|  |  |
| --- | --- |
|  | Приложение 14  к приказу руководителя *Организации*  от №\_\_\_\_ |

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

* 1. Настоящие Правила разработаны в соответствии с законодательством Российской Федерации и определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.
  2. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в информационных системах персональных данных *Организации* (далее – ИСПДн) организовывается проведение периодических проверок условий обработки персональных данных.
  3. Проверки осуществляются лицом, ответственным за организацию обработки персональных данных в *Организации*, либо комиссией, образуемой приказом руководителя *Организации*. В проведении проверки не может участвовать сотрудник, прямо или косвенно заинтересованный в её результатах.
  4. Проверки проводятся на основании утвержденного ежегодного плана внутренних проверок условий обработки персональных данных или на основании поступившего письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.
  5. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

1. порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
2. порядок и условия применения средств защиты информации;
3. эффективность принимаемых мер по обеспечению безопасности персональных данных;
4. состояние учета и хранения машинных носителей персональных данных;
5. соблюдение правил доступа к персональным данным;
6. соблюдение порядка доступа в помещения, где обрабатываются и хранятся бумажные носители с персональными данными;
7. наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
8. мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
9. осуществление мероприятий по обеспечению целостности персональных данных.
   1. Внутренние проверки осуществляются непосредственно на месте обработки персональных данных путем опроса, либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.
   2. При проведении проверки ответственный за организацию обработки персональных данных в *Организации* или назначенная комиссия имеет право:
10. запрашивать у сотрудников информацию, необходимую для проведения проверки;
11. требовать от сотрудников, допущенных к обработке персональных данных в ИСПДн уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем персональных данных;
12. принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;
13. вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
14. вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.
    1. По результатам каждой проверки составляется Протокол проведения внутренней проверки (приложение к Правилам).
    2. При выявлении в ходе проверки нарушений в протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.
    3. Протоколы хранятся у ответственного за организацию обработки персональных данных в *Организации* области в течение текущего года. Уничтожение протоколов проводится в первом квартале года, следующего за отчетным.
    4. О результатах проверки и мерах, необходимых для устранения нарушений, руководителю *Организации* докладывает председатель назначенной комиссии или ответственный за организацию обработки персональных данных в *Организации*.

|  |  |
| --- | --- |
|  | Приложение  к правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных |

Протокол

проведения внутренней проверки условий обработки персональных данных в

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Настоящий Протокол составлен в том, что «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_20\_\_ г. комиссией по внутреннему контролю проведена проверка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(тема проверки)

Проверка осуществлялась в соответствии с требованиями \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(название документа)

В ходе проверки проверено:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Выявленные нарушения:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Меры по устранению нарушений:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Срок устранения нарушений: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Председатель комиссии:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Ф.И.О.) (подпись)

Члены комиссии:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Ф.И.О.) (подпись)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Ф.И.О.) (подпись)

«\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.