**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ АМУРСКОЙ ОБЛАСТИ**
**ГОСУДАРСТВЕННОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ АМУРСКОЙ ОБЛАСТИ**
**«АМУРСКИЙ АГРАРНЫЙ КОЛЛЕДЖ»**

# ПРИКАЗ

___27.09.2019 № _27092-од___

г. Благовещенск

В соответствии с Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных», с целью организации и координации мероприятий по защите информации, обрабатываемой в информационной системе персональных данных(ИСПдН)

**п р и к а з ы в а ю :**

1.Утвердить и ввести в действие комплект организационно-распорядительной документации по организации обработки и защиты информации, обрабатываемой в ИС ГПОАУ АО «Амурский аграрный колледж» в соответствие со списком приложений к настоящему приказу:

| № приложения к приказу | Название документа |
|---|---|
| Организация обработки персональных данных | |
| Приложение №1 | Правила обработки персональных данных |
| Приложение №2 | Правила рассмотрения запросов субъектов персональных данных |
| Приложение №3 | Правила осуществления внутреннего контроля обработки персональных данных на соответствие требованиям к их защите |
| Приложение №4 | Порядок доступа сотрудников в помещения, в которых ведется обработка ПД |
| Приложение №5 | Положение о разрешительной системе допуска к ресурсам информационной системы персональных данных |
| Приложение №6 | Положение о неавтоматизированной обработке персональных данных |
| Приложение №7 | Сведения о реализуемых мерах по защите персональных данных |

2. Секретарю Сергиевич О.А. довести настоящий приказ до заинтересованных лиц под подпись.

3. Контроль за исполнением приказа оставляю за собой.

Исполняющий обязанности
директора Т.А.Романцова

Приложение №1
к приказу ГПОАУ АО «Амурский аграрный колледж»
от «_27_»_сентября 2019 г._ №__27092-од__

**ПРАВИЛА**
**обработки персональных данных в ГПОАУ АО «Амурский аграрный колледж»**

1.Общие положения

1.1. Настоящие правила обработки персональных данных (далее – Правила) в ГПОАУ АО «Амурский аграрный колледж» (далее – Учреждение) определяют цели, содержание и порядок обработки персональных данных (далее – ПДн), меры, направленные на защиту ПДн, а также мероприятия, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области ПДн при предоставлении услуг и обеспечения кадрового учета и бухгалтерской деятельности в Учреждении.
1.2. Настоящие Правила определяют политику Учреждения как оператора, осуществляющего обработку ПДн, в отношении обработки и защиты ПДн.
1.3. В целях настоящих Правил используются следующие понятия:
- Автоматизированная обработка ПДн – обработка ПДн с помощью средств вычислительной техники
- Блокирование ПДн – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн);
- Информационная система персональных данных (далее – ИСПДН) – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств;
- Конфиденциальность ПДн – обязанность оператора и иных лиц, получивших доступ к ПДн, не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом;
- Обезличивание ПДн – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн;
- Обработка ПДн – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;
- Оператор ПДн – Учреждения, самостоятельно или совместно с другими лицами организующий и (или) осуществляющий обработку ПДн, а также определяющий цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн при предоставлении государственных и муниципальных услуг и обеспечения кадрового учета и бухгалтерской деятельности;
- ПДн – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн);
- Предоставление ПДн – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц;
- Распространение ПДн – действия, направленные на раскрытие ПДн неопределенному кругу лиц;
- Уничтожение ПДн – действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.
1.4. Настоящие Правила разработаны в соответствии:

- Трудовым кодексом Российской Федерации;
- Налоговым кодексом Российской Федерации;
- Кодексом Российской Федерации об административных правонарушениях;
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);
- Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27 июля 2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (далее – Федеральный закон «Об организации предоставления государственных и муниципальных услуг»);
- Федеральным законом от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации»;
- постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- постановлением Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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».

1.5. Обработка ПДн в Учреждении осуществляется с соблюдением порядка и условий, предусмотренных настоящими Правилами и законодательством Российской Федерации в области ПДн.

1.6. В Учреждении ведется обработка ПДн следующих категорий субъектов ПДн:
- физические лица, обратившиеся в Учреждение с целью получения государственных услуг, и их представителей;
- физические лица, обработка ПДн которых необходима для предоставления государственных и муниципальных услуг;
- индивидуальные предприниматели (далее – ИП) и физические лица – представители юридических лиц, фигурирующие в договорах, контрактах, жалобах;
- физические лица, претендующие на замещение должностей в Учреждение;
- сотрудники Учреждения.

