



МИНИСТЕРСТВО ТРУДА И СОЦИАЛЬНОГО РАЗВИТИЯ
РЕСПУБЛИКИ ДАГЕСТАН

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ РЕСПУБЛИКИ ДАГЕСТАН
«КОМПЛЕКСНЫЙ ЦЕНТР СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ НАСЕЛЕНИЯ
В МУНИЦИПАЛЬНОМ ОБРАЗОВАНИИ «СЕРГОКАЛИНСКИЙ РАЙОН»

368510с. Сергокала, Сергокалинский район, РД, тел. (88722)55-27-55
ОКПО 49198568, ОГРН 1060548000809, ИНН/КПП 0527004378/052701001

П Р И К А З

Номер документа	Дата
032	24.12.2019 г.

Об организации работ по обработке и защите персональных данных, обрабатываемых в информационных системах персональных данных

В соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», в рамках реализации работ по защите персональных данных, обрабатываемых в информационных системах персональных данных,

ПРИКАЗЫВАЮ:

1. Утвердить:

- Перечень информационных систем персональных данных (ИСПДн) (приложение № 1).
- Порядок доступа в помещения, в которых ведется обработка ПДн в ИСПДн» (приложение № 2).
- Положение о разграничении прав доступа к обрабатываемым персональным данным в информационных системах персональных данных (приложение № 3)
- Положение об обработке и защите персональных данных получателей социальных услуг в государственном бюджетном учреждении республики Дагестан «Комплексный центр социального обслуживания населения в муниципальном образовании «Сергокалинский район» (приложение № 4)

2. Утвердить инструкции:

- Инструкцию по учету лиц, допущенных к работе с персональными данными в ГБУ РД КЦСОН в МО «Сергокалинский район» (приложение № 5).
- Инструкция пользователю ИСПДн (приложение №6)
- Инструкция по учету машинных носителей информации (приложение №7).
- Инструкцию ответственного за организацию работ по обработке ПДн (приложение №8).
- Инструкцию администратора безопасности информационной системы персональных данных (приложение №9)
- Инструкцию по порядку учета, хранения и уничтожения персональных данных в государственном бюджетном учреждении республики Дагестан «Комплексный центр социального обслуживания населения в муниципальном образовании «Сергокалинский район» (приложение №10)
- Инструкцию о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных в государственном бюджетном учреждении республики Дагестан «Комплексный центр социального обслуживания населения в муниципальном образовании «Сергокалинский район» (приложение №11)

- Инструкцию по проведению антивирусного контроля и информационных систем персональных данных в Государственном бюджетном учреждении республики Дагестан «Комплексный центр социального обслуживания населения в муниципальном образовании «Сергокалинский район» (приложение №12)
- Инструкцию по организации парольной защиты в Государственном бюджетном учреждении республики Дагестан «Комплексный центр социального обслуживания населения в муниципальном образовании «Сергокалинский район» (приложение №13)

3. Утвердить:

- Порядок работы с инцидентами информационной безопасности в государственном бюджетном учреждении республики Дагестан «Комплексный центр социального обслуживания населения в муниципальном образовании «Сергокалинский район» (Приложение № 14)
- Правила осуществления внутреннего контроля соответствия обработки персональных данных в государственном бюджетном учреждении республики Дагестан «Комплексный центр социального обслуживания населения в муниципальном образовании «Сергокалинский район» (Приложение № 15)
- Порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных (Приложение № 16)
- Положение об организации обработки персональных данных, осуществляемой без использования средств автоматизации в Государственном бюджетном учреждении республики Дагестан "Комплексный центр социального обслуживания населения в муниципальном образовании "Сергокалинский район" (Приложение № 17)
- Порядок хранения, использования и передачи персональных данных сотрудников ГБУ РД КЦСОН в МО «Сергокалинский район» (Приложение № 18)

4. Назначить ответственным за организацию работ по обработке ПДн, Идрисова Х.И.
5. Ответственному за организацию работ по обработке ПДн в своей деятельности руководствоваться инструкцией ответственного за организацию работ по обработке ПДн.
6. Назначить администратором безопасности информационных систем персональных данных оператора ПЭВМ Ибрагимову Л.И.
7. Установить, что сотрудники ГБУ РД КЦСОН в МО «Сергокалинский район» имеют доступ к персональным данным, обрабатываемым в информационных системах персональных данных и без использования средств автоматизации, в рамках выполнения служебных (трудовых) обязанностей и в соответствии с действующим законодательством о персональных данных.
8. Контроль исполнения приказа оставляю за собой.

Директор ГБУ РД КЦСОН в
МО «Сергокалинский район»



to shen

М.И. Мургузалиев

Лист ознакомления

[illegible]

Перечень информационных систем персональных данных ГБУ РД КЦСОН в МО «Сергокалинский район»

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информатизации и защите информации» в ГБУ РД КЦСОН в МО «Сергокалинский район» определен перечень информационных систем персональных данных:

№ п/п	Наименование ИСПДн, в которой обрабатываются персональные данные	Категория ПДн	Цель обработки
1.	«ИС: Предприятие. Зарплата и кадры»	Данные о работниках, в том числе фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения); число, месяц, год рождения; место рождения; информация о гражданстве; вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи; адрес места жительства (адрес регистрации); реквизиты страхового свидетельства государственного пенсионного страхования; идентификационный номер налогоплательщика; семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших); основания назначения перевода, перемещения на иную работу, результатов аттестации, а также сведения о прежнем месте работы; информация, содержащаяся в трудовом договоре, дополнительных соглашениях к трудовому договору; сведения о пребывании за границей; сведения о профессиональной переподготовке и (или) повышении квалификации; информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания; сведения о доходах; номер расчетного счета; номер банковской карты.	В целях осуществления трудовых отношений с работниками, учета результатов исполнения работниками должностных обязанностей, обеспечения установленных законодательством Российской Федерации условий оплаты труда, гарантий и компенсаций работникам.
2.	АС «Адресная социальная помощь» на базе АСУПД «Тула»	Данные о гражданах, которым оказывается социальная помощь, в том числе фамилия, имя, отчество, дата рождения, СНИЛС, паспортные данные, место жительства, место регистрации, доходы, сведения об имуществе, гражданство, ИНН.	В целях оказания социальной помощи населению.
3.	«ПУ - 6»	Данные о работниках, в том числе фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения); число, месяц, год рождения; место рождения; информация о гражданстве; вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи; адрес места жительства (адрес регистрации); реквизиты страхового свидетельства государственного пенсионного страхования; идентификационный номер налогоплательщика; семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших); основания назначения перевода, перемещения на иную работу, результатов аттестации,	В целях осуществления трудовых отношений с работниками

		а также сведения о прежнем месте работы; информация, содержащаяся в трудовом договоре, дополнительных соглашениях к трудовому договору; сведения о пребывании за границей; сведения о профессиональной переподготовке и (или) повышении квалификации; информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания	
--	--	---	--

Порядок доступа в помещения, в которых ведется обработка ПДн в ИСПДн

Порядок разработан в соответствии с требованиями Приказа ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Контролируемая зона

Контролируемая зона – территория, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования (сетевое оборудование, иные технические средства).

Контролируемая зона включает пространство (территорию, здание, часть здания), в котором исключено неконтролируемое пребывание работников (сотрудников) оператора и лиц, не имеющих постоянного допуска на объекты информационной системы (не являющихся работниками оператора), а также транспортных, технических и иных материальных средств.

Границами контролируемой зоны являются ограждающие конструкции зданий ГБУ РД КЦСОН в МО «Сергокалинский район».

Порядок доступа в помещения

В помещения допускаются лица, согласно утвержденному перечню.

Ответственность в рабочее время за исключение неконтролируемого доступа третьих лиц в помещения, где ведется работа в ИСПДн, несут сотрудники, допущенные в данные помещения, при этом запрещается оставлять помещения, в случае отсутствия в нем сотрудников незакрытыми или с ключами в двери.

Контроль и управление физическим доступом осуществляется ответственным за организацию обработки персональных данных.

Сотрудники, ведущие обработку информации на автоматизированных рабочих местах, размещают экраны мониторов так, чтобы исключить возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны.

По возможности исключаются случаи размещения устройства вывода (отображения, печати) информации напротив оконных проемов, входных дверей, технологических отверстий, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра.

Положение о разграничении прав доступа к обрабатываемым персональным данным в информационных системах персональных данных

Перечень сотрудников осуществляющих обработку персональных данных в информационных системах персональных данных ГБУ РД КЦСОН в МО «Сергокалинский район» (далее - ИСПДн), представлен в списке лиц, имеющих доступ к ИСПДн.

Разграничение прав доступа к БД ИСПДн осуществляет средствами специального ПО в соответствии с должностными обязанностями каждого сотрудника, имеющего права доступа к обрабатываемым персональным данным в ИСПДн.

Разграничением прав доступа к информационным ресурсам, используемым в ИСПДн, кроме баз данных, осуществляется средствами ОС системными администраторами. Список информационных ресурсов и права доступа к ним приведен в Приложении 1-4.

Разграничение прав осуществляется исходя из характера и режима обработки персональных данных в ИСПДн.

Разрешительная система доступа работников к ресурсам информационных систем персональных данных в ГБУ РД КЦСОН в МО «Сергокалинский район» представлена в Приложении 5

МАТРИЦА ДОСТУПА №1

пользователей к информационным и программным ресурсам
информационной системы персональных данных «1С «Бухгалтерия» Зарплата и кадры»

«-» - отсутствие доступа

«R» - Чтение

«W» - Запись

«E» - Исполнение (запуск)

№ п/п	Наименование информационных ресурсов, используемых в ИСПДн (логические диски, каталоги, программы, устройства и т.п.)	Права доступа субъекта к объекту доступа	
		Администратор	Пользователь
АРМ			
1	Права администратора	RWE	-
2	Доступ к CD/DVD	RWE	RWE
3	Доступ к Flash-накопителю	RWE	RWE
4	Средства ОС для запуска и работы ПЭВМ	RWE	RE
5	БД Бухгалтерия «1С «Бухгалтерия» Зарплата и кадры»	RWE	RWE

Ответственный за обеспечение безопасности ПДн

Мамин
В.К.

Мерзурева В.И.
Курбанова А.Т.

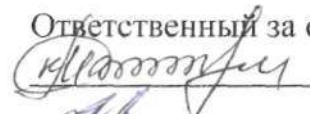
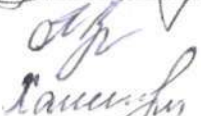
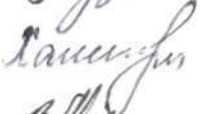
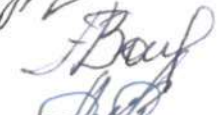
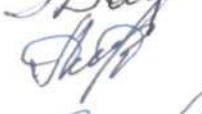
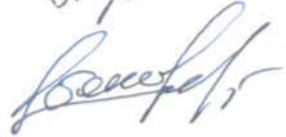
МАТРИЦА ДОСТУПА №2

пользователей к информационным и программным ресурсам
АС «Адресная социальная помощь» на базе АСУПД «Тула2

«-» - отсутствие доступа
«R» - Чтение
«W» - Запись
«E» - Исполнение (запуск)

№ п/п	Наименование информационных ресурсов, используемых в ИСПДн (логические диски, каталоги, программы, устройства и т.п.)	Права доступа субъекта к объекту доступа	
		Администратор	Пользователь
АРМ			
1	Права администратора	RWE	-
2	Доступ к CD/DVD	RWE	RWE
3	Доступ к Flach-накопителю	RWE	RWE
4	Средства ОС для запуска и работы ПЭВМ	RWE	RE
5	АС «Адресная социальная помощь» на базе АСУПД «Тула2	RWE	RWE

Ответственный за обеспечение безопасности ПДн

 (Абдурахманов К.Р.) зав. отделением.
 Таггиева Р.А. зав. отделением.
 Мамедова З.М. зав. отделением.
 Азизова З.М. зав. отд.
 Исмаилова З.Б. зав. отд.
 Шмева З.М. зав. отд.
 Бабаяева М.М. зав. отд.

МАТРИЦА ДОСТУПА №3
пользователей к информационным и программным ресурсам
информационной системы персональных данных «ПУ - 6»

«-» - отсутствие доступа
«R» - Чтение
«W» - Запись
«E» - Исполнение (запуск)

№ п/п	Наименование информационных ресурсов, используемых в ИСПДн (логические диски, каталоги, программы, устройства и т.п.)	Права доступа субъекта к объекту доступа	
		Администратор	Пользователь
АРМ			
1	Права администратора	RWE	-
2	Доступ к CD/DVD	RWE	RWE
3	Доступ к Flash-накопителю	RWE	RWE
4	Средства ОС для запуска и работы ПЭВМ	RWE	RE
5	«ПУ - 6»	RWE	RWE

Ответственный за обеспечение безопасности ПДн

Машин
Машин

(Меркурьева В.И.)
Меркурьева Т.Р.

