфиденциальной информации (персональных данных).

6.Меры обеспечения безопасности персональных данных

Оператор принимает необходимые организационные и технические меры 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.

6.1. Организационные меры защиты

Для обеспечения безопасности персональных данных при их обработке в информационных системах Оператора применяются следующие организационные меры:

– ознакомление работников с внутренними требованиями Оператора по защите персональных данных;

– допуск пользователей к соответствующим персональным данным, обрабатываемым в информационной системе, для исполнения служебных обязанностей на основании утвержденного Перечня должностей работников Оператора;

– обеспечение учета, хранения, обращения и уничтожения машинных носителей персональных данных;

– обеспечение контроля доступа в помещения, в которых находятся технические средства обработки персональных данных, хранятся носители персональных данных;

– размещение технических средств обработки персональных данных в пределах охраняемых помещений;

– обеспечение пропускного режима на территорию Оператора, контроля доступа и охраны помещений с установленными техническими средствами обработки персональных данных.

6.2.Технические меры защиты

Для обеспечения безопасности персональных данных при их обработке в информационных системах Оператора применяются следующие технические меры:

– установление и реализация правил разграничения доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты персональных данных;

– регистрация и учет действий пользователей, совершаемых с персональными данными в информационных системах;

– применение в необходимых случаях для обеспечения безопасности персональных данных средств криптографической защиты информации;

– осуществление антивирусного контроля;

– обеспечение восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– применение средств межсетевого экранирования;

– анализ защищенности информационных систем с применением специализированных программных средств (сканеров безопасности);

– централизованное управление системой защиты персональных данных.

6.3. Применяемые средства защиты информации

Средства защиты информации, применяемые в информационных системах персональных данных, должны проходить в установленном порядке процедуру оценки соответствия в случаях,

когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

Контроль соблюдения порядка и условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией, возлагается на администратора ИБ.

Работники Оператора, использующие средства защиты информации для обеспечения безопасности персональных данных, должны быть обучены правилам работы с ними.

6.4. Правила антивирусной защиты.

Настоящие правила определяют требования к организации защиты ИСПДн от разрушающего воздействия вредоносного программного обеспечения (ПО), компьютерных вирусов и устанавливает ответственность руководителя и сотрудников, эксплуатирующих и сопровождающих компьютеры в составе ИСПДн, за их выполнение. Настоящие правила распространяются на все объекты ИСПДн Оператора.

К использованию на компьютерах допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется администратором безопасности.

Администратор безопасности осуществляет периодическое обновление антивирусных пакетов и контроль их работоспособности.

Ярлык (ссылка) для запуска антивирусной программы должен быть доступен всем пользователям информационной системы.

Еженедельно в начале работы, после загрузки компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютеров.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Настройки средств антивирусной защиты должны быть выполнены в соответствии с требованиями безопасности персональных данных определенного уровня защищенности ИСПДн. Настройку средств антивирусной защиты выполняет администратор безопасности.

Файлы, помещаемые в электронный архив на магнитных носителях, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, администратором безопасности должна быть выполнена антивирусная проверка ИСПДн.

На компьютеры запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно (или вместе с администратором безопасности) должен провести внеочередной антивирусный контроль компьютера.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить обработку данных в ИСПДн;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ возможности, дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями настоящего Положения возлагается на ответственного за защиту информации.

Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на администратора безопасности и всех пользователей данной ИСПДн.

7.Режим безопасности технических средств

7.1. Порядок размещения технических средств

Помещения, в которых размещаются технические средства информационных систем персональных данных, а также в которых ведется работа с персональными данными, должны исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц, а также просмотра ведущихся в них работ.

Помещения выделяются с учетом максимально возможных размеров контролируемой зоны. Они должны иметь прочные стены, межэтажные перекрытия и прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.

Окна помещений, расположенных на первых или последних этажах зданий и других мест, откуда возможно проникновение в помещения посторонних лиц, оборудуются решетками или охранной сигнализацией, препятствующей неконтролируемому проникновению в помещения. Для предотвращения просмотра извне окна помещений должны быть защищены шторами или жалюзи.

Двери помещений должны быть постоянно закрыты на замок и открываться только для санкционированного прохода сотрудников и посетителей.

