Администрация муниципального образования

Кореновский район

МУНИЦИПАЛЬНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 4 ИМЕНИ В. ЧИКМЕЗОВА МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ КОРЕНОВСКИЙ РАЙОН

ПРИКАЗ

21.09.2020 **№ 682**

Ст. Раздольная

«О защите информации»

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

1. Возложить обязанности по защите информации и назначить ответственными:

-за организацию обработки персональных данных заместителя директора по учебной работе Рабцевич Викторию Сергеевну.

-за обеспечение безопасности персональных данных в информационных системах персональных данных заместителя директора по учебной работе Рабцевич Викторию Сергеевну.

2. Утвердить перечень должностей, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых)

обязанностей согласно приложению 1 к настоящему приказу.

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

4. Создать комиссию по защите информации:

4.1. Утвердить состав комиссии по защите информации согласно приложению 3 к настоящему приказу.

4.2. Утвердить положение о комиссии по защите информации согласно приложению 4 к настоящему приказу.

5. Утвердить перечень информационных систем персональных данных согласно приложению 5 к настоящему приказу.

6. Утвердить положение об обработке и защите персональных данных согласно приложению 6 к настоящему приказу.

7. Утвердить инструкции и правила по защите информации:

–Инструкцию ответственного за организацию обработки персональных данных согласно приложению 7 к настоящему приказу.

–Правила рассмотрения запросов субъектов персональных данных согласно приложению 8 к настоящему приказу.

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

–Инструкцию ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных согласно приложению 10 к настоящему приказу;

–Инструкцию по организации парольной защиты, согласно приложению 11 к настоящему приказу;

–Инструкцию по организации антивирусной защиты, согласно приложению 12 к настоящему приказу;

–Порядок уничтожения персональных данных при достижении целей обработки и (или) при наступлении законных оснований, согласно приложению 13 к настоящему приказу;

–Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, согласно

приложению 14 к настоящему приказу;

–Инструкцию по обработке персональных данных без использования средств автоматизации согласно приложению 15 к настоящему приказу;

–Инструкцию по работе с инцидентами информационной безопасности согласно приложению 16 к настоящему приказу.

8. Рабцевич В.С., ответственной за организацию обработки персональных данных подготовить план мероприятий по защите информации на 2020 -2021 учебный год.

9. Утвердить Правила обработки персональных данных, осуществляемой без использования средств автоматизации согласно приложению 17 к настоящему приказу.

10. Контроль за исполнение данного приказа оставляю за собой.

Директор школы Л.И. Рассохина

Приложение 1
к приказу МОБУ СОШ №4
им. В.Чикмезова
МО Кореновский район
от 21.09.2020 № 682

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

Должность	ИСПДн
-директор -заместитель директора по воспитательной работе -заместитель директора по учебной работе	Сетевой город. Образование Е – Услуги. Образование Официальный сайт образовательной организации АИС «Навигатор дополнительного образования детей Краснодарского края»
-учителя предметники	Сетевой город. Образование
-классный руководитель, -педагог-психолог, -педагог дополнительного образования, -социальный педагог	Сетевой город. Образование Официальный сайт образовательной организации АИС «Навигатор дополнительного образования детей Краснодарского края»
-главный бухгалтер - экономист	1С: предприятие Сетевой город. Образование
-секретарь	Сетевой город. Образование Е – Услуги. Образование Официальный сайт образовательной организации

Приложение 2
к приказу МОБУ СОШ №4
им.В.Чикмезова
МО Кореновский район
от 21.09.2020 № 682

Перечень должностей, ведущих обработку персональных данных без использования средств автоматизации

Должность
Директор
Заместитель директора по учебной работе
Заместитель директора по воспитательной работе
Учителя
Секретарь
Социальный педагог
Педагог –психолог
Педагог дополнительного образования
Главный бухгалтер, экономист

Приложение 3
к приказу МОБУ СОШ №4
им.В.Чикмезова
МО Кореновский район
от 21.09.2020 № 682

Состав комиссии по защите информации

Председатель комиссии	Рассохина Людмила Ивановна, директор
Члены комиссии	Рабцевич Виктория Сергеевна, заместитель директора по УР
	Семенова Марина Леонидовна, заместитель директора по ВР
	Котовец Ирина Валентиновна, секретарь

Приложение 4
к приказу МОБУ СОШ №4
им.В.Чикмезова
МО Кореновский район
от 21.09.2020 № 682

ПОЛОЖЕНИЕ
о комиссии по защите информации

1. Общие положения

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

2. Основные задачи комиссии

2.1. Основными задачами комиссии являются:

2.1.1. Сбор и анализ исходных данных по информационным системам персональных данных муниципального общеобразовательного бюджетного учреждения средней общеобразовательной школы №4 имени В.Чикмезова муниципального образования Кореновский район (далее МОБУ СОШ №4 им. В.Чикмезова МО Кореновский район).

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

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

2.1.4. Определение класса защищенности информационных систем, персональных данных МОБУ СОШ №4 им.В.Чикмезова МО Кореновский район на основании собранных данных.

2.1.5. Определение уровня защищенности персональных данных при их обработке в информационных системах персональных данных.

3. Порядок формирования комиссии

3.1. Комиссия формируется из числа штатных сотрудников МОБУ СОШ №4 им.В.Чикмезова МО Кореновский район, участвующих в процессе обработки персональных данных.

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

3.3. Члены комиссии назначаются приказом директора МОБУ СОШ №4 им.В.Чикмезова МО Кореновский район. В случае изменения состава Комиссии, в приказ вносятся соответствующие изменения.

4. Полномочия комиссии

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

4.1.1. Получать необходимые сведения у всех работников МОБУ СОШ №4 им. В.Чикмезова МО Кореновский район, участвующих в обработке персональных данных.

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

4.1.3. Отслеживать технологический процесс обработки персональных данных.

4.1.4. Выявлять или получать готовые сведения о структуре локальной вычислительной сети МОБУ СОШ №4 им.В.Чикмезова МО Кореновский район.

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

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

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

5. Отчетность комиссии

5.1. Комиссия при выполнении своих задач должна составить протокол заседания комиссии.

5.2.В результате своей деятельности Комиссия должна составить Акт(ы) определения уровня защищенности персональных данных и класса защищенности информационных систем персональных данных.

