РОССИЙСКАЯ ФЕДЕРАЦИЯ

ЛИПЕЦКАЯ ОБЛАСТЬ

ЛИПЕЦКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН

Администрация сельского поселения Боринский сельсовет

РАСПОРЯЖЕНИЕ

16.02.2021г                                                                                                                                                                                                                         № 10

**Об утверждении Правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Администрации сельского поселения Боринский сельсовет Липецкого муниципального района Липецкой области Российской Федерации**

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 Боринский сельсовет Липецкого муниципального района Липецкой области, администрация сельского поселения Боринский сельсовет Липецкого муниципального района Липецкой области

ПОСТАНОВЛЯЕТ:

1. Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Администрации сельского поселения Боринский сельсовет Липецкого муниципального района Липецкой области (приложение 1).

2. Утвердить План внутренних проверок режима защиты персональных данных в Администрации сельского поселения Боринский сельсовет Липецкого муниципального района Липецкой области (приложение 2).

3. Настоящее постановление вступает в силу со дня его подписания, обнародования и размещения на официальном сайте администрации сельского поселения Боринский сельсовет.

Глава сельского поселения Боринский сельсовет

Е.В.Воропаева

Приложение к Распоряжению администрации сельского поселения Боринский сельсовет от 16.02.2021 года № 10

**Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Администрации сельского поселения Боринский сельсовет Липецкого муниципального района Липецкой области**

**1. Общие положения**

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации сельского поселения Боринский сельсовет Липецкого муниципального района Липецкой области (далее - Правила) определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным действующим законодательством, в том числе Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", принятыми в соответствии с ним нормативными правовыми актами администрации сельского поселения Боринский сельсовет Липецкого муниципального района Липецкой области

1.2. Правила разработаны с учетом требований Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", постановления Правительства Российской Федерации от 21.03.2011 N 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", иных нормативных правовых актов.

**2. Порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям законодательства**

2.1. Цель проведения внутреннего контроля состоит в проверке и оценке соответствия обеспечения безопасности персональных данных (далее - ПДн) требованиям действующего законодательства, в том числе Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", политики администрации сельского поселения Боринский сельсовет Липецкого муниципального района Липецкой области в отношении обработки ПДн, правовых актов администрации сельского поселения Боринский сельсовет Липецкого муниципального района Липецкой области, регулирующих работу с ПДн в структурных подразделениях администрации сельского поселения Боринский сельсовет Липецкого муниципального района Липецкой области

2.2. При проведении контроля используются процедуры документальной проверки, опрос и интервью с муниципальными служащими, работниками, замещающими должности, не являющиеся должностями муниципальной службы, на основании трудового договора (далее - служащие) администрации сельского поселения Боринский сельсовет Липецкого муниципального района Липецкой области. При необходимости уточнения результатов документальной проверки, опросов и интервью в рамках внутреннего контроля в качестве дополнительного способа может применяться "проверка на месте", которая проводится для обеспечения уверенности в том, что конкретные защитные меры реализуются, правильно используются и проверяются с помощью тестирования.

2.3. При проведении внутреннего контроля должно быть обеспечено документальное и, если это необходимо, техническое подтверждение того, что:

- политика в отношении обработки ПДн соответствует требованиям законодательства Российской Федерации;

- организационная структура обеспечения безопасности ПДн создана;

- процессы выполнения требований безопасности ПДн исполняются и удовлетворяют поставленным целям;

- защитные меры (межсетевые экраны, средства защиты информации от несанкционированного доступа и т.п.) настроены и используются правильно;

- остаточные риски безопасности ПДн оценены и остаются приемлемыми;

- рекомендации предшествующих проверок реализованы.

2.4. При проведении внутреннего контроля могут использоваться журналы средств защиты информации для выявления попыток несанкционированного доступа к защищаемым ресурсам, а также журнал учета нештатных ситуаций информационных систем персональных данных (далее - ИСПДн), ведущийся администратором безопасности.

2.5. Ответственный за организацию обработки ПДн для проведения контроля имеет право привлекать администратора безопасности ИСПДн и других служащих.

