АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ «МЕЛЕКЕССКИЙ РАЙОН» УЛЬЯНОВСКОЙ ОБЛАСТИ

Р А С П О Р Я Ж Е Н И Е

18.01.2021

№10-р

Экз.№ _____

г.Димитровград

О защите информации в администрации муниципального образования «Мелекесский район» Ульяновской области

В соответствии с требованиями Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных, Постановление 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», Постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»:

1. Возложить обязанности по защите информации:

1.1. Назначить ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных консультанта по информационным технологиям и защите информации - Грешкова А.А.

1.2. Назначить ответственными за эксплуатацию информационных систем персональных данных руководителей отделов и управлений администрации муниципального образования «Мелекесский район» Ульяновской области.

1.3. Утвердить перечень должностей, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах

персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей, согласно приложению 1 к настоящему распоряжению.

1.4. Утвердить перечень должностей, ведущих обработку персональных данных без использования средств автоматизации, согласно приложению 2 к настоящему распоряжению.

1.5. Утвердить перечень лиц, ответственных за обезличивание персональных данных, согласно приложению 3 к настоящему распоряжению.

2. Создать комиссию по защите информации:

2.1. Утвердить состав комиссии по защите информации, согласно приложению 4 к настоящему распоряжению.

2.2. Утвердить положение о комиссии по защите информации, согласно приложению 5 к настоящему распоряжению.

3. Утвердить типовые журналы по защите информации, согласно приложению 6 к настоящему распоряжению:

3.1. ЖУРНАЛ учета машинных носителей персональных данных (стационарные носители).

3.2. ЖУРНАЛ учета машинных носителей персональных данных (съемные носители).

3.3. ЖУРНАЛ учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных.

3.4. ЖУРНАЛ учета средств защиты информации.

3.5. ЖУРНАЛ учета средств криптографической защиты информации.

3.6. ЖУРНАЛ учета согласий субъектов персональных данных .

3.7. ЖУРНАЛ учета хранилищ.

3.8. ЖУРНАЛ учета персональных идентификаторов и электронных ключей (для администратора зала).

3.9. ЖУРНАЛ учета выдачи персональных идентификаторов и электронных ключей (для администратора информационной безопасности).

3.10. ЖУРНАЛ учета обращений субъектов персональных данных по вопросам обработки персональных данных.

3.11. ЖУРНАЛ антивирусных проверок информационных систем.

3.12. ЖУРНАЛ учета выявленных инцидентов информационной безопасности.

3.13. ЖУРНАЛ учета передачи персональных данных.

3.14. ЖУРНАЛ периодического тестирования средств защиты информации.

3.15. ЖУРНАЛ учета проверок электронных журналов обращений к информационным системам персональных данных.

3.16. ЖУРНАЛ уничтожения носителей персональных данных.

4. Утвердить положение об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения, согласно приложению 7 к настоящему распоряжению.

5. Утвердить инструкции и правила по защите информации:

5.1. Правила рассмотрения запросов субъектов персональных данных, согласно приложению 8 к настоящему распоряжению.

5.2. Правила работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей, согласно приложению 9 к настоящему распоряжению;

5.3. Инструкцию ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных, согласно приложению 10 к настоящему распоряжению;

5.4. Инструкцию по организации резервного копирования, согласно приложению 11 к настоящему распоряжению;

5.5. Инструкцию по организации антивирусной защиты, согласно приложению 12 к настоящему распоряжению;

5.6. Инструкцию по проверке электронного журнала обращений к информационной системе персональных данных, согласно приложению 13 к настоящему распоряжению;

5.7. Инструкцию по обращению со средствами криптографической защиты информации, согласно приложению 14 к настоящему распоряжению;

5.8. Инструкцию по обработке персональных данных без использования средств автоматизации, согласно приложению 15 к настоящему распоряжению;

5.9. Правила работы с обезличенными данными, согласно приложению 16 к настоящему распоряжению;

5.10. Инструкцию по работе с инцидентами информационной безопасности, согласно приложению 17 к настоящему распоряжению;

5.11. Инструкцию ответственного за эксплуатацию информационных систем персональных данных, согласно приложению 18 к настоящему распоряжению.

6. Утвердить план мероприятий по защите информации, согласно приложению 19 к настоящему распоряжению.

7. Настоящее распоряжение вступает в силу с момента его подписания.

8. Контроль исполнения настоящего распоряжения возложить на руководителя аппарата администрации муниципального образования «Мелекесский район» Ульяновской области - Боеву Г.А.

Глава администрации С.А. Сандрюков

Приложение 1
к распоряжению администрации
муниципального образования
«Мелекесский район»
от _____ № ___

Перечень должностей, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей

1. Глава администрации муниципального образования «Мелекесский район» Ульяновской области.
2. Первый заместитель Главы администрации муниципального образования «Мелекесский район» Ульяновской области.
3. Руководитель аппарата администрации муниципального образования «Мелекесский район» Ульяновской области.
4. Начальник отдела правового обеспечения администрации муниципального образования «Мелекесский район» Ульяновской области.
5. Начальник отдела муниципальной службы, кадров и архивного дела администрации муниципального образования «Мелекесский район» Ульяновской области.
6. Главный специалист отдела муниципальной службы, кадров и архивного дела администрации муниципального образования «Мелекесский район» Ульяновской области.
7. Консультант по мобподготовке администрации муниципального образования «Мелекесский район» Ульяновской области.
8. Начальник отдела по делам ГО, ЧС и взаимодействию с правоохранительными органами администрации муниципального образования «Мелекесский район» Ульяновской области.
9. Главный специалист по делам ГО, ЧС отдела по делам ГО, ЧС и взаимодействию с правоохранительными органами администрации муниципального образования «Мелекесский район» Ульяновской области.
10. Начальник отдела бухгалтерского учёта и отчётности администрации муниципального образования «Мелекесский район» Ульяновской области.
11. Главный специалист отдела бухгалтерского учёта и отчётности администрации муниципального образования «Мелекесский район» Ульяновской области.
12. Начальник организационно-протокольного отдела администрации муниципального образования «Мелекесский район» Ульяновской области
13. Главный специалист организационно-протокольного отдела администрации муниципального образования «Мелекесский район» Ульяновской области.

Приложение 2
к распоряжению администрации
муниципального образования
«Мелекесский район»
от _____ № ___

Перечень должностей, ведущих обработку персональных данных без использования средств автоматизации

1. Глава администрации муниципального образования «Мелекесский район» Ульяновской области.
2. Первый заместитель Главы администрации муниципального образования «Мелекесский район» Ульяновской области.
3. Руководитель аппарата администрации муниципального образования «Мелекесский район» Ульяновской области.
4. Начальник отдела правового обеспечения администрации муниципального образования «Мелекесский район» Ульяновской области.
5. Начальник отдела муниципальной службы, кадров и архивного дела администрации муниципального образования «Мелекесский район» Ульяновской области.
6. Главный специалист отдела муниципальной службы, кадров и архивного дела администрации муниципального образования «Мелекесский район» Ульяновской области.
7. Консультант по мобподготовке администрации муниципального образования «Мелекесский район» Ульяновской области.
8. Начальник отдела по делам ГО, ЧС и взаимодействию с правоохранительными органами администрации муниципального образования «Мелекесский район» Ульяновской области.
9. Главный специалист по делам ГО, ЧС отдела по делам ГО, ЧС и взаимодействию с правоохранительными органами администрации муниципального образования «Мелекесский район» Ульяновской области.
10. Начальник отдела бухгалтерского учёта и отчётности администрации муниципального образования «Мелекесский район» Ульяновской области.
11. Главный специалист отдела бухгалтерского учёта и отчётности администрации муниципального образования «Мелекесский район» Ульяновской области.
12. Начальник организационно-протокольного отдела администрации муниципального образования «Мелекесский район» Ульяновской области
13. Главный специалист организационно-протокольного отдела администрации муниципального образования «Мелекесский район» Ульяновской области.