Приложение 5
к приказу МОБУ СОШ №4
им. В.Чикмезова МО Кореновский район
от 21. 09.2020 № 682

Перечень информационных систем персональных данных

Наименование	Адрес расположения
Сетевой город. Образование Е – Услуги. Образование Официальный сайт образовательной организации АИС «Навигатор дополнительного образования детей Краснодарского края» 1 С: предприятие	353160м, Краснодарский край, Кореновский район, ст. Раздольная, ул. Советская,126

Приложение №6
к Приказу № 682 от 21.09.2020 г.

УТВЕРЖДАЮ
Директор МОБУ СОШ №4
им.В.Чикмезова МО Кореновский район
_____Л.И.Рассохина
«21» сентября 2020г.

ПОЛОЖЕНИЕ
об обработке и защите персональных данных в МОБУ СОШ №4 им.В. Чикмезова МО Кореновский район

1. Общие положения

1.1. Настоящее Положение имеет своей целью закрепление механизмов обеспечения прав субъекта на сохранение конфиденциальности информации о фактах, событиях и обстоятельствах его жизни.
1.2. Настоящее Положение об обработке и защите персональных данных (далее - Положение) определяет порядок сбора, хранения, передачи и любого другого использования персональных данных работников, обучающихся (воспитанников) в соответствии с законодательством Российской Федерации и гарантии конфиденциальности сведений о работнике предоставленных работником работодателю.
1.3. Положение разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", иными нормативно-правовыми актами, действующими на территории Российской Федерации.

2. Основные понятия

Для целей настоящего Положения используются следующие понятия:
2.1. **Оператор персональных данных** (далее оператор) - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных. В рамках настоящего положения оператором является –муниципальное общеобразовательное бюджетное учреждение средняя общеобразовательная средняя школа №4 имени В.Чикмезова муниципального образования Кореновский район.;
2.2. **Персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация о физическом лице.
2.3. **Субъект** - субъект персональных данных.
2.4. **Работник** - физическое лицо, состоящее в трудовых отношениях с оператором.
2.5. **Обработка персональных данных** - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

2.6. **Распространение персональных данных** - действия, направленные на передачу персональны данных определенному кругу лиц (передача персональных данных) или на ознакомление персональными данными неограниченного круга лиц, в том числе обнародование персональны данных в средствах массовой информации, размещение в информационно-телекоммуникационны сетях или предоставление доступа к персональным данным каким-либо иным способом.
2.7. **Использование персональных данных** - действия (операции) с персональными данными совершаемые оператором в целях принятия решений или совершения иных действий, порождающи юридические последствия в отношении субъекта персональных данных или других лиц либо ины образом затрагивающих права и свободы субъекта персональных данных или других лиц.
2.8. **Блокирование персональных данных** - временное прекращение сбора, систематизации накопления, использования, распространения персональных данных, в том числе их передачи.
2.9. **Уничтожение персональных данных** - действия, в результате которых невозможн восстановить содержание персональных данных в информационной системе персональных данны или в результате которых уничтожаются материальные носители персональных данных.
2.10. К персональным данным относятся:
2.10.1. Сведения, содержащиеся в основном документе, удостоверяющем личность субъекта.
2.10.2. Информация, содержащаяся в трудовой книжке работника.
2.10.3. Информация, содержащаяся в страховом свидетельстве государственного пенсионног страхования.
2.10.4. Сведения, содержащиеся в документах воинского учета для военнообязанных и лиц подлежащих призыву на военную службу.
2.10.5. Сведения об образовании, квалификации или наличии специальных знаний или подготовки
2.10.6. Сведения, содержащиеся в свидетельстве о постановке на учет физического лица в налогово органе на территории Российской Федерации.
2.10.7. Сведения о семейном положении работника.
2.10.8. Информация медицинского характера, в случаях, предусмотренных законодательством.
2.10.9. Сведения о заработной плате работника.
2.10.10. Сведения о социальных льготах;
2.10.11. Сведения о наличии судимостей;
2.10.12. Место работы или учебы членов семьи;
2.10.13. Содержание трудового договора;
2.10.14. Подлинники и копии приказов по личному составу;
2.10.15. Основания к приказам по личному составу;
2.10.16. Документы, содержащие информацию по повышению квалификации и переподготовк сотрудника, его аттестация, служебное расследование.
2.10.17. Сведения о награждении государственными наградами

3. Обработка персональных данных

3.1. Общие требования при обработке персональных данных.
В целях обеспечения прав и свобод человека и гражданина при обработке персональных данны обязаны соблюдаться следующие требования:
3.1.1. Обработка персональных данных может осуществляться исключительно в целях обеспечени соблюдения Конституции Российской Федерации, законов и иных нормативных правовых актов Р , содействия субъектам персональных данных в трудоустройстве, продвижении по служб обучении, контроля количества и качества выполняемой работы, обеспечения личной безопасност субъекта персональных данных и членов его семьи, а также в целях обеспечения сохраннос принадлежащего ему имущества и имущества оператора.
3.1.2. Персональные данные не могут быть использованы в целях причинения имущественно и/или морального вреда гражданам, затруднения реализации прав и свобод граждан Российско Федерации.
3.1.3. При принятии решений, затрагивающих интересы субъекта персональных данных, нель основываться на персональных данных, полученных исключительно в результате автоматизированной обработки или электронного получения.