Приложение № 4 к Положению о разграничении права доступа к обрабатываемым персональным данным в информационных системах персональных данных

Разрешительная система доступа работников к ресурсам информационных систем персональных данных в ГБУ РД КЦСОН в МО «Сергокалинский район»

1. Для обеспечения безопасности персональных данных при их обработке в информационной системе «1С «Бухгалтерия» Зарплата и кадры» v.7.7, 8.2, 8.3, разрешить доступ к работе с информационной системой следующим лицам:

Должность	Права доступа	
	База данных СПДн	Системная информация
Главный бухгалтер Меджидова Р.М.	Чтение, запись, удаление	Чтение, запись, удаление
Бухгалтер Курбанова А.Г.	Чтение, запись, удаление	Чтение, запись,
Специалист по кадрам Манапова Г.Р.	Чтение, запись, удаление	Чтение, запись

3. Для обеспечения безопасности персональных данных при их обработке в информационной системе «ПУ -6», разрешить доступ к работе с информационной системой следующим лицам:

Должность	Права доступа	
	База данных СПДн	Системная информация
Главный бухгалтер Меджидова Р.М.	Чтение, запись, удаление	Чтение, запись
Бухгалтер Курбанова А.Г.	Чтение, запись, удаление	Чтение, запись
Специалист по кадрам Манапова Г.Р.	Чтение, запись, удаление	Чтение, запись

4. Для обеспечения безопасности персональных данных при их обработке в АС «Адресная социальная помощь» на базе АСУПД «Тула2 разрешить доступ к работе с информационной системой следующим лицам:

Должность	Права доступа	
	База данных СПДн	Системная информация
Заместитель директора Идрисов Х.И.	Чтение, запись, удаление	Чтение, запись
Заведующие отделением социального обслуживания на дому граждан пожилого возраста и инвалидов	Чтение, запись, удаление	Чтение, запись
Заведующая отделением социального обслуживания на дому детей и семей с детьми	Чтение, запись, удаление	Чтение, запись
Заведующий отделением дневного пребывания граждан пожилого возраста и инвалидов	Чтение, запись, удаление	Чтение, запись
Заведующий срочного социального обслуживания на дому	Чтение, запись, удаление	Чтение, запись
Специалисты по социальной работе	Чтение, запись, удаление	Чтение, запись

Положение
об обработке и защите персональных данных получателей социальных услуг в
государственном бюджетном учреждении республики Дагестан «Комплексный центр
социального обслуживания населения в муниципальном образовании «Сергокалинский
район»

1. Общие положения

1.1. Настоящее положение об обработке персональных данных получателей социальных услуг в ГБУ РД КЦСОН в МО «Сергокалинский район» (далее по тексту - Положение) разработано в соответствии с Конституцией Российской Федерации, Гражданским Кодексом Российской Федерации, Федеральным законом от 27.07.2006 года №152-ФЗ «О персональных данных», иными нормативными актами, действующими на территории Российской Федерации, Федеральным законом от 28.12.2013 №442-ФЗ «Об основах социального обслуживания граждан в Российской Федерации», Законами Республики Дагестан.

1.2. Цель настоящего Положения – определение порядка обработки персональных данных, обеспечение требований защиты прав граждан, обратившихся за оказанием социальных услуг, при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, уполномоченных на обработку персональных данных, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

Персональные данные могут обрабатываться только для целей, непосредственно связанных с деятельностью ГБУ РД КЦСОН в МО «Сергокалинский район» (далее по тексту - КЦСОН), в частности осуществление уставной деятельности. КЦСОН обрабатывает данные только в объеме, необходимом для достижения указанных целей.

1.3. Сбор, хранение, использование и распространение, в том числе передача третьим лицам, персональных данных без письменного согласия получателя социальных услуг не допускается. Режим конфиденциальности персональных данных снимается в случаях обезличивания или включения их в общедоступные источники персональных данных, если иное не определено действующим законодательством.

1.5. Работники КЦСОН, в обязанность которых входит обработка персональных данных получателя социальных услуг, обязаны обеспечить каждому получателю социальных услуг возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено действующим законодательством.

1.6. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда получателю социальных услуг, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с действующим законодательством.

1.7. Настоящее положение является обязательным для исполнения всеми работниками КЦСОН, имеющим доступ к персональным данным получателя социальных услуг.

2. Понятие и состав персональных данных.

2.1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (получателю социальных услуг).

2.2. В состав персональных данных получателя социальных услуг входят:

- фамилия, имя, отчество;
- сведения о месте жительства (фактический, регистрации);
- паспортные данные гражданина, в том числе законного представителя;
- сведения о месте учебы;

- (сведения) о наличии (отсутствии) доходов гражданина, членов его семьи, полученных в денежной форме, учитываемых при определении его среднедушевого дохода;
- сведения о лицах, зарегистрированных совместно с гражданином по месту его жительства;
- сведения, подтверждающие правовые основания отнесения лиц, проживающих совместно с гражданином по месту жительства, к членам его семьи;
- сведения, подтверждающие отнесение получателя социальных услуг к категориям граждан, имеющих право на получение социальных услуг бесплатно;
- другие персональные данные, позволяющие идентифицировать получателя социальных услуг.

2.3. Указанные документы, являются конфиденциальными. Учитывая их массовость и единое место обработки – соответствующий гриф на них не ставится.

2.4. Полный перечень персональных данных, обрабатываемых в ГБУ РД КЦСОН в МО «Сергокалинский район» в связи с реализацией трудовых отношений, а также в связи с оказанием государственных услуг, с использованием средств автоматизации и без использования таких средств приведен в Приложении №1

3. Принципы обработки персональных данных.

3.1. Обработка персональных данных осуществляется на основе следующих принципов:

- законности целей и способов обработки персональных данных, добросовестность обработки;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям КЦСОН;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям их обработки;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;
- уничтожения персональных данных после достижения целей обработки или в случае утраты необходимости в их достижении;
- личной ответственности работников КЦСОН за сохранность и конфиденциальность персональных данных, а также носителей этой информации;
- наличие четкой разрешительной системы доступа работников КЦСОН к документам и базам данных, содержащих персональные данные.

4. Обязанности работников

4.1. В целях обеспечения прав и свобод гражданина работники КЦСОН при обработке персональных данных получателя социальных услуг обязаны соблюдать следующие общие требования:

4.1.1. При сборе персональных данных работники КЦСОН обязаны предоставить получателю социальных услуг по его просьбе информацию, содержащую:

- подтверждение факта обработки персональных данных получателя социальных услуг, а также цель их обработки;
- способы обработки персональных данных;
- сведения о работниках КЦСОН, имеющих доступ к персональным данным получателя социальных услуг или которым предоставляется такой доступ;
- перечень обрабатываемых персональных данных получателя социальных услуг и источник их получения;
- сроки обработки персональных данных получателя социальных услуг, в том числе сроки их хранения;

- сведения о юридических последствиях для получателя социальных услуг при обработке его персональных данных.

4.1.2. В случае отказа в предоставлении персональных данных, работники КЦСОН обязаны разъяснить получателю социальных услуг ее причины.

4.1.3. В случае получения персональных данных не от получателя социальных услуг, за исключением случаев, если персональные данные были представлены работникам в соответствии с действующим законодательством или являются общедоступными, до начала обработки таких персональных данных работники КЦСОН обязаны предоставить получателю социальных услуг следующую информацию:

- наименование и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- права получателя социальных услуг.

4.2. Работники КЦСОН не имеют право получать и обрабатывать персональные данные получателя социальных услуг о его расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, предусмотренных действующим законодательством. Работники учреждения вправе обрабатывать указанные персональные данные только с письменного согласия получателя социальных услуг, также при наличии надлежащим образом оформленного запроса.

4.3. Хранение и защита персональных данных получателя социальных услуг от неправомерного их использования или утраты должна быть обеспечена за счет средств КЦСОН в порядке, установленном действующим законодательством.

5. Права получателя социальных услуг

5.1. Получатель социальных услуг имеет право на получение сведений о наличии у работников КЦСОН своих персональных данных, а также на ознакомление с такими персональными данными. Получатель социальных услуг вправе требовать от работников КЦСОН уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные действующим законодательством меры по защите своих прав.

5.2. Сведения о наличии персональных данных должны предоставляться получателю социальных услуг работниками КЦСОН в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим получателям социальных услуг.

5.3. Доступ к своим персональным данным предоставляется получателю социальных услуг или его законному представителю при обращении в устной либо письменной форме, а также электронной форме. Запрос должен содержать номер основного документа, удостоверяющего личность получателя социальных услуг или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись получателя социальных услуг или его законного представителя.

5.4. Получатель социальных услуг имеет право на получение при личном обращении, либо при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных, а также цель такой обработки;
- способы обработки персональных данных;
- сведения о работниках КЦСОН, имеющих доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для получателя социальных услуг может повлечь за собой обработка его персональных данных;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;

- сведения о том, какие юридические последствия для получателя социальных услуг может повлечь за собой обработка его персональных данных.

5.5. Право получателя социальных услуг на доступ к своим персональным данным ограничивается в случае, если:

- обработка персональных данных, в том числе полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

- обработка персональных данных осуществляется органами, осуществляющими задержание получателя социальных услуг по подозрению в совершении преступления, либо предъявившими получателю социальных услуг обвинение по уголовному делу, либо применившими к получателю социальных услуг меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

- предоставление персональных данных нарушает конституционные права и свободы других лиц.

5.6. Если получатель социальных услуг считает, что работники КЦСОН осуществляют обработку его персональных данных с нарушением требований

5.7. законодательства или иным образом нарушает его права и свободы, получатель социальных услуг вправе обжаловать их действия или бездействия в уполномоченный орган или в судебном порядке.

5.8. Получатель социальных услуг имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

6. Сбор, обработка и хранение персональных данных получателя социальных услуг

6.1. Обработка персональных данных – действия с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных.

6.2. Получатель социальных услуг принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своих интересах.

6.3. Документы, содержащие персональные данные получателя социальных услуг создаются путем:

- внесения сведений в утвержденные, а также учетные формы (в бумажном и электронном виде);

- копирования оригиналов документов (н-р: паспорт и др.);

- получения оригиналов документов (н-р: справка о составе семьи и др.).

6.4. При передаче персональных данных получателя социальных услуг работники КЦСОН должны соблюдать следующие правила:

6.4.1 Не сообщать персональные данные получателя социальных услуг третьей стороне без его письменного согласия, за исключением следующих случаев:

- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является получатель социальных услуг;

- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов гражданина, если получение его согласия невозможно.

6.4.2. Предупредить лиц, получающих персональные данные получателя социальных услуг о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены. Лица, получающие персональные данные граждан, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется в случае обезличивания персональных данных и в отношении общедоступных данных.

6.4.3. Разрешить доступ к персональным данным получателя социальных услуг только уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные гражданина, которые необходимы для выполнения конкретных функций.

6.5. Персональные данные получателя социальных услуг хранятся в его личном деле или карточке учета. Персональные данные получателя социальных услуг могут храниться как в бумажном, так и в электронном виде.

6.6. В КЦСОН персональные данные получателя социальных услуг на бумажном носителе хранятся в специально отведенных шкафах.

6.7. Персональные данные, хранящиеся в электронном виде, обеспечиваются системой парольной защиты.

6.8. Персональные данные на бумажных носителях после истечения срока хранения сдаются в архив КЦСОН.

6.9. Организация работы с получателями социальных услуг подчиняется в том числе решению задач обеспечения безопасности персональных данных, их защите:

- при работе с получателем социальных услуг работник КЦСОН не должен выполнять функции, не связанные с приемом. Вести служебные и личные переговоры по телефону. На рабочем столе не должно быть никаких документов, кроме касающихся данного получателя социальных услуг;

- не допускается отвечать на вопросы, связанные с передачей персональных данных по телефону.

6.10. Личные дела получателей социальных услуг, журналы и прочие документы в рабочее и нерабочее время хранятся в специально отведенных шкафах.

Не допускается при выходе из кабинета оставлять какие-либо документы, содержащие персональные данные, на рабочем столе, а также оставлять кабинет открытым.

6.11. На рабочем столе работника должен находиться тот массив документов, с которым в настоящее время он работает. Другие документы должны находиться в шкафу. Исполняемые документы не допускается хранить в россыпи. Их следует помещать в папки, на которых указывается вид производимых с ними действий (подшивка в личные дела, для отправки и др.).

6.12. Черновики, редакции документов, испорченные бланки, содержащие персональные данные в конце рабочего дня уничтожаются.

