



## РАСПОРЯЖЕНИЕ ТШÖКТÖМ

20 ноября 2018 г.  
с. Визинга, Республика Коми

№ 358 - р

О проведении внутренней проверки  
обработки персональных данных

С целью обеспечения безопасности персональных данных, обрабатываемых в информационных системах персональных данных администрации муниципального района «Сысольский» (далее – Администрация), в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановления Правительства Российской Федерации от 01.11.12 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 15.09.2007 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и других нормативных правовых актов в области защиты персональных данных:

1. Постоянно действующей комиссии по защите персональных данных провести полную внутреннюю проверку обработки персональных данных в Администрации.

2. При проведении полной внутренней проверки обработки персональных данных руководствоваться действующим в Администрации регламентом проведения внутренних мероприятий по контролю обеспечения защиты персональных данных согласно приложению.

3. По окончании проверки, представить отчет о результатах внутренней проверки обработки персональных данных.

4. В отчете о результатах проведения внутренней проверки обработки персональных данных указать следующую информацию:

- перечень выявленных информационных систем персональных данных;
- общую информацию о состоянии системы защиты персональных данных, включающую организационную, физическую и техническую подсистемы;

- общую информацию об информационных технологиях, применяемых в информационных системах персональных данных, и структуру локальной вычислительной сети Администрации;

- общую информацию о выявленных информационных системах персональных данных;

- рекомендации по обеспечению безопасности персональных данных в Администрации.

4. Для каждой выявленной информационной системы персональных данных указать:

- структуру информационной системы персональных данных;

- конфигурацию информационной системы персональных данных;

- состав обрабатываемых персональных данных;

- структуру обработки персональных данных;

- объекты защиты;

- среду и режим обработки персональных данных;

- пользователей информационных систем персональных данных.

4. Представить на утверждение план мероприятий по обеспечению безопасности персональных данных.

5. Контроль исполнения распоряжения возложить на председателя постоянно действующей комиссии по защите персональных данных.

Руководитель администрации

Р. В. Носков

Приложение  
к распоряжению администрации  
муниципального района «Сысольский»  
20 ноября 2018 г. № 358-р

## **РЕГЛАМЕНТ**

проведения внутренних мероприятий  
по контролю обеспечения защиты персональных данных

## **1. Информация о документе**

1.1. Регламент разработан в администрации муниципального района «Сысольский» (далее – Администрация) в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.12 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 15.09.2007 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и других нормативных правовых актов в области обработки и обеспечения безопасности персональных данных».

1.2. Регламент разработан с целью регулирования внутренних мероприятий по контролю обеспечения защиты персональных данных (далее - Контроль), проводимых постоянно действующей комиссией по защите персональных данных (далее - Комиссия).

1.3. Регламент вступает в силу с момента его утверждения руководителем Администрации и действует до замены его новым Регламентом или его отмены.

1.4. Пересмотр пунктов Регламента производится Комиссией на заседании.

1.4.1. Пересмотр пунктов Регламента производится в следующих случаях:

- при изменении процессов обработки персональных данных, местоположения объектов защиты, условий их содержания, хранения и использования;
- при определении такой необходимости по результатам проведения внутреннего контроля обеспечения защиты персональных данных, в целях повышения эффективности мероприятий, определенных в настоящем регламенте;
- при изменении состава, обязанностей и полномочий должностных лиц Администрации, задействованных в вводимых регламентом мероприятиях.

1.5. Любые изменения в Регламент вносятся распоряжением руководителя Администрации.

1.6. Контроль за соблюдением требований Регламента осуществляет председатель Комиссии.

1.7. Положения Регламента распространяются на всех работников, которые входят в состав Комиссии на основании действующего распоряжения руководителя Администрации, а также иных лиц, на которых локальными актами Администрации возлагается ответственность за осуществление мероприятий по контролю обеспечения защиты персональных данных.

1.8. Все лица, указанные в пункте 1.7 Регламента должны быть ознакомлены с Регламентом под подпись в журнале учета ознакомлений с локальными нормативными актами по защите персональных данных.

## **2. Общие положения**

2.1. Контроль в Администрации осуществляется с целью своевременного выявления и предотвращения несанкционированного доступа к персональным данным и других угроз безопасности персональных данных, актуальных для информационных систем персональных данных.

