РОССИЙСКАЯ ФЕДЕРАЦИЯ

ОРЛОВСКАЯ ОБЛАСТЬ

**НОВОСИЛЬСКИЙ РАЙОН**

**АДМИНИСТРАЦИЯ ПЕТУШЕНСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ**

ПОСТАНОВЛЕНИЕ

29 ноября 2019 г. № 26

 д. Михалево

**Об утверждении Правил** **осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Петушенского сельского поселения Новосильского района Орловской области**

В целях исполнения требований Постановление Правительства РФ от 21 марта 2012 г. № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», в целях обеспечения безопасности персональных данных при их обработке в администрации сельского поселения, администрация Петушенского сельского поселения **ПОСТАНОВЛЯЕТ:**

1. Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Петушенского сельского поселения Новосильского района Орловской области - согласно приложению.

2. Настоящее постановление вступает в силу с момента его подписания и подлежит размещению на информационном стенде администрации Петушенского сельского поселения.

3. Контроль за исполнением настоящего постановления оставляю за собой.

Глава Петушенского сельского поселения Е.И. Мурлыкина

Приложение

к постановлению администрации

Петушенского сельского поселения

 от 29.11.2019 г. № 26

**ПРАВИЛА**

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

**в администрации Петушенского сельского поселения**

**Новосильского района Орловской области**

**1. Общие положения**

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее  – Правила) в администрации Петушенского сельского поселения Новосильского района Орловской области (далее – Администрация), определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее – ПДн); основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки ПДн, необходимой для предоставления государственных и муниципальных услуг, требованиям к защите ПДн.

1.2. Настоящие Правила разработаны на основании Федерального закона РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федерального закона РФ от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» и в соответствии с частью 1 «Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», утвержденных постановлением Правительства РФ от 21 марта 2012 г. № 211.

1.3. Контрольные мероприятия за обеспечением уровня защищенности персональных данных и соблюдений условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в ИСПДн в администрации Петушенского сельского поселения Новосильского района Орловской области проводятся в следующих целях:

1.1.1. проверка выполнения требований организационно-распорядительной документации по защите информации в администрации Петушенского сельского поселения Новосильского района Орловской области и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

1.1.2. оценка уровня осведомленности и знаний работников администрации Петушенского сельского поселения Новосильского района Орловской области в области обработки и защиты персональных данных;

1.1.3. оценка обоснованности и эффективности применяемых мер и средств защиты.

**2. Тематика внутреннего контроля**

Тематика внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн:

2.1. Проверки соответствия обработки ПДн установленным требованиям в администрации Петушенского сельского поселения Новосильского района Орловской области разделяются на следующие виды:

* + регулярные;
	+ плановые;
	+ внеплановые.

2.2. Регулярные контрольные мероприятия проводятся Администратором АИС периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План, приложение 1) и предназначены для осуществления контроля выполнения требований в области защиты информации в администрации Петушенского сельского поселения Новосильского района Орловской области.

2.3. Плановые контрольные мероприятия проводятся постоянной комиссией периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План, приложение 1) и направлены на постоянное совершенствование системы защиты персональных данных ИСПДн в администрации Петушенского сельского поселения Новосильского района Орловской области.

2.4. Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности (создается на период проведения мероприятий). Решение о проведении внеплановых контрольных мероприятий и созданию комиссии по информационной безопасности может быть принято в следующих случаях:

2.1.1. по результатам расследования инцидента информационной безопасности;

2.1.2. по результатам внешних контрольных мероприятий, проводимых регулирующими органами;

2.1.3. по распоряжению главы администрации Петушенского сельского поселения Новосильского района Орловской области.

**3. Планирование контрольных мероприятий**

3.1. Для проведения плановых внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности персональных данных, разрабатывает План внутренних контрольных мероприятий на текущий год.

3.2. План проведения внутренних контрольных мероприятий включает следующие сведения по каждому из мероприятий:

3.1.1. цели проведения контрольных мероприятий;

3.1.2. задачи проведения контрольных мероприятий,

3.1.3. объекты контроля (процессы, подразделения, информационные системы и т.п.);

3.1.4. состав участников, привлекаемых для проведения контрольных мероприятий;

3.1.5. сроки и этапы проведения контрольных мероприятий.

3.3. Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Отчете, выполняемом по результатам проведенных контрольных мероприятий.

**4. Оформление результатов контрольных мероприятий**

4.1. По итогам проведения регулярных контрольных мероприятий результаты проверок фиксируется в Журнале учета событий информационной безопасности.

4.2. По итогам проведения плановых и внеплановых контрольных мероприятий лицо, комиссия, разрабатывает отчет, в котором указывается:

4.1.1. описание проведенных мероприятий по каждому из этапов;

4.1.2. перечень и описание выявленных нарушений;

4.1.3. рекомендации по устранению выявленных нарушений;

4.1.4. заключение по итогам проведения внутреннего контрольного мероприятия.