7. Доступ к персональным данным получателя социальных услуг

7.1. К обработке персональных данных получателя социальных услуг могут иметь доступ только работники КЦСОН, допущенные к работе с персональными данными получателя социальных услуг и подписание обязательства о соблюдении конфиденциальности персональных данных.

7.2. Перечень должностей работников, допущенных к обработке персональных данных получателей социальных услуг представлен в Приложении №2.

7.3. Право доступа к своим персональным данным в КЦСОН имеют получатели социальных услуг, как субъекты персональных данных.

8. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных.

8.1. Персональная ответственность является одним из главных требований к организации функционирования системы защиты персональных данных и обязательным условием обеспечения эффективности функционирования данной системы.

8.2. Работники учреждения, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут

дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с действующим законодательством.

ПЕРЕЧЕНЬ

**персональных данных, обрабатываемых в государственном бюджетном учреждении
республики Дагестан «Комплексный центр социального обслуживания населения в
муниципальном образовании «Сергокалинский район» в связи с реализацией трудовых
отношений, а также в связи с оказанием государственных услуг, с использованием
средств автоматизации и без использования таких средств**

Персональные данные, обрабатываемые в связи с реализацией трудовых отношений:

1. Фамилия, имя, отчество (в том числе информация о смене фамилии, имени, отчества);
2. День, месяц, год рождения, место рождения;
3. Гражданство;
3. Данные паспорта гражданина Российской Федерации;
4. Место и дата регистрации и место фактического проживания;
5. Номера контактных телефонов (личные, служебные);
6. Семейное положение (информация о вступлении в брак, в случае развода - данные о разводе);
7. Сведения о полученном образовании (название оконченных учебных заведений и год окончания, специальности и квалификации, наличие ученых степеней, данные о прохождении дополнительного профессионального образования);
8. Сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу;
9. Сведения об уровне специальных знаний (работа на компьютере, знание иностранного языка и языков народов Российской Федерации);
10. Сведения о периодах трудовой деятельности, общем трудовом стаже и стаже государственной, государственной гражданской службы Российской Федерации, муниципальной службы;
11. Заключение медицинского учреждения установленной формы об отсутствии заболевания, препятствующего трудоустройству в учреждение, исполнению должностных обязанностей;
12. Сведения о занимаемой должности;
13. Сведения о классных чинах, воинских и специальных званиях; сведения о награждении государственными и ведомственными наградами, иными наградами и знаками отличия;
14. Сведения об отпусках и командировках;
15. Сведения о прохождении аттестации, датах прохождения и принятых аттестационными комиссиями решениях и о вынесенных рекомендациях;
16. Сведения об участии в конкурсных процедурах, включении в кадровый резерв;
17. Информация о проведении служебных проверок, наложении дисциплинарных взысканий;
18. Сведения о поощрении;
19. Сведения о временной нетрудоспособности;
20. Материалы по расследованию и учету несчастных случаев на производстве и профессиональных заболеваний;
21. Реквизиты идентификационного номера налогоплательщика (ИНН);
22. Реквизиты страхового номера индивидуального лицевого счета в Пенсионном фонде Российской Федерации (СНИЛС);
23. Сведения о социальных льготах;
24. Информация о доходах, выплатах и удержаниях;

25. Номера банковских счетов;
26. Табельный номер;
27. Фото;
28. Сведения о близких родственниках (отец, мать, усыновители, усыновленные, братья и сестры, дети):
 - степень родства, фамилия, имя, отчество;
 - год рождения;

Персональные данные физических лиц, обрабатываемые в связи с рассмотрением обращений:

1. Фамилия, имя, отчество;
2. Место регистрации и(или) место фактического проживания;
3. Номера контактных телефонов;
4. Социальный статус заявителя;
5. Иные персональные данные, содержащиеся в обращении.

Персональные данные, обрабатываемые в целях заключения договоров и ведения расчетов с физическими лицами:

1. Фамилия, имя, отчество;
2. День, месяц, год рождения, место рождения;
3. Гражданство;
4. Данные паспорта гражданина Российской Федерации;
5. Место регистрации;
6. Реквизиты идентификационного номера налогоплательщика (ИНН);
7. Реквизиты страхового номера индивидуального лицевого счета в Пенсионном фонде Российской Федерации (СНИЛС);
8. Информация о выплатах;
9. Номера банковских счетов.

Персональные данные, обрабатываемые в целях оказания государственных услуг:

1. Фамилия, имя, отчество;
2. Данные паспорта гражданина Российской Федерации (свидетельства о рождении);
3. Место регистрации и место фактического проживания;
4. Гражданство;
5. Сведения о регистрации и расторжения брака;
6. Сведения о составе семьи, о несовершеннолетних детях;
7. Сведения о последнем месте работы;
8. Заключение медицинского учреждения установленной формы об отсутствии у заявителя медицинских противопоказаний к социальному обслуживанию;
9. Сведения о наличии инвалидности;
10. Сведения, подтверждающие льготную категорию заявителя;
11. Сведения о доходах получателя социальных услуг и совместно проживающих членов семьи;
12. Реквизиты страхового номера индивидуального лицевого счета в Пенсионном фонде Российской Федерации (СНИЛС);
13. Сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу;
14. Сведения об освобождении из мест лишения свободы;
15. Сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней;
16. Сведения в страховых полисах обязательного (добровольного) медицинского страхования;
17. Сведения о смерти близких родственников;
18. Сведения, подтверждающие факт назначения пенсии (пенсионное удостоверение);
19. Номера контактных телефонов;
20. Номер банковского счета;
21. Иные персональные данные, необходимые для оказания государственных услуг.

**Перечень должностей сотрудников ГБУ РД КЦСОН в МО
«Сергокалинский район», которые предусматривает осуществление
обработки персональных данных, либо осуществление доступа к
персональным данным**

	Структурное подразделение, наименование должности
1	Заместитель директора
2	Специалист по кадрам
3	Главный бухгалтер
4	Бухгалтер, экономист
	Отделения социального обслуживания граждан
5	Заведующие отделениями
6	Специалисты по социальному обслуживанию
7	Оператор ЭВМ

**Инструкция по учету лиц, допущенных
к работе с персональными данными в информационных системах персональных данных
ГБУ РД КЦСОН в МО «Сергокалинский район»**

1 Общие сведения

1.1 Настоящая инструкция разработана в соответствии с требованиями Положения об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденного постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 и определяет порядок учета лиц, допущенных к работе с персональными данными в информационных системах.

1.2 Настоящая инструкция определяет порядок допуска сотрудников и третьих лиц к персональным данным, обрабатываемым в информационной системе ГБУ РД КЦСОН в МО «Сергокалинский район» (далее - Учреждение), а так же их уровень прав доступа к обрабатываемым персональным данным в информационных системах персональных данных Учреждения (далее - ИСПДн).

1.3 Основанием для допуска сотрудников и третьих лиц к персональным данным является должностная инструкция пользователя ИСПДн и трудовой договор.

1.4 Основанием для прекращения допуска сотрудников и третьих лиц к персональным данным является прекращение трудовых отношений.

1.5 Допуск лиц к работе с персональными данными в ИСПДн осуществляется в соответствии со списком лиц, утвержденным руководством или уполномоченным лицом Учреждения.

1.6 К работе допускаются лица, ознакомившиеся с руководящими документами по защите персональных данных и прошедшие инструктаж.

1.7 Учет лиц, допущенных к работе с персональными данными в ИСПДн, ведется в журнале инструктажа персонала на рабочем месте.

**2 Действия по учету лиц, допущенных к работе
с персональными данными в ИСПДн.**

2.1 Руководители структурных подразделений предоставляют сотруднику ответственному за информационную безопасность список сотрудников, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей.

2.2 Сотрудник ответственный за информационную безопасность в соответствии с полученным списком из пункта 1 составляет список лиц, имеющих доступ к ИСПДн, и передает главному врачу Учреждения на утверждение.

2.3 Лица, допущенные к ИСПДн должны расписаться в журнале инструктажа персонала.

Инструкция пользователю ИСПДн

1 Общие положения

1.1. Настоящая инструкция определяет общие положения работы пользователей в защищенной от несанкционированного доступа информационных системах персональных данных (далее - ИСПДн).

1.2. Пользователь ИСПДн (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.

1.3. Пользователем является каждый сотрудник в государственном бюджетном учреждении социального обслуживания ГБУ РД КЦСОН в МО «Сергокалинский район» (далее – Учреждение), участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.4. Пользователь отвечает за правильность функционирования ИСПДн, входа в систему и все действия при работе в ИСПДн.

1.5. Пользователь в своей работе руководствуется настоящей инструкцией, и нормативными документами ФСТЭК России и регламентирующими документами Организации.

1.6. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

2 Должностные обязанности

2.1. Допуск пользователей для работы на АРМ осуществляется в соответствии со списком лиц допущенных к работе с персональными данными.

2.2. В процессе первичной регистрации пользователя руководитель отдела, в котором работает пользователь, заявляет Администратору информационной системы перечень необходимых для работы пользователя ресурсов, перечень персональных данных, состав необходимого общесистемного программного обеспечения для решения поставленных задач.

2.3. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору информационной безопасности.

2.4. Пользователь обязан:

- Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.
- Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Положении о разграничении прав доступа к обрабатываемым персональным данным в ИСПДн.
- Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.
- Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других (раздел 3).
- При работе со съемными носителями пользователь должен каждый раз перед началом работы проверить их на наличие вирусов с использованием штатных антивирусных программ.
- В случае обнаружения вирусов на машинных носителях информации (съемных носителях, жестком магнитном диске, твердотельном носителе) пользователь обязан немедленно сообщить Администратору информационной безопасности.

- В случае оставления рабочей станции без визуального контроля доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>, либо комбинацией клавиш Win + L.
- Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах, возложенных на него функций.

2.5. Пользователям запрещается:

- Разглашать защищаемую информацию третьим лицам.
- Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.
- Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.
- Несанкционированно открывать общий доступ к папкам на своей рабочей станции.
- Запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.
- Отключать (блокировать) средства защиты информации.
- Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн.
- Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.
- Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.
- Самостоятельно вносить изменения в аппаратно-программную конфигурацию ИСПДн, изменять месторасположение средств отображения информации.

2.6. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет дисциплинарную, административную, гражданско-правовую или уголовную ответственность граждан и юридических лиц.

3 Правила работы в сетях общего доступа и (или) международного обмена

3.1 Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

3.2 При работе в Сети запрещается:

- Осуществлять работу при отключенных средствах защиты (антивирус и других).
- Передавать по Сети защищаемую информацию без использования механизмов защиты.
- Запрещается скачивать из Сети программное обеспечение и другие файлы.
- Запрещается посещение сайтов сомнительной репутации (порно сайты, сайты, содержащие нелегально распространяемое ПО и другие).
- Запрещается нецелевое использование подключения к Сети.

Инструкция по учету машинных носителей информации

1. Общие положения

1.1. Настоящая Инструкция устанавливает основные требования к организации учета и использования машинных носителей данных, предназначенных для обработки и хранения персональных данных.

1.2. Учет машинных носителей информации осуществляется в соответствии с формой учетной документации.

1.3. Все машинные носители данных, используемые при работе со средствами вычислительной техники (СВТ) для обработки и хранения персональных данных, должны обязательно регистрироваться и учитываться. Допускается автоматизированный учет машинных носителей информации.

1.4. Проверка наличия машинных носителей данных, предназначенных для обработки и хранения персональных данных, проводится в сроки, установленные настоящей Инструкцией.

2. Учет машинных носителей информации

2.1 К машинным носителям информации относятся:

- съемные носители информации;
- несъемные жесткие магнитные диски;
- твердотельные накопители.

2.2 Персональную ответственность за сохранность полученных машинных носителей данных и предотвращении несанкционированного доступа к записанной на них информации несет сотрудник, получивший эти носители.

2.3 При обработке персональных данных на СВТ должен соблюдаться следующий общий порядок учета, хранения и уничтожения машинных носителей данных.

2.4.1 Учет машинных носителей данных из п. 2.1., предназначенных для записи персональных данных производится в Журнале учета машинных носителей персональных данных (Приложение 1).

2.4.2 Каждому носителю информации присваивается учетный номер, который состоит из серийного номера машинного носителя, номера объекта и порядкового номера по Журналу учета машинных носителей персональных данных.

2.4.3 Если на машинном носителе отсутствует серийный номер, то на носитель (корпус носителя) наносится учетный номер. Если невозможно маркировать непосредственно машинный носитель данных, то маркируется упаковка, в которой хранится носитель.

2.4.4 Хранение их должно осуществляться в условиях, исключающих возможность хищения, приведения в негодность или уничтожения содержащейся на них информации.

2.4.5 Машинные носители данных (см. п. 2.1.) после стирания с них персональных данных, с учета не снимают, а хранятся наравне с другими машинными носителями.

