**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**АДМИНИСТРАЦИЯ ТРУБЧЕВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА**

**П О С Т А Н О В Л Е Н И Е**

от 12.04.2016г. № 282

г. Трубчевск

|  |
| --- |
| Об утверждении Правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Трубчевского муниципального района |

Во исполнение требований Федерального закона от 27.07.2006 № 152 «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012г. № 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», Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», а также иных нормативных документов по защите информации:

1. Утвердить прилагаемые Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Трубчевского муниципального района.
2. Признать утратившим силу постановление администрации Трубчевского муниципального района от 30 сентября 2013 года № 671 «Об утверждении Правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Трубчевского муниципального района».
3. Руководителям отраслевых органов администрации Трубчевского муниципального района руководствоваться настоящими Правилами при осуществлении внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в соответствующем отраслевом органе администрации Трубчевского муниципального района.
4. Организационно-правовому отделу администрации Трубчевского муниципального района ознакомить всех работников администрации Трубчевского муниципального района с настоящим постановлением под роспись.
5. Настоящее постановление подлежит опубликованию на официальном сайте администрации Трубчевского муниципального района в течение 10 дней после его принятия.
6. Контроль за исполнением настоящего постановления возложить на заместителя главы администрации Трубчевского муниципального района Тубол С.Н.

**Глава администрации**

**Трубчевского муниципального района И.И. Обыдённов**

Утверждены

постановлением администрации

Трубчевского муниципального района

от 12.04.2016г. № 282

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Трубчевского муниципального района

**1. Общие положения**

1.1.         Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее  – Правила) в администрации Трубчевского муниципального района (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 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» 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», утвержденного постановлением Правительства РФ от 21 марта 2012 г. № 211.

1.3.         Для обработки ПДн, необходимых для систематизации сведений о лицах, пользующихся муниципальным имуществом, функционирует информационная система персональных данных (далее – ИСПДн) «БАРС-Аренда», предназначенная для осуществления деятельности по расчету, взиманию и контролю за арендной платой в отношении муниципального имущества и земельных участков, находящихся в пользовании у физических и юридических лиц.

1.4.         Для обработки ПДн сотрудников, необходимых для обеспечения кадровой и бухгалтерской деятельности, предоставления отчетности в соответствии с Трудовым кодексом Российской Федерации, иными законодательными и нормативными актами используется ИСПДн «1С.Предприятие 8.2» («Бухгалтерия государственного учреждения»), ИСПДн «1С.Предприятие 7.7» («Зарплата и кадры») и ИСПДн «СБиС++».

1.5.         Пользователем ИСПДн (далее – Пользователь) является сотрудник Администрации, участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, ПО, данным и средствам защиты информации (далее – СЗИ) ИСПДн.

1.6.         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 Администрации проводятся в следующих целях:

1.6.1    проверка выполнения требований организационно-распорядительной документации по защите информации в Администрации и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

1.6.2    оценка уровня осведомленности и знаний работников Администрации в области обработки и защиты персональных данных;

1.6.3    оценка обоснованности и эффективности применяемых мер и средств защиты.

1. **Тематика внутреннего контроля**

Тематика внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн:

2.1.         Проверки соответствия обработки ПДн установленным требованиям в Администрации 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 к настоящим Правилам) и предназначены для осуществления контроля выполнения требований в области защиты информации в Администрации.

2.3.         Плановые контрольные мероприятия проводятся постоянной комиссией периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План, приложение 1 к настоящим Правилам) и направлены на постоянное совершенствование системы защиты персональных данных ИСПДн Администрации.

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:

2.4.1    по результатам расследования инцидента информационной безопасности;

2.4.2    по результатам внешних контрольных мероприятий, проводимых регулирующими органами;

2.4.3    по решению руководителя Администрации (отраслевого органа Администрации).

1. **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.         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.

1. **Оформление результатов контрольных мероприятий**

4.1.         По итогам проведения плановых контрольных мероприятий результаты проверок фиксируются в Журнале учета событий информационной безопасности.

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

4.2.1    описание проведенных мероприятий по каждому из этапов;

4.2.2    перечень и описание выявленных нарушений;

4.2.3    рекомендации по устранению выявленных нарушений;

4.2.4    заключение по итогам проведения внутреннего контрольного мероприятия.

4.3.         отчет передается на рассмотрение руководству Администрации (отраслевого органа Администрации).

4.4.         Общая информации о проведенном контрольном мероприятий фиксируется в Журнале учета событий информационной безопасности.

4.5.         Результаты проведения мероприятий по внеплановому контролю заносятся в протокол проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в Администрации (приложение 2 к настоящим Правилам).

1. **Порядок проведения плановых и внеплановых контрольных мероприятий**

5.1.         Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственного 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.

5.2.         Лицо, ответственное за обеспечение безопасности ПДн, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех руководителей отраслевых органов, в которых планируется проведение контрольных мероприятий, и направляет им для ознакомления План проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

5.3.         Во время проведения контрольных мероприятий, в зависимости от целей мероприятий, могут выполняются 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 и регламентов по обеспечению безопасности информации в Администрации.

- Соблюдение Порядка доступа в помещения Администрации, где ведется обработка персональных данных.

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

- Знание Администраторами инструкций и регламентов по обеспечению безопасности информации в Администрации.

- 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 1  к Правилам осуществления внутреннего контроля  соответствия обработки персональных данных  требованиям к защите персональных данных в администрации Трубчевского муниципального района |

**ПЛАН**

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

в администрации Трубчевского муниципального района

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Мероприятие** | **Периодичность регулярных мероприятий** | **Периодичность плановых мероприятий** | **Исполнитель** |
| 1 | Контроль соблюдения правил доступа к ПДн | Еженедельно | Ежемесячно | Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных в Администрации |
| 2 | Контроль соблюдения режима защиты | Еженедельно | Ежемесячно | Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных в Администрации |
| 3 | Контроль выполнения антивирусной политики | Еженедельно | Ежемесячно | Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных в Администрации |
| 4 | Контроль выполнения парольной политики | Еженедельно | Ежемесячно | Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных в Администрации |
| 5 | Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена | Еженедельно | Ежемесячно | Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных в Администрации |
| 6 | Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн |  | Ежемесячно | Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных в Администрации |
| 7 | Контроль обновления ПО и единообразия применяемого ПО на всех элементах АИС \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ СПО | Еженедельно | Ежемесячно | Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных в Администрации |
| 8 | Контроль обеспечения резервного копирования |  | Ежемесячно | Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных в Администрации |
| 9 | Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз |  | Ежегодно | Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных в Администрации |
| 10 | Поддержание в актуальном состоянии нормативно-организационных документов |  | Ежемесячно | Ответственный за организацию обработки ПДн в Администрации |
| 11 | Контроль запрета на использование беспроводных соединений | Еженедельно | Ежемесячно | Ответственный за организацию обработки ПДн в Администрации |

|  |  |
| --- | --- |
|  | Приложение 2  к Правилам осуществления внутреннего контроля  соответствия обработки персональных данных  требованиям к защите персональных данных в администрации Трубчевского муниципального района |

ПРОТОКОЛ № \_\_\_\_

проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Трубчевского муниципального района

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*