|  |
| --- |
| Приложение 6  к распоряжению Администрации Заринского района  от \_\_\_\_\_\_\_\_\_\_ №\_\_\_\_\_\_\_\_ |

ПОРЯДОК

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Администрация района

1. Общие положения
   1. Настоящий Порядок осуществления внутреннего контроля соответствия обработки персональных данных (далее - ПДн) требованиям к защите ПДн в Администрации Заринского района Алтайского края (далее – Администрация района) разработан с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
   2. Настоящий Порядок определяет правила осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн и действует постоянно.
2. Тематика внутреннего контроля
   1. Тематика проверок обработки ПДн с использованием средств автоматизации:

* соответствие полномочий пользователей Матрице доступа;
* соблюдение пользователями информационных систем персональных данных (далее - ИСПДн) Администрации района парольной политики;
* соблюдение пользователями ИСПДн Администрации района антивирусной политики;
* соблюдение пользователями ИСПДн Администрации района правил работы со съемными носителями ПДн;
* соблюдение пользователями криптографических средств защиты информации правил работы с ними;
* соблюдение порядка доступа в помещения Администрации района, где расположены элементы ИСПДн;
* соблюдение порядка резервирования баз данных и хранения резервных копий;
* соблюдение порядка работы со средствами защиты информации;
* знание пользователей ИСПДн о своих действиях во внештатных ситуациях.
  1. Тематика проверок обработки ПДн без использования средств автоматизации:
* соблюдение правил хранения бумажных носителей с ПДн;
* соблюдение правил доступа к бумажным носителям ПДн;
* соблюдение правил доступа в помещения, где обрабатываются и хранятся бумажные носители с ПДн.

1. Правила проведения внутренних проверок
   1. В целях осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям Администрация района организует проведение периодических проверок условий обработки ПДн, но не реже 1 раза в 3 года (постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»).
   2. Проверки осуществляются ответственным за организацию обработки ПДн (далее – Ответственный) либо комиссией, образуемой главой района.
   3. Внутренние проверки проводятся в соответствии с «Планом проведения внутренних проверок соответствия условий обработки ПДн требованиям по защите ПДн».
   4. Проверки осуществляются непосредственно на месте обработки ПДн путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки ПДн.
   5. Для каждой проверки составляется «Протокол проведения внутренней проверки соответствия условий обработки ПДн требованиям по защите ПДн» (далее – Протокол).
   6. При выявлении в ходе проверки нарушений, Ответственным либо Председателем комиссии в Протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.
   7. Протоколы хранятся у Ответственного либо Председателя комиссии в течение года с момента проведения проверки.
   8. О результатах проверки и мерах, необходимых для устранения нарушений, главе района докладывает Ответственный либо Председатель комиссии.