



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

РАСПОРЯЖЕНИЕ

от 18.08.2017 № 172-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 соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 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»:

1. Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных согласно приложению.
2. Настоящее распоряжение подлежит опубликованию на официальном сайте муниципального образования – Ершичский район Смоленской области.
3. Контроль за исполнением настоящего распоряжения оставляю за собой.

Глава муниципального образования –
Ершичский район Смоленской области

К.Н. Серенков

Отп. 1экз. - в дело
Исп. М.В. Капцевич
Тел. 2-19-07

«___» _____

Разработчик:
М.В. Капцевич
Тел. 2-19-07

«___» _____

Визы:

М.М. Пахоменков

«___» _____

М.М. Бугаев

«___» _____

Разослать: управляющему делами,
отделу экономики имущественных
и земельных отношений.

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

1. Общие положения

Настоящие «Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных» (далее - Правила) определяют порядок планирования и проведения контроля безопасности режима обработки персональных данных (ПДн) в Администрации муниципального образования – Ершичский район Смоленской области, в том числе ее защищенности от несанкционированного доступа (НСД), распространения, искажения и утраты, а также порядок реагирования на инциденты информационной безопасности.

Целью контроля безопасности режима обработки ПДн в Администрации муниципального образования – Ершичский район Смоленской области является определение истинного состояния дел в области защиты ПДн, оценки эффективности принимаемых для исключения утечки ПДн мер, выявления возможных каналов утечки, выработки предложений и рекомендаций руководству Администрации муниципального образования – Ершичский район Смоленской области по совершенствованию системы защиты ПДн (СЗПДн).

Организация контроля возлагается на Администратора безопасности в Администрации муниципального образования – Ершичский район Смоленской области.

В число основных объектов контроля безопасности режима обработки ПДн входят:

- структурные подразделения Администрации муниципального образования – Ершичский район Смоленской области, привлекаемые к обработке ПДн;
- сотрудники Администрации муниципального образования – Ершичский район Смоленской области, допущенные в установленном порядке к ПДн, и их носителям, и выполняющие работы с их использованием;
- служебные помещения, в которых проводятся работы с носителями ПДн;
- места непосредственного хранения носителей ПДн (хранилища, сейфы, шкафы);
- непосредственно носители ПДн (документы, материалы, изделия, магнитные носители);

- компоненты информационных систем ПДн (ИСПДн), в которых осуществляется обработка ПДн;

- Локальная сеть Администрации муниципального образования – Ершичский район Смоленской области.

Особенности контроля безопасности ПДн в отдельных ИСПДн могут регулироваться дополнительными инструкциями и регламентами.

2. Планирование мероприятий по обеспечению и контролю безопасности персональных данных

2.1 Основные цели планирования мероприятий по обеспечению безопасности ПДн:

- организация проведения комплекса мероприятий по защите ПДн, направленных на исключение возможных каналов утечки ПДн;

- установление персональной ответственности всех должностных лиц Администрации муниципального образования – Ершичский район Смоленской области за решение вопросов защиты ПДн в ходе деятельности Администрации муниципального образования – Ершичский район Смоленской области;

- определение сроков (времени, периода) проведения конкретных мероприятий по защите ПДн;

- систематизация (объединение) всех проводимых на плановой основе мероприятий по различным направлениям защиты ПДн;

- установление системы контроля за обеспечением защиты ПДн в Администрации муниципального образования – Ершичский район Смоленской области, а также системы отчетности о выполнении конкретных мероприятий;

- уточнение (конкретизация) функций и задач по защите ПДн, решаемых отдельными должностными лицами и структурными подразделениями Администрации муниципального образования – Ершичский район Смоленской области.

Основой для планирования мероприятий по защите ПДн в Администрации муниципального образования – Ершичский район Смоленской области служат:

- требования законодательных и иных нормативных правовых актов по защите ПДн;

- положения внутренних организационно-распорядительных документов Администрации муниципального образования – Ершичский район Смоленской области (постановлений, распоряжений, положений, инструкций), определяющих порядок ведения деятельности по защите конфиденциальной информации, а также конкретизирующих вопросы защиты ПДн в Администрации муниципального образования – Ершичский район Смоленской области;

- результаты комплексного анализа состояния дел в области защиты ПДн, проводимого ответственным сотрудником Администрации муниципального образования – Ершичский район Смоленской области;

- результаты контроля за состоянием защиты ПДн, проводимого контролирующими органами;
- результаты проверки вышестоящими учреждениями;
- особенности повседневной деятельности Администрации муниципального образования – Ершичский район Смоленской области и специфика выполнения в Администрации муниципального образования – Ершичский район Смоленской области работ с использованием ПДн.