Приложение 3
к распоряжению администрации
муниципального образования
«Мелекесский район»
от _____ № ___

Перечень лиц, ответственных за обезличивание персональных данных

1. Глава администрации муниципального образования «Мелекесский район» Ульяновской области.
2. Первый заместитель Главы администрации муниципального образования «Мелекесский район» Ульяновской области.
3. Руководитель аппарата администрации муниципального образования «Мелекесский район» Ульяновской области.
4. Начальник отдела правового обеспечения администрации муниципального образования «Мелекесский район» Ульяновской области.
5. Начальник отдела муниципальной службы, кадров и архивного дела администрации муниципального образования «Мелекесский район» Ульяновской области.
6. Главный специалист отдела муниципальной службы, кадров и архивного дела администрации муниципального образования «Мелекесский район» Ульяновской области.
7. Консультант по мобподготовке администрации муниципального образования «Мелекесский район» Ульяновской области.
8. Начальник отдела по делам ГО, ЧС и взаимодействию с правоохранительными органами администрации муниципального образования «Мелекесский район» Ульяновской области.
9. Главный специалист по делам ГО, ЧС отдела по делам ГО, ЧС и взаимодействию с правоохранительными органами администрации муниципального образования «Мелекесский район» Ульяновской области.
10. Начальник отдела бухгалтерского учёта и отчётности администрации муниципального образования «Мелекесский район» Ульяновской области.
11. Главный специалист отдела бухгалтерского учёта и отчётности администрации муниципального образования «Мелекесский район» Ульяновской области.
12. Начальник организационно-протокольного отдела администрации муниципального образования «Мелекесский район» Ульяновской области
13. Главный специалист организационно-протокольного отдела администрации муниципального образования «Мелекесский район» Ульяновской области.

Приложение 4
к распоряжению администрации
муниципального образования
«Мелекесский район»
от _____ № ___

Состав комиссии по защите информации

Председатель комиссии	Боева Г.А. - руководитель аппарата администрации муниципального образования «Мелекесский район» Ульяновской области.
Члены комиссии	Харлова Д.Л. - начальник отдела муниципальной службы, кадров и архивного дела администрации муниципального образования «Мелекесский район» Ульяновской области.
	Пайметова Т.В. - начальник организационно-протокольного отдела администрации муниципального образования «Мелекесский район» Ульяновской области.
	Губанова Е.Н. - начальник отдела правового обеспечения администрации муниципального образования «Мелекесский район» Ульяновской области.
Секретарь	Грешков А.А. - консультант по информационным технологиям и защиты информации администрации муниципального образования «Мелекесский район» Ульяновской области.

Приложение 5
к распоряжению администрации
муниципального образования
«Мелекесский район»
от _____ № ___

ПОЛОЖЕНИЕ
о комиссии по защите информации

1. Общие положения

Настоящее Положение определяет основные задачи, порядок формирования, полномочия и ответственность комиссии.

2. Основные задачи комиссии

Основными задачами комиссии являются:

Сбор и анализ исходных данных по информационным системам персональных данных, по автоматизированным системам управления информационной инфраструктурой администрации муниципального образования «Мелекесский район» Ульяновской области;

Определение значений параметров для проведения классификации информационных систем в соответствии с Приказом ФСТЭК России от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

Определение значений параметров для установления уровня защищенности персональных данных в соответствии с постановлением Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Определение класса защищенности информационных систем персональных данных администрации муниципального образования «Мелекесский район» Ульяновской области на основании собранных данных;

Определение уровня защищенности персональных данных при их обработке в информационных системах персональных данных;

Анализ текущего состояния информационной безопасности в администрации муниципального образования «Мелекесский район» Ульяновской области;

Выявление, оценка и прогнозирование возможных угроз;

Анализ выполнения в администрации муниципального образования «Мелекесский район» Ульяновской области федеральных законов, указов Президента Российской Федерации, постановлений Правительства Российской Федерации, федеральных и региональных целевых программ, направленных на обеспечение информационной безопасности;

Разработка предложений по взаимодействию структурных подразделений администрации муниципального образования «Мелекесский район» Ульяновской области в ходе реализации решений Комиссии по обеспечению информационной безопасности и оценке их эффективности;

Рассмотрение вопросов организационного и материально-технического обеспечения информационной безопасности в администрации муниципального образования «Мелекесский район» Ульяновской области;

Рассмотрение предложений структурных подразделений администрации муниципального образования «Мелекесский район» Ульяновской области по вопросам обеспечения информационной безопасности;

Рассмотрение других вопросов, относящихся к защите информации.

3. Порядок формирования комиссии

Комиссия формируется из числа штатных сотрудников администрации муниципального образования «Мелекесский район» Ульяновской области, участвующих в процессе обработки персональных данных.

В состав Комиссии входит не менее четырех человек – членов Комиссии, в их числе – председатель Комиссии.

В случае изменения состава Комиссии, в протокол заседания комиссии по защите информации вносится соответствующая информация.

4. Полномочия комиссии

Для осуществления задач, указанных в разделе 2 настоящего Положения, Комиссия имеет право:

Получать необходимые сведения у всех работников администрации муниципального образования «Мелекесский район» Ульяновской области, участвующих в обработке персональных данных.

Просматривать электронные базы данных и бумажные носители, содержащие персональные данные, с целью выявления состава обрабатываемых персональных данных.

Отслеживать технологический процесс обработки персональных данных.

Выявлять или получать готовые сведения о структуре локальной вычислительной сети администрации муниципального образования «Мелекесский район» Ульяновской области.

Определять или получать готовые сведения о наличии и способах доступа к сетям общего пользования.

Определять или получать готовые сведения о технических и программных средствах обработки персональных данных.

Определять или получать готовые сведения об условиях, местах и способах передачи персональных данных в сторонние организации.

5. Отчетность комиссии

Комиссия при выполнении своих задач должна составить протокол заседания комиссии. Пример протокола - приложение 1 к настоящему положению. Председателя следит за ходом заседания, оглашает повестку дня, проводит голосование. Протокол после окончания совещания обязательно подписывается секретарем и председателем собрания, а также

при необходимости его участниками, которые таким образом подтверждают то, что все внесенные в него сведения верны.

В результате своей деятельности Комиссия должна составить Акт(ы) определения уровня защищенности персональных данных и класса защищенности информационных систем персональных данных, согласно приложению 2 к настоящему положению.

Определить Перечень информационных систем персональных данных, согласно приложению 3 к настоящему положению, а также Перечень обрабатываемых персональных данных в информационных систем персональных данных, согласно приложению 4 к настоящему положению.

В зависимости от появления новых угроз провести анализ и пересмотр имеющихся угроз безопасности персональных данных.

Приложение 1
к Положению о комиссии
по защите информации

ПРОТОКОЛ № 1
заседания комиссии по защите информации

Дата и время проведения _____
Место проведения _____

Председатель комиссии _____ ФИО
Члены комиссии
_____ ФИО
_____ ФИО
Секретарь _____ ФИО

Повестка дня

Определение информационных систем персональных данных (далее - ИСПДн), принадлежащих администрации муниципального образования «Мелекесский район» Ульяновской области.

1. Слушали: _____ доложил(а) исходные данные об ИСПДн «Наименование».

Выступил(а): _____предложил(а) утвердить акт определения уровня защищенности персональных данных и класса защищённости ИСПДн «Наименование».

Постановили:

Утвердить акт определения уровня защищенности персональных данных и класса защищённости ИС «Наименование».

2. Слушали: _____ доложил(а) исходные данные об ИСПДн «Наименование».

Выступил(а): _____предложил(а) утвердить акт определения уровня защищенности персональных данных и класса защищённости ИСПДн «Наименование».

Постановили:

Утвердить акт определения уровня защищенности персональных данных и класса защищённости ИС «Наименование».

Председатель комиссии _____ ФИО
Члены комиссии
ФИО
_____ ФИО
_____ ФИО
Секретарь _____ ФИО

Приложение 2
к Положению о комиссии
по защите информации

АКТ
определения уровня защищенности персональных данных при их обработке в информационных системах персональных данных «Наименование» и класса защищенности информационной системы «Наименование»

Председатель комиссии _____ ФИО
Члены комиссии
_____ ФИО
_____ ФИО
_____ ФИО

Рассмотрев исходные данные об информационной системе персональных данных (далее - ИСПДн), комиссия определила:

– Категории персональных данных обрабатываемых в ИСПДн: в информационной системе обрабатываются специальные категории персональных данных;

– Категории субъектов: персональные данные субъектов персональных данных, не являющихся сотрудниками оператора;

– Объем обрабатываемых персональных данных: менее 100 000;

– Тип актуальных угроз: для информационной системы актуальны угрозы 3-го типа;

– Уровень значимости информации: информация имеет низкий уровень значимости УЗ 3;

– Масштаб информационной системы: информационная система имеет объектовый масштаб.

Комиссия решила, в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а так же в соответствии с приказом ФСТЭК Российской Федерации от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и на основании анализа исходных данных, необходимо обеспечить третий уровень защищенности (УЗ 3) персональных данных и установить третий класс защищенности информационной системы (К3).