Размещение технических средств обработки персональных данных в помещениях, в которых они установлены, должно осуществляться таким образом, чтобы была исключена возможность несанкционированного просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные.

Помещения, как правило, оборудуются охранной сигнализацией, выведенной на пост охраны здания. Исправность сигнализации должна периодически проверяться уполномоченным лицом.

8.Организация доступа в информационные системы

8.1. Порядок предоставления доступа

Работник, доступ которому к обрабатываемым в информационных системах персональным данным необходим для выполнения служебных (трудовых) обязанностей, допускается к соответствующим персональным данным на основании утвержденного Перечня должностей работников.

Вновь принятый на работу сотрудник должен ознакомиться с организационно-распорядительными документами Оператора по вопросам персональных данных, пройти инструктаж и подписать Обязательство о неразглашении персональных данных.

Создание учетной записи Пользователя и предоставление ему доступа к ресурсам информационной системы персональных данных осуществляется Администратором системы на основании Заявки.

Администратор системы в течение рабочего дня регистрирует Пользователя и настраивает его права доступа, выдает ему необходимые атрибуты доступа (логин и пароль).

Каждому Пользователю предоставляется уникальная учетная запись (логин) и первоначальный пароль для входа в систему. После первого входа в систему первоначальный пароль должен быть изменен Пользователем с учетом требований к длине и сложности паролей, установленных «Парольной политикой».

Администратор системы, осуществляющий создание учетной записи, заполняет реестр, в котором указываются следующие данные Пользователя:

- фамилия, имя и отчество;
- структурное подразделение;
- учетная запись;
- информационная система, к которой предоставляется доступ;
- права доступа;
- дата доступа.

Пользователю должны предоставляться минимально необходимые для выполнения служебных обязанностей права доступа в информационную систему. Ответственность за минимальную достаточность прав доступа Пользователя несет руководитель структурного подразделения.

В ИСПДн должно быть предусмотрено ограничение неуспешных попыток входа (доступов к информационным системам) не более 5 (пяти), после чего возможность доступа должна блокироваться на период не менее 10 минут.

8.2. Изменение прав доступа

Пересмотр и изменение (корректировка) прав Пользователей проводится Администратором системы при назначении Пользователя на другую должность, при переводе в другое подразделение, а также при поступлении Заявки об изменении прав доступа.

Об изменении прав доступа Администратор системы ставит в известность Пользователя.

8.3. Прекращение доступа

При увольнении из Думы Далматовского муниципального округа Курганской области доступ Пользователя прекращается.

Администратор системы блокирует учетную запись Пользователя, а по истечении не более 90 дней с даты получения Заявки – удаляет ее из системы.

8.4. Обязанности пользователя

Пользователь обязан:

– использовать рабочую станцию только для выполнения разрешенных процедур автоматизированной обработки информации;

– знать и соблюдать установленные правила обеспечения безопасности персональных данных при их обработке в информационной системе;

– знать и соблюдать правила эксплуатации аппаратных средств, входящих в состав информационной системы персональных данных;

– знать и соблюдать правила обеспечения безопасности персональных данных при доступе к информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования);

– обеспечить размещение экрана монитора на своем рабочем месте так, чтобы исключалась возможность несанкционированного просмотра отображаемой на нем информации;

– хранить в тайне свой пароль и периодически менять его в соответствии с установленной парольной политикой;

– обеспечить надежное хранение персональных идентификаторов;

– соблюдать правила антивирусной защиты рабочей станции;

– обеспечить сохранность используемых машинных носителей информации с персональными данными;

– проверять все съемные носители информации при подключении к рабочей станции на отсутствие вирусов и вредоносных программ;

– осуществлять резервное копирование, уничтожение и восстановление информации в рамках выделенных полномочий самостоятельно, либо через Администратора информационных систем;

– при оставлении своего рабочего места блокировать рабочую станцию для предотвращения несанкционированного доступа к обрабатываемой информации;

– сообщать в службу информационных технологий о ставших известными каналах утечки информации, способах обхода системы защиты персональных данных;

– контролировать пребывание третьих лиц (посетителей, обслуживающего персонала) в помещениях Оператора для предотвращения несанкционированного доступа этих лиц к персональным данным;

– в случае возникновения нештатных ситуаций в работе информационной системы, нарушениях опломбирования блоков, подозрении в компрометации личного пароля прекратить выполняемые работы и сообщить руководителю о сбое (нарушении).