2.4.6 В последующем эти носители используются для записи персональных данных. Если носители не пригодны для дальнейшего использования, они подлежат уничтожению по соответствующему акту.

2.4.7 О фактах утраты машинных носителей с ПДн незамедлительно докладывается руководству Организации и проводится служебное расследование.

2.4.8 Машинные носители персональных данных выдаются операторам или другим лицом, участвующим в обработке информации, составляющей персональные данные, для работы под расписку в Журнале учета машинных носителей персональных данных. По завершению работы машинные носители данных сдаются ответственному за их хранение.

2.4.9 Копирование информации, составляющей персональные данные, с машинных носителей производится с разрешения руководства Организации.

2.4.10 Машинные носители с персональными данными, утратившими практическое значение или пришедшие в негодность, уничтожаются по соответствующему акту.

2.4 При подготовке документов должны соблюдаться следующие особенности учета, хранения и уничтожения машинных носителей данных.

2.5.1 Машинные носители персональных данных, предназначенные для записи персональных данных, выдаются сотрудникам по письменному разрешению руководителей структурных подразделений, в необходимом для работы количестве под расписку в Журнале учета машинных носителей персональных данных.

2.5.2 Несъемные жесткие магнитные диски и твердотельные накопители закрепляются за сотрудником, ответственным за СВТ, в котором они установлены.

2.5.3 В случае повреждения машинных носителей данных, содержащих персональные данные, сотрудник, в пользовании которого они находятся, обязан сообщить о случившемся ответственному за его сохранность.

2.5.4 В случае необходимости (командировка, отпуск и т. д.) съемные носители с персональными данными, сдаются сотрудником ответственному лицу на постоянное или временное хранение.

2.5.5 Копирование персональных данных, с машинных носителей с целью передачи другим сотрудникам производится с разрешения руководителя структурного подразделения сотрудником, постоянно работающим с данной информацией.

2.5.6 Копирование осуществляется только на тех СВТ, на которых разрешена обработка персональных данных, и только на те носители, которые соответствуют грифу «конфиденциально».

2.5.7 Хранящиеся на носителях и потерявшие актуальность персональные данные должны своевременно стираться (уничтожаться). Ответственность за это несет владелец информации.

2.5 Руководство Учреждения не реже одного раза в год создает комиссию по проверке наличия и условий хранения персональных данных.

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных в
государственном бюджетном учреждении республики Дагестан «Комплексный центр
социального обслуживания населения в муниципальном образовании «Сергокалинский
район»

1. Общие положения

- 1.1. Настоящая Инструкция разработана в соответствии со ст. 22.1 Федерального закона от 27.07.2006 № 152 - ФЗ «О персональных данных» и определяет обязанности, полномочия и ответственность лиц, ответственных за обработку персональных данных в ГБУ РД КЦСОН в МО «Сергокалинский район»
- 1.2. Ответственный за обработку персональных данных назначается приказом директора из числа работников ГБУ РД КЦСОН в МО «Сергокалинский район»
- 1.3. Ответственный за обработку персональных данных подчиняется директору.
- 1.4. Ответственный за организацию обработки персональных данных в своей деятельности руководствуется Трудовым кодексом РФ, Федеральным законом от 27 июля 2006 № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 15 сентября 2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства РФ от 21 марта 2012г. №211 «Перечень мер направленных на обеспечение выполнения обязанностей предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» и, настоящей инструкцией и внутренними документами ГБУ РД КЦСОН в МО «Сергокалинский район» по защите информации.

2. Обязанности ответственного за обработку персональных данных

- 2.1. Предоставлять субъекту персональных данных либо его представителю по запросу информацию об обработке его персональных данных.
- 2.2. Осуществлять внутренний текущий контроль за соблюдением требований законодательства Российской Федерации и правил обработки персональных данных в ГБУ РД КЦСОН в МО «Сергокалинский район» при обработке персональных данных, в том числе требований к защите персональных данных.
- 2.3. Доводить до сведения работников ГБУ РД КЦСОН в МО «Сергокалинский район» содержание положений законодательства РФ о персональных данных, внутренних нормативно - правовых актов ГБУ РД КЦСОН в МО «Сергокалинский район» по вопросам обработки персональных данных, требований по защите персональных данных.
- 2.4. Организовать прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль за приемом и обработкой таких обращений и запросов:
 - в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» субъект персональных данных или его представитель имеет право на получение информации, касающейся обработки его персональных данных на основании обращения либо при получении 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 оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись

субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с действующим законодательством;

- все обращения и запросы субъектов персональных данных подлежат обязательному учету;
- ответственный за обработку обязан фиксировать все обращения и запросы в журнале учета обращений граждан (субъектов персональных данных).

2.5. Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

2.6. Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

2.7. Получать обязательство о прекращении обработки персональных данных у лиц, непосредственно осуществляющих обработку персональных данных, в случае расторжения с ним договора (контракта).

2.8. Получать согласия на обработку персональных данных у субъектов персональных данных.

2.9. Разъяснять субъекту персональных данных юридические последствия отказа предоставления его персональных данных.

2.10. Обеспечивать постоянный контроль выполнения установленного комплекса мероприятий по обеспечению безопасности информации пользователями информационной системы персональных.

3. Ответственность

3.1. В случае нарушения положений настоящей Инструкции ответственные за обработку персональных данных лица несут ответственность в соответствии с действующим законодательством.

**Инструкция администратора безопасности информационной системы
персональных данных в государственном бюджетном учреждении республики Дагестан
«Комплексный центр социального обслуживания населения в муниципальном образовании
«Сергокалинский район»**

1. Общие положения

1.1. Настоящая инструкция разработана на основании:

- Федерального закона Российской Федерации от 27.07.2006г. №152-ФЗ «О персональных данных»;
- Положения «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного Постановлением Правительства Российской Федерации №781 от 17 ноября 2007г.;
- Приказа №58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных», утвержденного ФСТЭК России от 05.02.2010 г.;

1.2. Инструкция определяет основные задачи, функции, обязанности, права и ответственность Администратора безопасности информационной системы персональных данных (далее – ИСПДн) ГБУ РД КЦСОН в МО «Сергокалинский район» (далее - Учреждение).

1.3. Администратор безопасности ИСПДн (далее – Администратор) назначается приказом директора Учреждения.

1.4. Закрепление функциональных обязанностей и разделение зон ответственности производится приказом директора Учреждения.

1.5. В своей деятельности Администратор руководствуется требованиями действующих федеральных законов, общегосударственных, ведомственных, а также внутренних нормативных документов по вопросам защиты информации и обеспечивает их выполнение пользователями ИСПДн.

1.6. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам защиты информации и не исключает обязательного выполнения их требований.

2. Задачи и функции администратора

2.1. Основными задачами Администратора являются:

- сопровождение средств защиты информации (в том числе криптографических, шифровальных) от несанкционированного доступа (далее – СЗИ) и основных технических средств и систем (далее – ОТСС);
- организация разграничения доступа;
- контроль эффективности защиты информации.

2.2. Для выполнения поставленных задач на Администратора возлагаются следующие функции:

2.2.1. Допуск пользователей (разработчиков, эксплуатационного персонала) к техническим, программным средствам и информационным ресурсам ИСПДн.

2.2.2. Участие на стадии проектирования (внедрения) ИСПДн в разработке технологии обработки информации конфиденциального характера (далее – Информации) по вопросам:

- организация порядка учета, хранения и обращения с документами и носителями информации;
- подготовки инструкций, определяющих задачи, функции, ответственность, права и обязанности пользователей ИСПДн по вопросам защиты информации, а также ответственных по защите информации в процессе автоматизированной обработки информации;
- сопровождение СЗИ, в том числе средств криптографической защиты информации, на стадии эксплуатации ИСПДн, включая ведение служебной

информации СЗИ (управление ключевой системой, сопровождение правил разграничения доступа), оперативный контроль за функционированием СЗИ;

- контроль выполнения требований действующих нормативных документов по вопросам защиты информации при обработке информации в ИСПДн;
- контроль соответствия общесистемной программной среды эталону (контроль целостности программного обеспечения) и проверка включаемых в ИСПДн новых программных средств.

3. Обязанности администратора

3.1. Для реализации поставленных задач и возложенных функций Администратор ОБЯЗАН:

- Вести учет (по вопросам обеспечения безопасности информации) и знать перечень установленных в подразделениях Учреждениях СЗИ и перечень задач, решаемых с их использованием;
- Вести журнал учета эксплуатационной и технической документации СЗИ ИСПДн.
- Вести журнал учета машинных носителей персональных данных.
- Осуществлять непосредственное управление режимами работы и административную поддержку функционирования (настройку и сопровождение) применяемых на автоматизированных рабочих местах (далее – АРМ) специальных программных и программно-аппаратных СЗИ;
- Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных АРМ и серверов, осуществлять проверку работоспособности системы защиты после установки (обновления) программных средств ИСПДн;
- Периодически проверять состояние используемых СЗИ, осуществлять проверку правильности их настройки (выборочное тестирование);
- Контролировать соответствие технического паспорта ИСПДн фактическому составу (комплектности) ИСПДн и вести учет изменений аппаратно-программной конфигурации (архив заявок, на основании которых были произведены данные изменения в ИСПДн);
- Периодически контролировать целостность печатей (пломб, наклеек) на устройствах защищенных АРМ;
- Вести журнал учета нештатных ситуаций, фактов вскрытия и опечатывания АРМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств ИСПДн;
- Проводить периодический инструктаж сотрудников подразделения (пользователей ИСПДн) по правилам работы с используемыми средствами и системами защиты информации.

3.1.2. Организовывать разграничения доступа:

3.1.2.1. Участвовать в разработке и знать перечень защищаемых информационных ресурсов.

3.1.2.2. Разрабатывать для ИСПДн решения по:

- составу доменов сети, системы доверительных отношений между ними;
- составу групп (локальных и глобальных) каждого домена;
- приписке пользователей с одинаковыми правами, статусом безопасности и характером решаемых задач к соответствующим группам;
- определению информационных связей между сегментами сети и требований к изоляции сегментов с использованием средств аппаратной безопасности сегментов;
- вести учет заявок пользователей на допуск к информационным ресурсам ИСПДн;
- осуществлению контроля за наличием активных компьютеров сети, состоянием активных пользователей, использованием разделяемых ресурсов, процессом печати на общих принтерах;
- разработке порядка пользования электронной почтой (определение списка абонентов из состава пользователей сети, проектированию системы почтовых ящиков, использованию СЗИ при передаче закрытых документов);
- разработке порядка выхода пользователей в сети связи общего пользования (далее – Сети) и использованию встроенных СЗИ в сервисных программах;

- определению режимов использования СЗИ: защита паролей, защита в протоколах передачи данных, кодирование файлов, подключение дополнительных алгоритмов криптографической защиты;
- разработке политики аудита: определению состава регистрируемых событий и списка лиц, имеющих допуск к журналам аудита;
- осуществлять учет и периодический контроль за составом и полномочиями пользователей различных АРМ ИСПДн;
- контролировать и требовать соблюдения установленных правил по организации парольной защиты в ИСПДн в Учреждении;
- осуществлять оперативный контроль за работой пользователей защищенных АРМ, анализировать содержимое журналов событий операционных систем (далее - ОС), систем управления базами данных (далее - СУБД), пакетов прикладных программ (далее - ППП) и СЗИ всех АРМ и адекватно реагировать на возникающие нештатные ситуации. Обеспечивать своевременное архивирование журналов событий АРМ и надлежащий режим хранения данных архивов;
- принимать участие в работах по внесению изменений в аппаратно-программную конфигурацию серверов и АРМ ИСПДн;
- обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания АРМ и отправке их в ремонт (контролировать стирание информации на съемных носителях);
- организовывать учет, хранение, прием и выдачу персональных идентификаторов ответственным исполнителям, осуществлять контроль за правильностью их использования;
- осуществлять периодический контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных;
- по указанию руководства своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах по управлению СЗИ, установленных на АРМ ИСПДн;
- требовать от пользователей стирания остаточной информации на несъемных носителях (жестких дисках) установленным порядком, а в оперативной памяти по окончании обработки информации путем перезагрузки АРМ;
- контролировать обеспечение защиты конфиденциальной информации при взаимодействии абонентов с информационными сетями связи общего пользования.

3.1.3. Контролировать эффективность защиты информации:

- Проводить работу по выявлению возможности вмешательства в процесс функционирования ИСПДн и осуществления НСД к информации и техническим средствам АРМ;
- Докладывать ответственному по обеспечению безопасности о выявленных угрозах безопасности информации, обрабатываемой в ИСПДн, об имевших место попытках НСД к информации и техническим средствам АРМ;
- Проводить занятия с пользователями ИСПДн по правилам работы на АРМ, оснащенных СЗИ, и по изучению руководящих документов по вопросам обеспечения безопасности информации с разбором недостатков, выявленных при контроле эффективности защиты информации;
- Участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в ИСПДн.