## 2.Условия и порядок обработки ПДн физических лиц в связи с предоставлением государственных услуг

2.1. Обработка ПДн физических лиц, обратившихся в Учреждение для получения государственных услуг (далее – заявители), и их представителей осуществляется в целях организации предоставления государственных услуг, в том числе в электронной форме.

2.2. При организации предоставления государственных услуг заявителям и их представителям, их ПДн могут извлекаться для обработки из следующих документов, представляемых в форме документов на бумажном носителе или в форме электронных документов:
- документы, удостоверяющие личность гражданина Российской Федерации, в том числе военнослужащих, а также документы, удостоверяющие личность иностранного гражданина, лица без гражданства, включая вид на жительство и удостоверение беженца;

- документы воинского учета;
- свидетельства о государственной регистрации актов гражданского состояния;
- документы, подтверждающие регистрацию по месту жительства или по месту пребывания;
- документы на транспортное средство и его составные части, в том числе регистрационные документы;
- документы о трудовой деятельности, трудовом стаже и заработке гражданина, а также документы, оформленные по результатам расследования несчастного случая на производстве либо профессионального заболевания;
- документы о соответствующем образовании и (или) профессиональной квалификации, об ученых степенях и ученых званиях и документы, связанные с прохождением обучения, выдаваемые организациями, осуществляющими образовательную деятельность;
- справки, заключения и иные документы, выдаваемые организациями, входящими в государственную, муниципальную или частную систему здравоохранения;
- документы Архивного фонда Российской Федерации и другие архивные документы в соответствии с законодательством об архивном деле в Российской Федерации, переданные на постоянное хранение в государственные или муниципальные архивы;
- документы, выданные (оформленные) органами дознания, следствия либо судом в ходе производства по уголовным делам, документы, выданные (оформленные) в ходе гражданского судопроизводства либо судопроизводства в арбитражных судах, в том числе решения, приговоры, определения и постановления судов общей юрисдикции и арбитражных судов;
- решения, заключения и разрешения, выдаваемые органами опеки и попечительства в соответствии с законодательством Российской Федерации об опеке и попечительстве;
- правоустанавливающие документы на объекты недвижимости, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним;
- документы, выдаваемые федеральными государственными учреждениями медико-социальной экспертизы;
- удостоверения и документы, подтверждающие право гражданина на получение социальной поддержки, а также документы, выданные федеральными органами исполнительной власти, в которых законодательством предусмотрена военная и приравненная к ней служба, и необходимые для осуществления пенсионного обеспечения лица в целях назначения и перерасчета размера пенсий;
- документы о государственных и ведомственных наградах, государственных премиях и знаках отличия;
- первичные статистические данные, содержащиеся в формах федерального статистического наблюдения, предоставленных юридическими лицами или индивидуальными предпринимателями;
- письменные уполномочия (доверенности) на обращение в Учреждение для получения государственных и муниципальных услуг от имени юридических и физических лиц выдаваемые другим физическим лицам.

2.3. В Учреждении подлежат рассмотрению обращения граждан Российской Федерации, иностранных граждан и лиц без гражданства, обратившихся в Учреждение лично в консультативных целях, а также направивших индивидуальные или коллективные письменные обращения или обращения в виде электронного документа, составленные в свободной форме.

2.4. В рамках рассмотрения обращений граждан Российской Федерации, иностранных граждан и лиц без гражданства подлежат обработке следующие ПДн, которые могут содержаться в обращениях:
- фамилия, имя, отчество (последнее при наличии);
- почтовый адрес;
- паспортные данные;

- адрес электронной почты;
- указанный в обращении контактный телефон;
- иные ПДн, указанные в обращении (жалобе).

2.5. ПДн, содержащиеся в обращениях, обрабатываются в целях рассмотрения указанных обращений с последующим уведомлением обратившихся лиц о результатах рассмотрения их обращений.

2.6. Для обработки ПДн заявителей, являющихся специальными ПДн, согласно пункту 1 части 2 статьи 10 Федерального закона «О персональных данных» и части 5 статьи 7 Федерального закона «Об организации предоставления государственных и муниципальных услуг» необходимо получение согласия в письменной форме.

2.7. Заявитель при обращении за предоставлением государственной или муниципальной услуги подтверждает факт получения указанного согласия в форме, предусмотренной законодательством Российской Федерации, в том числе путем представления документа, подтверждающего факт получения указанного согласия, на бумажном носителе или в форме электронного документа.