2.2. Контроль и оценка эффективности защиты персональных данных являются неотъемлемой составной частью работ по защите персональных данных при создании и эксплуатации информационных систем персональных данных.

2.3. Основными задачами Контроля являются:

- проверка соответствия принятых и принимаемых мер по защите персональных данных требованиям законодательства РФ и локальных нормативных актов Администрации;
- проверка своевременности и полноты выполнения требований нормативных документов, регламентирующих организацию и порядок осуществления мероприятий по защите персональных данных.

## **3. Организация проведения внутренних мероприятий по контролю обеспечения защиты персональных данных**

3.1. Комиссия осуществляет постоянный внутренний Контроль в рамках исполнения своих задач и функций.

3.2. Основной формой Контроля является внутренняя проверка условий обработки и защиты персональных данных (далее внутренняя проверка).

3.3. Результаты Контроля оформляются актами, протоколами, заключениями и записями в специальных журналах и доводятся до сведения руководителя Администрации и должностных лиц в соответствии с видами Контроля.

3.4. Полная внутренняя проверка условий обработки и защиты персональных данных проводится Комиссией не реже 1 раза в 3 года в сроки, определяемые Комиссией, и санкционируется распоряжением руководителя Администрации.

3.5. По инициативе Администрации может проводиться аудит обеспечения безопасности персональных данных с привлечением третьей стороны – юридических лиц или индивидуальных предпринимателей, имеющих лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации, заключающийся в оценке соответствия текущего состояния информационной безопасности в Администрации требованиям правовых и нормативных документов в области защиты персональных данных.

#### **4. Порядок проведения внутренних мероприятий по контролю обеспечения защиты персональных данных**

4.1. Мероприятия могут быть плановыми и внеплановыми.

4.2. В рамках плановых мероприятий проверяется достаточность организационных, физических, технических и программно-аппаратных мер защиты персональных данных.

4.3. К плановым мероприятиям могут относиться:

- Проверка актуальности локальных нормативных актов Администрации по защите персональных данных;
- Контроль соблюдения порядка и требований обработки персональных данных;
- Контроль соблюдения требований парольной защиты;
- Контроль соблюдения требований антивирусной защиты;
- Контроль соблюдения требований информационной безопасности в сфере информационного обмена;
- Контроль соблюдения порядка доступа в помещения, выделенные для обработки персональных данных;
- Контроль соблюдения порядка проведения резервного копирования, хранения и корректности создаваемых резервных копий;
- Контроль соблюдения порядка использования средств защиты информации;
- Контроль соблюдения требований хранения материальных носителей персональных данных (бумажных и машинных);
- Контроль соблюдения требований работы в информационных системах персональных данных;
- Контроль соответствия состава обрабатываемых персональных данных заявленным целям их обработки;
- Контроль реагирования на обращения субъектов персональных данных об исполнении из законных прав;
- Контроль удаления персональных данных и уничтожения их материальных носителей;
- Контроль соблюдения порядка предоставления персональных данных и их материальных носителей третьим лицам;
- Выявление изменений порядка и условий обработки и защиты персональных данных;
- Анализ и переоценка угроз безопасности персональных данных, предсказание появления новых, еще не известных угроз;
- Контроль ведения журнальных форм;
- Проверка соответствия организационных мер требованиям действующего законодательства Российской Федерации;
- Проверка состояния средств физической защиты персональных данных;
- Проверка работоспособности средств вычислительной техники, антивирусного программного обеспечения, межсетевых экранов, средств резервного копирования устройств бесперебойного электропитания;
- Антивирусная проверка, обновление баз данных;

- Проверка обновления операционных систем;
- Проверка функционирования средств разграничения доступа;
- Проверка соответствия прав доступа к автоматизированным рабочим местам, на которых обрабатываются персональные данные, установленным матрицам доступа;
- Проверка состояния материальных носителей персональных данных и контроль соблюдения требований работы с ними;
- Проверка осведомленности персонала в части требований локальных нормативных актов Администрации и действующего законодательства РФ по защите персональных данных;
- Проверка актуальности информации, указанной в уведомлении уполномоченного органа по защите прав субъектов персональных данных об обработке (о намерении осуществлять обработку) персональных данных.