Результат оценки вреда:

Для информационной системы актуальны угрозы 3-го типа.

Уровень значимости информации определен степенью возможного ущерба для обладателя информации от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации, руководствуясь следующей формулой:

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)], где степень возможного ущерба определяется обладателем информации.

Комиссия утвердила следующее:

УЗ = [(конфиденциальность, низкая степень ущерба) (целостность, низкая степень ущерба) (доступность, низкая степень ущерба)] – таким образом, комиссия установила низкий уровень значимости (УЗ 3) (возможны незначительные негативные последствия).

Председатель комиссии _____ ФИО
Члены комиссии
_____ ФИО
_____ ФИО
_____ ФИО

«___»_____20___ г.

Приложение 3

к Положению о комиссии
по защите информации

Перечень информационных систем персональных данных

Наименование	Адрес расположения

Приложение 4
к Положению о комиссии
по защите информации

ПЕРЕЧЕНЬ
обрабатываемых персональных данных

Таблица 1. Перечень обрабатываемых персональных данных

Группа персональных данных	Состав персональных данных	Цели обработки персональных данных
Общие сведения о гражданах		
Общие сведения о работниках		
Сведения о родственниках работника		

Таблица 2. Правовое основание обработки персональных данных и сроки их хранения

Группа персональных данных	Основание для обработки персональных данных
Общие сведения о гражданах	
Общие сведения о работниках	
Сведения о родственниках работника	

Приложение 6
к распоряжению администрации
муниципального образования
«Мелекесский район»
от _____ № ___

ЖУРНАЛ
учета машинных носителей персональных данных (стационарные носители)

№ п/п	Регистрационный номер	Тип и ёмкость	Дата и место установки (использования)	Ответственное должностное лицо (Ф.И.О)

ЖУРНАЛ
учета машинных носителей персональных данных (съемные носители)

№ п/п	Регистрационный номер	Тип и ёмкость	Получил (Ф.И.О, дата, подпись)	Сдал (Ф.И.О, дата, подпись)	Место хранения	Ответственное должностное лицо (Ф.И.О)

ЖУРНАЛ
учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных

№ п/п	Сведения о допуске к персональным данным				Сведения о прекращении допуска к персональным данным	
	Наименование информационной системы персональных данных/способ обработки ПДн	ФИО, должность получившего допуск	Дата и номер приказа о допуске	Дата и подпись допускаемого лица	Дата и номер приказа о прекращении допуска	Номер приказа об увольнении или дата и подпись лица об ознакомлении с документом, прекращающим допуск к ПДн

ЖУРНАЛ
учета средств защиты информации

№ п/п	Индекс и наименование средства защиты информации	Серийный (заводской) номер	Номер специального защитного знака	Наименование организации, установившей СЗИ	Место установки	Примечание

ЖУРНАЛ
учета средств криптографической защиты информации

№ п/п	Наименование криптосредства, эксплуатационной и	Регистрационные номера СКЗИ, эксплуатационн	Номера экземпляров	Отметка о получении	Отметка о выдаче	Отметка о подключении (установке) СКЗИ	Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов	Примечания

				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя криптосредств	Дата и расписка в получении	Ф.И.О. пользователя криптосредств, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших Подключение (установку)	Номера аппаратных средств, в которые установлены или к кот-рым подключены криптосредства	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка Об уничтожении	

ЖУРНАЛ
учета согласий субъектов персональных данных

№ п/п	Дата и номер согласия	Ф.И.О. субъекта персональных данных

ЖУРНАЛ
учета хранилищ

№ п/п	Регистрационный (учетный) номер хранилища	Вид хранилища	Дата постановки на учет	Фамилия и подпись принявшего (ответственного), дата	Место расположения (номер помещения)	Дата и номер акта о выводе из эксплуатации	Примечание

ЖУРНАЛ
учета персональных идентификаторов и электронных ключей

№ п/п	Ф.И.О.	Получил	Дата	Время	Отметка о возврате (подпись администратора)

ЖУРНАЛ
учета выдачи персональных идентификаторов и электронных ключей

№ п/п	Ф.И.О.	№ идентификатора	Получил	Дата	Сдал	Отметка о возврате

ЖУРНАЛ
учета обращений субъектов персональных данных по вопросам обработки персональных данных

№ п/п	Дата обращения	ФИО обратившегося	Цель обращения	Отметка о предоставлении информации или отказе в ее предоставлении / дата предоставления или отказа в предоставлении информации	Подпись ответственного	Примечание

ЖУРНАЛ
антивирусных проверок информационных систем

№ п/п	Дата и время проверки	Наименование ИСПДн (составной части ИСПДн)	Какими средствами проводилась проверка	Наименование инфицированных файлов, источника поступления (носитель, организация)	Примечание (принятые меры)	Фамилия и подпись лица, проводившего проверку

ЖУРНАЛ
учета выявленных инцидентов информационной безопасности

№ п/п	Дата и время	Описание инцидента	Ответственный за реагирование на инцидент	Отметка об устранении инцидента	Дата устранения инцидента	Подпись ответственного лица	Примечание

ЖУРНАЛ
учета передачи персональных данных

№ п/п	Сведения о запрашивающем лице	Состав запрашиваемых персональных данных	Цель получения персональных данных	Отметка о передаче или отказе в передаче персональных данных	Дата передачи/отказа в передаче персональных данных	Подпись запрашивающего лица

ЖУРНАЛ
периодического тестирования средств защиты информации

№ п/п	Наименование средства защиты информации от НСД или криптосредства	Регистрационные номера СЗИ от НСД или криптосредства	Дата тестирования	Фамилия и подпись ответсвенного пользователя, проводившего тестирование	Наименование теста, используемые средства для проведения теста	Результат тестирования (успешный/неуспешный), комментарий	Дата очередного тестирования

ЖУРНАЛ
учета проверок электронных журналов обращений к информационным системам персональных данных

№ п/п	Дата проверки	Наименование ИСПДн, компьютера, технического средства	Наименование проверяемого журнала	Выявленные нарушения требований безопасности, нештатные	Подпись администратора безопасности	Примечание

				ситуации		

ЖУРНАЛ
уничтожения носителей персональных данных

№ п/п	Наименование ИСПДн, в которой уничтожаются персональные данные	Ф.И.О. субъекта, персональные данные которого подлежат уничтожению	Обоснование уничтожения	Наименование файла, и его месторасположение	Дата уничтожения	Ф.И.О. и подпись Исполнителя	Ф.И.О. и подпись ответственного за обработку персональных данных

Приложение 7
к распоряжению администрации
муниципального образования
«Мелекесский район»
от _____ № ___

Положение об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения

1. Общие положения

Положение об организации режима обеспечения безопасности помещений администрации муниципального образования «Мелекесский район» Ульяновской области (далее – Оператор), в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (далее – Положение) разработано в соответствии с Постановлением правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСБ России от 10.07.2014 №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

Защита от проникновения посторонних лиц в помещения Оператора обеспечивается организацией порядка доступа.

2. Границы контролируемой зоны

Контролируемая зона – границы пространства (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска.

План-схема контролируемой зоны помещений по адресу 433508, Ульяновская область, г. Димитровград, ул. Хмельницкого, д. 93 приведена в приложении 1 к настоящему Положению.

3. Порядок доступа в помещения

Перечень лиц, доступ которых в помещения находящиеся в пределах границы контролируемой зоны, необходим для выполнения ими служебных (трудовых обязанностей) приведен в приложении 1 к настоящему распоряжению.

Неконтролируемое пребывание лиц в помещениях, находящихся в пределах границы контролируемой зоны, указанных в п. 3.1 настоящего Положения разрешено в период рабочего времени в соответствии с утвержденным графиком работы Оператора, либо вне периода рабочего времени с письменного разрешения ответственного за организацию обработки персональных данных или ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных.

Лица, не указанные в приложении 1 настоящего распоряжения, допускаются в помещения в присутствии лиц, имеющих право пребывания в данных помещениях.

Приложение 1
к Положению
об организации режима
обеспечения безопасности
помещений

План-схема границ контролируемой зоны

Приложение 8
к распоряжению администрации
муниципального образования
«Мелекесский район»
от _____ № ___

Правила рассмотрения обращений и запросов субъектов персональных данных или их законных представителей в администрации муниципального образования «Мелекесский район» Ульяновской области

1. Общие положения

Правила рассмотрения обращений и запросов субъектов персональных данных или их законных представителей в администрации муниципального образования «Мелекесский район» Ульяновской области (далее – Правила) разработаны в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (далее – Федеральный закон №152-ФЗ), Федеральным законом от 02.05.2006 №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», постановлением 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 и муниципальными органами» и определяют порядок организации работы по приему, регистрации и рассмотрению поступивших в администрацию муниципального образования «Мелекесский район» Ульяновской области (далее – Администрация) обращений и запросов субъектов персональных данных или их представителей.

