Приложение 11

к распоряжению администрации Бобровского муниципального района Воронежской области

от 01.11.2013 г. № 372-р

**Положение**

**по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в администрации Бобровского муниципального района Воронежской области**

1. Назначение документа

1.1. Настоящие Положение определяет порядок организации и проведения работ по обеспечению безопасности персональных данных (далее - ПДн) при их обработке в информационных системах персональных данных (далее - ИСПДн) администрации Бобровского муниципального района Воронежской области (далее - администрация) и содержит общие принципы защиты персональных данных.

Данный документ направлен на достижение следующих целей:

- выполнение требований законодательства в области обеспечения безопасности ПДн;

- защиту прав и свобод граждан РФ при обработке их ПДн в ИСПДн администрации;

- защиту ПДн, обрабатываемых администрацией, от несанкционированного доступа (далее - НСД) и от других несанкционированных действий.

2. Область действия

Требования настоящего Положения распространяются на все подразделения администрации, которые участвуют в обработке ПДн, либо в организации обработки ПДн, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение функционирования ИСПДн.

Настоящий документ обязаны знать и использовать в работе все работники администрации, а также другие лица, допущенные к работе в ИСПДн.

3. Общие положения

Настоящее Положение устанавливает требования по защите ПДн, принципы обработки ПДн в ИСПДн администрации.

Настоящее Положение разработано в соответствии со следующими нормативными актами:

- Федеральным законом Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;

- постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- методическими документами ФСБ России, ФСТЭК России, Роскомнадзора.

Настоящее Положение является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности ПДн;

- принятия управленческих решений и разработки практических мер по воплощению политики безопасности ПДн и выработки комплекса согласованных мер нормативно-правового, технического и организационно-технического характера, направленных на выявление, отражение и уменьшение угроз безопасности персональных данных (далее - УБПДн);

- координации деятельности при проведении работ по созданию, развитию и эксплуатации ИСПДн с соблюдением требований по обеспечению безопасности ПДн;

- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в ИСПДн.

Принципы и требования по обеспечению безопасности ПДн распространяются:

- на все возможные формы существования информации, такие как: физические поля (электрические, акустические, электромагнитные, оптические и т.п.); носители на бумажной, магнитной, оптической и иной основе;

- на все возможные форматы представления ПДн, такие как: документы; голос; изображения; файлы; почтовые сообщения; базы данных; записи базы данных; другие информационные массивы.

Предотвращение несанкционированного и нелегитимного доступа к ИСПДн, технологиям и информационным ресурсам, результатом которого может стать уничтожение, модификация, искажение, копирование, распространение, блокирование ПДн требует применения комплекса правовых, организационных, организационно-технических мер защиты с использованием сертифицированных средств защиты информации (далее - СЗИ).

Настоящее Положение определяет:

- роли, полномочия, ответственность за обеспечение безопасности ПДн, подразделений администрации;

- порядок организации и проведения работ по обеспечению безопасности ПДн при их обработке в ИСПДн;

- мероприятия по обеспечению безопасности ПДн;

- требования по управлению процессом обеспечения безопасности ПДн;

- требования к составу и содержанию документов администрации, регламентирующих защиту и работу с ПДн.

Целью создания систем (подсистем) защиты персональных данных (далее - СЗПДн) является исключение неправомерного или случайного доступа к ПДн, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий.

В общем случае можно выделить следующие основные цели защиты ПДн, это обеспечение:

- конфиденциальности ПДн;

- целостности ПДн;

- доступности ПДн;

- неотказуемости.

Конкретный состав целей защиты ПДн зависит от конкретной ИСПДн и определяется по результатам разработки модели угроз безопасности ПДн.

К основным задачам в области обеспечения безопасности ПДн относится:

- определение новых ИСПДн;

- инвентаризация и управление изменениями в составе и структуре ИСПДн;

- сбор согласий на обработку ПДн с субъектов ПДн;

- разработка и актуализация перечня сведений конфиденциального характера;

- уничтожение ПДн;

- управление взаимодействиями с внешними контрагентами по вопросам обработки ПДн;

- взаимодействие с субъектами ПДн по вопросам обработки их ПДн;

- классификация ИСПДн;

- разработка (актуализация) документации на СЗПДн;

- выбор и внедрение необходимых и достаточных мер и средств защиты ПДн;

- эксплуатация СЗПДн в соответствии с документацией на нее;

- контроль уровня защищенности ПДн;

- обучение персонала по вопросам защиты ПДн;

- учет применяемых СЗИ, эксплуатационной и технической документации к ним, носителей ПДн;

- учет лиц, допущенных к обработке ПДн;

- взаимодействие с регуляторными органами по вопросам защиты ПДн;

- актуализация и подача уведомлений в уполномоченный орган по защите прав субъектов ПДн.