4.4. К внеплановым проверкам, кроме проверок указанных в пунктах 2.3 и 2.4 настоящего регламента относятся:

- Проверки достоверности персональных данных;
- Проверка знаний персонала вновь изданного локального нормативного акта Администрации;
- Проверка состояния защищенности объектов защиты в соответствии с требованиями вновь изданного нормативного правового акта Российской Федерации в области обеспечения безопасности персональных данных.

4.5. Плановые проверки проводятся в соответствии с утвержденным планом мероприятий по обеспечению безопасности персональных данных (далее План).

4.6. План разрабатывает председатель Комиссии.

4.7. Плановая проверка проводится в срок, указанный в плане.

4.8. Периодичность проведения того или иного мероприятия, а также ответственные за проведения мероприятия лица устанавливаются по решению Комиссии. Некоторые мероприятия следует проводить внепланово, в случае изменения внешних факторов, например, изменения действующего законодательства РФ в области обработки и защиты персональных данных.

4.9. Внеплановые мероприятия проводятся в случае:

- при возникновении или после возникновения инцидента информационной безопасности (например, утечки персональных данных);
- изменения действующего законодательства РФ в области обработки и защиты персональных данных;
- изменения структуры процессов обработки персональных данных;
- появления жалоб субъектов персональных данных.

4.10. Решение о проведении внеплановых мероприятий принимается председателем Комиссии, и оформляется распоряжением руководителя Администрации.

4.11. Внеплановость мероприятий подразумевает:

- максимально короткий срок между выходом приказа о проведении и проведением;
- минимизация круга лиц, которые заранее знают о готовящемся мероприятии;
- отсутствие периодичности в сроках проведения таких мероприятий.

4.12. Внутренние контролирующие мероприятия осуществляются Комиссией.

4.13. Председатель Комиссии отвечает за организацию и проведение внутренних проверок.

4.14. Комиссия проводит плановые и внеплановые внутренние проверки на основании действующего в Администрации положения о Комиссии.

4.15. В рамках проведения внутренней проверки Комиссия имеет право:

- запрашивать у работников, осуществляющих обработку персональных данных в рамках своих полномочий, необходимую для проведения проверки информацию;
- принимать меры по блокированию или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации в области защиты персональных данных;
- вносить руководителю Администрации предложения по совершенствованию системы защиты персональных данных.

4.16. В случае выявления в ходе выполнения контролирующих мероприятий инцидентов безопасности персональных данных, Комиссия руководствуется утвержденной в Администрации Инструкцией о порядке обеспечения безопасности персональных данных в случае нештатных ситуаций.

4.17. Результаты проведения внутренних мероприятий по контролю фиксируются в Протоколах проведения внутренних проверок. В случае выявления нарушений, председателем Комиссии в протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения. Протоколы хранятся у председателя Комиссии до конца текущего года. Уничтожение протоколов проводится Комиссией самостоятельно в январе следующего за проверочным годом.

4.18. По результатам внутреннего планового Контроля разрабатывается план по устранению недостатков в обеспечении информационной безопасности и по совершенствованию системы защиты персональных данных, в соответствии с которым в Администрации разрабатываются и проводятся необходимые мероприятия.

4.19. При повседневном Контроле осуществляется анализ событий произошедших в информационных системах персональных данных по различным системным журналам, включая журналы средств защиты информации от несанкционированного доступа. Для расследования инцидентов, связанных с нештатными ситуациями или нарушением безопасности ПДн, в Администрации для их расследований могут создаваться специальные Комиссии.

4.20. Все проводимые мероприятия по защите персональных данных подлежат обязательному учету в журнале.

4.21. Сведения о проведенном мероприятии заносится в журнал проводившим мероприятием лицом сразу после осуществления данного мероприятия.

4.22. В случае невозможности проведения того или иного мероприятия в запланированный заранее день, оно может быть проведено ранее или позднее (не более чем на неделю) намеченной даты.

4.23. Плановые мероприятия устанавливаются локальными нормативными актами Администрации, включая настоящий регламент, регламентирующими защиту и обработку персональных данных.