Основные понятия, используемые в настоящих Правилах, соответствуют основным понятиям, установленным Федеральным законом от 27.07.2006 года №152-ФЗ «О персональных данных».

2. Прием, регистрация и порядок рассмотрения обращений и запросов

Сведения, касающиеся обработки персональных данных субъекта персональных данных, предоставляются Администрации субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его представителя.

Запрос может быть подан лично, письменно или направлен в форме электронного документа, подписанного электронной подписью.

Информация об Администрации, включая информацию о месте нахождения, графике работы, контактных телефонах, а также о порядке обработки персональных данных, размещается:

а) на стендах, расположенных в помещениях, занимаемых Администрацией;

б) на официальном сайте Администрации: http://www.adm-melekess.ru/

Прием субъектов персональных данных или их представителей ведется сотрудниками, ответственными за прием и регистрацию обращений.

При приеме субъект персональных данных или его представитель предъявляет документ, удостоверяющий его личность, а также документ, подтверждающий полномочия представителя (в случае обращения представителя).

Содержание обращения субъекта персональных данных заносится в журнал личного приёма, затем делается соответствующая запись в «Журнале учета обращений и запросов субъектов персональных данных по вопросам обработки персональных данных», согласно приложению №1 к настоящим Правилам.

Все поступившие запросы регистрируются в день их поступления. На запросе проставляется входящий номер и дата регистрации. Днем обращения считается дата регистрации запроса субъекта персональных данных или его представителя.

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Администрацией (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Администрацией, подпись субъекта персональных данных.

Рассмотрение запросов субъектов персональных данных или их представителей осуществляется сотрудниками Администрации, наделенными полномочиями по рассмотрению и подготовке ответов (далее – уполномоченные сотрудники Администрации).

При рассмотрении обращений и запросов обеспечивается:

а) объективное, всестороннее и своевременное рассмотрение обращений и запросов;

б) принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов персональных данных;

в) направление письменных ответов по существу обращений и запросов.

В случае поступления запроса субъекта персональных данных на ознакомление с его персональными данными, обрабатываемыми в Администрации, при условии подтверждения факта обработки и в отсутствие ограничений на доступ субъекта к его персональным данным, Администрацией предоставляется следующая информация:

подтверждение факта обработки персональных данных;

правовые основания и цели обработки персональных данных;

цели и применяемые способы обработки персональных данных;

место нахождения Администрации, сведения о лицах (за исключением работников), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Администрацией или на основании Федерального закона №152-ФЗ;

обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом №152-ФЗ;

сроки обработки персональных данных, в том числе сроки их хранения;

порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом №152-ФЗ;

информацию об осуществленной или о предполагаемой трансграничной передаче данных;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Администрации, если обработка поручена или будет поручена такому лицу;

иные сведения, предусмотренные Федеральным законом №152-ФЗ или другими федеральными законами.

Выполнение данного запроса осуществляется уполномоченными сотрудниками Администрации в порядке и в сроки, предусмотренные статьями 14, 20 Федерального закона №152-ФЗ.

Возможность ознакомления с персональными данными предоставляется субъекту персональных данных безвозмездно.

Администрация вправе отказать субъекту персональных данных в предоставлении информации, касающейся обработки его персональных данных, в следующих случаях:

в случае нарушения требований к содержанию запроса, сформулированных в части 3 статьи 14 Федерального закона №152-ФЗ;

в случае поступления повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона №152-ФЗ;

в случае наличия ограничений прав субъекта на доступ к персональным данным, предусмотренных частью 8 статьи 14 Федерального закона №152-ФЗ, Администрация разъясняет субъекту персональных данных причину отказа и предоставляет доказательства обоснованности отказа.

При обращении субъекта персональных данных с требованием об уточнении его персональных данных, их блокировании или уничтожении, уполномоченные сотрудники Администрация осуществляют проверку порядка обработки персональных данных субъекта, а также соблюдение принципов обработки.

В случае подтверждения информации о том, что обрабатываемые в Администрации персональные данные субъекта являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также в случае выявления иной неправомерной обработки персональных данных, уполномоченными сотрудниками Администрации принимаются необходимые меры по устранению нарушений в порядке и в сроки, предусмотренные статьей 21 Федерального закона №152-ФЗ.

Об устранении допущенных нарушений Администрация уведомляет субъекта персональных данных.

Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы.

При рассмотрении обращений и запросов субъектов персональных данных в Администрации применяются типовые формы в соответствии с приложениями 2 – 9 к настоящим Правилам.

3. Контроль за соблюдением порядка рассмотрения обращений и запросов субъектов персональных данных или их представителей

Ответственный за организацию обработки персональных данных осуществляет контроль за соблюдением установленного законодательством и настоящими Правилами порядка рассмотрения обращений и запросов.

При осуществлении контроля проверяется законность и обоснованность принятых решений по запросам субъектам персональных данных, обращается внимание на соблюдение сроков, установленных законодательством РФ о персональных данных, на выполнение обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных, а также требований субъекта об уточнении персональных данных, их блокировании или уничтожении, и своевременность направления ответов по существу запроса субъектам персональных данных.

Нарушение установленного порядка приема, регистрации и рассмотрения обращений и запросов субъектов персональных данных влечет в отношении виновных сотрудников ответственность в соответствии с законодательством Российской Федерации.

Приложение 1
к Правилам рассмотрения
обращений и запросов
субъектов персональных
данных или их законных
представителей

Журнал учета обращений и запросов субъектов персональных данных по вопросам обработки персональных данных

№ п/п	Сведения о запрашивающем лице	Цель запроса	Краткое содержание обращения	Отметка о предоставлении информации / отказе в ее предоставлении	Причина отказа в предоставлении информации	Дата передачи /отказа в предоставлении информации	Подпись Ответственного лица	Примечание

Приложение 2
к Правилам рассмотрения
обращений и запросов
субъектов персональных
данных или их законных
представителей

В администрацию
муниципального образования
«Мелекесский район»
Ульяновской области

_____
(ФИО заявителя)

_____

_____
(наименование и реквизиты документа,
удостоверяющего личность заявителя)

заявление

Я, _____,
(Ф.И.О.)

имею следующие основания полагать, что администрацией муниципального образования «Мелекесский район» Ульяновской области осуществляется обработка сведений, содержащих мои персональные данные:

_____
(дата и номер договора/ иные сведения, подтверждающие факт осуществления обработки)

в связи с чем, в соответствии со статьей 14 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» прошу предоставить мне для ознакомления информацию, касающуюся обработки моих персональных данных, содержащую:

подтверждение факта обработки персональных данных;

правовые основания и цели обработки персональных данных;

способы обработки персональных данных;

сведения о лицах, которые имеют доступ к персональным данным (за исключением работников администрации МО «Мелекесский район» Ульяновской области);

обрабатываемые персональные данные и источник их получения

сроки обработки персональных данных, в том числе сроки их хранения;

информацию об осуществленной или о предполагаемой трансграничной передаче данных;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению администрации МО «Мелекесский район» Ульяновской области;

иные сведения:

_____

Ответ прошу направить в _____ форме по адресу_____ в срок, предусмотренный Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных».

_____ _____ / _____
(дата) (подпись) (ФИО)

Приложение 3
к Правилам рассмотрения
обращений и запросов
субъектов персональных
данных или их законных
представителей

Уведомление об обработке персональных данных

Уважаемый(ая)_____(Ф.И.О.), администрацией муниципального образования «Мелекесский район» Ульяновской области, расположенной по адресу: г. Димитровград, ул.Хмельницкого, д.93, производится обработка сведений, составляющих Ваши персональные данные:

_____
(указать сведения)

Источник получения персональных данных: _____

Персональные данные обрабатываются на основании:_____

Цели обработки: _____

Способы обработки: _____

Трансграничная передача персональных данных не осуществляется.