Обработка ПДн должна осуществляться в соответствии со следующими принципами:

- законности целей и способов обработки ПДн и добросовестности;

- соответствия целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям администрации;

- соответствия объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;

- достоверности ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;

- недопустимости объединения созданных для несовместимых между собой целей баз данных ИСПДн.

Администрация должна проводить регулярный анализ соответствия процессов обработки ПДн указанным принципам. Данный анализ проводится в случае:

- создания новых ИСПДн;

- внесения изменений в технологические процессы, существующие в ИСПДн;

- изменения нормативной базы затрагивающей принципы и (или) процессы обработки ПДн в ИСПДн администрации;

- проведения контрольных и проверочных мероприятий на предмет оценки соответствия процессов обработки ПДн заявленным принципам.

Отнесение сведений администрацией к ПДн, безопасность которых должна обеспечиваться СЗПДн, представляет собой процесс обоснованного установления (документального оформления и утверждения) критериев их выделения из всей совокупности сведений, находящихся в обращении.

В качестве такого критерия в администрации разрабатывается и утверждается Перечень обрабатываемых персональных данных.

4. Организационная структура системы защиты персональных данных

СЗПДн является частью общей системы обеспечения информационной безопасности администрации.

Основу организационной структуры СЗПДн составляют следующие организационные структуры:

- ответственный за организацию обработки ПДн;

- ответственный за обеспечение безопасности ПДн - администратор безопасности ИСПДн;

- структурные подразделения и работники администрации, участвующие в процессах обработки ПДн.

Должностные обязанности и функции ответственного за организацию обработки ПДн и ответственного за обеспечение безопасности ПДн - администратора безопасности ИСПДн определяются соответствующими инструкциями, утверждаемыми правовыми актами администрации.

Структурные подразделения и работники администрации, участвующие в процессах обработки ПДн, выполняют следующие основные функции:

- осуществляют взаимодействие с субъектами ПДн по вопросам обработки их ПДн;

- осуществляют уведомление субъектов ПДн в случаях определенных нормативными актами;

- эксплуатируют СЗПДн в соответствии с документацией на нее;

- соблюдают требования нормативных документов по защите ПДн;

- осуществляют обработку ПДн в соответствии с заданием и предоставленными полномочиями.

Распределение ролей и полномочий осуществляется в соответствии с утверждаемой ответственным за организацию обработки персональных данных Разрешительной системой доступа к информационным ресурсам, программным и техническим средствам информационных систем персональных данных.

5. Порядок организации и проведения работ по обеспечению безопасности персональных данных

Работы по обеспечению безопасности ПДн при их обработке в ИСПДн являются неотъемлемой частью работ выполняемых в рамках жизненного цикла ИСПДн, на следующих этапах:

- инициация проекта ИСПДн;

- планирование проекта ИСПДн;

- реализация проекта ИСПДн, в составе: выбор технического решения - концепция реализации; проектирование ИСПДн; производство ИСПДн; приемка ИСПДн; внедрение ИСПДн; передача системы в эксплуатацию; документирование проекта;

- эксплуатация ИСПДн;

- модернизация ИСПДн;

- вывод из эксплуатации.

6. Допуск персонала к обработке персональных данных

При допуске к ПДн администрация руководствуется утвержденным списком лиц, допущенных к обработке ПДн.

Перечень лиц, допущенных к обработке ПДн, составляется и корректируется ответственным за обеспечение безопасности ПДн - администратором безопасности ИСПДн, на основании данных, подаваемых руководителями и начальниками структурных подразделений администрации.

7. Контроль изменений в составе и структуре информационных систем персональных данных

Все изменения в составе и структуре ИСПДн должны контролироваться и регламентироваться ответственным за обеспечение безопасности ПДн - администратором безопасности ИСПДн.