Приложение к Распоряжению администрации сельского поселения Боринский сельсовет от 16.02.2021 года № 10

**План внутренних проверок режима защиты персональных данных в Администрации сельского поселения Боринский сельсовет Липецкого муниципального района Липецкой области**

**1. Общие положения**

1.1. План внутренних проверок режима защиты персональных данных в администрации сельского поселения Боринский сельсовет Липецкого муниципального района Липецкой области (далее - План) содержит перечень мероприятий (внутренних проверок) по проверке режима защиты персональных данных в администрации сельского поселения Боринский сельсовет Липецкого муниципального района Липецкой области.

1.2. План содержит следующую информацию:

- название проводимого мероприятия;

- периодичность проведения;

- исполнитель мероприятия.

1.3. План распространяется на все структурные подразделения администрации сельского поселения Боринский сельсовет Липецкого муниципального района Липецкой области, в которых осуществляется обработка персональных данных либо имеется доступ к персональным данным.

Руководители структурных подразделений администрации сельского поселения Боринский сельсовет Липецкого муниципального района Липецкой области доводят до сведения муниципальных служащих и (или) работников, замещающих должности, не являющиеся должностями муниципальной службы, на основании трудового договора, назначенных ответственными за организацию обработки персональных данных в соответствующем структурном подразделении администрации сельского поселения Боринский сельсовет Липецкого муниципального района Липецкой области, настоящий План под роспись.

**2. Мероприятия по проверке режима защиты персональных данных**

2.1. Мероприятия по проверке режима защиты персональных данных имеют следующую периодичность:

- ежедневные мероприятия - мероприятия, предусматривающие постоянный контроль за выполнением требований действующего законодательства ответственным за организацию обработки персональных данных в соответствующем структурном подразделении администрации сельского поселения Боринский сельсовет Липецкого муниципального района Липецкой области (далее - ответственный исполнитель) и незамедлительное реагирование на инциденты информационной безопасности;

- еженедельные и ежемесячные мероприятия - мероприятия, предусматривающие проведение мероприятий ответственными исполнителями в один и тот же день недели или месяца. Факт проведения мероприятия должен быть зафиксирован в журнале, указанном в разделе 3 настоящего Плана;

- ежегодные или проводимые раз в несколько лет - мероприятия, предусматривающие проведение мероприятий в четко определенные ответственными исполнителями периоды времени. В ходе мероприятий должны быть учтены результаты проводимых ранее мероприятий по проверке режима защиты персональных данных в данном периоде.

**3. Журнал учета мероприятий по контролю обеспечения защиты персональных данных**

3.1. Информация о периодически проводимых мероприятиях и их результатах фиксируется в журнале учета мероприятий по контролю за соблюдением режима защиты персональных данных (далее - Журнал). Форма Журнала представлена в Приложении N 1 к настоящему Плану.

В Журнале отмечаются мероприятия в соответствии с Планом, носящие периодический характер.

В Журнал заносится следующая информация:

- название проведенного мероприятия;

- дата проведенного мероприятия;

- исполнитель мероприятия;

- результат (отчет, действия) мероприятия (при необходимости).