Перечень лиц, которые имеют доступ к информации, содержащей Ваши персональные данные, или могут получить такой доступ:

	Наименование (ФИО)	Вид доступа	Примечание

Сроки обработки и хранения персональных данных:_____

Наименования лиц, осуществляющих обработку персональных данных по поручению администрации муниципального образования «Мелекесский район» Ульяновской области:

	Наименование(ФИО)	Адрес	Примечание

По результатам обработки указанной информации нами планируется принятие следующих решений, которые будут доведены до Вашего сведения:

_____

Против принятого решения Вы имеете право заявить свои письменные возражения в _____ срок.

_____ _____ / _____
(дата) (подпись) (ФИО)

Приложение 4
к Правилам рассмотрения
обращений и запросов
субъектов персональных
данных или их законных
представителей

В администрацию
муниципального образования
«Мелекесский район»
Ульяновской области

_____
(ФИО заявителя)

_____

_____

_____
(наименование и реквизиты документа,
удостоверяющего личность заявителя)

заявление

В соответствии со статьей 14 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» прошу уточнить обрабатываемые Вами мои персональные данные в соответствии со сведениями:

_____
(указать перечень персональных данных, которые необходимо уточнить)

в связи с тем, что _____
(указать причину уточнения персональных данных)

Ответ прошу направить в _____ форме по адресу_____в срок, предусмотренный Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных».

_____ _____ / _____
(дата) (подпись) (ФИО)

Приложение 5
к Правилам рассмотрения
обращений и запросов
субъектов персональных
данных или их законных
представителей

В администрацию
муниципального образования
«Мелекесский район»
Ульяновской области

_____
(ФИО заявителя)

_____
(наименование и реквизиты документа,
удостоверяющего личность заявителя)

заявление

В соответствии со статьей 14 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», прошу заблокировать обрабатываемые Вами мои персональные данные:

_____
(указать перечень персональных данных, которые необходимо заблокировать)

на срок: _____, в связи с _____

_____
(указать причину блокирования персональных данных)

Ответ прошу направить в _____ форме по адресу_____ в срок, предусмотренный Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных».

_____ _____ / _____
(дата) (подпись) (ФИО)

Приложение 6
к Правилам рассмотрения
обращений и запросов
субъектов персональных
данных или их законных
представителей

В администрацию
муниципального образования
«Мелекесский район»
Ульяновской области

_____
(ФИО заявителя)

_____
(наименование и реквизиты документа,
удостоверяющего личность заявителя)

заявление

В соответствии со статьей 14 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», прошу прекратить обработку и уничтожить мои персональные данные:

_____
(указать перечень персональных данных, которые необходимо уничтожить)

в связи с тем, что_____
(указать причину уничтожения персональных данных)

Ответ прошу направить в _____ форме по адресу_____в срок, предусмотренный Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных».

_____ _____ / _____
(дата) (подпись) (ФИО)

Приложение 7
к Правилам рассмотрения
обращений и запросов
субъектов персональных
данных или их законных
представителей

Уведомление об уточнении персональных данных

Уважаемый(ая) _____
(Ф.И.О.)

В связи с_____сообщаем Вам, что администрацией муниципального образования «Мелекесский район» Ульяновской области уточнены ваши персональные данные в соответствии со сведениями:

_____
(перечень сведений)

_____ _____ / _____
(дата) (подпись) (ФИО)

Приложение 8
к Правилам рассмотрения
обращений и запросов
субъектов персональных
данных или их законных
представителей

Уведомление о блокировании персональных данных

Уважаемый(ая) _____,
(Ф.И.О.)

в связи с _____сообщаем Вам, что администрацией муниципального образования «Мелекесский район» Ульяновской области Ваши персональные данные:

_____
(перечень персональных данных)

заблокированы на срок _____

_____ _____ / _____
(дата) (подпись) (ФИО)

Приложение 9
к Правилам рассмотрения
обращений и запросов
субъектов персональных
данных или их законных
представителей

Уведомление о прекращении обработки и удалении персональных данных

Уважаемый(ая) _____,
(Ф.И.О.)

в связи с _____сообщаем Вам, что администрацией муниципального образования «Мелекесский район» Ульяновской области прекращена обработка Ваших персональных данных и Ваши персональные данные

_____
(перечень персональных данных)

_____уничтожены.

_____ _____ / _____
(дата) (подпись) (ФИО)

Приложение 9
к распоряжению администрации
муниципального образования
«Мелекесский район»
от _____ № ___

Правила
работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей

Допуск для работы на автоматизированных рабочих местах (далее – АРМ) состоящих в составе информационной системы персональных данных (далее – ИСПДн) осуществляется на основании утвержденного перечня лиц, доступ которых к персональным данным, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей (далее – Пользователи ИСПДн).

Пользователь ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для хранения и записи информации, содержащей персональные данные (далее – ПДн), разрешается использовать только машинные носители информации, учтенные в журнале учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации.

Пользователь несет ответственность за правильность включения и выключения АРМ, входа и выхода в систему и за все свои действия при работе в ИСПДн.

Вход пользователя в систему осуществляется по выдаваемому ему электронному идентификатору и по персональному паролю.

При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов и иных вредоносных программ с использованием штатных антивирусных средств, установленных на АРМ. В случае обнаружения вирусов либо вредоносных программ пользователь ИСПДн обязан немедленно прекратить их использование и действовать в соответствии с требованиями инструкции по организации антивирусной защиты.

Каждый работник, участвующий в рамках своих служебных обязанностей в процессах обработки персональных данных в ИСПДн и имеющий доступ к АРМ, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

Строго соблюдать установленные соответствующими инструкциями правила обеспечения безопасности информации в ИСПДн;

Знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ;

Хранить в тайне свой пароль (пароли). Выполнять требования инструкции по организации парольной защиты в полном объеме;

Хранить индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);

Выполнять требования инструкции по организации антивирусной защиты в полном объеме;

Немедленно известить ответственного за обеспечение безопасности персональных данных в случае утери электронного идентификатора или при

подозрении компрометации личных ключей и паролей, а также при обнаружении:

Несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ;

Отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования компонентов АРМ, а также перебоев в системе электроснабжения;

Некорректного функционирования установленных на АРМ технических средств защиты;

Непредусмотренных отводов кабелей и подключенных устройств.

Пользователю АРМ категорически запрещается:

Использовать компоненты программного и аппаратного обеспечения АРМ в личных целях;

Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения АРМ;

Записывать и хранить конфиденциальную информацию (содержащую персональные данные) на неучтенных машинных носителях информации (гибких магнитных дисках, флэш-накопителях и т.п.);

Оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

Оставлять без личного присмотра на рабочем месте или в ином месте свой электронный идентификатор, машинные носители и распечатки, содержащие персональные данные;

Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты;

Размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации, содержащей персональные данные.

Приложение 10
к распоряжению администрации
муниципального образования
«Мелекесский район»
от _____ № ___

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных

1.Общие положения

Настоящая инструкция определяет права и обязанности лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – ИСПДн).

Лицо ответственное за обеспечение безопасности персональных данных в ИСПДн (далее – администратор информационной безопасности) это лицо, отвечающее за обеспечение заданных характеристик информации, содержащей персональные данные (конфиденциальности, целостности и доступности) в процессе их обработки в ИСПДн.

Администратор информационной безопасности в ИСПДн осуществляет контроль за выполнением требований нормативно-правовых и организационно-распорядительных документов по организации обработки и обеспечению безопасности персональных данных при их обработке в ИСПДн с использованием автоматизированных рабочих мест.

2.Обязанности администратора информационной безопасности

Администратор информационной безопасности обязан:

Знать требования нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности персональных данных при их обработке в ИСПДн;

Знать перечень обрабатываемых персональных данных, состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных.

Уметь пользоваться средствами защиты информации и осуществлять их непосредственное администрирование;

Еженедельно осуществлять резервное копирование информации, содержащей персональные данные (при необходимости);

Обязан осуществлять периодический контроль за выполнением работниками эксплуатирующими ИСПДн (пользователями ИСПДн), мероприятий по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн;

Участвовать в работе по проведению внутреннего контроля соответствия обработки персональных данных требованиям по защите информации;

Обязан анализировать журнал системы защиты информации от несанкционированного доступа (НСД), проводить проверки электронного журнала обращений к информационным системам персональных данных;

Обязан обеспечивать строгое выполнение требований по обеспечению защиты информации при организации технического обслуживания АРМ;

Обязан вести журнал учета средств защиты информации, используемых в ИСПДн;

Обязан присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию АРМ;

Обязан проводить инструктаж пользователей ИСПДн по правилам работы с используемыми техническими средствами и средствами защиты информации в соответствии с технической документацией на используемые средства защиты;

Обязан проводить мероприятия по организации антивирусной защиты;

Осуществлять организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями, согласно Политики парольной защиты в администрации муниципального образования «Мелекесский район» Ульяновской области;

Обязан организовать ведение журнала учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации;

Обязан немедленно сообщать ответственному за организацию обработки персональных данных, информацию об имевших место попытках несанкционированного доступа к информации и техническим средствам АРМ, а также принимать необходимые меры по устранению нарушений:

Установить причины, по которым стал возможным НСД;

Установить последствия, к которым привел НСД;

Зафиксировать случай НСД в виде документа (акта, служебной записки и т.д.) с описанием причин НСД, предполагаемых или установленных нарушителей и последствий;

Провести проверку настроек средств защиты информации и операционных систем на соответствие требованиям руководящих документов и разрешительной системы доступа пользователей к защищаемым информационным ресурсам и объектам доступа ИСПДн, при необходимости провести настройку;

Провести инструктаж пользователей ИСПДн по выполнению требований по обеспечению защиты персональных данных.