4.24. Перечень плановых мероприятий формируется Комиссией и утверждается руководителем Администрации в виде Годового плана.

## **5. Годовые планы мероприятий**

### **5.1. Общие сведения**

5.1.1. Годовой план формируется Комиссией ежегодно, на один (следующий) год для каждого из ответственных лиц. После формирования, годовые планы утверждаются руководителем Администрации.

5.1.2. Годовые планы на следующий год должны быть подготовлены и утверждены не позднее 15 декабря текущего года.

5.1.3. После утверждения годовой план передается ответственному лицу. В случае если в качестве ответственного лица выступает Комиссия, план передается ее председателю.

5.1.4. Вопросы пересмотра плана на текущий год решаются на заседании Комиссии.

5.1.5. Выполненные планы передаются ответственному лицу и хранятся в течение трех лет.

### **5.2. Структура годового плана**

5.2.1. В годовой план включаются все устанавливаемые локальными нормативными актами Администрации мероприятия в области защиты персональных данных, мероприятия для данного ответственного с указанием их наименований и дат проведения.

5.2.2. Годовой план состоит из двух разделов:

- Еженедельные мероприятия (и более частые);
- Прочие мероприятия.

5.2.3. В первый раздел годового плана включаются мероприятия, выполнение которых необходимо осуществлять еженедельно или чаще (ежедневно, два раза в неделю и т.п.). Данную часть плана рекомендуется оформлять в виде таблицы из 7-ми строк – на каждый день недели. В каждую ячейку этой таблицы необходимо поместить соответствующие мероприятия и ссылку на локальный акт, их вводящий.

5.2.4. Во второй раздел включаются мероприятия, осуществляемые с периодичностью от одного раза в неделю (не включительно).

5.2.4.1. Для каждого такого мероприятия должна быть определена периодичность выполнения или срок выполнения, или конкретная дата, в которую данное мероприятие должно быть выполнено. При выборе даты проведения мероприятия необходимо ориентироваться по календарю выходных и праздничных дней на соответствующий год.

### **5.3. Обновление годового плана**

5.3.1. Вопросы обновления годовых планов на текущий год рассматриваются на заседании Комиссии.

5.3.2. При необходимости дополнить годовой план новыми мероприятиями, либо изменить состав или порядок мероприятий в плане на оставшийся период года – годовой план изменяется.

5.3.3. Мероприятия, размещенные в старой версии плана, не переносятся в новую. Новая версия должна содержать только мероприятия, актуальные до конца года. На обложке новой версии плана указывается с какой даты он действует.

5.3.4. Обновленная версия утверждается руководителем Администрации и незамедлительно, в течение одного дня, передается ответственному лицу, старая версия изымается. На обложке старой версии годового плана делается пометка о его неактуальности, начиная с указанной даты.

### **5.4. Обращение ответственного с годовым планом**

5.4.1. Ответственный за выполнение мероприятий годового плана обязан ежедневно уточнять состав ближайших мероприятий с целью подготовки к ним, а также выполнять все мероприятия, запланированные на текущий день.

5.4.2. Ответственный обязан обеспечить сохранность находящегося у него годового плана и предоставлять его по требованию Комиссии (но не более чем на один день).

5.4.3. По окончании года ответственный обязан передать план председателю Комиссии.

## **6. Квартальные планы мероприятий**

### **6.1. Общие сведения**

6.1.1. В целях качества, своевременности и полноты выполнения годового плана, допускается составление квартального плана.

6.1.2. Квартальные планы на следующий квартал должны быть подготовлены и утверждены не позднее 15 числа последнего месяца текущего квартала.

6.1.3. Под кварталом понимается промежуток времени равный трем месяцам, начиная с 1 января текущего года.

6.1.4. Последним днем, четвертого квартала является 31 декабря текущего года

6.1.5. После утверждения квартальный план передается ответственному лицу. В случае если в качестве ответственного лица выступает Комиссия, план передается ее председателю.

6.1.6. Вопросы пересмотра плана на текущий квартал решаются на заседании Комиссии.

6.1.7. Выполненные планы передаются ответственному лицу и хранятся в течение трех лет.