3.2. Администратору ЗАПРЕЩАЕТСЯ:

- 3.2.1. Используя служебное положение, создавать ложные информационные сообщения и учетные записи пользователей, получать доступ к информации и предоставлять его другим с целью ознакомления, модификации, копирования, уничтожения, блокирования доступа к информации.
- 3.2.2. Использовать ставшие доступными в ходе исполнения обязанностей идентификационные данные пользователей (имя, пароль, ключи и т.п.) для маскирования своих действий.
- 3.2.3. Самостоятельно (без согласования с подразделением автоматизации) вносить изменения в настройки серверной части ИСПДн.

3.2.4. Использовать в своих и в чьих-либо личных интересах ресурсы ИСПДн, предоставлять такую возможность другим.

3.2.5. Выключать СЗИ без письменной санкции руководства.

3.2.6. Передавать третьим лицам тем или иным способом сетевые адреса, имена, пароли, информацию о привилегиях пользователей, конфигурационные настройки.

3.2.7. Производить в рабочее время действия, приводящие к сбою, остановке, замедлению работы ИСПДн, блокированию доступа, потере информации без санкции руководства и предупреждения пользователей.

3.2.8. Нарушать правила эксплуатации оборудования ИСПДн.

3.2.9. Корректировать, удалять, подменять журналы аудита.

4. Права и ответственность администратора

4.1. Администратор имеет право:

- получать доступ к программным и аппаратным средствам ИСПДн, средствам их защиты, а также просмотру прав доступа к ресурсам на серверах ИСПДн и АРМ пользователей;

- требовать от пользователей ИСПДн выполнения инструкций по обеспечению безопасности и защите информации в ИСПДн;

- участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИСПДн;

- осуществлять оперативное вмешательство в работу пользователя при явной угрозе безопасности информации в результате несоблюдения установленной технологии обработки информации и невыполнения требований по безопасности;

- производить анализ защищенности ИСПДн путем применения специального программного обеспечения, осуществления попыток взлома системы защиты ИСПДн. Такие работы должны проводиться в часы наименьшей информационной

нагрузки с обязательным уведомлением сотрудников подразделений автоматизации и обеспечение безопасности информации;

- вносить свои предложения по совершенствованию мер защиты в ИСПДн.

4.2. Администратор несет ответственность за:

- реализацию принятой в НГГУ политики информационной безопасности;

- программно - технические и криптографические средства защиты информации, средства вычислительной техники, информационно - вычислительные комплексы, сети и ИСПДн обработки информации, закрепленные за ним приказом Ректора НГГУ, а также за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями;

- разглашение сведений, конфиденциального характера, ставших известными ему по роду работы;

- качество и последствия проводимых им работ по контролю действий пользователей при работе в ИСПДн.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

АИБ ИС ПДн – администратор информационной безопасности информационных систем персональных ;

ИС ПДн – информационная система персональных данных;

ЛВС- локально-вычислительная сеть;

ПО - программное обеспечение;

СЗИ - средства защиты информации;

НСД - несанкционированный доступ;

Аудентификация- проверка подлинности пользователя путём сравнения введённого им пароля с паролем, сохранённым в базе данных пользователей;

ОТТС – основные технические средства и системы;

ВТСС – вспомогательные технические средства и системы;

ПЭВМ- персональная электронно-вычислительная машина

С инструкцией ознакомлен М.И.С. «24» 12 20 18 г

ИНСТРУКЦИЯ

по порядку учета, хранения и уничтожения персональных данных в государственном бюджетном учреждении республики Дагестан «Комплексный центр социального обслуживания населения в муниципальном образовании «Сергокалинский район»

Общие положения

- 1.1. Все информационные ресурсы, содержащие персональные данные, подлежат учету.
- 1.2. Учет осуществляется по журналам установленной формы, в том числе автоматизировано с использованием средств вычислительной техники.
- 1.3. Ведется Перечень информационных ресурсов, содержащих персональные данные.
- 1.4. В журнале указываются следующие реквизиты информационных ресурсов, содержащих персональные данные: учетный номер и дата поступления, откуда поступил, срок обработки, а также другие возможные реквизиты, идентифицирующие информационный ресурс.
- 1.5. Носители информационных ресурсов, содержащих персональные данные, должны сдаваться на хранение.

2. Хранение и уничтожение персональных данных

- 2.1. Персональные данные субъекта ПДн хранятся в подразделении (ином структурном отделе) государственного бюджетного учреждения республики Дагестан «Комплексный центр социального обслуживания населения в муниципальном образовании «Сергокалинский район» (далее – учреждение), которое производит их обработку и отвечает за взаимодействие с субъектом.
- 2.2. ПДн на бумажном носителе хранятся в папках в сейфе или в металлическом шкафу.
- 2.3. Персональные данные субъекта ПДн в электронном виде хранятся в локализованных электронных базах данных компьютерной сети. Доступ к электронным базам данных, содержащим персональные данные субъекта, обеспечиваются Системой защиты персональных данных.
- 2.4. В нерабочее время помещение, где хранятся ПДн (хранилище ПДн), должно закрываться на ключ. В рабочее время помещение должно быть закрыто на ключ или оставлено под ответственность лиц, назначенных руководителем.
- 2.5. Сотрудник организации, имеющий доступ к персональным данным субъектов ПДн, в связи с исполнением трудовых обязанностей, обеспечивает хранение информации, содержащей персональные данные субъекта, исключая доступ к ним третьих лиц.
- 2.6. В отсутствие сотрудника на его рабочем месте не должно быть документов, содержащих персональные данные субъектов (соблюдение "политики чистых столов").
- 2.7. При уходе в отпуск, служебной командировке и иных случаях длительного отсутствия сотрудника на своем рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные субъектов ПДн лицу, на которое приказом (распоряжением) будет возложено исполнение его трудовых обязанностей.

- 2.8. В случае если такое лицо не назначено, то документы и иные носители, содержащие персональные данные субъектов ПДн по указанию руководителя структурного подразделения, передаются другому сотруднику, имеющему доступ к персональным данным субъектов ПДн.
- 2.9. При увольнении сотрудника, имеющего доступ к персональным данным субъектов ПДн, документы и иные носители, содержащие персональные данные субъектов ПДн, по указанию руководителя структурного подразделения передаются другому сотруднику, имеющему доступ к персональным данным субъектов ПДн.
- 2.10. Повседневный контроль за выполнением требований по защите хранилищ ПДн осуществляют лица, ответственные за помещение (хранилище ПДн).
- 2.11. Периодический контроль эффективности мер защиты хранилищ ПДн осуществляется постоянно действующей технической комиссией учреждения (ПДТК).
- 2.12. Уничтожение персональных данных субъектов ПДн на бумажном носителе, либо удаление электронных баз данных, содержащих персональные данные субъектов ПДн в электронном виде, осуществляется по истечении установленного срока обработки ПДн постоянно действующей технической комиссией учреждения (ПДТК).

3. Ответственность

3.1. Сотрудники, нарушившие требования настоящей Инструкции, несут ответственность в соответствии с действующим законодательством и локальными правовыми актами.

ИНСТРУКЦИЯ

о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных в государственном бюджетном учреждении республики Дагестан «Комплексный центр социального обслуживания населения в муниципальном образовании «Сергокалинский район»

1. Назначение и область действия

1.1. Данная Инструкция определяет действия, связанные с мерами и средствами поддержания непрерывной работы и восстановления работоспособности информационных систем в ГБУ РД КЦСОН в МО «Сергокалинский район»

1.2. Настоящая Инструкция регламентирует:

- меры защиты от потери информации;
- действия по восстановлению в случае потери информации.

1.3. Действие настоящей Инструкции распространяется на администраторов информационных систем, ответственных за резервное копирование информации.

2. Меры обеспечения надежной работы и восстановления ресурсов при возникновении инцидентов

2.1. Технические меры.

2.1.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как:

- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;

2.1.2. Системы жизнеобеспечения информационных систем персональных данных (далее – ИСПДн) включают:

- пожарные, охранные сигнализации;
- системы вентиляции и кондиционирования;

2.1.3. Все критичные помещения (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации.

2.1.4. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

2.1.5. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на носитель (ленту, жесткий диск и т.п.).

2.2. Организационные меры.

2.2.1. Резервное копирование и хранение данных должно осуществляться на периодической основе:

- для обрабатываемых персональных данных – не реже раза в неделю или по требованию пользователя ИСПДн;
- для системной информации – не реже раза в месяц;

2.2.2. Данные о проведении процедуры резервного копирования должны отражаться в специально созданном Журнале учета, по форме согласно приложения к настоящей Инструкции.

2.2.3. Носители должны храниться в негорючем шкафу или помещении, оборудованном системой пожаротушения.

2.2.4. Носители и резервные копии данных должны храниться не менее года для возможности восстановления данных.

3. Порядок проведения резервирования информации

3.1. Перед проведением процедуры резервного копирования необходимо убедиться в том, что все пользователи информационной системы завершили свою работу с информационной системой.

3.2. Резервирование информации в информационных системах персональных данных проводится при помощи штатных средств, поставляемых в составе специализированного программного обеспечения для построения информационной системы, либо, в случае отсутствия таковых, штатными средствами операционной системы или системы управления базами данных (при использовании таковой).

3.3. Архивация может производиться как штатными средствами, поставляемыми в составе специализированного программного обеспечения для построения информационной системы, так и сторонним программным обеспечением (например, 7zip, WinRar).

3.4. Резервные копии должны сохраняться на носители, не входящие в состав технических средств информационной системы персональных данных (внешние жесткие диски, CD/DVD диски, flash диски).

3.5. После завершения процедуры резервного копирования информации и записи резервной копии на носитель, необходимо поместить носитель с резервной копией в специально отведенное для хранения место и проставить соответствующую отметку в Журнале.

4. Порядок проведения восстановления информации

4.1. Перед проведением процедуры восстановления информации необходимо убедиться в том, что все пользователи информационной системы завершили свою работу с информационной системой.

4.2. Восстановление информации следует проводить из наиболее актуальной резервной копии.

4.3. В случае, если специализированное программное обеспечение для построения информационной системы не позволяет работать с заархивированными резервными копиями, то перед восстановлением информации необходимо разархивировать файлы резервной копии при помощи стороннего программного обеспечения (например, 7zip, WinRar).

4.4. Восстановление информации в информационных системах персональных данных проводится при помощи штатных средств, поставляемых в составе специализированного программного обеспечения для построения информационной системы, либо, в случае отсутствия таковых, штатными средствами операционной системы или системы управления базами данных (при использовании таковой).

4.5. После завершения процедуры восстановления необходимо убедиться в работоспособности информационной системы персональных данных.

4.6. В случае успешного восстановления оповестить пользователей информационной системы о возможности продолжения работы. В противном случае необходимо изучить документацию, прилагаемую к программному обеспечению либо обратиться в службу технической поддержки.

5. Ответственность

5.1. Работники, нарушившие требования данной Инструкции, несут ответственность

ИНСТРУКЦИЯ
по проведению антивирусного контроля и информационных систем персональных
данных в Государственном бюджетном учреждении республики Дагестан «Комплексный
центр социального обслуживания населения в муниципальном образовании
«Сергокалинский район»

1. ОБЩИЕ ПОЛОЖЕНИЯ

- 1.1. Настоящая Инструкция определяет требования к организации антивирусной защиты информационных систем персональных данных ГБУ РД КЦСОН в МО «Сергокалинский район» (далее - Учреждение).
- 1.2. Настоящая Инструкция предназначена для должностного лица, выполняющего функции уполномоченного лица безопасности информации, и пользователей, осуществляющих обработку персональных данных в Учреждении.
- 1.3. В целях обеспечения защиты от деструктивных воздействий компьютерных вредоносных программ производится антивирусный контроль. Обязательному антивирусному контролю подлежит любая информация, поступающая на средства вычислительной техники, в том числе получаемая на внешних носителях из сторонних организаций.
- 1.4. Вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на ресурсы информационных систем. Вредоносная программа способна выполнять ряд функций, в том числе:
- скрывать признаки своего присутствия в программной среде рабочей станции (сервера);
 - обладать способностью к самодублированию, ассоциированию себя с другими программами и/или переносу своих фрагментов в иные области оперативной или внешней памяти;
 - разрушать (искажать произвольным образом) код программ в оперативной памяти;
 - сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
 - искажать произвольным образом, блокировать и/или подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.
- 1.6. Основными задачами системы обеспечения антивирусной защиты являются:
- исключение или существенное затруднение противоправных действий в отношении ИСПДн Учреждения как носителей защищаемой информации;
 - обеспечение условий для устойчивой бесперебойной работы объектов, сетей передачи данных.
- 1.7. Обеспечение антивирусной защиты включает:
- регулярные профилактические работы;
 - анализ ситуации проявления вредоносных программ и причины их появления;
 - уничтожение вредоносных программ на автоматизированных рабочих местах (АРМ) (серверах);
 - принятие мер по предотвращению причин появления вредоносных программ.
- 1.8. Организация работ по антивирусной защите и ответственность за сопровождение системы антивирусной защиты возлагается на техника-программиста
- 1.9. Работники, на которых возлагается ответственность по антивирусной защите, имеют полномочный доступ ко всем АРМ, серверам и другому оборудованию ИСПДн Учреждения.
- 1.10. Все процессы производятся в автоматическом режиме без участия пользователей и без помех для работы основного и специального ПО.
- Процесс плановой полной проверки файловой системы рабочих станций пользователей и серверов ИСПДн Учреждения проводится во время наименьшей нагрузки оборудования пользовательскими задачами.