3.Права администратора информационной безопасности.

Администратор информационной безопасности имеет право:

Требовать от пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкции о порядке работы пользователей в ИСПДн в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;

Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн;

Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности персональных данных к ответственному за

организацию обработки персональных данных в ИСПДн и/или ответственному за эксплуатацию ИСПДн;

4.Ответственность администратора информационной безопасности

На администратора информационной безопасности возлагается персональная ответственность за качество проводимых им работ по обеспечению безопасности ПДн в ИСПДн;

Администратор информационной безопасности в ИСПДн несет ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение 11
к распоряжению администрации
муниципального образования
«Мелекесский район»
от _____ № ___

ИНСТРУКЦИЯ
по организации резервного копирования

1.Общие положения

Настоящая инструкция разработана с целью обеспечения возможности оперативного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

Инструкция определяет правила и объемы резервного копирования, а также порядок восстановления работоспособности информационной системы персональных данных (далее – ИСПДн).

2.Резервируемое программное обеспечение и базы персональных данных

В ИСПДн резервированию подлежит:

Общее программное обеспечение (операционная система и программные драйверы устройств (принтера, монитора, видеокарты и т.п.), поставляемые с компонентами автоматизированных рабочих мест (далее – АРМ), входящими в состав ИСПДн);

Прикладное программное обеспечение, используемое для обработки персональных данных (средства обработки текстов и таблиц, специализированные программы и т.п.);

Базы персональных данных (тестовые и табличные файлы, а также файлы баз данных специализированных программ);

Программное обеспечение средств защиты информации, в том числе средств антивирусной защиты.

3.Порядок резервирования и хранения резервных копий

Резервное копирование общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации обеспечивается путем хранения у администратора информационной безопасности в ИСПДн машинных носителей информации, содержащих дистрибутивы данного программного обеспечения.

Машинные носители информации обновлений общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации должны также храниться у администратора информационной безопасности в ИСПДн.

Допускается хранение машинных носителей прикладного программного обеспечения и машинных носителей с обновлениями к нему в структурных подразделениях, эксплуатирующих ИСПДн.

Резервное копирование баз персональных данных, а также текстовых и табличных файлов, содержащих персональные данные, допускается только на учтенные установленным порядком машинные носители информации.

Резервное копирование осуществляется ежемесячно.

Резервные носители персональных данных хранятся в структурных подразделениях, эксплуатирующих ИСПДн, в порядке, предусмотренном для носителей информации персональных данных.

К резервному носителю персональных данных должна быть приложена учетная карточка, согласно Приложению 1 к настоящей инструкции, в которой делаются отметки о дате создания копии.

Резервные носители персональных данных не могут быть переданы за пределы структурных подразделений, эксплуатирующих ИСПДн.

Копирование информации с резервных носителей персональных данных, за исключением случая восстановления работоспособности ИСПДн, запрещается.

4.Порядок восстановления работоспособности ИСПДн

Восстановление работоспособности ИСПДн осуществляется в случаях сбоев, отказов и аварий технических средств и систем ИСПДн, а также ее программного обеспечения.

Данные работы осуществляются администратором информационной безопасности в ИСПДн в соответствии с эксплуатационной документацией на программное обеспечение до полного восстановления работоспособности.

В случае необходимости привлечения для восстановления работоспособности ИСПДн представителей сторонних организаций, должна быть обеспечена невозможность их ознакомления с персональными данными. Ответственность за выполнение данного требования возлагается на администратора информационной безопасности в ИСПДн и руководителя структурного подразделения, обеспечивающего ее эксплуатацию.

Приложение 1
к Инструкции

по организации резервного
копирования

Учетная карточка резервного носителя персональных данных
№ _____

Дата резервного копирования	Объект копирования	Кто производил копирование	Подпись

Приложение 12
к распоряжению администрации
муниципального образования
«Мелекесский район»
от _____ № ___

ИНСТРУКЦИЯ
по организации антивирусной защиты

1.Общие требования

Настоящая инструкция определяет требования к организации антивирусной защиты информационных систем персональных данных (далее – ИСПДн) от разрушающего воздействия вирусов и вредоносных программ и устанавливает ответственность руководителя и работников структурных подразделений, эксплуатирующих и сопровождающих ИСПДн, за их выполнение. Инструкция распространяется на все существующие и вновь разрабатываемые ИСПДн. Для отдельных ИСПДн могут быть разработаны свои инструкции, учитывающие особенности работы.

К использованию в ИСПДн допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

Установка и настройка средств антивирусного контроля осуществляется администратором информационной безопасности в ИСПДн или специально назначенным лицом в соответствии с эксплуатационной документацией на антивирусных средств.

2.Применение средств антивирусного контроля

При загрузке рабочего места в автоматическом режиме (далее - АРМ) должен проводиться антивирусный контроль служб операционной системы, исполняемых приложений, находящихся в автозагрузке, реестра операционной системы.

Полному антивирусному контролю АРМ должны подвергаться не реже одного раза в неделю.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, оптических и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов и других вредоносных программ. Непосредственно после установки (изменения) программного обеспечения, администратором информационной безопасности в ИСПДн должна быть выполнена антивирусная проверка на защищаемых серверах и пользовательских АРМ.

При возникновении подозрения на наличие вируса либо вредоносной программы (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) работник структурного подразделения самостоятельно или вместе с администратором информационной безопасности в ИСПДн должен провести внеочередной антивирусный контроль своего АРМ.

В случае обнаружения при проведении антивирусной проверки зараженных вирусами либо вредоносными программами файлов, необходимо:

Приостановить работу в ИСПДн;

Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя структурного подразделения и администратора информационной безопасности в ИСПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

Провести лечение или уничтожение зараженных файлов.

3.Ответственность

Ответственность за проведение мероприятий антивирусного контроля в подразделениях и соблюдение требований настоящей Инструкции возлагается на администратора информационной безопасности в ИСПДн и всех работников, являющихся пользователями ИСПДн.

Приложение 13
к распоряжению администрации
муниципального образования
«Мелекесский район»
от _____ № ___

ИНСТРУКЦИЯ
по проверке электронного журнала обращений к информационной системе персональных данных

1.Задачи проверки

Под проверкой понимается отслеживание событий, происходивших на автоматизированных рабочих местах (далее – АРМ) в течение определенного времени.

Общими задачами проверки являются:

контролирование состояния защищенности системы;

выявление причин произошедших изменений;

определение лиц или процессов, деятельность которых привела к изменению состояния защищенности системы или к несанкционированному доступу;

установление времени изменений.

Проверку средств защиты осуществляет администратор информационной безопасности.

2.Журналы записей о событиях

События, происходящие на АРМ, входящие в состав информационной системы персональных данных (далее – ИСПДн), регистрируются в журналах.

Каждому событию соответствует отдельная запись в журнале, содержащая подробную информацию для анализа события.

В состав используемых в ИСПДн средств защиты информации может входить специальное программное средство для аудита журналов событий, предназначенное для загрузки и просмотра журналов (далее — программа просмотра журналов). В программу просмотра журналов могут быть загружены записи следующих журналов:

штатные журналы операционной системы Windows;

журналы событий средств защиты информации.

2.1. Штатные журналы операционной систем.

В штатных журналах ОС Windows регистрируются только те события, которые имеют отношение к операционной системе. События используемых средств защиты информации в них не регистрируются.