4. План внутренних проверок режима защиты персональных данных

|  |  |  |  |
| --- | --- | --- | --- |
| N п/п | Мероприятие | Периодичность | Исполнитель |
| 1. | Контроль за соблюдением режима защиты персональных данных, политики в отношении обработки персональных данных, за выполнением работниками обязанностей по защите персональных данных, определенных в организационно-распорядительной документации | Ежедневно | Руководитель структурного подразделения администрации сельского поселения Боринский сельсовет, производящего обработку персональных данных (далее - руководитель подразделения).  Администратор безопасности информационных систем персональных данных |
| 2. | Контроль выполнения требований по режиму доступа в защищаемые помещения и на автоматизированные рабочие места, на которых производится обработка персональных данных | Ежедневно | Руководитель подразделения |
| 3. | Контроль соблюдения правил работы с носителями персональных данных | Ежедневно | Руководитель подразделения |
| 4. | Контроль целостности средств вычислительной техники, используемых для обработки персональных данных. Контроль корректной работы системного и прикладного программного обеспечения, средств защиты информации.  Контроль состава технических средств. | Ежедневно | Пользователь информационной системы персональных данных |
| 5. | Контроль за соблюдением режима обработки персональных данных | Еженедельно | Лицо, ответственное за организацию обработки персональных данных в структурном подразделении администрации сельского поселения Боринский сельсовет |
| 6. | Пересмотр и, при необходимости, корректировка учетных записей пользователей | Еженедельно | Администратор безопасности информационных систем персональных данных |
| 7. | Проверка журналов средств защиты информации для своевременного обнаружения фактов несанкционированного доступа к персональным данным | Еженедельно | Администратор безопасности информационных систем персональных данных |
| 8. | Контроль за выполнением антивирусной защиты, неизменностью настроек средств антивирусной защиты и своевременным обновлением антивирусных баз | Еженедельно | Администратор безопасности информационных систем персональных данных |
| 9. | Контроль за соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена | Еженедельно | Администратор безопасности информационных систем персональных данных |
| 10. | Контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации | Еженедельно | Администратор безопасности информационных систем персональных данных |
| 11. | Контроль за обеспечением резервного копирования, проверка работоспособности резервных копий | Ежемесячно | Администратор безопасности информационных систем персональных данных |
| 12. | Контроль за соблюдением правил эксплуатации криптосредств, хранения криптосредств, эксплуатационной документации к ним | Ежемесячно | Ответственный пользователь криптосредств |
| 13. | Поддержание в актуальном состоянии организационно-распорядительных документов | Ежемесячно | Лицо, ответственное за организацию обработки персональных данных в структурном подразделении администрации сельского поселения Боринский сельсовет |
| 14. | Контроль за разработкой и внесением изменений в программное обеспечение собственной разработки или штатное программное обеспечение, специально дорабатываемое собственными разработчиками или сторонними организациями | Ежемесячно | Администратор безопасности информационных систем персональных данных |
| 15. | Контроль установленного (инсталлированного) в информационных системах персональных данных программного обеспечения на предмет соответствия его перечню программного обеспечения, разрешенному к установке в информационной системе персональных данных | Ежемесячно | Администратор информационных систем персональных данных |
| 16. | Контроль состава технических средств и средств защиты информации, применяемых в информационных системах персональных данных | Ежемесячно | Администратор безопасности информационных систем персональных данных |
| 17. | Контроль работоспособности, параметров настройки и правильности функционирования средств защиты информации | Ежемесячно | Администратор безопасности информационных систем персональных данных |
| 18. | Контроль правил генерации и смены паролей пользователей | Раз в три месяца | Администратор безопасности информационных систем персональных данных |
| 19. | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения | Раз в три месяца | Администратор информационных систем персональных данных |
| 20. | Проверка наличия машинных носителей информации, содержащей персональные данные | Раз в полгода | Администратор безопасности информационных систем персональных данных |
| 21. | Проверка знаний и осведомленности работников в области защиты персональных данных | Раз в полгода | Лицо, ответственное за организацию обработки информационных систем персональных данных |
| 22. | Контроль реализации правил разграничения доступа, полномочий пользователей в информационных системах персональных данных согласно матрице доступа и исполненным заявкам | Раз в полгода | Администратор безопасности информационных систем персональных данных |
| 23. | Пересмотр модели угроз | Ежегодно  По факту изменения целей, технологии или иного значимого аспекта информационной безопасности  По факту обнаружения недостатков в ходе мероприятий по контролю уровня защищенности персональных данных | Лицо, ответственное за организацию обработки персональных данных в структурном подразделении администрации сельского поселения Боринский сельсовет.  Администратор безопасности информационных систем персональных данных |
| 24. | Пересмотр организационно-распорядительной документации, регламентирующей порядок обработки персональных данных и требования по защите персональных данных, с учетом проводимых мероприятий по контролю | Ежегодно  По факту изменения целей, технологии или иного значимого аспекта информационной безопасности | Лицо, ответственное за организацию обработки персональных данных в структурном подразделении администрации сельского поселения Боринский сельсовет. Администратор безопасности информационных систем персональных данных |
| 25. | Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты персональных данных | Ежегодно | Лицо, ответственное за организацию обработки персональных данных в структурном подразделении администрации сельского поселения Боринский сельсовет |
| 26. | Поиск и анализ уязвимостей информационных систем персональных данных, и оценка достаточности принятых мер защиты | Ежегодно | Администратор безопасности информационных систем персональных данных |
| 27. | Обучение и повышение осведомленности работников в области защиты ПДн | Ежегодно  В случае изменения законодательной базы, внутренних нормативных актов в области защиты персональных данных не позднее одного месяца с момента изменений | Лицо, ответственное за организацию обработки персональных данных в структурном подразделении администрации сельского поселения Боринский сельсовет |
| 28. | Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных | Раз в три года | Лицо, ответственное за организацию обработки персональных данных в структурном подразделении администрации сельского поселения Боринский сельсовет. Администратор безопасности информационных систем персональных данных  или  Юридическое лицо или индивидуальный предприниматель, имеющий лицензию на осуществление деятельности по технической защите конфиденциальной информации, привлеченные на договорной основе |
| 29. | Контроль заведения и удаления учетных записей пользователей | Прием/увольнение работника | Администратор безопасности информационных систем персональных данных |