3.1.4. Работники или их законные представители должны быть ознакомлены под расписку с документами оператора, устанавливающими порядок обработки персональных данных субъектов, а также их права и обязанности в этой области.
3.1.5. Субъекты персональных данных, не являющиеся работниками, или их законные представители имеют право ознакомиться с документами оператора, устанавливающими порядок обработки персональных данных субъектов, а также их права и обязанности в этой области.
3.1.6. Субъекты персональных данных не должны отказываться от своих прав на сохранение и защиту тайны.
3.2. Получение персональных данных.
3.2.1. Все персональные данные следует получать непосредственно от субъекта персональных данных. Субъект самостоятельно принимает решение о предоставление своих персональных данных и дает письменное согласие на их обработку оператором.
3.2.2. В случае недееспособности либо несовершеннолетия субъекта персональных данных все персональные субъекта следует получать от его законных представителей. Законный представитель самостоятельно принимает решение о предоставлении персональных данных своего подопечного и дает письменное согласие на их обработку оператором.
3.2.3. Письменное согласие не требуется, если обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных.
3.2.4. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случаях указанных в пункте 3.2.2 настоящего положения согласие может быть отозвано законным представителем субъекта персональных данных.
3.2.5. В случаях, когда оператор может получить необходимые персональные данные субъекта только у третьей стороны, субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. В уведомлении оператор обязан сообщить о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа субъекта дать письменное согласие на их получение. Согласие оформляется в письменной форме в двух экземплярах: один из которых предоставляется субъекту, второй хранится у оператора.
3.2.6. Запрещается получать и обрабатывать персональные данные субъекта о его политических, религиозных и иных убеждениях и частной жизни.
3.2.7. Запрещается получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.
3.2.8. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации оператор вправе получать и обрабатывать данные о частной жизни субъекта только с его письменного согласия.
3.3. Хранение персональных данных.
3.3.1. Хранение персональных данных субъектов осуществляется кадровой службой, бухгалтерией,на бумажных и электронных носителях с ограниченным доступом.
3.3.2. Личные дела хранятся в бумажном виде в папках. Личные дела хранятся в специальном замыкающемся шкафу, обеспечивающем защиту от несанкционированного доступа.
3.3.3. Подразделения, хранящие персональные данные на бумажных носителях, обеспечивают их защиту от несанкционированного доступа и копирования согласно "Положению об особенностях обработки персональных данных. Осуществляемой без использования средств автоматизации", утвержденному постановлением правительства РФ 15 сентября 2008 г. N 687.
3.4. Передача персональных данных
3.4.1. При передаче персональных данных субъекта оператор обязан соблюдать следующие требования:
- не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта или его законного представителя, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами.
- предупредить лиц, получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения

того, что это правило соблюдено. Лица, получающие персональные данные субъекта, обязаны соблюдать требования конфиденциальности;
- не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения им трудовой функции;
- передавать персональные данные субъекта представителям субъектов в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функций;
3.4.2. Все меры конфиденциальности при сборе, обработке и хранении персональных данных субъекта распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.
3.4.3. Внутренний доступ (доступ внутри организации) к персональным данным субъекта. Право доступа к персональным данным субъекта имеют:
- директор;
- бухгалтер;
- секретарь;
- заместитель директора по учебной работе и по воспитательной работе по направлению деятельности (доступ к персональным данным , непосредственно находящихся в его подчинении);
- психолог, социальный педогог (доступ к персональным данным субъектов в части его касающейся);
- классный руководитель (доступ к персональным данным учеников своего класса в части его касающейся);
- учитель (доступ к информации, содержащейся в классных журналах тех классов, в которых он ведет занятия;
- сам субъект, носитель данных.
3.4.4. Все сотрудники, имеющие доступ к персональным данным субъектов, обязаны подписать соглашение о неразглашении персональных данных.
3.4.5. К числу массовых потребителей персональных данных вне учреждения относятся государственные и негосударственные функциональные структуры: налоговые инспекции; правоохранительные органы; органы статистики; страховые агентства; военкоматы; органы социального страхования; пенсионные фонды; подразделения федеральных, республиканских и муниципальных органов управления. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.
3.4.6. Организации, в которые субъект может осуществлять перечисления денежных средств (страховые Общества, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения) могут получить доступ к персональным данным субъекта только в случае его письменного разрешения.
3.5. Уничтожение персональных данных
3.5.1. Персональные данные субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.
3.5.2. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

4. Права и обязанности субъектов персональных данных и оператора

4.1. В целях обеспечения защиты персональных данных субъекты имеют право:
- получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);

- осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;
- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства;
- при отказе оператора или уполномоченного им лица исключить или исправить персональные данные субъекта - заявить в письменной форме о своем несогласии, представив соответствующее обоснование;
- дополнить персональные данные оценочного характера заявлением, выражающим его собственную точку зрения;
- требовать от оператора или уполномоченного им лица уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них изменениях или исключениях из них;
- обжаловать в суд любые неправомерные действия или бездействие оператора или уполномоченного им лица при обработке и защите персональных данных субъекта.

4.2. Для защиты персональных данных субъектов оператор обязан:
- за свой счет обеспечить защиту персональных данных субъекта от неправомерного их использования или утраты в порядке, установленном законодательством РФ;
- ознакомить работника или его представителей с настоящим положением и его правами в области защиты персональных данных под расписку;
- по запросу ознакомить субъекта персональных данных, не являющегося работником, или в случае недееспособности либо несовершеннолетия субъекта, его законных представителей с настоящим положением и его правами в области защиты персональных данных;
- осуществлять передачу персональных данных субъекта только в соответствии с настоящим Положением и законодательством Российской Федерации;
- предоставлять персональные данные субъекта только уполномоченным лицам и только в той части, которая необходима им для выполнения их трудовых обязанностей в соответствии с настоящим положением и законодательством Российской Федерации;
- обеспечить субъекту свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законодательством;
- по требованию субъекта или его законного представителя предоставить ему полную информацию о его персональных данных и обработке этих данных.

4.3. Субъект персональных данных или его законный представитель обязуется предоставлять персональные данные, соответствующие действительности..

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

5.1. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, содержащему персональные данные, несет персональную ответственность за данное разрешение.

5.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

6. Типовые документы по защите информации.