Информация о событиях, происходящих на АРМ под управлением ОС Windows, сохраняется в следующих штатных журналах:

Журнал приложений – содержит сведения об ошибках, предупреждениях и других событиях, возникающих при исполнении приложений;

Системный журнал – содержит сведения об ошибках, предупреждениях и других событиях, возникающих в операционной системе;

Журнал безопасности – хранит информацию о попытках регистрации, а также о событиях, связанных с использованием ресурсов.

Подробное описание содержимого штатных журналов ОС Windows отражено в документации к операционной системе.

Загрузка и просмотр записей штатных журналов может осуществляться как в программе просмотра журналов средств защиты, так и с помощью стандартных средств работы с журналами ОС Windows — в оснастке «Просмотр событий» («Eventviewer»).

2.2. Журнал событий средств защиты информации.

Журналы средств защиты информации (далее – СЗИ) хранят информацию о событиях, отслеживаемых средствами самих СЗИ, в этом журнале регистрируются события, заданные параметрами СЗИ для локальной политики безопасности.

3. Аудит

Сведения, содержащиеся в журнале, позволяют отслеживать использование механизмов защиты, которые предоставляют средства защиты информации АРМ (шифрование файлов, полномочное управление, замкнутая программная среда и др.) подробное описание регистрируемых событий указано в соответствующих руководствах к используемым СЗИ.

4. Просмотр событий электронных журналов.

Администратор информационной безопасности в ИСПДн производит проверку электронных журналов.

В случае обнаружения нарушений администратор информационной безопасности докладывает о данном факте ответственному за организацию обработки персональных данных.

Приложение 14
к распоряжению администрации
муниципального образования
«Мелекесский район»
от _____ № ___

ИНСТРУКЦИЯ
по обращению со средствами криптографической защиты информации

1. Общие положения

Настоящая инструкция регламентирует порядок обращения с шифровальными средствами (средствами криптографической защиты информации, СКЗИ), предназначенными для защиты информации, не содержащей сведений, составляющих государственную тайну, в процессе их получения, транспортировки, учета, хранения, уничтожения, встраивания в прикладные системы, тестирования, передачи клиентам, а также порядок допуска к работам с шифровальными средствами.

Все сотрудники, допущенные к работе с СКЗИ, должны ознакомиться с данной инструкцией под подпись и строго выполнять требования настоящей инструкции в части, их касающейся, а также строго выполнять требования нормативных правовых актов Российской Федерации, относящихся к деятельности с СКЗИ, нормативных и методических документов лицензирующего органа.

Разработка и проведение мероприятий по обеспечению безопасности при работе с СКЗИ осуществляется ответственным за эксплуатацию СКЗИ.

Работы с СКЗИ должны проводиться с учетом Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).

2. Требования по размещению, оборудованию и охране помещений

Размещение, оборудование, охрана и режим в помещениях, в которых проводятся работы с СКЗИ (далее – помещения), должны обеспечивать безопасность СКЗИ, сведение к минимуму возможности неконтролируемого доступа посторонних лиц. Доступ сотрудников в эти помещения должен быть ограничен в соответствии со служебной необходимостью и определяться перечнем лиц, допущенных в кабинеты.

Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Для предотвращения просмотра извне окна помещений должны быть защищены (жалюзи, шторы и т.п.).

3. Порядок обращения с СКЗИ

Пользователи средств криптографической защиты информации обязаны:

не разглашать информацию о ключевых документах;

не допускать вывод ключевых документов на дисплей (монитор) или принтер;

не допускать установки ключевых документов в другие ЭВМ.

Все поступающие СКЗИ, инсталлирующие СКЗИ носители, эксплуатационная и техническая документация (при наличии) к ним должны браться на поэкземплярный учет в журнале установленной формы, согласно Приложению 6 к настоящему распоряжению. Ведет журналы администратор информационной безопасности.

Единицей поэкземплярного учета СКЗИ является:

для аппаратных и программно-аппаратных СКЗИ - конструктивно законченное техническое устройство;

для программных СКЗИ – инсталлирующий СКЗИ носитель (дискета, компакт-диск (CD-ROM) и т.п.).

Должны быть приняты организационные меры с целью исключения возможности несанкционированного копирования СКЗИ.

Хранение инсталлирующих СКЗИ носителей допускается в одном хранилище с другими документами при условиях, исключающих непреднамеренное их уничтожение или иное, не предусмотренное правилами пользования СКЗИ применение.

В случае отсутствия у сотрудника индивидуального хранилища инсталлирующие СКЗИ носители по окончании рабочего дня должны сдаваться лицу, ответственному за их хранение.

В случае утери носителя СКЗИ или вероятном копировании сотрудник обязан немедленно сообщить об этом лицу, ответственному за обеспечение безопасности при обращении с СКЗИ.

Ответственным за эксплуатацию СКЗИ периодически должен проводиться контроль сохранности и работоспособности установленного СКЗИ, а также всего используемого совместно с СКЗИ программного обеспечения для предотвращения внесения программно-аппаратных закладок и вирусов.

4.Ответственность за нарушение требований Инструкции

За нарушение требований настоящей Инструкции виновные лица несут дисциплинарную, либо материальную ответственность в зависимости от характера нарушения и тяжести наступивших отрицательных последствий.

Приложение 15
к распоряжению администрации
муниципального образования
«Мелекесский район»
от _____ № ___

ИНСТРУКЦИЯ
по обработке персональных данных без использования средств автоматизации

1.Общие положения

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому гражданину, обратившемуся в администрацию муниципального образования «Мелекесский район» Ульяновской области, или сотруднику (далее – субъекту персональных

данных) администрации муниципального образования «Мелекесский район» Ульяновской области.

Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные настоящим Положением, должны применяться с учетом требований Постановления Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», а также требований нормативных правовых актов федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации.

2.Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники администрации муниципального образования «Мелекесский район» Ульяновской области или лица, осуществляющие такую обработку по договору с администрацией муниципального образования «Мелекесский район» Ульяновской области), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется администрацией муниципального образования «Мелекесский район» Ульяновской области без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов

исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами администрации муниципального образования «Мелекесский район» Ульяновской области.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес учреждения, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых учреждением способов обработки персональных данных;

типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации,– при необходимости получения письменного согласия на обработку персональных данных;

типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.

При ведении журналов (журналов регистрации, журналов посещений), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в помещения администрации муниципального образования «Мелекесский район» Ульяновской области или в иных аналогичных целях, должны соблюдаться следующие условия:

необходимость ведения такого журнала должна быть предусмотрена актом администрации муниципального образования «Мелекесский район» Ульяновской области, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных;

копирование содержащейся в таких журналах информации не допускается;

персональные данные каждого субъекта персональных данных могут заноситься в такой журнал не более одного раза в каждом случае пропуска субъекта персональных данных.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом,

исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, зачеркивание, стирание).

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя,– путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

3.Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

Приложение 16
к распоряжению администрации
муниципального образования
«Мелекесский район»
от _____ № ___

ПРАВИЛА
работы с обезличенными данными

1.Общие положения

Настоящие Правила работы с обезличенными персональными данными администрации муниципального образования «Мелекесский район» Ульяновской области разработаны с учетом Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», Приказа Роскомнадзора от 5.09.2013 №996 «Об утверждении требований и методов по обезличиванию персональных данных», Методических рекомендаций по применению Приказа Роскомнадзора №996 (утверждены 13.12.2013) и

определяют порядок работы с обезличенными данными администрации муниципального образования «Мелекесский район» Ульяновской области.

2.Термины и определения

В соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» в настоящих Правилах используются следующие понятия:

персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);

обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

3.Условия обезличивания

Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных администрации муниципального образования «Мелекесский район» Ульяновской области и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Способы обезличивания при условии дальнейшей обработки персональных данных:

уменьшение перечня обрабатываемых сведений;

замена части сведений идентификаторами;

обобщение – понижение точности некоторых сведений;

понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только населенный пункт)

деление сведений на части и обработка в разных информационных системах;

другие способы.

Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

4.Порядок работы с обезличенными персональными данными

Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

парольной политики;

антивирусной политики;

правил работы со съемными носителями (если они используется);

правил резервного копирования;

правил доступа в помещения, где расположены элементы информационных систем.

При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

правил хранения бумажных носителей;

правил доступа к ним и в помещения, где они хранятся.

Приложение 17
к распоряжению администрации
муниципального образования
«Мелекесский район»
от _____ № ___

ИНСТРУКЦИЯ
по работе с инцидентами информационной безопасности

Ответственность за выявление инцидентов информационной безопасности и реагирование на них в администрации муниципального образования «Мелекесский район» Ульяновской области возлагается на администратора информационной безопасности.