2.8. Согласие на обработку ПДн заполняется заявителями в соответствии с типовой формой согласия на обработку ПДн:

- согласие на ПДн данных может быть представлено в виде электронного документа, подписанного квалифицированной электронной подписью.
- согласие на обработку ПДн заявителя также может быть подано представителем заявителя, если иное не установлено федеральным законом. В случае получения согласия на обработку ПДн от представителя заявителя, полномочия данного представителя на дачу согласия от имени заявителя проверяются Учреждением.

2.9. Для обработки ПДн лиц, не являющихся заявителями, обработка ПДн которых необходима для предоставления государственной или муниципальной услуги, на основании части 3 статьи 7 Федерального закона от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», необходимо получения согласия указанных лиц или их законных представителей в установленной форме.

2.10. Действие пункта 2.9 настоящих Правил не распространяется на лиц, признанных безвестно отсутствующими, и на разыскиваемых лиц, место нахождения которых не установлено уполномоченным федеральным органом исполнительной власти.

2.11. Обработка ПДн заявителей, необходимых для организации предоставления государственных и муниципальных услуг включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

2.12. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) ПДн заявителей для получения государственной услуги, осуществляется путем:

- получения оригиналов необходимых документов (заявление);
- заверения копий документов;
- внесения сведений в учетные формы (на бумажных и электронных носителях);
- внесения ПДн в прикладное программное обеспечение.

2.13. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) ПДн осуществляется путем получения ПДн непосредственно от заявителей или от их законных представителей.

2.14. При организации предоставления государственной услуги запрещается запрашивать у заявителей и третьих лиц ПДн, а также обрабатывать такие ПДн в случаях, не предусмотренных законодательством Российской Федерации.

2.15. При сборе ПДн сотрудники Учреждения, осуществляющие получение ПДн непосредственно от заявителей, обязаны разъяснить указанным заявителям юридические последствия отказа предоставить ПДн. Форма разъяснения субъекту ПДн юридических

последствий отказа представить свои ПДн в связи с предоставлением государственной и муниципальной услуги утверждается приказом директора.
2.16. Передача (предоставление, доступ) и использование ПДн заявителей осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

## 3.Условия и порядок обработки ПДн сотрудников Учреждения

3.1. ПДн сотрудников Учреждения обрабатываются в целях обеспечения кадровой и бухгалтерской деятельности в Учреждении, а также в целях обучения и должностного роста, учета результатов исполнения работниками должностных обязанностей, обеспечения им условий труда, гарантий и компенсаций, сохранности принадлежащего им имущества.
3.2. В целях, предусмотренных пунктом 2.1 настоящих Правил, обрабатываются следующие категории ПДн сотрудников Учреждения:
- фамилия, имя отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);
- серия и номер паспорта, кем и когда выдан;
- информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);
- дата и место рождения;
- адрес прописки и проживания;
- телефонные номера (домашний, рабочий, сотовый);
- состояние в браке;
- ИНН и СНИЛС;
- трудовая деятельность до приема на работу;
- место работы и должность;
- период работы и данные о трудовом договоре;
- номер, серия и дата выдачи трудовой книжки;
- сведения о доходах и заработной плате;
- исполнительные листы;
- лицевые счета;
- сведения о контрагентах;
- сведения о квалификации и переподготовке;
- данные о повышении квалификации;
- наименование образовательного учреждения и документ, подтверждающий образование (номер, дата выдачи, специальность);
- ученая степень и звание;
- сведения о наличии специальных знаний или специальной подготовки;
- данные воинского учета;
- данные о наградах, медалях, поощрениях, почетных званиях;
- постановка на учет в ранние сроки беременности;
- временная нетрудоспособность;
- иные ПДн, необходимые для достижения целей, предусмотренных пунктом 3.1 настоящих Правил.
3.3. Обработка ПДн сотрудников Учреждения осуществляется без согласия указанных лиц в рамках целей, определенных пунктом 3.1 настоящих Правил, в соответствии с пунктом 2 части 1 статьи 6 и частью 2 статьи 11 Федерального закона «О персональных данных», Трудовым кодексом Российской Федерации.
3.4. Обработка специальных категорий ПДн сотрудников Учреждения может осуществляться в рамках целей, определенных пунктом 3.1 настоящих Правил, в соответствии с подпунктом 2.3. пункта 2 части 2 статьи 10 Федерального закона «О персональных данных» и положениями Трудового кодекса Российской Федерации, за исключением случаев получения ПДн сотрудника у третьей стороны, при которых в соответствии с пунктом 3 статьи 86 Трудового кодекса Российской Федерации требуется письменное согласие.