1.11. Работник, отвечающий за ежедневное сопровождение антивирусной защиты, обладает необходимыми практическими навыками и теоретическими знаниями по данному вопросу. В основные обязанности по антивирусной защите входит:

- проведение периодического анализа и оценки ситуации по обеспечению антивирусной безопасности для контроля степени защищенности ИСПДн и выработки предложений по изменению и улучшению состояния дел;
- проверка соблюдения порядка обновления средств и баз данных антивирусной защиты;
- осуществление контроля за состоянием средств антивирусной защиты на серверах, рабочих ПК ;
- осуществление контроля за соблюдением работниками требований по обеспечению антивирусной защиты;
- обеспечение контроля за соблюдением требований при работе с сетью Интернет, а также за характером и объемом трафика, получаемого из сети Интернет, и его соответствия служебной необходимости;

Работник ответственный осуществляют следующие действия:

- контроль и анализ еженедельных отчетов по состоянию антивирусной защиты;
- проведение служебных расследований по фактам обнаружения вредоносных программ, повлекших неустойчивую работу и (или) разрушение технологического оборудования, локально-вычислительной сети и информационных систем
- организацию мероприятий по улучшению антивирусной защиты Учреждения

1.12. Устанавливаемое (изменяемое) ПО в ИСПДн Учреждения предварительно проверяется представителем эксплуатирующего подразделения на отсутствие вредоносных программ. Непосредственно после установки (изменения) ПО администратор безопасности либо уполномоченный работник подразделения ИТ выполняет антивирусную проверку на рабочих станциях и серверах ИСПДн Учреждения

1.13. При возникновении подозрения на наличие вредоносных программ (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) администратор безопасности либо уполномоченный работник подразделения ИТ проводит внеочередной антивирусный контроль рабочих станций (серверов) ИСПДн Учреждения

1.18. Для пользователей рабочих станций ИСПДн Учреждения запрещена возможность изменения настроек и параметров защиты антивирусных средств на своей рабочей станции, эти действия производит администратор безопасности или уполномоченный работник подразделения ИТ с помощью средств централизованного управления или вручную.

1.19. По факту появления и проникновения вредоносных программ, повлекших неустойчивую работу и (или) вывод из строя технологического оборудования, локально-вычислительной сети и информационных массивов

Учреждения, проводится служебное расследование Группой реагирования на инциденты информационной безопасности.

1.20. Результаты расследования причин появления и последствий воздействия вредоносных программ на рабочую станцию (сервер) докладываются руководителю Отдела информационной безопасности территориального органа Учреждения с предложениями по принятию мер, предотвращающих в будущем повторение подобных фактов.

2. ТРЕБОВАНИЯ К АНТИВИРУСНОМУ ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

2.1. Применение только лицензионного антивирусного ПО.

2.2. Возможность обнаружения как можно большего числа известных вредоносных программ, в том числе вирусов, деструктивного кода (макро-вирусы, объектов ActiveX, апплетов языка Java и т.п.), а также максимальная готовность быстрого реагирования на появление новых видов вирусных угроз.

2.3. Исчерпывающий список защищаемых точек (почтовые серверы, файловые серверы, автоматизированные рабочие места и т.д.) возможного проникновения вредоносных программ.

- 2.4. Обеспечение обновлений, консультаций и других форм сопровождения эксплуатации поставщиком антивирусного ПО.
- 2.5. Возможность автоматического распространения обновлений антивирусных баз на каждую рабочую станцию (сервер) в ИСПДн Учреждения
- 2.6. Соответствие системных требований антивирусного ПО платформам, характеристикам и комплектации применяемой вычислительной техники.
- 2.7. Надежность и работоспособность антивирусного ПО в любом из предусмотренных режимов работы, по возможности, в русскоязычной среде.
- 2.8. Наличие документации, необходимой для практического применения и освоения антивирусного ПО, на русском языке.

3. МЕРОПРИЯТИЯ ПО ШТАТНОМУ УПРАВЛЕНИЮ СРЕДСТВАМИ АНТИВИРУСНОГО КОНТРОЛЯ

3.1. В штатном режиме работы системы антивирусной уполномоченный работник подразделения ИТ выполняет:

- установку средств антивирусной защиты на все объекты антивирусной защиты, добавляемые в средства защиты ИСПДн Учреждения в порядке, описанном в эксплуатационной документации;
- контроль наличия связи между сервером администрирования и защищаемыми объектами;
- необходимые обновления версий средств антивирусной защиты на объектах антивирусной защиты;
- контроль над выполнением задач постоянной защиты;
- настройку автоматических проверок объектов антивирусной защиты не реже одного раза в неделю с целью профилактики;
- контроль актуальности версий антивирусных баз и модулей сканирования ПО сервера администрирования;
- непрерывный мониторинг информационного обмена в средствах защиты ИСПДн Учреждения с целью выявления проявлений программно-математических воздействий;
- обработку сведений, поступающих от средств антивирусной защиты;
- формирование сводных отчетов о работе средств антивирусной защиты, инцидентах и проч.;
- обработку отчетов о состоянии логических сетей;
- формирование отчетов о работе средств антивирусной защиты логической сети.

3.2. Процесс управления системой антивирусной защиты включает в себя следующие действия администратора безопасности либо уполномоченного работника подразделения ИТ:

- внесение изменений в политику антивирусной защиты;
- управление средствами антивирусной защиты, входящими в состав системы антивирусной защиты;
- мониторинг событий, информация о которых поступает от средств антивирусной защиты с объектов защиты.

3.3. В обязанности администратора безопасности либо уполномоченного работника подразделения ИТ входит проведение мероприятий, обеспечивающих возможность анализа результатов работы средств системы антивирусной защиты:

- разработка отчетов о работе средств антивирусной защиты;
- разработка сводных отчетов о работе средств антивирусной защиты, инцидентах и пр. за месяц.

В отчетах о состоянии системы антивирусной защиты отражается следующая информация:

- количество обнаруженных вредоносных программ за данный период;
- наиболее активные обнаруженные вредоносные программы;
- объекты, где наблюдается наибольшая частота обнаружения вредоносных программ;
- список зараженных объектов.

4. МЕРОПРИЯТИЯ ПО НЕШТАТНОМУ УПРАВЛЕНИЮ СРЕДСТВАМИ АНТИВИРУСНОГО КОНТРОЛЯ

4.1. В случае заражения рабочих станций (серверов) вредоносными программами администратор безопасности выполняет следующие действия:

- централизованно обновляет антивирусные базы сервера администрирования и всех объектов антивирусной защиты;
 - проверяет состояние всех объектов антивирусной защиты, наличие зараженных рабочих станций в случае обнаружения пораженных узлов;
 - оперативно принимает меры по предотвращению распространения заражения вредоносными программами и при необходимости отключает от сети зараженный ПК
 - проводит действия, направленные на устранение вредоносной программы на всех пораженных узлах ИСПДн Учреждения;
 - по завершении мероприятий по устранению последствий заражения восстанавливает работоспособность рабочей станции и передает ее ответственному пользователю.
- 4.2. Все или часть вышеперечисленных мероприятий может быть делегирована уполномоченному работнику подразделения ИТ.

5. УНИЧТОЖЕНИЕ ВРЕДНОСНЫХ ПРОГРАММ

- 5.1. Уничтожение вредоносных программ выполняется уполномоченным работником подразделения ИТ.
- 5.2. Если вредоносная программа поразила какие-либо программы, то уничтожение вредоносной программы выполняется путем уничтожения программы на жестком диске либо на ином магнитном носителе. После уничтожения зараженной программы восстанавливают программу, используя ее резервную копию.
- 5.3. Если вредоносная программа поразила файлы, то вредоносная программа уничтожается либо путем стирания этих файлов, либо путем использования специального "лечащего" режима антивирусного ПО. Использование "лечащего" режима не дает полной гарантии восстановления файла, поэтому после "лечения" необходима проверка восстановления данного файла. "Лечащие" программы используются лишь в тех случаях, когда отсутствует резервная копия зараженной программы или файла с данными либо восстановление уничтоженного файла с помощью резервной копии очень трудоемко.
- 5.4. В любом случае после уничтожения вредоносных программ и восстановления зараженных программ и файлов с данными еще раз выполняется проверка наличия вредоносных программ, используя антивирусную программу с установленными последними обновлениями. Перед повторной проверкой производится перезагрузка сервера или рабочей станции через выключение и последующее их включение. Если повторная проверка не выявила вредоносных программ, то можно быть уверенным в их отсутствии.

6. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЕЙ

- 6.1. Организация мероприятий по централизованной антивирусной защите ИСПДн Учреждения возлагается на техника -программиста
- 6.2. Техник -программист несет ответственность за формирование политики антивирусной защиты, организацию своевременной инсталляции средств антивирусной защиты информации и централизованное обновление баз данных вирусных описаний на комплексе программно-технических средств ИСПДн Учреждения
- 6.3. Выполнение технических мероприятий по централизованной антивирусной защите в ИСПДн Учреждения производится непосредственно администратором безопасности либо делегируется уполномоченному работнику подразделения ИТ.
- 6.4. Непосредственную ответственность за соблюдение в повседневной деятельности установленных норм обеспечения антивирусной защиты информации и требований настоящей Инструкции в части защиты ИСПДн Учреждения несут пользователи, за которыми закреплены соответствующие рабочие станции ИСПДн Учреждения

Инструкция
по организации парольной защиты в Государственном бюджетном учреждении
республики Дагестан «Комплексный центр социального обслуживания населения в
муниципальном образовании «Сергокалинский район»

1. Общие положения

1.1. Настоящая Инструкция определяет порядок организации парольной защиты на объекте информатизации «Информационная система персональных данных в государственном бюджетном учреждении республики Дагестан «Комплексный центр социального обслуживания населения в муниципальном образовании «Сергокалинский район» (далее - ИСПДн).

1.2. Настоящая Инструкция предназначена для использования в работе в ИСПДн и определяет порядок обеспечения защиты информации (далее – ЗИ) при использовании подсистемы парольной защиты от несанкционированного доступа (далее – НСД).

1.3. Парольная защита при работе в ИСПДн осуществляется с целью предотвращения НСД к конфиденциальной информации, содержащей персональные данные.

1.4. Парольная защита ИСПДн является составной частью подсистемы управления доступом общей системы защиты от НСД.

К основным видам (категориям) паролей относятся: пароли BIOS; пароль доступа средств защиты информации (далее – СЗИ) от НСД; пароли систем доступа, встроенных в используемые операционные системы (далее – ОС); пароли доступа к прикладным программам, обеспечивающим доступ к защищаемой информации; пароли доступа к специализированному программному обеспечению (далее - СПО), предназначенному для работы с защищаемой информацией.

1.5. Порядок работы с паролями вводится с момента подписания данной Инструкции.

2. Требования к организации парольной защиты объекта информатизации

Личные пароли доступа к ИСПДн, СЗИ от НСД ИСПДн, первично назначаются пользователям Администратором информационной системы при формировании персонального идентификатора, при этом необходимо руководствоваться следующими требованиями: длина пароля должна быть не менее 8 символов;

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства, наименования ИСПДн, общепринятые сокращения (ЭВМ, ЛВС, USER, SYSOP, GUEST, ADMINISTRATOR и т.д.), и другие данные, которые могут быть подобраны путем анализа информации об ответственном исполнителе;

- не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

- не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т. п.);

- при смене пароля новое значение должно отличаться от предыдущего не менее, чем в 5 позициях;

- в числе символов пароля могут присутствовать латинские буквы, цифры, символьные знаки;

- не использовать ранее использовавшиеся пароли.