Планирование мероприятий по обеспечению и контролю безопасности ПДн осуществляется на календарный год, в отдельных случаях могут составляться планы на календарный месяц, неделю, а также на иной определенный срок.

Разработка планирующих документов по защите ПДн в Администрации муниципального образования – Ершичский район Смоленской области осуществляется сотрудником, ответственным за обеспечение безопасности ПДн в Администрации муниципального образования – Ершичский район Смоленской области, в тесном взаимодействии с другими подразделениями (отдельными должностными лицами). Кроме того, при подготовке планов должны учитываться предложения структурных подразделений Администрации муниципального образования – Ершичский район Смоленской области, осуществляющих обработку ПДн.

2.2 Структура и основное содержание планов по обеспечению и контролю безопасности ПДн.

Основным организационно - планирующим документом Администрации муниципального образования – Ершичский район Смоленской области в сфере защиты ПДн является «План мероприятий по защите информации в Администрации муниципального образования – Ершичский район Смоленской области на календарный год», содержащий необходимый перечень мероприятий для обеспечения защиты ПДн.

«План мероприятий по защите информации в Администрации муниципального образования – Ершичский район Смоленской области» составляется на основании списка мер, методов и средств защиты, определенных нормативными правовыми актами и методическими документами по защите ПДн, действующими приказами.

«План мероприятий по защите информации в Администрации муниципального образования – Ершичский район Смоленской области на календарный год» утверждается Главой муниципального образования – Ершичский район Смоленской области до начала календарного года, на который он разработан. Утвержденный план под роспись доводится до сведения ответственных за проведение и организацию указанных в плане мероприятий в части их касающейся.

Основным видом контроля режима обработки ПДн в Администрации муниципального образования – Ершичский район Смоленской области являются проверки, подразделяемые на плановые и внеплановые.

Плановые проверки организуются заблаговременно, включаются в соответствующий План внутренних проверок режима защиты ПДн, включающий периодичность проведения внутренних проверок и ответственных исполнителей.

Внеплановые проверки организуются и проводятся при необходимости по указанию Главы муниципального образования – Ершичский район Смоленской области или ответственным за организацию работ по защите информации. Они могут проводиться как в масштабах всего, так и в его структурных подразделениях. Особенность организации таких проверок состоит в том, что они отсутствуют в Планах внутренних проверок режима защиты ПДн.

Алгоритм подготовки и проведения внеплановой проверки следующий:

- 1) принятие решения о проведении проверки (например, после инцидента безопасности);
- 2) подготовка перечня проверяемых вопросов;
- 3) определение ответственных за проведение проверки лиц;
- 4) определение сроков проверки;
- 5) непосредственное проведение проверки;
- 6) оформление результатов работы;
- 7) выработка предложений и рекомендаций;
- 8) доклад результатов проверки на месте;
- 9) анализ недостатков с проверяемыми;
- 10) доклад результатов лицу, назначившему проверку.

В ходе выполнения проверки осуществляется сопоставление результатов выполнения конкретных мероприятий по обеспечению безопасности ПДн с положениями нормативно-методических документов по защите ПДн и соответствующими стандартами Администрации муниципального образования – Ершичский район Смоленской области.

При этом проверочные мероприятия подразделяются на проверки режима неавтоматизированной обработки ПДн и с использованием средств автоматизации.

В проведении проверок участвуют сотрудники состоящие в Комиссии по информационной безопасности при Администрации муниципального образования – Ершичский район Смоленской области. Результаты проверки оформляются в виде акта и доводятся до сведения руководителя проверенного структурного подразделения. В данном акте перечисляются выявленные недостатки, а также формулируются предложения по их устранению, повышению эффективности работы должностных лиц (сотрудников) в области защиты ПДн. Проверяющие лица устанавливают конкретные сроки устранения выявленных недостатков и реализации предложений (рекомендаций).