3.5. Обработка ПДн сотрудников Учреждения осуществляется при условии получения от них письменного согласия на обработку ПДн в следующих случаях:
- при передаче (распространении, предоставлении) их ПДн третьим лицам, кроме случаев, предусмотренных действующим законодательством Российской Федерации;
- при принятии решений, порождающих юридические последствия в отношении сотрудников или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их ПДн.
3.6. В случаях, предусмотренных пунктом 3.5 настоящих Правил, согласие сотрудника на обработку его ПДн оформляется в письменной форме, если иное не установлено Федеральным законом «О персональных данных». Форма согласия утверждается приказом директора.
3.7. Непосредственная обработка ПДн сотрудников Учреждения осуществляется специалистами бухгалтерии, специалистами отдела кадров.
3.8. Обработка ПДн сотрудников Учреждения включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.
3.9. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) ПДн сотрудников, а также граждан, претендующих на замещение должностей в Учреждении, осуществляется путем получения ПДн непосредственно от указанных лиц:
- получения оригиналов необходимых документов (заявление, трудовая книжка, иные документы, предоставляемые в Отдел правового, кадрового, информационно-аналитического и организационного обеспечения;
- копирования оригиналов документов;
- внесения сведений в учетные формы (на бумажных и электронных носителях);
- формирования ПДн в ходе кадровой работы;
- внесения ПДн в ИСПДн, используемые отделом кадров и бухгалтерии.
3.10. В случае возникновения необходимости получения ПДн сотрудников, у третьей стороны, следует известить об этом сотрудника заранее, получить его письменное согласие и сообщить ему о целях, предполагаемых источниках и способах получения ПДн.
3.11. Запрещается получать, обрабатывать и приобщать к личному делу сотрудника ПДн, не предусмотренные пунктом 3.2 настоящих Правил, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.
3.12. При сборе ПДн сотрудник отдела кадров, осуществляющий сбор (получение) ПДн непосредственно от сотрудников, а также граждан, претендующих на замещение вакантных должностей вУчреждении, обязан разъяснить указанным субъектам ПДн юридические последствия отказа предоставить их ПДн.
3.13. Форма разъяснения субъекту ПДн юридических последствий отказа представить свои ПДн в связи с поступлением на работу и ее выполнением в Учреждения утверждается приказом директора.
3.14. Передача (распространение, предоставление) и использование ПДн сотрудников, а также граждан, претендующих на замещение вакантных должностей в Учреждении, осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

## 4.Порядок обработки ПДн субъектов ПДн в ИСПДн

4.1. Обработка ПДн субъектов ПДн осуществляется в ИСПДн Учреждения (далее – АИС Учреждения), ИСПДн и ИСПДн.
4.2. АИС Учреждения содержит ПДн заявителей, предусмотренные настоящими Правилами, и предназначена для обеспечения деятельности Учреждения.

4.3. ИСПДн и ИСПДн содержат ПДн сотрудников Учреждения, предусмотренные настоящими Правилами, и предназначены для обеспечения кадровой и бухгалтерской деятельности в Учреждении.
4.4. Классификация ИСПДн Учреждения осуществляется в порядке, установленном законодательством Российской Федерации.
4.5. Сотрудниками Учреждения, имеющими право осуществлять обработку ПДн в ИСПДн, подписывается «Обязательство о неразглашении информации, содержащей персональные данные», по утвержденной форме.
4.6. Таким сотрудникам предоставляется уникальный логин и пароль для доступа к соответствующей ИСПДн. Доступ предоставляется к прикладным программным подсистемам в соответствии с функциями, предусмотренными должностными обязанностями сотрудников.
4.7. Информация с ПДн вносится в базы с ПДн и в другие места хранения информации в электронном виде в ручном режиме, при получении информации на бумажном носителе.
4.8. Обеспечение безопасности ПДн, обрабатываемых в ИСПДн, достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, а также принятия мер по обеспечению безопасности.