6.1

Лист ознакомления с Положением об обработке и защите персональных данных МОБУ СОШ №4 им. В.Чикмезова МО Кореновский район

№ п/п	Ф.И.О.	Должность	Дата	Подпись

6.2

Журнал учета передачи персональных данных

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

6.3

Журнал учета обращений субъектов персональных данных о выполнении их законных прав в области защиты персональных данных

№ п/п	Сведения о запрашиваемом лице	Краткое содержание обращения	Цель получения информации	Отметка о предоставлении или отказе в предоставлении информации	Дата передачи/отказа в предоставлении информации	Подпись запрашивающего лица	Подпись ответственного сотрудника

6.4 **Согласие на обработку персональных данных**

ЗАЯВЛЕНИЕ

о согласии на обработку персональных данных

Я, _____
фамилия, имя, отчество
паспорт: серия _____ номер _____ кем выдан _____
_____
дата выдачи «_____» _____
адрес регистрации по месту жительства: _____
_____
адрес регистрации по месту пребывания: _____
_____
с целью исполнения определенных сторонами условий трудового договора даю согласие МОБУ СОШ № 4 им. В. Чикмезова МО Кореновский район на обработку в документальной и /или / электронной форме нижеследующих персональных данных: фамилия, имя, отчество; дата рождения; пол; гражданство; знание иностранного языка; образование, квалификация, профессиональная подготовка, сведения о повышении квалификации или наличие специальных знаний; профессия (специальность); общий трудовой стаж, сведения о приемах, перемещениях и увольнениях по предыдущим местам работы; размер заработной платы; факты биографии; состояние в браке, состав семьи, место работы или учебы членов семьи и родственников; паспортные данные; адрес места жительства ; дата регистрации по месту жительства; номер телефона; идентификационный номер налогоплательщика; номер страхового свидетельства государственного пенсионного страхования; сведения включенные в трудовую книжку; религиозные и политические убеждения (принадлежность к религиозной конфессии, членство в политической партии, участие в общественных объединениях, в том числе в профсоюзе); сведения о воинском учете; фотография; сведения о состоянии здоровья, которое относится к вопросу о возможности выполнения работником трудовой функции.

Настоящее согласие действует в течение всего срока действия трудового договора. Настоящее согласие может быть отозвано мной в письменной форме.

«____» _____202 г.

_____
личная подпись

6.5 **Разъяснение субъекту персональных данных**

Разъяснение
субъекту персональных данных

Мне, _____
разъяснены юридические последствия отказа предоставить свои персональные данные в МОБУ СОШ №4 им. В. Чикмезова МО Кореновский район.

В соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152 ФЗ «О персональных данных», определен перечень персональных данных, которые субъект персональных данных обязан предоставить в МОБУ СОШ №4 им.В.Чикмезова МО Кореновский район в связи с поступлением на работу.

Без представления субъектом персональных данных обязательных для заключения трудового договора сведений, трудовой договор не может быть заключен.

_____	_____	_____
дата	подпись	Расшифровка

6.6 **Обязательство о неразглашении информации**

Обязательство
о неразглашении информации, содержащей персональные данные

Я, _____

(фамилия, имя, отчество полностью)

являясь работником МОБУ СОШ №4 им. В.Чикмезова МО Кореновский район, в должности _____
_____,

(указать должность и наименование структурного подразделения)

обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной трудового договора.

В соответствии со статьей 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией, и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставшие известными мне в связи с исполнением должностных обязанностей.

Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен(а) к ответственности в соответствии с законодательством Российской Федерации.

_____ _____ _____

дата подпись Расшифровка

6.7 **Протокол заседания комиссии по защите информации**

ПРОТОКОЛ № 1
заседания комиссии по защите информации

Дата и время проведения _____
Место проведения _____

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

Повестка дня

Определение информационных систем персональных данных (далее - ИСПДн), принадлежащих МОБУ СОШ №4 им.В.Чикмезова МО Кореновский район.

1. Слушали: _____

доложил(а) исходные данные об ИСПДн «Наименование».

Выступил(а): _____ _____

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

Постановили:

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

2. Слушали: _____

доложил(а) исходные данные об ИСПДн «Наименование».

Выступил(а): _____

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

Постановили:

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

6.8 Акт об уничтожении персональных данных

АКТ

Об уничтожении персональных данных субъектов персональных данных

Комиссия в составе:

Роль	ФИО	Должность
Председатель		
Члены комиссии		

Установила, что на основании достижения цели обработки персональных данных, в соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных» гл. 2, ст. 5, пункт 7, подлежат уничтожению сведения, составляющие персональные данные:

№ п/п	Сведения, содержащие персональные данные	Место хранения	Кол-во ед. хранения	Примечание

Указанные персональные данные уничтожены путем_____ _____

(удаления с помощью средств гарантированного удаления информации, уничтожения носителя и т.п.)

Председатель комиссии: _____ _____

подпись расшифровка

Члены комиссии: _____ _____

подпись расшифровка

_____ _____

подпись расшифровка

Приложение 7
к приказу МОБУ СОШ №4
им.В.Чикмезова МО Кореновский район
от 21. 09.2020 №682

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных

1. Общие положения

Настоящая инструкция определяет права, обязанности и ответственность лица, ответственного за организацию обработки персональных данных.

Ответственный за организацию обработки персональных данных в своей деятельности руководствуется:

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119;
- Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687;
- Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 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 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2. Обязанности

Ответственный за организацию обработки персональных данных обязан:

- Доводить до сведения работников положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к обеспечению безопасности персональных данных;
- Осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, а именно организовывать проведение периодических (не менее одного раза в год) проверок соответствия обработки персональных данных. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывать непосредственному руководителю в письменном виде;

– 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.

3. Ответственность

За неисполнение (ненадлежащее исполнение) своих должностных обязанностей, предусмотренных настоящей инструкцией, ответственный за организацию обработки персональных данных несет персональную ответственность в соответствии с законодательством Российской Федерации.

4. Права

Ответственный за организацию обработки персональных данных имеет право:

– Требовать от работников письменных объяснений по фактам нарушения ими требований законодательства Российской Федерации, локальных актов о персональных данных и защите персональных данных;

– Вносить предложения непосредственному руководителю об отстранении работников от обработки персональных данных, применению к ним дисциплинарных взысканий, при обнаружении нарушения ими требований законодательства Российской Федерации, локальных актов по вопросам обработки персональных данных или требований к защите персональных данных.

Приложение 8
к приказу МОБУ СОШ №4
им.В.Чикмезова МО Кореновский район
от 21. 09.2020 №682

Правила
рассмотрения запросов субъектов персональных данных или их представителей в МОБУ СОШ №4 им.В. Чикмезова МО Кореновский район

1. Настоящими Правилами рассмотрения запросов субъектов персональных данных или их представителей в МОБУ СОШ №4 им.В. Чикмезова МО Кореновский район (далее – Правила) определяются порядок учета (регистрации), рассмотрения запросов субъектов персональных данных или их представителей (далее – запросы).

2. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных (часть 7 статьи 14 Федерального закона), в том числе содержащей:

- подтверждение факта обработки персональных данных в МОБУ СОШ №4 им.В.Чикмезова МО Кореновский район (далее – школа);
- правовые основания и цели обработки персональных данных;
- цели и применяемые в школе способы обработки персональных данных;
- наименование и место нахождения школы, сведения о лицах (за исключением работников Управления), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора со школой или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;

- порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

- информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

- иные сведения, предусмотренные Федеральным законом или другими федеральными законами.

3. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с частью 8 статьи 14 Федерального закона.

4. Субъект персональных данных вправе требовать от школы уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

5. Сведения, указанные в части 7 статьи 14 Федерального закона, должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

6. Сведения, указанные в части 7 статьи 14 Федерального закона, предоставляются субъекту персональных данных или его представителю школы при обращении либо при получении запроса субъекта персональных данных или его представителя.

7. 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 Управлением (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт

обработки персональных данных школой, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

8. Рассмотрение запросов является служебной обязанностью должностных лиц, в чьи обязанности входит обработка персональных данных (далее – должностные лица Управления).

9. Должностные лица школы обеспечивают:

- объективное, всестороннее и своевременное рассмотрения запроса;
- принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов персональных данных;
- направление письменных ответов по существу запроса.

10. Ведение делопроизводства по запросам осуществляется сотрудником школы.

11. Все поступившие запросы регистрируются в день их поступления. На запросе проставляется штамп, в котором указывается входящий номер и дата регистрации.

12. Запрос прочитывается, проверяется на повторность, при необходимости сверяется с находящейся в архиве предыдущей перепиской. В случае, если сведения, указанные в части 7 статьи 14 Федерального закона, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в школу или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона, и ознакомления с такими персональными данными не ранее чем через 30 дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

Субъект персональных данных вправе обратиться повторно в школу или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в настоящем пункте, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду с необходимыми сведениями должен содержать обоснование направления повторного запроса.

13. Управление вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона. Такой отказ должен быть мотивированным.

14. Прошедшие регистрацию запросы представляются директору школы либо лицу, его заменяющему, который определяет порядок и сроки их рассмотрения, дает по каждому из них письменное указание исполнителям.

15. Директор школы, заместители директора и другие должностные лица школы при рассмотрении и разрешении запроса обязаны:

- внимательно разобраться в их существе, в случае необходимости истребовать дополнительные материалы или направить сотрудников на места для проверки фактов, изложенных в запросах, принять другие меры для объективного разрешения поставленных заявителями вопросов, выявления и устранения причин и условий, порождающих факты нарушения законодательства о персональных данных;

- принимать по ним законные, обоснованные и мотивированные решения и обеспечивать своевременное и качественное их исполнение;

- сообщать в письменной форме субъекту персональных данных о решениях, принятых по их запросам, со ссылками на законодательство Российской Федерации, а в случае отклонения запроса - разъяснять также порядок обжалования принятого решения.

16. Школа обязана сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его

представителя в течение 30 дней с даты получения запроса субъекта персональных данных или его представителя, если иное не предусмотрено другими нормативными актами.

17. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении, либо при получении запроса субъекта персональных данных или его представителя должностные лица школы обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 дней со дня обращения субъекта персональных данных или его представителя, либо с даты получения запроса субъекта персональных данных или его представителя, если иное не предусмотрено другими нормативными актами.

18. Школа обязана предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных, если иное не предусмотрено другими нормативными актами.

19. В срок, не превышающий 7 рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, должностные лица школы обязаны внести в них необходимые изменения.

20. В срок, не превышающий 7 рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, должностные лица школы обязаны уничтожить такие персональные данные.

21. Школа обязана уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

22. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных должностные лица школы обязаны осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных с момента такого обращения или получения указанного запроса на период проверки.

23. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных должностные лицашколы обязаны осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

24. В случае подтверждения факта неточности персональных данных должностные лица школы на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязаны уточнить персональные данные в течение 7 рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

25. В случае выявления неправомерной обработки персональных данных должностные лица школы в срок, не превышающий 3 рабочих дней с даты этого выявления, обязаны прекратить неправомерную обработку персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно, должностные лица Управления в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки персональных данных, обязаны уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных школа обязана уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос

уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

26. Для проверки фактов, изложенных в запросах при необходимости организуются служебные проверки в соответствии с законодательством Российской Федерации.

27. По результатам служебной проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных материалов. Если при проверке выявлены факты совершения сотрудниками школы действия (бездействия), содержащего признаки административного правонарушения или состава преступления информация передается незамедлительно в правоохранительные органы. Результаты служебной проверки представляются директору школы.

28. Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы субъекту персональных данных или его представителю.

29. Ответы на запросы оформляются на бланке школы установленной формы.

30. Должностные лица, виновные в нарушении установленного порядка рассмотрения запросов подлежат привлечению к ответственности в соответствии с законодательством Российской Федерации.

Приложение 9
к приказу МОБУ СОШ №4
им.В.Чикмезова
МО Кореновский район
от 21.09.2020 № 682

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

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

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

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

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

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

– Каждый работник, участвующий в рамках своих служебных обязанностей в процессах обработки персональных данных в ИСПДн и

имеющий доступ к АРМ, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

- Строго соблюдать установленные соответствующими инструкциями правила обеспечения безопасности информации в ИСПДн;
- Знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ;
- Хранить в тайне свой пароль (пароли). Выполнять требования инструкции по организации парольной защиты в полном объеме;
- Хранить индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);
- Выполнять требования инструкции по организации антивирусной защиты в полном объеме;
- Немедленно известить ответственного за обеспечение безопасности персональных данных в случае утери электронного идентификатора или при подозрении компрометации личных ключей и паролей, а также при обнаружении:
    - Несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ;
    - Отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования компонентов АРМ, а также перебоев в системе электроснабжения;
    - Некорректного функционирования установленных на АРМ технических средств защиты;
    - Непредусмотренных отводов кабелей и подключенных устройств.
- Пользователю АРМ категорически запрещается:
    - Использовать компоненты программного и аппаратного обеспечения АРМ в личных целях;
    - Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не

предусмотренные архивом дистрибутивов установленного программного обеспечения АРМ;

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

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

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

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

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

Приложение 10
к приказу МОБУ СОШ №4
им. В.Чикмезова МО Кореновский район
от 21. 09.2020 № 682

