Приложение № 4

Утверждено

постановлением Администрации

Ельцовского района

от 07.10.2024 № 220

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в информационных системах персональных данных

Цель внутреннего контроля.

1. Внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных осуществляется с целью проверки соответствия обработки персональных данных требованиям к защите персональных данных, установленных Федеральным законом №152-ФЗ «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами Администрации Ельцовского района Алтайского края.

Виды и периодичность внутреннего контроля.

1. Внутренний контроль соответствия обработки персональных данных делится на текущий и периодический.
2. Текущий внутренний контроль осуществляется на постоянной основе Ответственным за обеспечение безопасности персональных данных.
3. Периодический внутренний контроль осуществляется комиссией в соответствии с поручением главы Ельцовского района.

Периодичность проверки - не реже одного раза в шесть месяцев.

Порядок создания комиссии для осуществления внутреннего контроля.

* 1. Проверки осуществляются комиссией, созданной распоряжением Главы Ельцовского района, из числа сотрудников Администрации Ельцовского района, допущенных к обработке персональных данных. В проведении проверки не может участвовать лицо, прямо или косвенно заинтересованное в её результатах.
  2. Проверки осуществляются непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.

Порядок проведения внутренней проверки.

* + 1. При проведении внутренней проверки комиссией должны быть полностью, объективно и всесторонне установлены:
* порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке;
* порядок и условия применения средств защиты информации;
* эффективность принимаемых мер по обеспечению безопасности персональных данных;
* состояние учёта бумажных и машинных носителей персональных данных;
* соблюдение правил доступа к персональным данным;
* наличие (отсутствие) фактов несанкционированного доступа к персональным данным;
* мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
* осуществление мероприятий по обеспечению целостности персональных данных.
  1. Осуществлении внутреннего контроля мероприятий проводятся комиссией периодически в соответствии с Перечнем мероприятий для осуществления внутреннего контроля за выполнением требований к защите персональных данных при их обработке в информационных системах персональных данных. Форма Перечня мероприятий для осуществления внутреннего контроля за выполнением требований к защите персональных данных при их обработке в информационных системах персональных данных приведена в Приложении 1 к настоящим Правилам.

Для каждой проверки составляется Протокол проведения внутренней проверки. Форма Протокола приведена в Приложении 2 к настоящим Правилам.

1. При выявлении в ходе проверки нарушений в Протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.
2. Протоколы хранятся у председателя комиссии в течение текущего года. Уничтожение Протоколов проводится комиссией самостоятельно по истечении срока хранения.
3. О результатах проверки и мерах, необходимых для устранения нарушений председатель комиссии докладывает Главе.
4. Срок проведения проверки не может составлять более 30 (тридцати) дней со дня принятия решения о её проведении.

Приложение 1

к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в информационных системах персональных данных

Перечень

мероприятий для осуществления внутреннего контроля за выполнением требований к защите персональных данных при их обработке в информационных системах персональных данных

|  |  |
| --- | --- |
| № п/п | Краткое описание мероприятий |
| 1 | Проверка режима допуска в помещения, где размещены средства ИСПДн и осуществляется обработка персональных данных |
| 2 | Проверка наличия и соответствия средств защиты информации в соответствии с указанными в техническом паспорте на ИСПДн |
| 3 | Проверка правильности применения средств защиты информации |
| 4 | Проверка неизменности настроенных параметров антивирусной защиты на рабочих станциях пользователей |
| 5 | Контроль за обновлениями программного обеспечения и единообразия применяемого программного обеспечения на всех элементах ИСПДн |
| 6 | Проверка соблюдения правил парольной защиты |
| 7 | Проверка работоспособности системы резервного копирования |
| 8 | Проведение мероприятий по проверке организации учета и условий хранения съемных носителей персональных данных |
| 9 | Проверка соблюдения требований по обеспечению безопасности при использовании ресурсов сети "Интернет" |
| 10 | Проверка знаний работниками руководящих документов, технологических 14 инструкций, предписаний, актов, заключений и уровня овладения работниками технологией безопасной обработки информации, изложенных в инструкциях |
| 11 | Проверка знаний инструкций по обеспечению безопасности информации пользователями ИСПДн |
| 12 | Проверка наличия документов, подтверждающих возможность применения технических и программных средств вычислительной техники для обработки персональных данных и применения средств защиты (сертификатов соответствия и других документов) |

Приложение 2

к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в информационных системах персональных данных

Протокол № \_

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

в \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Настоящий протокол составлен в том, что «\_\_»\_\_\_\_\_\_\_202\_ г.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (комиссией)

*(должность, Ф.И.О. сотрудника)*

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:

*фамилия и инициалы / подпись / должность*

Члены комиссии:

*фамилия и инициалы / подпись / должность*

*фамилия и инициалы / подпись / должность*