4.1.5. отчет передается на рассмотрение главе администрации Петушенского сельского поселения Новосильского района Орловской области.

4.3. Общая информации о проведенном контрольном мероприятии фиксируется в Журнале учета событий информационной безопасности.

4.4. Результаты проведения мероприятий по внеплановому контролю заносятся в протокол проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Петушенского сельского поселения Новосильского района Орловской области (приложение 2).

**5. Порядок проведения плановых и**

**внеплановых контрольных мероприятий**

5.1. Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственном за обеспечение безопасности ПДн, также по его ходатайству к проведению контрольных мероприятий могут привлекаться администраторы АИС, и ответственный за обеспечение безопасности персональных данных информационных систем персональных данных администрации Петушенского сельского поселения Новосильского района Орловской области.

5.2. Лицо, ответственное за обеспечение безопасности ПДн, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет руководителя. При проведении внеплановых контрольных мероприятий уведомление не требуется.

5.3. Во время проведения контрольных мероприятий, в зависимости от целей мероприятий, могут выполнятся следующие проверки:

- Соответствие полномочий Пользователя правилам доступа.

- Соблюдение Пользователями требований инструкций по организации антивирусной и парольной политики, инструкции по обеспечению безопасности ПДн.

- Соблюдение Администраторами инструкций по обеспечению безопасности информации в администрации Петушенского сельского поселения Новосильского района Орловской области.

- Соблюдение Порядка доступа в помещения администрации Петушенского сельского поселения Новосильского района Орловской области, где ведется обработка персональных данных.

- Знание Пользователей положений Инструкции пользователя по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций.

- Знание Администраторами инструкций по обеспечению безопасности информации в администрации Петушенского сельского поселения Новосильского района Орловской области.

- Порядок и условия применения средств защиты информации.

- Состояние учета машинных носителей персональных данных.

- Наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер.

- Проведенные мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

- Технические мероприятия, связанные со штатным и нештатным функционированием средств защиты.

- Технические мероприятия, связанные со штатным и нештатным функционированием подсистем системы защиты информации.

|  |  |
| --- | --- |
|  | Приложение 1к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных |

**ПЛАН**

внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных

|  |  |  |  |
| --- | --- | --- | --- |
| **Мероприятие** | **Периодичность регулярных мероприятий** | **Периодичность плановых мероприятий** | **Исполнитель** |
| Контроль соблюдения правил доступа к ПДн | Раз в полгода | Раз в полгода | ведущий специалист администрации Петушенского сельского поселения Новосильского района Орловской области |
| Контроль соблюдения режима защиты | Раз в полгода | Раз в полгода | ведущий специалист администрации Петушенского сельского поселения Новосильского района Орловской области |
| Контроль выполнения антивирусной политики | Раз в полгода | Раз в полгода | ведущий специалист администрации Петушенского сельского поселения Новосильского района Орловской области |
| Контроль выполнения парольной политики | Раз в полгода | Раз в полгода | ведущий специалист администрации Петушенского сельского поселения Новосильского района Орловской области |
| Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена | Раз в полгода | Раз в полгода | ведущий специалист администрации Петушенского сельского поселения Новосильского района Орловской области |
| Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн | Раз в полгода | Раз в полгода | ведущий специалист администрации Петушенского сельского поселения Новосильского района Орловской области |
| Контроль обновления ПО и единообразия применяемого ПО на всех элементах АИС администрации Петушенского сельского поселения Новосильского района Орловской области | Раз в полгода | Раз в полгода | ведущий специалист администрации Петушенского сельского поселения Новосильского района Орловской области |
| Контроль обеспечения резервного копирования | Раз в полгода | Раз в полгода | ведущий специалист администрации Петушенского сельского поселения Новосильского района Орловской области |
| Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз | Раз в полгода | Раз в полгода | ведущий специалист администрации Петушенского сельского поселения Новосильского района Орловской области |
| Поддержание в актуальном состоянии нормативно-организационных документов | Раз в полгода | Раз в полгода | ведущий специалист администрации Петушенского сельского поселения Новосильского района Орловской области |
| Контроль запрета на использование беспроводных соединений | Раз в полгода | Раз в полгода | ведущий специалист администрации Петушенского сельского поселения Новосильского района Орловской области |

|  |  |
| --- | --- |
|  | Приложение 2к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных |

**ПРОТОКОЛ № \_\_\_\_**

проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Петушенского сельского поселения

Новосильского района Орловской области

Настоящий Протокол составлен в том, что «\_\_»\_\_\_\_\_\_\_201\_ 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*