



**АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ -
ЕРШИЧСКИЙ РАЙОН СМОЛЕНСКОЙ ОБЛАСТИ**

РАСПОРЯЖЕНИЕ

от 03.05.2018 № 108-р

с. Ершичи

Ершичского района

Смоленской области

Об утверждении Правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Администрации муниципального образования – Ершичский район Смоленской области

В целях исполнения требований Постановления 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 муниципального образования – Ершичский район Смоленской области:

1. Утвердить:

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Администрации муниципального образования – Ершичский район Смоленской области Приложению;

2. Признать утратившим силу Постановление Администрации муниципального образования – Ершичский район Смоленской области от 18.08.2017 № 172-р «Об утверждении Правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Администрации муниципального образования – Ершичский район Смоленской области»

2. Настоящее распоряжение вступает в силу с момента его принятия.
3. Контроль за исполнением настоящего распоряжения оставляю за собой.

Глава муниципального образования –
Ершичский район Смоленской области

К.Н. Серенков

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Администрации муниципального образования – Ершичский район Смоленской области

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) в Администрации муниципального образования – Ершичский район Смоленской 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 соблюдения условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в ИСПДн в Администрации муниципального образования – Ершичский район Смоленской области проводятся в следующих целях:

- 1.3.1 проверка выполнения требований организационно-распорядительной документации по защите информации в Администрации муниципального образования – Ершичский район Смоленской области и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;
- 1.3.2 оценка уровня осведомленности и знаний работников Администрации муниципального образования – Ершичский район Смоленской области в области обработки и защиты персональных данных;

1.3.3 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 муниципального образования – Ершичский район Смоленской 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 муниципального образования – Ершичский район Смоленской 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 Администрации муниципального образования – Ершичский район Смоленской 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:

- 2.4.1 по результатам расследования инцидента информационной безопасности;
- 2.4.2 по результатам внешних контрольных мероприятий, проводимых регулирующими органами;
- 2.4.3 по решению руководителя Администрации муниципального образования – Ершичский район Смоленской 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:

- 3.2.1 цели проведения контрольных мероприятий;
- 3.2.2 задачи проведения контрольных мероприятий,
- 3.2.3 объекты контроля (процессы, подразделения, информационные системы и т.п.);

3.2.4 состав участников, привлекаемых для проведения контрольных мероприятий;

3.2.5 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:

4.2.1 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 муниципального образования – Ершичский район Смоленской области.

4.4. Общая информации о проведенном контрольном мероприятии 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 муниципального образования – Ершичский район Смоленской области (приложение 2).

5. Порядок проведения плановых и внеплановых контрольных мероприятий

5.1. Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственному 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 муниципального образования – Ершичский район Смоленской области.

5.2. Лицо, ответственное за обеспечение безопасности ПДн, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех руководителей подразделений, 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 выполняться 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 муниципального образования – Ершичский район Смоленской области.

- Соблюдение Порядка доступа в помещения Администрации муниципального образования – Ершичский район Смоленской области, 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 муниципального образования – Ершичский район Смоленской 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 1
к 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	Главный специалист по защите информации, информационных технологий, связи и обеспечению предоставления услуг в электронном виде
Контроль соблюдения режима защиты	Раз в полгода	Раз в полгода	Главный специалист по защите информации, информационных технологий, связи и обеспечению предоставления услуг в электронном виде
Контроль выполнения антивирусной политики	Раз в полгода	Раз в полгода	Главный специалист по защите информации, информационных технологий, связи и обеспечению предоставления услуг в электронном виде
Контроль выполнения парольной политики	Раз в полгода	Раз в полгода	Главный специалист по защите информации, информационных технологий, связи и обеспечению предоставления услуг в электронном виде
Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	Раз в полгода	Раз в полгода	Главный специалист по защите информации, информационных технологий, связи и обеспечению предоставления услуг в электронном виде
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Раз в полгода	Раз в полгода	Главный специалист по защите информации, информационных технологий, связи и обеспечению предоставления услуг в электронном виде
Контроль обновления ПО и единообразия применяемого ПО на всех элементах АИС Администрации муниципального	Раз в полгода	Раз в полгода	Главный специалист по защите информации, информационных технологий, связи и обеспечению предоставления услуг в электронном виде

образования – Ершичский район Смоленской области			
Контроль обеспечения резервного копирования	Раз в полгода	Раз в полгода	Главный специалист по защите информации, информационных технологий, связи и обеспечению предоставления услуг в электронном виде
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз	Раз в полгода	Раз в полгода	Главный специалист по защите информации, информационных технологий, связи и обеспечению предоставления услуг в электронном виде
Поддержание в актуальном состоянии нормативно-организационных документов	Раз в полгода	Раз в полгода	Главный специалист по защите информации, информационных технологий, связи и обеспечению предоставления услуг в электронном виде
Контроль запрета на использование беспроводных соединений	Раз в полгода	Раз в полгода	Главный специалист по защите информации, информационных технологий, связи и обеспечению предоставления услуг в электронном виде

Приложение 2
к 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
муниципального образования – Ершичский район Смоленской 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