Пользователю запрещается:

– передавать (предоставлять) персональные данные при телефонных переговорах по незащищенным каналам связи;

– передавать персональные данные в составе сообщений электронной почты в незащищенном (незашифрованном) виде;

– осуществлять запись персональных данных на неучтенные установленным порядком носители информации;

– выносить за пределы служебных помещений Оператора учтенные машинные носители информации, а также документы, содержащие персональные данные, без разрешения уполномоченных лиц;

– передавать машинные носители информации и документы, содержащие персональные данные лицам, не допущенным к обработке таких данных;

– оставлять на рабочем месте без присмотра машинные носители информации и документы, содержащие персональные данные;

– подключать к рабочей станции и информационной системе личные носители информации, в том числе мобильные устройства;

– хранить машинные носители информации вблизи источников электромагнитных излучений и прямых солнечных лучей;

– вносить изменения в конфигурацию программно-аппаратных средств информационной системы (в том числе изменять расположение аппаратных средств) без разрешения руководителя;

– записывать посторонние программы и иную информацию на машинные носители информации, используемые для обработки персональных данных;

– осуществлять обработку персональных данных в присутствии посторонних лиц, а также допускать их к решению задач (производству расчетов, формированию документов и т.п.);

– выполнять работы при обнаружении нарушенных печатей и пломб узлов и блоков информационной системы, самовольно срывать такие пломбы;

– разглашать сведения о применяемых средствах защиты информации;

– производить обработку персональных данных с выключенными или нерабочими средствами защиты.

9.Порядок обращения с носителями персональных данных

9.1. Перечень машинных носителей персональных данных.

Для обработки персональных данных в Думе Далматовского муниципального округа Курганской области могут использоваться машинные носители информации. К машинным носителям информации относятся следующие:

– накопители на жестких магнитных дисках (НЖМД);
– оптические диски (CD, DVD);
– Flash-накопители;
– другие электронные устройства для хранения информации.

9.2. Регистрация и учет носителей информации

Все машинные носители информации, на которых производится обработка персональных данных, подлежат обязательному учету с присвоением им (фиксацией) уникальных регистрационных (серийных, заводских) номеров.

Учет машинных носителей персональных данных осуществляет администратор информационной безопасности.

Необходимые данные регистрируемого машинного носителя информации заносятся в Журнал учета машинных носителей информации (форма – Приложение № 4 к настоящему Положению).

При регистрации машинного носителя информации, помимо заполнения граф Журнала учета, на его основу любым доступным способом (образцы – Приложение № 5 к настоящему Положению) наносятся следующие реквизиты:

– гриф «Конфиденциально»;
– учетный номер по Журналу учета;
– подпись лица, ответственного за организацию учета.

При невозможности доступа к носителю информации с целью нанесения на него учетных данных, такая информация наносится на корпус технического средства, в котором установлен машинный носитель информации.

Машинные носители информации могут сниматься с учета в случае уничтожения (удаления, стирания) в них персональных данных.

Уничтожение (удаление, стирание) информации с машинного носителя информации может быть произведено с использованием специализированных программных, аппаратных или программно-аппаратных средств.

9.3. Порядок хранения носителей персональных данных

Хранение носителей персональных данных организует Ответственный за организацию обработки персональных данных. Соблюдение порядка обращения с носителями персональных данных в структурных подразделениях Оператора, работники которых имеют доступ к персональным данным, организуют их непосредственные руководители.

Для хранения носителей персональных данных используются специальные хранилища (сейфы, металлические шкафы и т.п.), исключающие возможность несанкционированного доступа к ним посторонних лиц, подмены, хищения или уничтожения.

Места хранения носителей персональных данных утверждаются председателем Думы Далматовского муниципального округа Курганской области.

При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки устройств с элементами накопления и хранения персональных данных. Отладочные и экспериментальные работы (опробование программ, формирование массивов информации и др.) проводятся с использованием информации, не содержащей персональных данных, либо при условии их обезличивания.

В случае необходимости передачи машинных носителей информации, на которых могут быть записаны персональные данные, в стороннюю организацию, такая передача может быть осуществлена только при условии гарантированного обезличивания или удаления (стирания) персональных данных.