2.1. Лица, использующие пароли, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по использованию парольной защиты;
 - своевременно сообщать Администратору информационной системы обо всех нештатных ситуациях, нарушениях работы подсистем защиты от НСД, возникающих при работе с паролями.
- 2.2. При организации парольной защиты запрещается: записывать свои пароли в очевидных местах (внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.п.); хранить пароли в записанном виде в рабочих тетрадях, на отдельных листах бумаги; сообщать посторонним лицам свои пароли, а также сведения о применяемой системе защиты от НСД.
- 2.2. Специалист, в ведении которого находится ИСПДн, несет личную ответственность за организацию работ по безусловному выполнению требований настоящей инструкции и других документов, регламентирующих использование парольной защиты.
- 2.3. Ответственность за непосредственную работу с паролями (своевременный ввод, замену и уничтожение) возлагается на Администратора информационной системы.
- 2.4. На Администратора информационной системы возлагаются следующие задачи: обеспечение руководства над функционированием системы парольной защиты; контроль над реализацией требований по обеспечению безопасности информации при использовании паролей и их своевременную смену в ИСПДн.

3. Порядок применения парольной защиты

- 3.1. Порядок применения парольной защиты основанной на использовании СЗИ от НСД приведен в руководствах Администратора БИ и пользователя ИСПДн. Защита с применением паролей других программно – технических средств и программных продуктов осуществляется, при их наличии, в соответствии с эксплуатационной документацией на эти средства. Полная плановая смена паролей в ИСПДн проводится регулярно Администратором информационной системы и пользователями, не реже одного раза в 2 (два) месяца.
- 3.2. Удаление (в т.ч. внеплановая смена) личного пароля должна производиться в следующих случаях:
- по окончании срока действия;
 - в случае прекращения полномочий пользователя (увольнение, переход на другую работу, не связанную с обработкой персональных данных);
 - по указанию заведующей отделением или администратора информационной безопасности.
- 3.3. Пароли, используемые для локального доступа к ресурсам ИСПДн, вводятся пользователем с клавиатуры.
- 3.4. Компрометация действующих паролей является нештатной ситуацией, о чем Администратор информационной системы незамедлительно сообщает руководителю.
- 3.5. Под компрометацией понимается хищение, утрата действующих паролей, передача или сообщение их лицам, не имеющим на то право, другие действия должностных лиц, приведшие к получению его пароля лицами, не имеющими на то права.
- 3.6. Скомпрометированные пароли и связанные с ними персональные идентификаторы пользователей выводятся из действия. Порядок внеплановой смены пароля аналогичен плановой смене паролей.

ПОРЯДОК
работы с инцидентами информационной безопасности в государственном бюджетном
учреждении республики Дагестан «Комплексный центр социального обслуживания
населения в муниципальном образовании «Сергокалинский район»

I. Общие положения

1. Порядок работы с инцидентами информационной безопасности в государственном бюджетном учреждении республики Дагестан «Комплексный центр социального обслуживания населения в муниципальном образовании «Сергокалинский район» разработан в целях выявления наиболее актуальных угроз информационной безопасности, определения порядка действий пользователей информационных систем ГБУ РД КЦСОН в МО «Сергокалинский район» при возникновении инцидентов информационной безопасности (далее – Учреждение) и повышения общего уровня защищенности информационных ресурсов и информационных систем Учреждение.

Настоящий Порядок разработан в соответствии с Федеральным законом № 152-ФЗ «О персональных данных», Федеральным законом № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2. Инцидент информационной безопасности – одно событие или группа событий, которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности, в том числе при обработке персональных данных.

Инциденты информационной безопасности могут быть преднамеренными или случайными и могут вызываться как техническими, так и физическими средствами. Их последствиями могут быть такие события, как несанкционированное изменение информации, ее уничтожение или другие события, которые сделают информацию недоступной.

3. К инцидентам информационной безопасности относятся:

- разглашение информации ограниченного распространения, не составляющей государственную тайну (далее – защищаемая информация);
- передача защищаемой информации по открытым каналам связи;
- обработка защищаемой информации на незащищенных технических средствах обработки информации;
- опубликование защищаемой информации в средствах массовой информации;
- передача носителя защищаемой информации лицу, не имеющему права доступа к ней;
- утрата или хищение носителя с защищаемой информацией;
- несанкционированное изменение защищаемой информации;
- несанкционированное копирование защищаемой информации;
- несанкционированный доступ к информационным системам комитета;
- использование закладочных устройств и программных закладок;
- применение программных вирусов;
- неконтролируемые изменения в информационной системе;

нарушение функционирования технических средств обработки информации, в том числе дефекты, сбои, отказы, аварии технических средств;
дефекты, сбои, отказы в работе программного обеспечения.

4. В случае возникновения инцидентов информационной безопасности, порядок действий при которых не регламентирован настоящим Порядком, администратором информационной безопасности, а также пользователем информационной системы и сотрудником, осуществляющим техническое обслуживание информационных систем комитета, вырабатывается конкретный план действий с учетом текущей ситуации.

5. Работа с инцидентами информационной безопасности включает в себя следующие направления:

- определение лиц, ответственных за выявление инцидентов и реагирование на них;
- обнаружение, идентификация и регистрация инцидентов;
- своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационных системах пользователями и администраторами;
- анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а так же оценка их последствий;
- принятие мер по устранению последствий инцидентов;
- планирование и принятие мер по предотвращению повторного возникновения инцидентов.

II. Ответственные за выявление инцидентов информационной безопасности и реагирование на них

6. В информационных системах комитета ответственными за выявление инцидентов информационной безопасности являются:

- работники Учреждения, имеющие право доступа к информационной системе;
- руководитель подразделения Учреждения, в котором выявлен инцидент;
- сотрудники, осуществляющие техническое обслуживание информационной системы;
- администратор информационной безопасности.

7. Ответственными за реагирование на инциденты в информационной системе являются:

- работники Учреждения, имеющие право доступа к информационной системе;
- руководитель подразделения Учреждения, в котором выявлен инцидент;
- сотрудники, осуществляющие техническое обслуживание информационной системы;
- администратор информационной безопасности;
- работник Учреждения, ответственный за организацию обработки персональных данных, в случае, если информационная система является информационной системой персональных данных;

8. Вне информационной системы ответственными за выявление инцидентов являются все работники Учреждения.

- Ответственными за реагирование на инциденты вне информационной системы являются:
- работник Учреждения, обнаруживший инцидент;
- руководитель подразделения, в котором выявлен инцидент;
- администратор информационной безопасности;
- работник Учреждения, ответственный за организацию обработки персональных данных комитета, в случае, если существует угроза безопасности персональных данных.

III. Порядок действий при возникновении инцидентов информационной безопасности

9. Работа по обнаружению инцидентов информационной безопасности включает в себя мероприятия, направленные на выявление инцидентов в области информационной безопасности с помощью технических средств, в ходе контрольных мероприятий, с помощью работников Учреждения.

10. Работник Учреждения (пользователь), обнаруживший инцидент в информационной системе, должен незамедлительно, любым доступным способом, сообщить об инциденте непосредственному руководителю, администратору информационной безопасности, работнику Учреждения, ответственному за организацию обработки персональных данных (в случае, если информационная система является информационной системой персональных данных).

11. Администратор информационной безопасности осуществляет регистрацию инцидентов в журнале учета нештатных ситуаций Учреждения и принимает незамедлительные меры к идентификации источника инцидента информационной безопасности, восстановлению работоспособности информационной системы и устранению дестабилизирующих факторов.

Хранение журнала осуществляется в местах, исключающих доступ к журналу посторонних лиц. Журнал хранится в течение 5 лет после завершения ведения. Ответственный за хранение ведения и хранение журнала – администратор информационной безопасности Учреждения.

12. Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а так же оценку их последствий осуществляет администратор информационной безопасности совместно с сотрудниками, осуществляющими техническое обслуживание информационных систем Учреждения.

13. Меры по устранению последствий инцидентов включают в себя мероприятия, направленные на определение границ инцидента и ущерба от реализации угроз информационной безопасности, а также на ликвидацию последствий инцидента и полное, либо частичное возмещение ущерба.

14. Оценка последствий инцидента производится на основании потенциально возможного ущерба.

15. Планирование и принятие мер по предотвращению повторного возникновения инцидентов информационной безопасности основывается на проведении мероприятий по обучению работников Учреждения правилам и способам работы со средствами защиты информационных систем, доведении до работников Учреждения норм и требований законодательства Российской Федерации и законодательства Ставропольского края, нормативных правовых актов Учреждения, устанавливающих ответственность за нарушение требований информационной безопасности, своевременной модернизации системы обеспечения информационной безопасности с учетом возникновения новых угроз информационной безопасности, своевременном обновлении программного обеспечения, в том числе баз сигнатур антивирусных средств.

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных
данных в государственном бюджетном учреждении республики Дагестан «Комплексный
центр социального обслуживания населения в муниципальном образовании
«Сергокалинский район»

Правила осуществления внутреннего контроля соответствия обработки персональных данных в государственном бюджетном учреждении республики Дагестан «Комплексный центр социального обслуживания населения в муниципальном образовании «Сергокалинский район» требованиям к защите персональных данных (далее – Правила) определяют порядок организации и осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в структурных подразделениях государственном бюджетном учреждении республики Дагестан «Комплексный центр социального обслуживания населения в муниципальном образовании «Сергокалинский район» (далее – Учреждение).

1. Общие положения

1.1. Настоящими Правилами определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных.

1.2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон), постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.3. В настоящих Правилах используются основные понятия в значениях, определённых статьёй 3 Федерального закона.

1.4. Внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных (далее – внутренний контроль) в структурных подразделениях Учреждения осуществляется с целью определения наличия несоответствий между требуемым уровнем защиты персональных данных и его фактическим состоянием, а также выработки мер по их устранению и недопущению в дальнейшем.

1.5. Внутренний контроль осуществляется комиссией по проведению внутреннего контроля соответствия обработки персональных данных в Учреждении требованиям к защите персональных данных (далее – комиссия) путём проведения проверок.

Состав комиссии утверждается приказом директора Учреждения.

1.6. Внутренний контроль проводится в форме плановых и внеплановых проверок.

Плановые проверки соответствия обработки персональных данных установленным требованиям проводятся один раз в год в каждом структурном подразделении Учреждения. План проведения внутреннего контроля на очередной год формируется заместителем директора (председателем комиссии)

до 10 декабря и утверждается директором Учреждения.

Сроки проведения плановых проверок доводятся до сведения руководителей проверяемых структурных подразделений не позднее, чем за 10 дней до начала проверки.

Проведение внеплановой проверки организуется председателем комиссии, а в его отсутствие – заместителем председателя комиссии в течение 3-х рабочих дней с даты

поступления письменного заявления субъекта персональных данных о нарушении правил обработки персональных данных.

Внеплановые проверки могут быть контрольными и по частным вопросам:

1.6.1. Контрольные проверки проводятся для установления полноты выполнения рекомендаций плановых проверок.

Сроки проведения контрольных проверок доводятся до сведения руководителей проверяемых структурных подразделений не позднее, чем за 24 часа до начала проверки;

1.6.2. Проверки по частным вопросам охватывают отдельные направления по защите персональных данных и могут проводиться в случаях, когда стали известны факты несанкционированного доступа, утечки либо утраты персональных данных субъектов персональных данных Учреждения или нарушения требований по защите персональных данных.

Проверки по частным вопросам могут проводиться без уведомления руководителей проверяемых структурных подразделений.

2. Порядок подготовки к проверке

2.1. В проведении проверки принимают участие члены комиссии (далее

– проверяющие лица) в составе, утверждаемом приказом директора. Председатель комиссии (старший по проверке) подготавливает в адрес руководителя проверяемого структурного подразделения распоряжение о проверке и перечень вопросов проверки (при необходимости). Председатель комиссии распределяет обязанности по проверке конкретных участков работы между проверяющими лицами.

За 3-4 дня до начала проверки проверяющие лица должны изучить материалы предыдущих проверок данного подразделения, уточнить наличие в нём защищаемых ресурсов, сил и средств защиты персональных данных, а также особенности их функционирования.

3. Порядок проведения проверки

3.1. Для проведения проверки председатель комиссии представляет руководителю проверяемого структурного подразделения Учреждения прибывших на проверку лиц. Допуск лиц, прибывших на проверку, к конкретным информационным ресурсам, охраняемым сведениям и техническим средствам производится руководителем структурного подразделения на основании распоряжения о проверке. Подобный допуск должен исключать ознакомление проверяющих лиц с конкретными персональными данными. В случае, если в ходе проведения мероприятий внутреннего контроля проверяющим лицам стали известны персональные данные, в обязательном порядке обеспечивается конфиденциальность этих персональных данных.

На период проведения контрольных мероприятий обработку персональных данных необходимо по возможности прекращать.