6.1.8. Квартальные планы на год должны включать в себя полный перечень мероприятий, предусмотренный Годовым планом.

### **6.2. Структура квартального плана**

6.2.1. В квартальные планы включаются все устанавливаемые локальными нормативными актами Администрации мероприятия в области защиты персональных данных, мероприятия для данного ответственного с указанием их наименований и дат проведения, в соответствии с периодичностью, сроками и датами, предусмотренными Годовым планом, а также мероприятия необходимые для обеспечения безопасности персональных данных не предусмотренные Годовым планом, если такие мероприятия не противоречат положениям действующего законодательства РФ.

6.2.1.1. Мероприятия периодичностью менее трех месяцев должны включаться в каждый квартальный план.

6.2.1.2. Мероприятия периодичностью более трех месяцев включаются в квартальные планы при необходимости, в зависимости от периодичности.

6.2.1.3. Мероприятия с указанием срока выполнения должны включаться в квартальный план допускающий выполнение мероприятия в установленный срок.



6.2.1.4. Мероприятия с указанием срока выполнения должны включаться в квартальный план допускающий выполнение мероприятия в установленный срок.

6.2.1.5. Мероприятия с указанием конкретной даты выполнения должны включаться в квартальный план, содержащий соответствующую дату.

### **6.3. Обновление квартального плана**

6.3.1. Вопросы обновления квартальных планов на текущий квартал рассматриваются на заседании Комиссии.

6.3.2. При необходимости дополнить квартальный план новыми мероприятиями, либо изменить состав или порядок мероприятий в плане на оставшийся период квартала – квартальный план изменяется.

6.3.3. Мероприятия, размещенные в старой версии плана, не переносятся в новую. Новая версия должна содержать только мероприятия, актуальные до конца квартала. На обложке новой версии плана указывается с какой даты он действует.

6.3.4. Обновленная версия утверждается руководителем Администрации и незамедлительно, в течение одного дня, передается ответственному лицу, старая версия изымается. На обложке старой версии квартального плана делается пометка о его неактуальности, начиная с указанной даты.

### **6.4. Обращение ответственного с квартальным планом**

6.4.1. Ответственный за выполнение мероприятий квартального плана обязан не реже чем раз в рабочую неделю уточнять состав квартального плана с целью подготовки к ним, а также выполнять все мероприятия, запланированные на текущий день.

6.4.2. Ответственный обязан обеспечить сохранность находящегося у него квартального плана и предоставлять его по требованию Комиссии (но не более чем на один день).

6.4.3. По окончании квартала ответственный обязан передать план председателю Комиссии.

## **7. Контроль выполнения плановых мероприятий**

7.1. Контроль выполнения плановых мероприятий осуществляется ежеквартально Комиссией.

7.2. Для контроля Комиссией привлекается соответствующий годовой план (в том числе его старые версии, при необходимости), квартальный план (при его наличии) и Журнал.

7.3. Осуществляется контроль выполнения мероприятий за истекший квартал.

7.4. В случае невыполнения без уважительных причин запланированных мероприятий, ответственное лицо может быть подвергнуто дисциплинарному взысканию.

## **8. Ответственность**

8.1. Все лица, указанные в пункте 1.7 настоящего регламента, в случае нарушения его положений, несут персональную ответственность в соответствии с действующим законодательством РФ.

Приложения:

1. Типовая форма протокола проведения внутренней проверки условий обработки и защиты персональных данных на 2 л. в 1 экз.

2. Типовая форма акта проведения внутренней проверки условий обработки и защиты персональных данных на 9 л. в 1 экз.

Приложение № 1  
к регламенту проведения внутренних мероприятий  
по контролю обеспечения защиты персональных  
данных

**Типовая форма протокола проведения внутренней проверки условий обработки и защиты  
персональных данных**

**Администрация МР «Сысольский»**

**ПРОТОКОЛ**

«\_\_» \_\_\_\_\_ 20\_\_ г.

№ \_\_\_\_\_

с. Визинга

Проведения внутренней проверки условий  
обработки и защиты персональных данных

Председатель:

Члены комиссии:

**ПРОВЕРЯЕМЫЕ ОБЪЕКТЫ:**

1. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
2. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
3. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

1.Дата проверки объекта:

«\_\_» \_\_\_\_\_ 20\_\_ г.