9.4. Порядок уничтожения носителей персональных данных

Персональные данные на бумажных и машинных носителях подлежат уничтожению в следующих случаях:

- при достижении целей обработки персональных данных, если иное не предусмотрено федеральным законодательством;
- при неправомерной обработке персональных данных;
- если машинные носители пришли в негодность или отслужили установленный срок.

Персональные данные должны быть уничтожены в следующие сроки:

1) при достижении цели обработки – в течение не более десяти дней с даты достижения цели обработки персональных данных;

2) при неправомерной обработке - в течение не более десяти рабочих дней с даты выявления неправомерной обработки персональных данных;

3) в случае отсутствия технической возможности уничтожения персональных данных в течение сроков, указанных в п. 1) и 2), носители должны быть уничтожены в срок не более чем шесть месяцев.

Уничтожение персональных данных, размещенных на машинных носителях информации, может производиться путем физического уничтожения носителя или путем удаления (стирания) персональных данных без повреждения носителя для обеспечения возможности его последующего использования.

Уничтожение машинных носителей информации производится любым способом, исключающим возможность дальнейшего использования элемента носителя информации, содержащего информационные массивы данных (область записи данных). Для уничтожения машинных носителей информации могут применяться следующие способы:

- измельчение носителя любым доступным механическим способом (например, в уничтожителе бумаги при наличии в нем такой функциональной возможности);
- демонтаж корпуса с последующим физическим дроблением (значительной деформацией) магнитных дисков и интегральных микросхем накопителя;
- сжигание носителя.

Уничтожение персональных данных производится комиссией, назначенной распоряжением Думы Далматовского муниципального округа Курганской области, с оформлением Акта об уничтожении персональных данных (форма в приложении 4 к Положению об обработке персональных данных Думы Далматовского муниципального округа Курганской области).

10.Организация резервного копирования и восстановления

10.1. Информационные ресурсы, подлежащие резервному копированию

Для обеспечения непрерывности деятельности и (или) восстановления функционирования информационных систем персональных данных Оператором применяется система резервного копирования и восстановления данных.

Резервному копированию подлежат следующие информационные ресурсы Оператора, содержащие персональные данные субъектов:

- файлы баз данных;
- электронные документы;
- файлы сообщений электронной почты;
- электронные копии документов и фотографии субъектов.

Резервному копированию также подвергаются:

- системное и прикладное программное обеспечение информационной системы;
- программное обеспечение средств защиты информации.

10.2. Резервирование персональных данных

Периодическое резервное копирование информации осуществляется в автоматическом режиме с использованием специализированного программного обеспечения ИСПДн на внешние машинные носители информации.

Создание резервных копий происходит путем копирования и архивирования файлов и папок данных.

Резервные копии хранятся в виде архивных файлов (архивов).

Практическое решение задач, связанных с резервированием персональных данных возлагается на Администратора системы.

Различают два вида резервирования персональных данных: полное и неполное.

При полном резервировании осуществляется резервное копирование всех персональных данных, обрабатываемых в информационной системе.

При неполном резервировании осуществляется сохранение изменений в информационной системе с момента полного резервирования персональных данных.

Периодичность проведения работ по резервированию определяется руководителем с учетом специфики работы информационной системы, но не реже одного раза в месяц – для полного резервирования и одного раза в неделю – для неполного резервирования.

В случаях, когда персональные данные хранятся на рабочих станциях пользователей локально, допускается проводить неполное резервирование персональных данных силами Пользователей.

10.3. Хранение резервных копий персональных данных

Для хранения носителей с резервными копиями персональных данных используются системы хранения данных, исключающие возможность несанкционированного к ним доступа, подмены, хищения или уничтожения. Хранение резервных копий персональных данных должно осуществляться отдельно от других носителей информации.

Хранение машинных носителей информации должно осуществляться в условиях, исключающих воздействие на них теплового, светового (ультрафиолетового) или ионизирующего излучений. Не допускается размещение мест хранения носителей с резервными копиями вблизи источников сильных электромагнитных полей и приборов отопления.

Машинные носители информации с резервными копиями персональных данных не выдаются для работы пользователям и служат исключительно для восстановления данных в случае выхода из строя основного носителя информации.