Контролю подлежат следующие изменения:

- внесение новых устройств в состав ИСПДн (АРМ, серверов, сетевого и телекоммуникационного оборудования и т.п.);

- изменение мест включения существующих компонент ИСПДн;

- удаление устройства из состава ИСПДн;

- прокладка новых кабельных линий связи и внешних линий связи или удаление старых кабельных линий связи;

- изменение мест установки устройства из состава ИСПДн;

- существенное изменение состава и конфигурации системного и прикладного программного обеспечения, участвующего в обработке ПДн;

- создание новых и изменение существующих технологических процессов связанных с обработкой ПДн.

Каждое изменение состава ИСПДн, типов технических средств, топологии ИСПДн должно отслеживаться и анализироваться на предмет соответствия требованиям по защите ИСПДн. При необходимости должна производиться модернизация СЗПДн.

8. Защита от несанкционированного физического доступа к элементам информационных систем персональных данных

Мероприятия по физическому контролю доступа включают:

- мероприятия по контролю доступа на территорию;

- мероприятия по контролю доступа в помещения с оборудованием ИСПДн;

- мероприятия по контролю доступа к техническим средствам ИСПДн;

- мероприятия по контролю перемещений физических компонентов ИСПДн.

Мероприятия по контролю доступа на территорию должны обеспечить контролируемое нахождение посетителей на территории администрации.

Двери телекоммуникационных шкафов с серверным и сетевым оборудованием ИСПДн должны быть постоянно закрыты на замок и открываться только для санкционированного доступа.

Двери помещений, в которых размещаются АРМ пользователей ИСПДн, должны быть оборудованы замками, либо в этих помещениях должны обеспечиваться мероприятия по контролю действий находящихся в них посторонних лиц.

Нахождение в помещении лиц, не участвующих в технологических процессах обработки ПДн (обслуживающий персонал, другие работники), должно производиться только в присутствии работников, участвующих в соответствующих технологических процессах.

Расположение мониторов рабочих станций должно препятствовать их несанкционированному просмотру со стороны других лиц, не допущенных к обработке ПДн.

При выносе устройств, хранящих ПДн, за пределы контролируемой зоны (далее - КЗ) для ремонта, замены и т.п. должно быть обеспечено гарантированное уничтожение информации хранимой на этих устройствах.

9. Резервирование персональных данных

Резервирование ПДн должно обеспечить возможность восстановления информации при нарушении целостности основных хранилищ данных.

Резервированию должна подвергаться информация на серверах ИСПДн.

Резервирование должно осуществляться на различные носители информации с соответствующим уровнем надежности и долговечности.

Хранение резервных копий должно осуществляться в надежных сейфах (металлических шкафах). Хранение (по возможности) должно осуществляться в месте, территориально удаленном от основного хранилища информации.

Доступ к резервным копиям должен быть строго регламентирован.

10. Контроль за обеспечением необходимого уровня защищенности

персональных данных

Для эффективности обеспечения безопасности ПДн проводится:

- контроль за соблюдением требований по обработке и защите персональных данных;

- контроль за соблюдением условий использования средств защиты ПДн, предусмотренных эксплуатационной и технической документацией;

- контроль эффективности средств защиты ПДн.

Контрольные мероприятия могут быть:

- текущими;

- внезапными;

- плановыми внешними;

- плановыми внутренними.

Ответственность за текущий и плановый контроль эффективности обеспечения безопасности ПДн возлагается на ответственного за обеспечение безопасности ПДн - администратора безопасности ИСПДн.

Внезапные проверки эффективности при необходимости могут проводиться специальными группами по решению ответственного за обеспечение безопасности ПДн - администратора безопасности ИСПДн.

При проведении контроля эффективности в общем случае должно проверяться:

- наличие установленных СЗИ;

- корректность настроек СЗИ;

- выполнение пользователями и администраторами требований инструктивных материалов по защите ПДн;

- исполнение требований к процедурам обработки ПДн (уничтожению ПДн, сбору согласий, допуску персонала к ПДн и т.п.);

- правильность организации работы с носителями ПДн;

- правильность обращения ключевой информации;

- соответствие СЗПДн реальному положению дел в администрации.

11. Реагирование на нештатные ситуации

Администрация должна проводить расследования инцидентов, связанных с несанкционированным доступом и другими несанкционированными действиями затрагивающими безопасность ПДн.

В рамках данного процесса должны решаться следующие задачи:

- расследование инцидентов, связанных с безопасностью ПДн;

- ликвидация последствий инцидентов связанных с безопасностью ПДн;

- принятие мер по недопущению возникновения подобных инцидентов в дальнейшем.