Выявленные нарушения:

---

---

---

---

---

---

Постановили:

---

---

---

---

---

---

Примечание:

2.Дата проверки объекта:

«\_»\_\_\_\_\_20\_\_г.

Выявленные нарушения:

---

---

---

---

---

---

Постановили:

---

---

---

---

---

---

Примечание:

3.Дата проверки объекта:

«\_»\_\_\_\_\_20\_\_г.

Выявленные нарушения:

---

---

---

---

---

---

Постановили:

---

---

---

---

---

---

Примечание:

Председатель комиссии \_\_\_\_\_ / \_\_\_\_\_

Приложение № 1  
к регламенту проведения внутренних мероприятий  
по контролю обеспечения защиты персональных  
данных

УТВЕРЖДАЮ

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
«    » \_\_\_\_\_ 201\_ г.

АКТ №\_\_

проведения полной внутренней проверки  
условий обработки и защиты  
персональных данных

Основание: распоряжение администрации МР «Сысольский» от \_\_.\_\_.20\_\_ № \_\_\_\_ «О  
проведении полной внутренней проверки условий обработки и защиты персональных данных».

Составлен комиссией:

Председатель: \_\_\_\_\_.

Члены комиссии: \_\_\_\_\_.

\_\_\_\_\_  
\_\_\_\_\_.

Комиссия «    » \_\_\_\_\_ 201\_ года провела полную внутреннюю проверку условий  
обработки                    и                    защиты                    персональных                    данных                    в

\_\_\_\_\_  
\_\_\_\_\_, по  
адресу:  
\_\_\_\_\_.

Проверка осуществлялась в соответствии с:

- требованиями законодательства РФ о персональных данных;
- требованиями локальных нормативных актов \_\_\_\_\_.

В ходе проверки проверено:

- Локальная нормативная база;
- Организация режима защиты;
- Реализация технической защиты информации;
- Обучение и ознакомление работников;
- Регулярность проведения периодических проверочных мероприятий.

В ходе проверки:

1. Установлены следующие оценки: 0 баллов \_\_\_\_\_;  
1 балл \_\_\_\_\_;  
2 балла \_\_\_\_\_;  
3 балла \_\_\_\_\_.

Итоговая оценка: \_\_\_\_\_.

Протокол проведения полной внутренней проверки условий обработки и защиты персональных данных прилагается.

2. Выявлены нарушения, подлежащие устранению:

- \_\_\_\_\_;
- \_\_\_\_\_;
- \_\_\_\_\_;
- \_\_\_\_\_;
- \_\_\_\_\_;
- \_\_\_\_\_.

По итогам проверки проведен анализ нарушений и разработаны меры по их устранению:

- \_\_\_\_\_;
- \_\_\_\_\_;
- \_\_\_\_\_;
- \_\_\_\_\_;
- \_\_\_\_\_;
- \_\_\_\_\_.

Протокол анализа нарушений, выявленных в ходе проведения полной внутренней проверки условий обработки и защиты персональных данных прилагается.

Меры по устранению нарушений полностью/(частично) выполнены, проверка эффективности проведена, повторная проверка проведена. Все нарушения устранены/(Нарушения не устранены, требуются дополнительные меры по их устранению).

Составлен в 2-х экземплярах:

1-ый экземпляр – \_\_\_\_\_;

2-ой экземпляр – \_\_\_\_\_.

Председатель комиссии:

\_\_\_\_\_ / \_\_\_\_\_ /

Члены комиссии:

\_\_\_\_\_ / \_\_\_\_\_ /

\_\_\_\_\_ / \_\_\_\_\_ /

\_\_\_\_\_ / \_\_\_\_\_ /

Приложение №1  
к акту проведения полной внутренней проверки  
условий обработки и защиты персональных данных

**ПРОТОКОЛ**

от \_\_.\_\_.20\_\_

с. Визинга

№ \_\_\_\_\_

Проведения полной внутренней проверки  
условий обработки и защиты  
персональных данных

Настоящий протокол составлен в том, что «      » \_\_\_\_\_ 201\_\_ г. постоянно действующей комиссией по защите персональных данных, под руководством председателя комиссии \_\_\_\_\_ проведена полная внутренняя проверка условий обработки                      и                      защиты                      персональных                      данных  
в \_\_\_\_\_

\_\_\_\_\_ (далее – \_\_\_\_\_), по адресу:  
\_\_\_\_\_.