Для повышения уровня обеспечения непрерывности деятельности Оператора рекомендуется руководствоваться также следующим:

– во избежание любого повреждения минимально необходимые для работы резервные копии должны храниться в территориально удаленном от зданий Оператора месте;

– носители с резервными копиями должны быть гарантированно защищены от несанкционированного доступа и от воздействий окружающей среды;

– должно быть обеспечено одновременное хранение не менее двух носителей информации, хранящих полную резервную копию персональных данных.

В случае удаления персональных данных субъекта из информационной системы, должна быть также удалена резервная копия этих данных из резервных носителей.

10.4. Восстановление персональных данных

В случае аварии или сбоя в работе информационной системы, восстановление персональных данных из резервных копий осуществляют уполномоченные лица.

Администратор информационной системы обязан немедленно уведомить руководителя о факте аварии или сбоя в работе информационной системы, повлекших нарушение целостности персональных данных.

Восстановление информации производится в случае ее частичной или полной утраты путем переноса данных с резервных копий на основные носители в соответствии с эксплуатационной документацией на используемую систему восстановления данных.

По завершении восстановления осуществляется проверка работоспособности и целостности данных.

В случае аварии при применении системы «горячего» резервирования, дальнейшая работа может производится на дублирующем оборудовании. При этом дублирующее оборудование переводится в разряд основного, а восстановленная система выполняет функции «горячего» резерва.

При нарушении целостности (полной утрате) системного и (или) прикладного программного обеспечения его восстановление производится с исходных дистрибутивов.

Для восстановления системы защиты персональных данных предусматривается ведение и контроль работоспособности копий программных компонентов средств защиты информации.

Оборудование резервного копирования, процедуры восстановления должны регулярно подвергаться тестированию.

Периодически следует актуализировать сроки хранения резервных копий и требования к архивным копиям долговременного хранения.

По всем случаям утраты персональных данных проводится анализ причин инцидента с составлением заключения в свободной форме. При этом первичная диагностика выполняется до начала процесса устранения, а по его завершению проводится полная диагностика информационной системы персональных данных

Временной норматив по восстановлению персональных данных устанавливается с учетом специфики работы информационных систем.

11.Управление взаимодействием с информационными системами сторонних организаций

Передача сведений, содержащих персональные данные или информацию конфиденциального характера, сторонней организации может осуществляться только после заключения с этой организацией Соглашения о конфиденциальности или наличия в договоре пункта о гарантировании сторонней организацией безопасности, полученной в связи с исполнением договора конфиденциальной информации или персональных данных.

Электронный обмен конфиденциальной информацией со сторонними организациями должен вестись в зашифрованном виде, при наличии соответствующих технических возможностей со стороны получателя, в противном случае, электронный обмен информацией необходимо осуществлять путем передачи данных внутри архивов, защищенных паролем. При использовании архивов, защищенных паролем, должен выбираться пароль, соответствующий требованиям Парольной политики.

Решение о предоставлении представителям сторонней организации удаленного доступа к информационным системам Оператора должно быть обосновано необходимостью выполнения контрактных обязательств.

Представители сторонней организации перед получением доступа к информационным системам Оператора, должны подписывать Соглашение о конфиденциальности.

Удаленный доступ работников контрагента к информационным системам Оператора должен ограничиваться в зависимости от времени суток и дня недели.

В качестве существенных условий договоров со сторонними организациями должны быть определены их обязанности и ответственность за обеспечение конфиденциальности и безопасности информации (включая персональные данные), предоставляемой этим организациям Оператором.

В договорах на разработку/приобретение/внедрение ИС, заключаемых со сторонними организациями, должны содержаться функциональные требования/спецификации по информационной безопасности, требования к документации и требования по предоставлению гарантий безопасности, предъявляемые к разработке и тестированию ИС со ссылками на утвержденные Профили защиты (при их наличии).

Закупки ИС и их компонентов должны осуществляться только через надежных авторизованных поставщиков, прошедших через соответствующие конкурсные процедуры. Способность данных поставщиков обеспечить надлежащий уровень информационной безопасности и гарантии бесперебойности поставок должна подтверждаться результатами независимого аудита второй или третьей стороны.

Разработчики ИС, а также подрядные организации, осуществляющие внедрение, сопровождение и/или техническую поддержку ИС, должны иметь документированные процедуры управления конфигурацией ИС, включающие в себя: контроль вносимых в систему изменений на этапах проектирования, разработки, внедрения и эксплуатации; выявление и отслеживание уязвимостей в ПО; авторизацию вносимых в систему изменений.