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

1. Общие положения

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

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

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

-

2. Обязанности администратора информационной безопасности

- Администратор информационной безопасности обязан:
  - Знать требования нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности персональных данных при их обработке в ИСПДн;
  - Знать перечень обрабатываемых персональных данных, состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных.
  - Уметь пользоваться средствами защиты информации и осуществлять их непосредственное администрирование;

- Еженедельно осуществлять резервное копирование информации, содержащей персональные данные (при необходимости);
- Обязан осуществлять периодический контроль за выполнением работниками эксплуатирующими ИСПДн (пользователями ИСПДн), мероприятий по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн;
- Участвовать в работе по проведению внутреннего контроля соответствия обработки персональных данных требованиям по защите информации;
- Обязан анализировать журнал системы защиты информации от несанкционированного доступа (НСД), проводить проверки электронного журнала обращений к информационным системам персональных данных;
- Обязан обеспечивать строгое выполнение требований по обеспечению защиты информации при организации технического обслуживания АРМ;
- Обязан вести журнал учета средств защиты информации, используемых в ИСПДн;
- Обязан присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию АРМ;
- Обязан проводить инструктаж пользователей ИСПДн по правилам работы с используемыми техническими средствами и средствами защиты информации в соответствии с технической документацией на используемые средства защиты;
- Обязан проводить мероприятия по организации антивирусной защиты;
- Осуществлять организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями, согласно инструкции по организации парольной защиты в информационных системах персональных данных;
- Обязан организовать ведение журнала учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации;

- Обязан немедленно сообщать ответственному за организацию обработки персональных данных, информацию об имевших место попытках несанкционированного доступа к информации и техническим средствам АРМ, а также принимать необходимые меры по устранению нарушений:
- Установить причины, по которым стал возможным НСД;
- Установить последствия, к которым привел НСД;
- Зафиксировать случай НСД в виде документа (акта, служебной записки и т.д.) с описанием причин НСД, предполагаемых или установленных нарушителей и последствий;
- Провести проверку настроек средств защиты информации и операционных систем на соответствие требованиям руководящих документов и разрешительной системы доступа пользователей к защищаемым информационным ресурсам и объектам доступа ИСПДн, при необходимости провести настройку;
- Провести инструктаж пользователей ИСПДн по выполнению требований по обеспечению защиты персональных данных.

3. Права администратора информационной безопасности.

Администратор информационной безопасности имеет право:

- Требовать от пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкции о порядке работы пользователей в ИСПДн в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;
- Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн;
- Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности персональных данных к ответственному за организацию обработки персональных данных в ИСПДн и/или ответственному за эксплуатацию ИСПДн;

4. Ответственность администратора информационной безопасности

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

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

Приложение 11
к приказу МОБУ СОШ №4
им. В.Чикмезова
МО Кореновский район
от 21.09.2020 № 682

ИНСТРУКЦИЯ
по организации парольной защиты

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах персональных данных (далее – ИСПДн), а также контроль за действиями пользователей при работе с паролями.

Личные пароли генерируются и распределяются централизованно Администратором информационной безопасности:

- Длина пароля должна быть не менее 8 символов;
- В числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);
- Символы паролей должны вводиться в режиме латинской раскладки клавиатуры;
- Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- При смене пароля новое значение должно отличаться от предыдущих;
- Пользователь не имеет права сообщать личный пароль другим лицам;

Полная плановая смена паролей пользователей ИСПДн должна проводиться регулярно, не реже одного раза в 3 месяца.

Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение и т.п.) должна производиться администратором информационной безопасности в ИСПДн немедленно после окончания последнего сеанса работы данного пользователя ИСПДн с системой на основании письменного указания непосредственного руководителя структурного подразделения.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) администратора информационной безопасности в ИСПДн.

В случае компрометации (утеря, передача другому лицу) личного пароля, Пользователь ИСПДн обязан незамедлительно сообщить об этом администратору информационной безопасности для принятия соответствующих мер.

Приложение 12
к приказу МОБУ СОШ №4
им.В.Чикмезова
МО Кореновский район
от 21.09.2020 №682

ИНСТРУКЦИЯ
по организации антивирусной защиты

1. Общие требования

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

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

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

2. Применение средств антивирусного контроля

– При загрузке АРМ в автоматическом режиме должен проводиться антивирусный контроль служб операционной системы, исполняемых приложений, находящихся в автозагрузке, реестра операционной системы.

– Полному антивирусному контролю автоматизированные рабочие места (АРМ) должны подвергаться не реже одного раза в неделю.

– Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, оптических и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего

аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

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

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

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

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

- Приостановить работу в ИСПДн;
- Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя структурного подразделения и администратора информационной безопасности в ИСПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- Провести лечение или уничтожение зараженных файлов.

3. Ответственность

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

Приложение 13
к приказу МОБУ СОШ №4
им.В.Чикмезова
МО Кореновский район
от 21. 09.2020 № 682

ПОРЯДОК
уничтожения персональных данных при достижении целей обработки и (или) при наступлении иных законных оснований

Настоящий документ устанавливает порядок уничтожения информации, содержащей персональные данные, при достижении целей обработки или при наступлении иных законных оснований в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

– Документы, дела, книги и журналы учета, содержащие персональные данные, при достижении целей обработки, или при наступлении иных законных оснований, (например, утратившие практическое значение, а также с истекшим сроком хранения), подлежат уничтожению.

Уничтожение документов производится в присутствии ответственного за организацию обработки персональных данных, который несет персональную ответственность за правильность и полноту уничтожения перечисленных в акте документов (Акт составляется в свободной форме).

– Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста или сжигаются.

– После уничтожения материальных носителей ответственный за организацию подписывает акт в двух экземплярах, также в номенклатурах и описях дел проставляется отметка «Уничтожено. Акт №__(дата)».

Уничтожение информации на носителях необходимо осуществлять путем стирания информации с использованием сертифицированного программного обеспечения, установленного на АРМ с гарантированным уничтожением (в соответствии с заданными характеристиками для установленного программного обеспечения с гарантированным уничтожением).

Информация, содержащая персональные данные при достижении целей обработки или при наступлении иных законных оснований (например,

утратившие практическое значение, с истекшим сроком хранения) в электронном виде, подлежит уничтожению.

Приложение 14

к приказу МОБУ СОШ №4
им.В.Чикмезова
МО Кореновский район
от 21. 09.2020 № 682

УТВЕРЖДАЮ
директор МОБУ СОШ №4
им. В.Чикмезова
МО Кореновский район
_____ Л.И.Рассохина

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МОБУ СОШ №4 им. В.Чикмезова МО Кореновский район

1. Общие положения

1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных МОБУ СОШ №4 им. В.Чикмезова МО Кореновский район (далее – школа) разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным Законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

2. Настоящие правила определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных и действуют постоянно.

2. Тематика внутреннего контроля

3. Тематика проверок обработки персональных данных в учреждении:

1) соблюдение работниками школы, ответственным за обработку персональных данных, (далее – работник) правил обработки персональных данных;

2) соблюдение работниками правил рассмотрения запросов субъектов персональных данных или их представителей;

3) соблюдение работниками правил порядка доступа в помещения, в которых ведется обработка персональных данных;

4) соблюдение работниками, работающими в информационных системах, парольной и антивирусной политики, использование ими средств защиты информации.

3. Порядок проведения проверок

4. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям, МОБУ СОШ №4 им. В.Чикмезова МО Кореновский район не реже **1 раза в год** организует проведение периодических проверок.

Срок проведения проверки не должен превышать 30 календарных дней.

5. Проверки в школе проводятся плановые, согласно плану внутренних проверок (по форме согласно Приложение 1 к настоящим правилам), утвержденному приказом руководителя и внеплановые.

Внеплановые проверки проводятся при рассмотрении жалоб и обращений граждан или юридических лиц по вопросам, связанным с обработкой персональных данных. Внеплановые проверки проводятся на основании распоряжения руководителя.

6. Проверки осуществляются ответственным за организацию обработки персональных данных (далее – ответственный), в составе комиссии, образуемой на основании распоряжения руководителя, состоящей из работников, работающих с персональными данными, не менее 2-х человек.

7. В день окончания проведения проверки составляется Протокол по форме согласно Приложению 2 настоящих правил. Протокол подписывается всеми лицами, принимающими участие в проверке.

8. При выявлении в ходе проверки нарушений, в Протоколе делается запись о мероприятиях и сроках по их устранению.

9. О результатах проверки и мерах, необходимых для устранения нарушений ответственный докладывает руководителю.

10. По окончании проверок материалы передаются на хранение в архив.

Приложение 1
к Правилам осуществления внутреннего
контроля соответствия обработки
персональных данных требованиям
к защите персональных данных

План
Проведения внутренних проверок условий обработки персональных данных

МОБУ СОШ №4 им.В.Чикмезова МО Кореновский район

№ п/п	*Тема проверки*	*Срок проведения*	*Исполнитель*
1	*соблюдение работниками образовательного учреждениями, ответственными за обработку персональных данных правил обработки персональных данных*		
2	*Соблюдение работниками образовательного учреждениями, ответственными за обработку персональных данных, правил рассмотрения запросов субъектов персональных данных или их представителей*		
3.	*Соблюдение работниками образовательного учреждениями, ответственными за обработку персональных данных, правил порядка доступа в помещения, в которых ведется обработка персональных данных*		
4	*Соблюдение работниками образовательного учреждениями, работающими в информационных системах, парольной и антивирусной политики, использование ими средств защиты информации*		

Ответственный за организацию обработки персональных данных _____ *подпись* _____ *(данные)*

*Руководитель*_____

Приложение 2

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

П Р О Т О К О Л

проведения проверки условий обработки персональных данных

МОБУ СОШ №4 им.В.Чикмезова МО Кореновский район

Дата _____

*Настоящий протокол составлен ответственным за организацию обработки персональных данных МОБУ СОШ №4 им.В.Чикмезова МО Кореновский район*_____

В присутствии комиссии
1. _____
2. _____

*Проверка осуществлена на основании: (наименование документа)*_____

*В ходе проверки проверено:*_____

*Выявлены нарушения:*_____

*Меры по устранению нарушений:*_____

*Срок устранения нарушений:*_____

Ответственный за организацию обработки персональных данных _____ _____
подпись *(данные)*

Члены комиссии _____ _____
подпись *(данные)*

_____ _____
подпись *(данные)*

Ознакомлен(ы):

Проверяемый(е) сотрудник(и) _____
_____

подпись *(данные)*

Приложение 15
к приказу МОБУ СОШ №4
им. В.Чикмезова
МО Кореновский район
от 21. 09.2020 №682

ИНСТРУКЦИЯ
по обработке персональных данных без использования средств автоматизации

1. Общие положения.

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому гражданину, обратившемуся в МОБУ СОШ №4 им. В.Чикмезова МО Кореновский район, или сотруднику (далее – субъекту персональных данных) МОБУ СОШ №4 им. В.Чикмезова МО Кореновский район.

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

Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные настоящим Положением, должны применяться с учетом требований Постановления Правительства Российской Федерации «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 г. № 687, а также требований нормативных правовых актов федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации.

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

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

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

Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники МОБУ СОШ №4 им. В.Чикмезова МО Кореновский район или лица, осуществляющие такую обработку по договору с МОБУ СОШ №4 им. В.Чикмезова МО Кореновский район), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется МОБУ СОШ №4 им. В.Чикмезова МО Кореновский район 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 МОБУ СОШ №4 им. В.Чикмезова МО Кореновский район.

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

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

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

– типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе,

имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.

При ведении журналов (журналов регистрации, журналов посещений), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в помещения МОБУ СОШ №4 им. В.Чикмезова МО Кореновский район или в иных аналогичных целях, должны соблюдаться следующие условия:

– необходимость ведения такого журнала должна быть предусмотрена актом МОБУ СОШ №4 им. В.Чикмезова МО Кореновский район, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных;

– копирование содержащейся в таких журналах информации не допускается;

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

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, зачеркивание, стирание).

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

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

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

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

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

Приложение 16
к приказу МОБУ СОШ №4
им. В.Чикмезова
МО Кореновский район
от 21. 09.2020 № 682

ИНСТРУКЦИЯ

по работе с инцидентами информационной безопасности

Ответственность за выявление инцидентов ИБ и реагирование на них в МОБУ СОШ №4 им. В.Чикмезова МО Кореновский район возлагается на администратора информационной безопасности.