**РЕГЛАМЕНТ внутреннего контроля соответствия обработки персональных данных**

Настоящий регламент разработан в соответствии с ФЗ «О персональных данных», Политикой в отношении обработки персональных данных (далее — Политика), Положением по обработке персональных данных субъектов (далее — Положение-1) и Положением по обработке персональных данных (далее — Положение-2).

Целью контроля является проверка соответствия фактического порядка обработки и защиты персональных данных требованиям законодательства, Политики, Положения-1, Положения-2 и других локальных нормативных актов ТФТЛ.

Внутренний контроль осуществляет либо лицо, ответственное за обработку персональных данных, либо исполнитель, которому были делегированы такие полномочия.

Контрольные мероприятия в ТФТЛ проводятся ответственным лицом.

Контрольные мероприятия в ТФТЛ проводятся выборочно.

Проверка проводится на основании распоряжения главы администрации сельского поселения Боринский сельсовет ТФТЛ. Периодичность проведения контрольных мероприятий — два раза в год.

Срок проведения проверки не может превышать десяти рабочих дней.

В процессе проверки исполнитель имеет право:

- доступа ко всем информационным ресурсам (ИР) и местам хранения персональных данных;

- ознакомления с локальными актами по вопросам обработки персональных данных, а так же журналами регистрации запросов, уничтожения персональных данных;

- получать объяснения от лиц, имеющих доступ к персональным данным и(или) осуществляющих их обработку;

- проверять знания по вопросам обработки персональных данных и их защите.

Ответственное лицо обязано:

- проводить проверку в отношении всех информационных ресурсов персональных данных;

- разрабатывать рекомендации по устранению нарушений, выявленных в процессе проверки.

В процессе проверки ответственное лицо заполняет контрольный лист (Приложение №1), при этом отметки проставляются по каждому информационному ресурсу в отдельности. Данный документ является обязательным приложением к акту (Приложение №2) по результатам контроля и аудита.

Акт по результатам контроля и приложение к нему хранятся в ТФТЛ, в местах определенных ответственным лицом.

Приложение № 1

Контрольный лист по проведению внутреннего контроля по выполнению требований ФЗ «О персональных данных»

|  |
| --- |
|  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |

№ Критерии проверки ИР1 ИР2 Примечание

1 Соответствие состава фактически собираемых и обрабатываемых персональных данных утвержденному перечню

2 Соблюдение ограниченного доступа к персональным данным

3 Соблюдение мер по обеспечению безопасности персональных данных:

3.1 физическая защита материальных носителей персональных данных

3.2 защита персональных данных, обрабатываемых с помощью средств вычислительной техники

4 Соблюдение порядка уточнения, блокирования и уничтожения персональных данных

5 Контроль ведения регистрационных журналов

6 Организация хранения персональных данных/Соответствие хранения персональных данных «Перечню мест хранения»

7 Работа с обращениями субъектов персональных данных:

7.1 регистрация запросов

7.2 соблюдение сроков рассмотрения запросов

7.3 уведомление субъектов о принятых действиях

8 Соблюдение правил передачи персональных данных третьим лицам

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Фамилия И.О., должность, подпись)

Приложение N 2

УТВЕРЖДАЮ

Акт внутреннего контроля за \_\_\_ полугодие 20\_\_\_ года № \_\_\_\_\_

Составлен: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

На основании: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с \_\_\_\_\_\_\_\_\_\_ по \_\_\_\_\_\_\_\_\_\_\_.

Были проведены мероприятия по контролю:

- соответствия фактического состояния порядка обработки персональных данных с требованиями законодательства и Политики, и прочими локальными нормативными актами;

- мер по обеспечению безопасности персональных данных.

В ходе контрольных мероприятий установлено:

- нарушений установленных законодательством и локальными нормативными актами не выявлено.

По итогам внутреннего контроля был заполнен контрольный лист являющийся неотъемлемым приложением к данному акту

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Фамилия И.О., должность, подпись)