Разработчики и/или подрядные организации, осуществляющие внедрение ИС, должны предоставить средства, посредством которых Оператор может самостоятельно выполнить проверку целостности (дистрибутивов) ПО после его поставки/внедрения.

12.Заключительные положения

Иные права и обязанности работников, допущенных к обработке персональных данных с использованием средств автоматизации, определяются также их должностными инструкциями.

Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут административную, гражданско-правовую или уголовную ответственность в порядке, установленном действующим законодательством.

Приложение 1 к Положению
об организации и проведении работ
по обеспечению безопасности
персональных данных при их обработке в
информационных системах персональных
данных Думы Далматовского
муниципального округа Курганской области

УТВЕРЖДАЮ:
Председатель Думы Далматовского
муниципального округа Курганской области
_____
«___» _____ 20___ г.

АКТ
определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных _____

Основание:
Необходимость определения уровня защищенности информационной системы персональных данных в соответствии с Постановлением от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
Составлен комиссией:
Председатель комиссии –
Члены комиссии:

Комиссия, рассмотрев следующие исходные данные на информационную систему персональных данных:

1) категория обрабатываемых персональных данных - информационная система, обрабатывающая иные категории персональных данных сотрудников оператора;
2) актуальные угрозы - угрозы 3-го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе;
3) объем обрабатываемых персональных данных (Хнпд) менее чем 100000 субъектов персональных данных;

определила установить информационной системе _____ необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе.
Настоящий акт составлен в единственном экземпляре.

Председатель комиссии _____ (личная подпись) _____ (фамилия и инициалы)

Члены комиссии _____ (личная подпись) _____ (фамилия и инициалы)

_____ (личная подпись) _____ (фамилия и инициалы)

Приложение 2 к Положению
об организации и проведении работ
по обеспечению
безопасности персональных данных
при их обработке в информационных
системах персональных данных
Думы Далматовского
муниципального округа Курганской области

УТВЕРЖДАЮ:
Председатель Думы Далматовского
муниципального округа Курганской области
_____
«___» _____ 20___ г.

АКТ
ввода в эксплуатацию средства защиты информации

_____
(наименование)

В соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119, комиссией, назначенной распоряжением председателя Думы Далматовского муниципального округа Курганской области от ДД.ММ.ГГГГ № NN в составе:

Председатель комиссии: _____
(должность назначенного лица, фамилия и инициалы)

Члены комиссии: _____
(должность назначенного лица, фамилия и инициалы)

произведена установка, настройка и проверка готовности

_____
(наименование средства защиты информации)

Информация о настройках средств защиты информации

_____
(наименование документа, по которому проводилась настройка средства защиты информации)

Выполнение требований по сертификации средства защиты информации

_____
(реквизиты сертификата на средство защиты информации/не проводилась)

Комиссией установлено, что средство защиты информации

_____
(наименование средства защиты информации)

готово к использованию в информационной системе персональных данных Думы Далматовского муниципального округа курганской области и может быть введено в эксплуатацию.

Председатель комиссии	_____ (личная подпись)	_____ (фамилия и инициалы)
Члены комиссии	_____ (личная подпись)	_____ (фамилия и инициалы)
	_____ (личная подпись)	_____ (фамилия и инициалы)

Приложение 3 к Положению
об организации и проведении работ
по обеспечению безопасности
персональных данных при их обработке в
информационных системах
персональных данных Думы
Далматовского муниципального округа
Курганской области

ЖУРНАЛ
учета машинных носителей информации

№ п/п	Учетный номер	Дата постановки на учет	Тип (модель) машинного носителя	Серийный (заводской) номер	Отметка о выдаче		Отметка в обратном приеме		Отметка об уничтожении носителя (стирании информации)
					Фамилия и инициалы	Дата, подпись	Фамилия и инициалы	Дата, подпись	
1									
2									
3									

Приложение 4 к Положению
об организации и проведении работ
по обеспечению безопасности
персональных данных при их обработке в
информационных системах
персональных данных Думы
Далматовского муниципального округа
Курганской области

ОБРАЗЦЫ
учета машинных носителей информации

На оптическом носителе информации

На накопителе на жестком магнитном диске

На Flash-диске