Администратор информационной безопасности имеет полномочия инициировать проведение служебных проверок (ходатайствовать о наложении дисциплинарного взыскания перед Главой администрации муниципального образования «Мелекесский район» Ульяновской области) по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации.

Администратор информационной безопасности обязан вести журнал учёта инцидентов (Приложение 9 настоящего распоряжения) информационной безопасности (событий, действий повлекших за собой риски безопасности защищаемой информации и создающих предпосылки к нарушению критериев безопасности информации). Сюда относятся

нарушения пользователями положений организационно-распорядительных документов, установленных порядков и технологии работы в информационных системах, разглашение защищаемой информации и любые действия, направленные на это, не антропогенные инциденты (сбои программного обеспечения, стихийные бедствия).

В журнале в свободной форме описывается инцидент с указанием следующих данных:

даты и времени;

причин (умышленные и неумышленные действия, не антропогенные инциденты и т.п.) и описания инцидента и задействованных лиц;

информации о последствиях;

информации о возможных последствиях (экономические убытки (в связи с заменой средства защиты информации, повторной аттестации; временные и трудозатраты на устранение последствий, нарушение работы пользователей, ущерб субъектам персональных данных и юридические последствия для администрации муниципального образования «Мелекесский район» Ульяновской области и т.п.).

Журнал с данным отчётом об инциденте предоставляется на ознакомление ответственному за организацию обработки персональных данных для принятия мер по предотвращению рецидива (возникновения повторного инцидента).

В случае возникновения рецидива со стороны пользователя или администратора информационной безопасности, по ходатайству ответственного за организацию обработки персональных данных руководителем администрации муниципального образования «Мелекесский район» Ульяновской области накладывается дисциплинарное взыскание.

Сокрытие нарушений и инцидентов информационной безопасности, вызванных любыми должностными лицами администрации муниципального образования «Мелекесский район» Ульяновской области, является грубым нарушением трудовой дисциплины. Сокрытие нарушений и инцидентов информационной безопасности, вызванных действиями администратора информационной безопасности и ответственным за организацию обработки персональных данных, является грубейшим нарушением дисциплины, и при выяснении данного факта должно строго наказываться.

Любой сотрудник должен согласовывать следующие действия с администратором информационной безопасности:

замена прикладного оборудования (мышь, клавиатура, принтер, монитор);

установка дополнительного программного обеспечения;

изменение сетевых настроек рабочего места;

замена, изменение любой аппаратной части рабочего места.

Ответственный за организацию обработки персональных данных не может требовать от администратора информационной безопасности действий, направленных на нарушение настоящего руководства и других

организационно-распорядительных документов администрации муниципального образования «Мелекесский район» Ульяновской области, требовать сокрытия инцидентов информационной безопасности, вызванных любыми должностными лицами, требовать сообщения ему паролей на средства защиты информации и нарушения установленного разграничения прав по допуску к информационным ресурсам, установленным матрицей доступа к информационными ресурсам информационных систем.

Приложение 18
к распоряжению администрации
муниципального образования
«Мелекесский район»
от _____ № ___

ИНСТРУКЦИЯ
ответственного за эксплуатацию информационных систем персональных данных

1. Общие положения

Ответственный за эксплуатацию информационной системы персональных данных (далее – ИСПДн) в администрации муниципального образования «Мелекесский район» назначается ответственным за организацию обработки персональных данных.

Методическое руководство работой ответственного за эксплуатацию ИСПДн осуществляется ответственным за организацию обработки персональных данных в администрации муниципального образования «Мелекесский район».

Ответственный за эксплуатацию в своей работе руководствуется положениями, руководящими и нормативными документами ФСТЭК и ФСБ России по защите информации и организационно-распорядительными документами для данной ИСПДн, а также иными нормативными документами в части защиты информации.

Ответственный за эксплуатацию ИСПДн несет ответственность за свои действия, и действия сотрудников вверенного структурного подразделения в соответствии с действующим законодательством РФ.

2. Функции ответственного за эксплуатацию ИСПДн

Осуществление контроля за целевым использованием ИСПДн, всех периферийных устройств и технических средств, входящих в состав ИСПДн.

Контроль за отсутствием в период обработки защищаемой информации в помещении, где осуществляется обработка, посторонних лиц, не допущенных к обрабатываемой информации.

Контроль использования сотрудниками структурных подразделений, эксплуатирующими ИСПДн, средств защиты информации, установленных на АРМ, входящих в состав ИСПДн.

Контроль за правильностью использования и хранения сотрудниками структурных подразделений, эксплуатирующими ИСПДн, машинных носителей информации и документов, содержащих персональные данные.

Представление заявок на пользователей, допускаемых к защищаемым ресурсам ИСПДн, с целью закрепления за ними носителей информации устройств блокировки, паролей и других средств разграничения доступа к информации, а также прав пользования средствами вычислительной техники.

Организация повышения уровня осведомленности подчиненных должностных лиц по вопросам информационной безопасности.

3. Обязанности ответственного за эксплуатацию ИСПДн

Четко знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководств по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

Обеспечивать функционирование ИСПДн в пределах возложенных на него функций.

Обеспечивать контроль выполнения установленного комплекса мероприятий по обеспечению безопасности ПДн.

Контролировать целостность печатей (пломб) на устройствах ИСПДн.

Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств ИСПДн и отправке их в ремонт.

Присутствовать при выполнении технического обслуживания ИСПДн при установке (модификации) программного обеспечения.

Информировать администратора информационной безопасности о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

Контролировать соответствие состава ИСПДн техническому паспорту на ИСПДн.

Приложение 19
к распоряжению администрации
муниципального образования
«Мелекесский район»
от _____ № ___

ПЛАН
мероприятий по защите информации в администрации муниципального образования «Мелекесский район» Ульяновской области

1. Общие положения

План мероприятий по обеспечению защиты персональных данных (далее – План мероприятий), содержит необходимый перечень мероприятий для обеспечения защиты персональных данных в информационных системах персональных данных администрации муниципального образования «Мелекесский район» Ульяновской области.

Выбор конкретных мероприятий осуществляется на основании перечня актуальных угроз безопасности, указанных в Модели угроз безопасности для соответствующей ИСПДн.

В План мероприятий включены следующие категории мероприятий:

организационные (административные);

физические;

технические (аппаратные и программные);

контролирующие.

В План мероприятий включена следующая информация:

название мероприятия;

периодичность мероприятия (разовое/периодическое);

исполнитель мероприятия/ответственный за исполнение.

План внутренних проверок составляется на все информационные системы персональных данных администрации муниципального образования «Мелекесский район» Ульяновской области.

План мероприятий по защите информации

Мероприятие	**Периодичность**	**Исполнитель/ Ответственный**
Организационные мероприятия		
Обследование информационных систем	Разовое срок до	
Определение перечня ИСПДн	Разовое срок до	
Определение обрабатываемых ПДн и объектов защиты	Разовое срок до	
Определение круга лиц, участвующих в обработке ПДн	Разовое срок до.	
Определение прав разграничения доступа пользователей ИСПДн, необходимых для выполнения должностных обязанностей	Разовое срок до	
Назначение ответственного за обеспечение безопасности ПДн	Разовое срок до	
Классификация всех выявленных ИСПДн	Разовое срок до	
Организация режима и контроля доступа (охраны) в помещения, в которых установлены аппаратные средства ИСПДн.	Разовое срок до	
Организация порядка резервного копирования защищаемой информации на твердые носители	Разовое срок до.	
Организация информирования сотрудников о порядке обработки ПДн и их обучения	Разовое срок до	
Организация информирования сотрудников о введенном режиме защиты ПДн	Разовое срок до	

Мероприятие	**Периодичность**	**Исполнитель/ Ответственный**
Подготовка и утверждение комплекта нормативной документации, регламентирующей обработку ПДн в ИСПДн	Разовое срок до	
Физические мероприятия		
Установление границ контролируемой зоны ИСПДн	Разовое срок до	
Установка жалюзи, штор на окнах или другие меры, исключающие несанкционированный доступ к ПД снаружи здания	Разовое срок до	
Технические мероприятия		
Внедрение специальной подсистемы управления доступом, регистрации и учета	Разовое срок до	
Внедрение межсетевого экранирования	Разовое срок до	
Внедрение криптографической защиты	Разовое срок до	
Контролирующие мероприятия		
Контроль над соблюдением режима обработки ПДн	Еженедельно	
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Ежегодно	
Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	Еженедельно	
Контроль за обеспечением резервного копирования	Ежемесячно	
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз	Ежегодно	
Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно	