РЕСПУБЛИКА АДЫГЕЯ

ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ (ПОВЫШЕНИЯ КВАЛИФИКАЦИИ) РЕСПУБЛИКИ АДЫГЕЯ «УЧЕБНО-МЕТОДИЧЕСКИЙ ЦЕНТР ПО ГРАЖДАНСКОЙ ОБОРОНЕ, ЗАЩИТЕ ОТ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ И ПОЖАРНОЙ БЕЗОПАСНОСТИ»

ПРИКАЗ

«24» сентября 2019 № 16

Майкоп

Об утверждении комиссии по квалификации информационных систем персональных данных и по уничтожению персональных данных в ГАУ ДПО РА УМЦ ГОЧС и ПБ

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 17.11.2007 № 781 «Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и в целях обеспечения режима конфиденциальности при работе с материальными носителями персональных данных в ГАУ ДПО РА УМЦ ГОЧС и ПБ,

п р и к а з ы в а ю:

1. Утвердить состав комиссии по классификации информационных систем персональных данных и по уничтожению персональных данных (ИСПДн), в соответствии с приложением № 1 к настоящему приказу.
2. Комиссии, при проведении классификации ИСПДн, руководствоваться должностной инструкцией пользователя информационной системы персональных данных, согласно инструкции, приложение № 2 и должностной инструкцией ИСПДн приложение № 3.
3. Утвердить места хранения материальных носителей персональных данных.
4. Обеспечить раздельное хранение материальных носителей персональных данных ответственными лицами, в соответствии с приложением № 4 к настоящему приказу.
5. Делопроизводителю Шевченко Н.Д., довести до лиц, ответственных за обеспечение сохранности материальных носителей персональных данных, под роспись.
6. Приказ от 10.11.2016 № 9 «Об утверждении мест хранения материальных носителей персональных данных в ГАУ ДПО РА УМЦ ГОЧС и ПБ», считать утратившим силу.
7. Контроль, за исполнением настоящего приказа, возложить на ответственного за организацию обработки персональных данных.

Директор _____ О. Широбоков

В дело № 03-08

24.09 2019 г.

С приказом ознакомлен(а):

М.С. Болоков

З.А. Курбанова

Н.Д. Шевченко

Н.С. Широбокова

А.И. Цыганкова

А.А. Фокина

Приложение № 1

к приказу № 16 от 24.09. 2019 г.

СОСТАВ КОМИССИИ

по классификации информационных систем персональных данных и по уничтожению персональных данных (ИСПДн)

Председатель комиссии:	- заместитель директора	Болоков М.С.
Члены комиссии:	- главный бухгалтер	Курбанова З.А.
	- делопроизводитель	Шевченко Н.Д.
	- методист	Цыганкова А.И.
	- методист	Широбокова Н.С.
	- методист	Фокина А.А.

Приложение № 2

к приказу № 16 от 24.09. 2019 г.

ИНСТРУКЦИЯ
КОМИССИИ ПО КЛАССИФИКАЦИИ И ПО УНИЧТОЖЕНИЮ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. Данная Инструкция содержит обязательные для всех сотрудников ГАУ ДПО РА УМЦ ГОЧС и ПБ требования по обеспечению конфиденциальности документов, содержащих персональные данные.

1.2. Персональные данные – это 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.

1.3. Обеспечение конфиденциальности персональных данных не требуется в случае обезличивания персональных данных или в отношении общедоступных персональных данных. В общедоступные источники персональных данных (в том числе справочники, адресные книги) в целях информационного обеспечения с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

1.4. Конфиденциальность персональных данных (приложение 1) предусматривает обязательное согласие субъекта персональных данных или наличие иного законного основания на их обработку. Согласие субъекта персональных данных не требуется на обработку данных:

§ в целях исполнения обращения, запроса субъекта персональных данных, трудового или иного договора с ним;

§ адресных данных, необходимых для доставки почтовых отправлений организациями почтовой связи;

§ данных, включающих в себя только фамилии, имена и отчества;

§ в целях однократного пропуска или в иных аналогичных целях;

§ персональных данных, обрабатываемых без использования средств автоматизации.

1.5. В учреждении формируется и ведется перечень конфиденциальных данных с указанием, мест хранения и ответственных за хранение и обработку данных. Осуществлять обработку и хранение конфиденциальных данных, не внесенных в перечень, запрещается.

1.6. Основные требования и мероприятия по обеспечению безопасности при обработке и хранении персональных данных установлены постановлениями Правительства Российской Федерации от 17 ноября 2007 г. № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" и от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации". Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

1.7. Общие правила хранения и передачи персональных данных:

§ Запрещается оставлять материальные носители с персональными данными без присмотра в незапертом помещении. Все сотрудники, постоянно работающие в помещениях, в которых ведется обработка персональных данных, должны быть допущены к работе с соответствующими видами персональных данных.

§ Сотрудникам учреждения, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью. После подготовки и передачи документа в соответствии с резолюцией, файлы черновиков и вариантов документа переносятся подготовившим их сотрудником на маркированные носители, предназначенные для хранения персональных данных. Без согласования с директором учреждения, формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

§ Передача персональных данных допускается только в случаях, установленных Федеральными законами Российской Федерации «О персональных данных», «О порядке рассмотрения обращений граждан Российской Федерации», действующими инструкциями по работе со служебными документами и обращениями граждан, а также по письменному поручению (резолюции) вышестоящих должностных лиц.

§ Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и действующими инструкциями по работе со служебными документами и обращениями граждан. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах конфиденциальные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

1.8. Сотрудники учреждения, осуществляющие обработку или хранение конфиденциальных данных, несут ответственность за обеспечение информационной безопасности. Лица, виновные в нарушении норм, регулирующих обработку и хранение конфиденциальных данных, несут дисциплинарную, административную или уголовную ответственность в соответствии с законодательством и ведомственными нормативными актами.

1.9. Сотрудники учреждения и лица, выполняющие работы по договорам и контрактам, имеющие отношение к работе с персональными данными, должны быть в обязательном порядке ознакомлены под расписку с настоящей Инструкцией.

2. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемой без использования средств автоматизации, и условия хранения персональных данных.

2.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должны 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.

2.2. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

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

2.4. 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, исключающее одновременное копирование иных персональных данных, не подлежащих распространению и использованию.

низационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

3.2. Допуск лиц к обработке персональных данных в информационной системе осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

3.3. Размещение информационных систем, специальное оборудование и организация работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в этих помещениях посторонних лиц. Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается.

3.4. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, запрещается.

3.5. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

3.6. При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

§ использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

§ недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

§ постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

§ недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения

3.7. При обработке персональных данных в информационной системе разработчиками и администраторами систем должны обеспечиваться:

§ обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

§ учет лиц, допущенных к работе с персональными данными в информационной системе, прав и паролей доступа;

§ учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

§ контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

§ описание системы защиты персональных данных.

3.8. Специфические требования по защите персональных данных в автоматизированной информационно-аналитической системе устанавливается инструкцией по ее использованию и эксплуатации.

4. Порядок учета, хранения и обращения со съемными носителями персональных данных, твердыми копиями и их утилизации.

4.1. Все находящиеся на хранении и в обращении съемные носители с персональными данными подлежат учёту. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

4.2. Учет и выдачу съемных носителей персональных данных по форме (приложение № 2) осуществляют ответственным за защиту ИСПДн на которого возложены функции хранения носителей персональных данных. Сотрудники учреждения получают учтенный съемный носитель от администратора сети для выполнения работ на конкретный срок. При полу-

2.5. Использование типовых форм документов и журналов учета (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 (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес Оператора, 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 Оператором 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;

§ типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

2.6. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в помещение, на котором находится Оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:

§ необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом Оператора, 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, а также сведения о порядке пропуска субъекта персональных данных в помещение, в котором находится Оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

§ копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

§ персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных в помещение, в котором находится Оператор).

2.7. Порядок уничтожения или обезличивания 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, вымарывание). 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. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемой с использованием средств автоматизации, правила доступа, хранения и пересылки персональных данных:

3.1. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей орга-

низационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

3.2. Допуск лиц к обработке персональных данных в информационной системе осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

3.3. Размещение информационных систем, специальное оборудование и организация работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в этих помещениях посторонних лиц. Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается.

3.4. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, запрещается.

3.5. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

3.6. При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

§ использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

§ недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

§ постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

§ недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения

3.7. При обработке персональных данных в информационной системе разработчиками и администраторами систем должны обеспечиваться:

§ обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

§ учет лиц, допущенных к работе с персональными данными в информационной системе, прав и паролей доступа;

§ учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

§ контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

§ описание системы защиты персональных данных.

3.8. Специфические требования по защите персональных данных в автоматизированной информационно-аналитической системе устанавливается инструкцией по ее использованию и эксплуатации.

4. Порядок учета, хранения и обращения со съемными носителями персональных данных, твердыми копиями и их утилизации.

4.1. Все находящиеся на хранении и в обращении съемные носители с персональными данными подлежат учёту. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

4.2. Учет и выдачу съемных носителей персональных данных по форме (приложение № 2) осуществляют ответственным за защиту ИСПДн на которого возложены функции хранения носителей персональных данных. Сотрудники учреждения получают учтенный съемный носитель от администратора сети для выполнения работ на конкретный срок. При полу-

чении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

4.3. Сотрудникам запрещается:

§ хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

§ выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому и т. д.

4.4. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

4.5. О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений немедленно ставится в известность начальник соответствующего структурного подразделения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы персонального учета съемных носителей персональных данных.

4.6. Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется уполномоченной комиссией. По результатам уничтожения носителей составляется акт по форме (Приложение № 3).

С инструкцией ознакомлен(а): _____ _____

(подпись) (расшифровка подписи)

Приложение № 1
к инструкции

Статья 7. Конфиденциальность персональных данных

Операторы и иные лица, 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.

(Статья в редакции, введенной в действие с 27 июля 2011 г. Федеральным законом от 25 июля 2011 года N 261-ФЗ, "О внесении изменений в Федеральный закон "О персональных данных").

Приложение № 2
к инструкции

ЖУРНАЛ
учета съемных носителей персональных данных

Начат «___» _____ 20__ г.

Окончен «___» _____20___ г.

На _____ листах

№ п/п	Метка съемного носителя (учетный номер)	Фамилия исполнителя	(Получил, вернул, передал)	Дата записи информации	Подпись исполнителя	Подпись ответственного за хранение	Примечание
1	2	3	4	5	6	7	8

Приложение № 3
к инструкции

УТВЕРЖДАЮ

_____
(руководитель)

_____
(подпись)

«___» _____ 20__ г.

АКТ
уничтожения съемных носителей персональных данных

Комиссия, наделенная полномочиями, приказом директора ГАУ ДПО РА УМЦ ГОЧС и ПБ от «___» _____ 20__ № ___ в составе:

Председатель - _____

Члены комиссии - _____

\- _____

провела отбор носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации _____ информация, записанная на них в процессе эксплуатации, подлежит гарантированному уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя ПДн	Примечание

Всего съемных носителей _____
(цифрами и прописью)

На указанных носителях персональные данные уничтожены путем

_____
(механическое уничтожение, сжигания и т.п.)

Перечисленные съемные носители ПДн уничтожены путем

_____
(разрезания, сжигания, механического уничтожения информации, и т.п.),

Председатель комиссии _____/ _____/ «___» _____ 20__ г.

Члены комиссии _____/ _____/ «___» _____20__ г.
_____/ _____/ «___» _____20__ г.
_____/ _____/ «___» _____20__ г.

Приложение № 3
к приказу № 16 от 24.09. 2019 г.

Должностная инструкция
пользователя информационной системы персональных данных

Настоящий документ подготовлен в рамках выполнения работ по обеспечению безопасной эксплуатации информационной системы персональных данных (далее – ИСПДн) государственного автономного учреждения дополнительного профессионального образования (повышения квалификации) Республики Адыгея «Учебно-методический центр по гражданской обороне, защите от чрезвычайных ситуаций и пожарной безопасности».

1. Общие положения

1.1. Пользователь ИСПДн (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных ГАУ ДПО РА УМЦ ГОЧС и ПБ.

1.2. Пользователем является каждый работник ГАУ ДПО РА УМЦ ГОЧС и ПБ участвующий в рамках своих функциональных обязанностей в процессах обработки информации без использования средств автоматизации и имеющий доступ к аппаратных средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, Положением о защите персональных данных, руководящими и нормативными документами ФСТЭК России и другими локальными актами ГАУ ДПО РА УМЦ ГОЧС и ПБ.

1.5. Методическое руководство работой пользователя осуществляется ответственными за организацию обработки персональных данных, назначаемым приказом директора.

2. Должностные обязанности

2.1. Знать и выполнять требования настоящей инструкции и других внутренних распоряжений, регламентирующих порядок действий по защите персональных данных.

2.2. Выполнить на автоматизированном рабочем месте (далее – АРМ) только те процедуры обработки персональных данных, которые определены для него должностной инструкцией.

2.3. 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.

2.4. Соблюдать правила при работе в сетях общего доступа Интернет.

2.5. Обо всех выявленных нарушениях, связанных с информационной безопасностью ГАУ ДПО РА УМЦ ГОЧС и ПБ, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться к ответственному за организацию обработки персональных данных.

2.6. 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 ИСПДн, информации, хранящейся на бумажных носителях.
- 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 от помещений ИСПДн.

- привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с директором или ответственному за организацию обработки персональных данных.

Приложение № 4

к приказу № 16 от 24.09. 2019 г.

N п/п	Категория персональных данных	Место хранения	Ответственное лицо (должность, фамилия и инициалы)
1.	**Бумажные носители персональных данных** (трудовая книжка; журналы учета трудовых книжек; личные дела; журнал учета командировок; личная карточка Т-2; журналы сверки по военнообязанным; приказы по личному составу);	специально отведенный железный сейф в кабинете N 3	Делопроизводитель Шевченко Н.Д.
	- материалы по учету рабочего времени, паспортные данные, ИНН, страховое свидетельство	специально отведенный железный сейф в кабинете N 6	Главный бухгалтер Курбанова З.А.
2.	Электронные носители персональных данных: жесткий диск, съемный носитель	Кабимнет № 3 Кабинет № 6	Документовед Шевченко Н.Д. Главный бухгалтер Курбанова З.А.
3.	Бумажные носители персональных данных обучающихся	Кабинет № 11 специально отведенный железный сейф в кабинете N 11	Методист Широбокова Н.С. (обучение на бюджетной основе). Методист Цыганкова А.И. (обучение на коммерческой основе) Методист Фокина А.А. (дистанционное обучение слушателей на коммерческой основе)