В ходе проверки оценивалась локальная нормативная база \_\_\_\_\_, организация режима защиты, реализация технической защиты персональных данных, обучение и ознакомление работников и регулярность проведения плановых контролирующих мероприятий.

Оценки выставлялись следующим образом:

- критерий полностью соответствует действующим нормам и выполняется – 3 балла;
- критерий полностью соответствует действующим нормам, но не выполняется – 2 балла;
- критерий не полностью соответствует действующим нормам, но выполняется – 2 балла;
- критерий не полностью соответствует действующим нормам и не выполняется – 1 балл;
- критерий не соответствует действующим нормам, но выполняется – 1 балл;
- критерий не соответствует действующим нормам и не выполняется – 0 баллов.

Результаты оценки содержатся в таблице 1.

Таблица 1 – Оценки

№	Критерий	Оценка				Примечание
		3	2	1	0	
<b>Локальная нормативная база</b>						
1.	Полнота организационно-распорядительной документации по режиму защиты персональных данных					
2.	Актуальность перечня обрабатываемых персональных данных					
3.	Полнота содержащихся сведений в типовых формах					
4.	Актуальность документации об организации режима защиты персональных данных					
5.	Актуальность технической документации об организации режима обработки и защиты персональных данных					
6.	Наличие введенных журнальных форм по различным видам учета					
<b>Организация режима защиты</b>						
7.	Назначение ответственного за соблюдение режима защиты персональных данных					
8.	Организация режима допуска в помещения, где обрабатываются персональные данные					
9.	Организация разграничения прав доступа к информационным системам персональных данных					
10.	Организация архивного хранения документов, содержащих персональные данные					
11.	Публикация политики Учреждения в отношении обработки персональных данных в общедоступном месте					
12.	Назначение ответственного за регистрацию запросов от субъектов персональных данных					
13.	Назначение ответственных за ведение журнальных форм					



14.	Организация учета средств защиты информации, криптографических средств					
15.	Организация учета съемных носителей информации					
16.	Организация учета входящих и исходящих документов, содержащих персональные данные					
<b><i>Техническая защита информации</i></b>						
17.	Исполнение требований по реализации подсистемы антивирусной защиты					
18.	Исполнение требований по реализации подсистемы разграничения прав доступа					
19.	Исполнение требований по реализации подсистемы резервного копирования					
20.	Исполнение требований по реализации подсистемы межсетевое экранирование					
21.	Исполнение требований по реализации подсистемы защиты от несанкционированного доступа (в т.ч. подсистема парольной защиты)					
22.	Исполнение требований по реализации подсистемы контроля съемных носителей информации					
23.	Контроль установленного ПО, не связанного с должностными обязанностями					
<b><i>Обучение и ознакомление персонала</i></b>						
24.	Проведения обучения персонала на предмет знаний основ работы с персональными данными					
25.	Ознакомление персонала с действующей документацией об организации режима защиты персональных данных					
26.	Ознакомление с инструкциями о порядке работы с персональными данными					
27.	Обучение руководителей структурных подразделений о порядке обработки персональных данных в структурном подразделении в соответствии с функциями и задачами					
<b><i>Исполнение обязательных проверочных мероприятий</i></b>						

28.	Проведение регулярных проверок в соответствии с планом мероприятий					
29.	Осуществление проверок знаний о порядке организации обработки и защиты персональных данных					
<b>Итого: количество ответов по столбцам</b>						
<b>Количество баллов по столбцам</b>						
Фактическое кол-во баллов / / Возможное кол-во баллов						Итоговая оценка:

Председатель комиссии: \_\_\_\_\_ / \_\_\_\_\_ /

Члены комиссии:  
 \_\_\_\_\_ / \_\_\_\_\_ /  
 \_\_\_\_\_ / \_\_\_\_\_ /  
 \_\_\_\_\_ / \_\_\_\_\_ /

Приложение №2  
к акту проведения полной внутренней проверки  
условий обработки и защиты персональных данных

**ПРОТОКОЛ**

от \_\_. \_\_.20\_\_

с. Визинга

№ \_\_\_\_\_

Анализа нарушений, выявленных  
в ходе проведения полной внутренней проверки  
условий обработки и защиты персональных данных

1. Исходные данные: протокол проведения полной внутренней проверки условий обработки и защиты персональных данных от \_\_. \_\_.201\_\_ № \_\_\_\_\_.