3.2. В ходе осуществления контроля выполнения требований по защите персональных данных в структурном подразделении Учреждения проверке могут подлежать следующие показатели:

3.2.1. В части общей организации работ по защите персональных данных:

- соответствие информации, указанной в уведомлении об обработке персональных данных, реальному положению дел;
- наличие нормативных документов по защите персональных данных;
- знание нормативных документов сотрудниками, имеющими доступ к персональным данным;
- полнота и правильность выполнения требований нормативных документов сотрудниками, имеющими доступ к персональным данным;
- наличие лиц, назначенных ответственными за организацию обработки персональных данных в структурном подразделении, уровень их профессиональной подготовки и способность выполнить возложенные обязанности;

- наличие согласий на обработку персональных данных субъектов персональных данных. Соответствие объема персональных данных и сроков обработки целям обработки персональных данных;

- соответствие схемы контролируемой зоны, перечня мест хранения материальных носителей, перечня лиц, допущенных к обработке персональных данных, фактическому состоянию;

3.2.2. В части защиты персональных данных в информационных системах персональных данных (далее – ИСПДн):

- соответствие средств вычислительной техники ИСПДн показателям, указанным в документации на ИСПДн;

- структура и состав локальных вычислительных сетей, организация разграничения доступа пользователей к сетевым информационным ресурсам, порядок защиты охраняемых сведений при передаче (обмене) персональных данных в сети передачи данных (СПД);

- контроль целостности пломб на аппаратных средствах, с которыми осуществляется штатное функционирование средств криптографической защиты информации;

- соблюдение установленного порядка использования средств вычислительной техники ИСПДн;

- наличие и эффективность применения средств и методов защиты персональных данных, обрабатываемых на средствах электронно-вычислительной техники (ЭВТ);

- соблюдение требований, предъявляемых к паролям на информационные ресурсы;

- соблюдение требований и правил антивирусной защиты персональной электронно-вычислительной машины (ПЭВМ) и программ;

- контроль журналов учёта носителей персональных данных. Сверка основного журнала с дублирующим (если требуется ведение дублирующего учёта носителей);

- тестирование реализации правил фильтрации межсетевого экрана, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления настроек межсетевого экрана;

3.2.3. В части защиты информационных ресурсов и помещений:

- правильность отнесения обрабатываемой информации к персональным данным;

- правильность классификации информационной системы;

- закрепление гражданско-правовой ответственности в сфере информационной безопасности и соблюдения режима конфиденциальности персональных данных в правилах внутреннего трудового распорядка, положениях о подразделениях Учреждения, должностных инструкциях сотрудников и трудовых договорах;

- порядок передачи персональных данных органам государственной власти, местного самоуправления и сторонним организациям (контрагентам);

- действенность принимаемых мер по защите охраняемых сведений в ходе подготовки материалов к открытому опубликованию и при изготовлении буклетов;

- состояние конфиденциального делопроизводства, соблюдение установленного порядка подготовки, учёта, использования, хранения и уничтожения документов, содержащих персональные данные; - выполнение требований по правильному оборудованию защищаемых помещений и предотвращению утечки охраняемых сведений при проведении мероприятий конфиденциального характера;

- соответствие защищаемых помещений их техническим паспортам.

3.3. Комиссия при проверке имеет право:

3.3.1. Запрашивать у руководителей структурных подразделений Учреждения информацию и (или) документы, необходимые для осуществления внутреннего контроля;

3.3.2. Требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путём персональных данных.

3.4. Проверка должна быть завершена не позднее чем через 15 дней с даты начала проверки.

3.5. В ходе работы проверяющие лица должны принимать меры по устранению на месте отмечаемых нарушений и недостатков. Для этого с должностными лицами структурного подразделения, ответственными за конкретные участки работы, где отмечались недостатки, одновременно должны проводиться разъяснения требований руководящих документов и оказываться практическая помощь в правильной постановке работы.

Недостатки, которые не могут быть устранены на месте, включаются в итоговый документ по результатам проверки.

4. Оформление результатов проверки

Результаты проверки оформляются секретарём комиссии в виде акта внутреннего контроля, составленного по форме согласно Приложению к настоящим Правилам, который подписывается членами комиссии в количестве не менее 3-х человек и утверждается председателем комиссии, а в его отсутствие – заместителем председателя комиссии.

Акт составляется в двух экземплярах, подписывается председателем и членами комиссии, докладывается под роспись руководителю структурного подразделения.

Один экземпляр документа хранится у ответственного за организацию обработки персональных данных в Учреждении. Второй экземпляр документа передаётся руководителю структурного подразделения.

В случае несогласия с выводами комиссии руководитель структурного подразделения может выразить в письменном виде своё особое мнение (прилагается к акту).

Результаты проверок подразделений периодически обобщаются председателем комиссии и доводятся до сведения руководителя. При необходимости принятия решений по результатам проверок структурных подразделений о мерах, необходимых для устранения выявленных нарушений, директору Учреждения председателем комиссии готовится соответствующая служебная записка.

**Порядок доступа сотрудников в помещения, в которых ведется
обработка персональных данных**

1. Настоящий Порядок доступа сотрудников ГБУ РД КЦСОН в МО «Сергокалинский район» в помещения, в которых ведется обработка персональных данных (далее - Порядок), разработан в соответствии с Федеральным законом «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации».

2. Персональные данные относятся к конфиденциальной информации.

Сотрудники ГБУ РД КЦСОН в МО «Сергокалинский район», получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3. Обеспечение безопасности персональных данных от уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных достигается, в том числе установлением правил доступа в помещения, где обрабатываются персональные данные в информационной системе персональных данных и без использования средств автоматизации.

4. Размещение информационных систем, в которых обрабатываются персональные данные, осуществляется в охраняемых помещениях. Для помещений, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

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

5. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители персональных данных, допускаются только сотрудники ГБУ РД КЦСОН в МО «Сергокалинский район», уполномоченные на обработку персональных данных приказом Председателя.

6. Нахождение в помещениях ГБУ РД КЦСОН в МО «Сергокалинский район», в которых ведется обработка персональных данных, лиц, не являющихся сотрудниками ГБУ РД КЦСОН в МО «Сергокалинский район», уполномоченными на обработку персональных данных, возможно только в сопровождении сотрудника ГБУ РД КЦСОН в МО «Сергокалинский район», уполномоченного на обработку персональных данных, на время, ограниченное необходимостью решения вопросов, связанных с оказанием государственных услуг.

7. Ответственность за соблюдение порядка доступа в помещения ГБУ РД КЦСОН в МО «Сергокалинский район», в которых ведется обработка персональных данных, возлагается на начальников структурных подразделений ГБУ РД КЦСОН в МО «Сергокалинский район», обрабатывающих персональные данные.

Положение
об организации обработки персональных данных,
осуществляемой без использования средств автоматизации в Государственном бюджетном
учреждении республики Дагестан "Комплексный центр социального обслуживания
населения в муниципальном образовании "Сергокалинский район"

1. Общие положения

1.1. Настоящее Положение об организации обработки персональных данных, осуществляемой без использования средств автоматизации (далее – Положение) разработаны на основании требований Федерального закона Российской Федерации от 27 июля 2006 года № 152 - ФЗ «О персональных данных» и устанавливают порядок обработки, распространения и использования персональных данных в ГБУ РД КЦСОН в МО «Сергокалинский район» (далее - Учреждение).

1.2. Положение обработки персональных данных, осуществляемой без использования средств автоматизации осуществляются с учетом требований Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

2. Термины и определения

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

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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;

Материальный носитель – материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

хранятся персональные данные; контроль доступа в помещения посторонних лиц; хранение материальных носителей в надежных местах), обеспечивающие сохранность ПДн и исключающие возможность несанкционированного доступа к ним.

4.2 Бумажные документы и иные материальные носители, содержащие ПДн, должны храниться в закрытых для визуального просмотра шкафах (в сейфах и/или запираемых шкафах желательно закрывающиеся под ключ).

4.3 В рабочее время документы, в которых содержатся ПДн, не должны находиться на столах сотрудников подразделения дольше времени необходимого на их обработку. Во время обработки документы, содержащие ПДн, по возможности размещаются таким образом, чтобы в них отсутствовала возможность просмотра информации посторонними лицами.

4.4 В конце рабочего дня все документы, дела, листы бумаги и блокноты с рабочими записями, инструктивные и справочные материалы должны быть убраны в предназначенные для этого шкафы, сейфы. Черновики и редакции документов, испорченные бланки, листы со служебными записями в конце рабочего дня уничтожаются в установленном порядке.

ПОРЯДОК
хранения, использования и передачи персональных данных
сотрудников ГБУ РД КЦСОН в МО «Сергокалинский район»

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий Порядок хранения, использования и передачи персональных данных сотрудников ГБУ РД КЦСОН в МО «Сергокалинский район» (далее - Порядок) разработан в соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

Цель разработки настоящего Порядка - определение порядка обработки (хранения, использования, передачи) персональных данных сотрудников ГБУ РД КЦСОН в МО «Сергокалинский район» (далее - Учреждение, Оператор); обеспечение защиты прав и свобод сотрудников Учреждения при обработке их персональных данных.

2. ХРАНЕНИЕ И ИСПОЛЬЗОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
СОТРУДНИКОВ

Хранение персональных данных должно осуществляться в форме, позволяющей определить сотрудника Учреждения, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого является сотрудник. Обрабатываемые персональные данные подлежат уничтожению, либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом. Хранение персональных данных сотрудников Учреждения может осуществляться на бумажных и машинных носителях, доступ к которым ограничен списком лиц, допущенных к обработке персональных данных.

Все отчуждаемые машинные носители персональных данных подлежат строгому учету. Форма Журнала учета отчуждаемых машинных носителей персональных данных утверждена нормативным актом Учреждения.

Персональные данные сотрудников, содержащиеся на машинных носителях персональных данных, должны храниться на автоматизированных рабочих местах и серверах информационных систем персональных данных Учреждения, установленных в пределах помещений, утвержденных Приказом об обеспечении безопасности помещений, в которых размещены информационные системы персональных данных.

Персональные данные сотрудников, содержащиеся на материальных носителях персональных данных, должны храниться в пределах помещений, утвержденных Приказом об обеспечении безопасности материальных носителей персональных данных.

Все хранимые или используемые средства защиты информации (далее - СЗИ), эксплуатационная и техническая документация к ним подлежат поэкземплярному учету и выдаются под расписку в Журнале поэкземплярного учета СЗИ, эксплуатационной и технической документации к ним пользователям СЗИ, несущим персональную ответственность за их сохранность. Форма соответствующего Журнала утверждена нормативным актом Учреждения.

Хранение персональных данных сотрудников должно происходить в порядке, исключающем их утрату или их неправомерное использование.

Использование персональных данных сотрудников осуществляется Учреждением исключительно в целях выполнения требований трудового законодательства Российской Федерации.

Обработка персональных данных сотрудников Учреждения осуществляется только специально уполномоченными лицами, перечень которых утверждается приказом Учреждения, при этом указанные в приказе сотрудники должны иметь право получать только те персональные данные субъекта, которые необходимы для выполнения непосредственных должностных обязанностей.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором 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 Учреждения (при их наличии).

Передача персональных данных сотрудников между структурными подразделениями Учреждения осуществляется только между сотрудниками, включенными в перечень лиц, имеющих доступ к персональным данным.

Обработка персональных данных сотрудников должна осуществляться только в пределах помещений Учреждения и с использованием средств вычислительной техники Учреждения.

Учреждение вправе поручить обработку персональных данных сотрудников другим юридическим или физическим лицам на основании договора (далее - поручение Учреждения) с согласия сотрудника, если иное не предусмотрено Федеральным законом

«О персональных данных». Лицо, осуществляющее обработку персональных данных по поручению Учреждения, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных».

Сотрудники Учреждения и иные лица, получающие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия сотрудников, если иное не предусмотрено федеральным законодательством в сфере защиты персональных данных.

3. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

При передаче персональных данных сотрудника Оператор должен соблюдать следующие требования:

не сообщать персональные данные сотрудника третьей стороне без письменного согласия сотрудника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника, а также в случаях, предусмотренных Гражданским кодексом Российской Федерации или иными федеральными законами;

предупреждать лица, получающие персональные данные сотрудников, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц обеспечения конфиденциальности полученных персональных данных;

не сообщать персональные данные сотрудника в коммерческих целях без его письменного согласия;

передавать персональные данные сотрудника представителям сотрудников в порядке, установленном Гражданским кодексом Российской Федерации, и

ограничивать эту информацию только теми персональными данными сотрудника, которые необходимы для выполнения указанными представителями их функций;

не отвечать на вопросы, связанные с передачей персональных данных сотрудника по телефону или факсу, за исключением случаев, связанных с выполнением соответствующими сотрудниками своих непосредственных должностных обязанностей, адресатам в чью компетенцию входит получение такой информации.

В целях обеспечения контроля правомерности использования переданных по запросам персональных данных лицами, их получившими, сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в их предоставлении, а также состав переданной информации фиксируются в Журнале учета передачи персональных данных. Форма соответствующего Журнала утверждена локальным актом Учреждения.