При осуществлении контроля режима обработки ПДн особое внимание уделяется вопросам обращения с носителями ПДн и их хранения в структурных подразделениях Администрации муниципального образования – Ершичский район Смоленской области. Проверяются:

- порядок учета, хранения, размножения (копирования) и уничтожения носителей ПДн;
- оборудование помещений, в которых хранятся указанные носители или осуществляется работа с ними; порядок передачи носителей одними исполнителями другим, в том числе и при убытии лиц в командировку (отпуск, на лечение) и т.д.

Постоянному контролю подлежат также вопросы допуска и доступа всех категорий должностных лиц к ПДн, в том числе и непосредственно к носителям

ПДн, вопросы организации и осуществления пропускного и внутриобъектового режимов в Администрации муниципального образования – Ершичский район Смоленской области.

Сотрудник, ответственный за обеспечение безопасности ПДн, организует и ведет учет результатов контроля, всех видов проводимых проверок.

В план внутренних проверок могут быть включены следующие пункты:

1) Контроль соблюдения организационно-режимных требований в помещениях, в которых осуществляется обработка ПДн.

Ежегодно в соответствии с Планом внутренних проверок должна быть проведен контроль соблюдения организационно-режимных требований в помещениях, в которых осуществляется обработка ПДн. Данный вид контроля включает:

- проверку актуальности перечня лиц, имеющих право самостоятельного доступа в помещение;
- проверку корректности расположения мониторов рабочих станций, на которых осуществляется обработка ПДн, исключающего несанкционированный ПДн не допущенными лицами; наличие жалюзи на окнах;
- контроль отсутствия конфиденциальных документов, содержащих ПДн, без присмотра на рабочих столах сотрудников;
- контроль сохранности пломб на технических средствах передачи и обработки ПДн, а также на устройствах их защиты;
- и т.п.

2. Контроль доступа к приложениям информационных систем, в которых осуществляется обработка ПДн.

Ежеквартально в целях снижения рисков несанкционированного доступа к информации должен проводиться контроль доступа к приложениям ИСПДн, включающий в себя:

- контроль фактов подачи заявок на блокирование доступа к ИСПДн, в которых осуществляется обработка конфиденциальной информации, увольняемых сотрудников и своевременности подачи таких заявок;
- контроль использования предоставленных прав доступа (в том числе и право удаленного доступа). Если предоставленные права доступа не используются в течение трех и более месяцев, администратор безопасности может инициироваться расследование правомерности подачи заявки на доступ;

и т.п.

4. Контроль порядка обращения с носителями ПДн.

Ежеквартально ответственным сотрудником должен осуществляться контроль порядка обращения с носителями ПДн, включающий в себя:

- проверку корректности ведения журнала учета машинных носителей и соответствия записей в журнале записям в автоматизированной системе контроля съемных магнитных носителей информации;

5. Контроль нейтрализации выявленных нарушений режима обработки ПДн.

Ежеквартально должен осуществляться контроль нейтрализации выявленных нарушений режима обработки ПДн, включающий в себя проверку корректности ведения базы данных инцидентов информационной безопасности, заполнения отчетов об инцидентах, а также все ли обнаруженные инциденты нейтрализованы.

6. Организация анализа и пересмотра имеющихся угроз безопасности ПДн.

Ежегодно на основании анализа произошедших инцидентов информационной безопасности, изменений в условиях обработки ПДн в ИСПДн должна осуществляться корректировка Моделей угроз безопасности ПДн при их обработке в ИСПДн, а при необходимости и моделирование новых Моделей угроз безопасности ПДн в соответствии с действующими нормативными правовыми актами и методическими документами ФСТЭК и ФСБ России.

7. Поддержание в актуальном состоянии нормативно-организационных документов по вопросам обеспечения безопасности ПДн

Ежегодно следует проводить актуализацию нормативно-организационных документов по вопросам обеспечения безопасности ПДн в соответствии с:

- изменениями требований законодательных и иных нормативных правовых актов по защите ПДн, отраслевых стандартов;
- результатами анализа состояния дел в области защиты ПДн, проводимого ответственным сотрудником на основании материалов плановых проверок и расследований выявленных инцидентов информационной безопасности;
- результатами контроля за состоянием защиты ПДн, проводимого контролирующими органами.