Описание выявленных нарушений:

1.1. \_\_\_\_\_;

1.2. \_\_\_\_\_;

1.3. \_\_\_\_\_;

1.4. \_\_\_\_\_;

1.5. \_\_\_\_\_;

1.6. \_\_\_\_\_.

Результаты анализа существования (актуальности) нарушений:

1.1. \_\_\_\_\_;

1.2. \_\_\_\_\_;

1.3. \_\_\_\_\_;

1.4. \_\_\_\_\_;

1.5. \_\_\_\_\_;

1.6. \_\_\_\_\_.

2. Меры по устранению нарушений целесообразны:

\_\_\_\_\_ / \_\_\_\_\_ /  
(да/нет)                      подпись                      инициалы, фамилия

3. Меры по устранению нарушений «Утверждаю»:

\_\_\_\_\_ / \_\_\_\_\_ /

подпись                      инициалы, фамилия

№	Содержание мер по устранению нарушений	Ответственный	Срок	Отметка о выполнении
1.				
2.				
3.				
4.				
5.				
6.				

4. \_\_\_\_\_ провести проверку эффективности в срок до «    » \_\_\_\_\_ 201\_ г.  
 (ответственному)

\_\_\_\_\_.

(способ и (или) метод проверки)

5. Проверка эффективности проведена: Дата \_\_\_\_\_ Результат \_\_\_\_\_

\_\_\_\_\_.

6. Необходимы дополнительные меры по устранению нарушений:

\_\_\_\_\_ / \_\_\_\_\_ /  
 (да/нет)                      подпись                      инициалы, фамилия

- \_\_\_\_\_ ;
- \_\_\_\_\_ ;
- \_\_\_\_\_ ;
- \_\_\_\_\_ ;
- \_\_\_\_\_ ;

Меры по устранению нарушений согласованы и составлены.

Председатель комиссии: \_\_\_\_\_ / \_\_\_\_\_ /

Члены комиссии: \_\_\_\_\_ / \_\_\_\_\_ /

\_\_\_\_\_ / \_\_\_\_\_ /

\_\_\_\_\_ /

/

\_\_\_\_\_ /

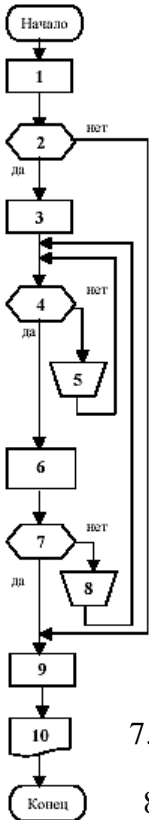
/

Приложение №3  
к акту проведения полной внутренней проверки  
условий обработки и защиты персональных  
данных

**АЛГОРИТМ**

проведения полной внутренней проверки условий обработки и защиты персональных данных

Полная внутренняя проверка условий обработки и защиты персональных данных в проводится поэтапно:



0. Началом работы является приказ заместителя начальника Учреждения о проведении полной внутренней проверки условий обработки и защиты персональных данных;
1. Анализ выявленных нарушений, установление причин;
2. Оценка необходимости разработки мер по устранению нарушений;
3. Разработка мер по устранению нарушений;
4. Согласование и утверждение мер по устранению нарушений;
5. Доработка мер по устранению нарушений;
6. Внедрение мер по устранению нарушений;
7. Проверка эффективности мер по устранению нарушений;
8. Разработка дополнительных мер по устранению нарушений;
9. Утверждение протокола анализа нарушений, выявленных в ходе проведения полной внутренней проверки условий обработки и защиты персональных данных;
10. Протокол анализа нарушений, выявленных в ходе проведения полной внутренней проверки условий обработки и защиты персональных данных.