Администратор информационной безопасности имеет полномочия инициировать проведение служебных проверок (ходатайствовать о наложении дисциплинарного взыскания перед руководителем МОБУ СОШ №4 им. В.Чикмезова МО Кореновский район) по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации.

Администратор информационной безопасности обязан вести журнал учёта инцидентов ИБ (событий, действий, повлекших за собой риски безопасности защищаемой информации и создающих предпосылки к нарушению критериев безопасности информации). Сюда относятся нарушения пользователями положений организационно-распорядительных документов, установленных порядков и технологии работы в ИС, разглашение защищаемой информации и любые действия, направленные на это, не антропогенные инциденты (сбои ПО, стихийные бедствия).

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

- даты и времени;
- причин (умышленные и неумышленные действия, не антропогенные инциденты и т.п.) и описания инцидента и задействованных лиц;
- информации о последствиях;
- информации о возможных последствиях (экономические убытки (в связи с заменой СЗИ, повторной аттестации; временные и трудозатраты на устранение последствий, нарушение работы пользователей, ущерб субъектам ПДн и юридические последствия для МОБУ СОШ №4 им. В.Чикмезова МО Кореновский район и т.п.).

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

В случае возникновения рецидива со стороны пользователя или администратора информационной безопасности, по ходатайству ответственного за организацию обработки персональных данных руководителем МОБУ СОШ №4 им. В.Чикмезова МО Кореновский район накладывается дисциплинарное взыскание.

Сокрытие нарушений и инцидентов ИБ, вызванных любыми должностными лицами МОБУ СОШ №4 им. В.Чикмезова МО Кореновский район, является грубым нарушением трудовой дисциплины. Сокрытие нарушений и инцидентов ИБ, вызванных действиями администратора информационной безопасности и ответственным за организацию обработки персональных данных, является грубейшим нарушением дисциплины, и при выяснении данного факта должно строго наказываться.

Любой сотрудник должен согласовывать следующие действия с администратором информационной безопасности:

- замена прикладного оборудования (мышь, клавиатура, принтер, монитор);
- установка дополнительного ПО;
- изменение сетевых настроек рабочего места;
- замена, изменение любой аппаратной части рабочего места.

Ответственный за организацию обработки персональных данных не может требовать от администратора информационной безопасности действий, направленных на нарушение настоящего руководства и других организационно-распорядительных документов МОБУ СОШ №4 им. В.Чикмезова МО Кореновский район, требовать сокрытия инцидентов ИБ, вызванных любыми должностными лицами, требовать сообщения ему паролей на средства защиты информации и нарушения установленного разграничения прав по допуску к информационным ресурсам, установленным матрицей доступа к информационными ресурсам ИС.

Приложение 17
к приказу МОБУ СОШ №4
им. В.Чикмезова
МО Кореновский район
от 21. 09.2020 № 682

УТВЕРЖДАЮ:
Директор МОБУ СОШ №4 им.в.Чикмезова
МО Кореновский район
(наименование учреждения)

_____ / _Рассохина Л.И._____ /
подпись расшифровка подписи

ПРАВИЛА
обработки персональных данных, осуществляемой без использования средств автоматизации

Данные правила устанавливают особенности обработки персональных данных,

осуществляемой без использования средств автоматизации, и меры по обеспечению

безопасности персональных данных.

Обработка персональных данных, содержащихся в информационной системе

персональных данных либо извлечённых из такой системы считается осуществлённой без

средств автоматизации, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляется при непосредственном участии человека.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилахописанныхвданномдокументе.Фактинформированияфиксируетсявлистеознакомления.

Типовые формы документов должны соответствовать п.7 Постановления

Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении

Положения об особенностях обработки персональных данных, осуществляемой без

использования средств автоматизации».

Персональные данные при их обработке, осуществляемой без использования

средств автоматизации, должны обособляться от иной информации, в частности путём

фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

Не допускается фиксация на одном материальном носителей персональных данных, цели обработки которых заведомо не совместимы. Для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Законом «О персональных данный» устанавливаются следующие категории:

персональные данные, общедоступные, специальные и биометрические.

Необходимо обеспечить хранение материальных носителей, цели обработки

которых различны.

При обработке персональных данных без использования средств автоматизации

уточнение производится путём обновления или изменения данных на материальном

носителе. Если это не допускается техническими особенностями материального носителя,

на том же материальном носителе фиксируются сведения о вносимых изменениях в

персональные данные либо изготавливается новый материальный носитель с уточнёнными персональными данными.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять

обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных

Данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению использованию, и используется (распространяется) копия персональных данных;

- при необходимости уничтожения или блокирования части персональных данных

уничтожается или блокируется материальный носитель с предварительным копированием

сведений, не подлежащих уничтожению или блокированию, способом, исключающим

одновременное копирование персональных данных, подлежащих уничтожению или

блокированию.

Уничтожение или обезличивание части персональных данных, если это не

допускается материальным носителем, может производиться способом, исключающим

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

При обработке персональных данных для каждой категории персональных данных

должны быть определены места хранения и перечень лиц, осуществляющих обработку

персональных данных либо имеющих к ним доступ.

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

В целях обеспечения сохранности персональных данных и исключения несанкционированногодоступакнимдолжнысоблюдатьсяследующиемерыбезопасности:

- надёжно запирающиеся взломостойкие двери в помещении, где хранятся

документы с персональными данными;

- решётки на окнах, исключающие проникновение, шторы или жалюзи, а также

любыедругиеорганизационныемерыдляисключениявозможностивизуальногопросмотра документов посторонними;

- охранно-пожарная сигнализация, связанная с постом охраны;

- сейфы или запирающиеся металлические шкафы, при необходимости могут быть

оборудованы механизмом опечатывания;

- особый порядок хранения основных и запасных ключей от помещений, сейфов и

Металлических шкафов, предусматривающий возможность опечатывания пенала с ключами при сдаче их на хранение;

- порядок действий сотрудников, ведущих обработку и хранения персональных

данных, при возникновении чрезвычайной ситуации.

Указанныемерыдолжныбытьреализованыпридействительнойнатонеобходимости. Ответственные за реализацию указанных мер и сохранность персональных данных назначаются приказом руководителя подразделения.