## 5.Сроки обработки и хранения ПДн

5.1. ПДн граждан, обратившихся в Учреждение лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, хранятся в Учреждении до достижения целей обработки.
5.2. Заявления и соответствующие документы настоящих Правил, предоставляемые заявителями на бумажном носителе в связи с организацией предоставления государственных и муниципальных услуг, хранятся на бумажных носителях до достижения целей обработки.
5.3. ПДн, содержащиеся в приказах по личному составу (о приеме, о переводе, об увольнении, об установлении надбавок о поощрениях и т.д.), подлежат хранению в отдел кадров в течение 75 лет.
5.4. Документы, содержащие ПДн сотрудников, в том числе сведения о заработной плате, подлежат хранению в бухгалтерии 75 лет.
5.5. ПДн при их обработке, осуществляемой без использования средств автоматизации, обособляются от иной информации, в частности путем фиксации их на разных материальных носителях ПДн, в специальных разделах или на полях форм (бланков).
5.6. В Учреждении обеспечивается раздельное хранение ПДн на разных материальных носителях, обработка которых осуществляется в различных целях, определенных настоящими Правилами.
5.7. Контроль хранения и использования материальных носителей ПДн, не допускающих несанкционированное использование, уточнение, распространение и уничтожение ПДн, находящихся на этих носителях, осуществляют руководители структурных подразделений, осуществляющих обработку ПДн субъектов ПДн.
5.8. Срок хранения ПДн, внесенных в ИСПДн, указанные в пунктах 4.1, 4.2 и 4.3 настоящих Правил, должен соответствовать сроку хранения бумажных оригиналов.
5.9. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом «О персональных данных».

## 6.Порядок уничтожения ПДн при достижении целей обработки или при наступлении иных законных оснований

6.1. Ответственным за организацию обработки персональных данных в Учреждении осуществляется систематический контроль и выделение документов, содержащих ПДн, с истекшими сроками хранения и подлежащих уничтожению.
6.2. Вопрос об уничтожении выделенных документов, содержащих ПДн, рассматривается на заседании комиссии, состав которой утверждается приказом директора.
6.3. По итогам заседания составляются протокол и акт о выделении к уничтожению документов, опись уничтожаемых дел; дела проверяются на их комплектность, акт подписывается председателем и членами комиссии и утверждается директором.
6.4. Уничтожение документов, содержащих ПДн, производится членами комиссии путем сжигания или аппаратного измельчения.
6.5. По окончании процедуры уничтожения Ответственным за организацию обработки персональных данных в Учреждении составляется соответствующий акт об уничтожении документов, содержащих ПДн.
6.6. Уничтожение ПДн на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление ПДн, или программным удалением необходимой информации принятыми для конкретного типа носителя методами.

## 7.Ответственные за организацию обработки ПДн

7.1. Директором Учреждения назначается ответственный за организацию обработки персональных данных, который курирует вопросы защиты информации в Учреждении. В полномочия Ответственного за организацию обработки персональных данных входит:
- принятие правовых, организационных и технических мер для обеспечения защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;
- организация внутренних проверок на предмет соблюдения сотрудниками требований законодательства Российской Федерации в области ПДн, в том числе требований к защите ПДн;
- инициирование разработки локальных актов по вопросам обработки ПДн, требований к защите ПДн;
- организация контроля приема и обработки обращений и запросов от субъектов ПДн;
- а случае нарушения в Учреждении требований к защите ПДн, принимать необходимые меры по восстановлению нарушенных прав субъектов ПДн.
7.2. Ответственный за организацию обработки ПДн, в соответствии с должностной инструкцией, вправе привлекать к реализации вышеуказанных мер по защите информации иных работников Учреждения с возложением на них соответствующих обязанностей и закреплением ответственности, а также вправе иметь доступ к информации, касающейся обработки ПДн и включающей:
- цели обработки ПДн;
- категории обрабатываемых ПДн;
- категории субъектов, ПДн которых обрабатываются;
- правовые основания обработки ПДн;
- перечень действий с ПДн, общее описание используемых в Учреждении способов обработки ПДн;
- описание мер, предусмотренных статьями 18.1 и 19 Федерального закона «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

- дату начала обработки ПДн;
- срок или условия прекращения обработки ПДн;
- сведения об обеспечении безопасности ПДн в соответствии с требованиями к защите ПДн, установленными Правительством Российской Федерации.

7.3. Непосредственное руководство работами, направленных на обеспечение защиты ПДн, а также контроль проводимых работ обеспечивает ответственный за обеспечение безопасности персональных данных информационных систем персональных данных Учреждения, которому могут быть делегированы полномочия, перечисленные в пункте 7.2.

7.4. Ответственного за обеспечение безопасности персональных данных информационных систем персональных данных Учреждения согласно должностной инструкции участвует в разработке внутренних нормативных документов по защите ПДн.

7.5. Администрация Учреждения, сотрудники администрации несут персональную ответственность за соблюдение установленного режима обработки ПДн субъектов ПДн.

7.6. Должностные лица, при проведении работ, связанных с обработкой ПДн, руководствуются законодательством Российской Федерации в области ПДн и настоящими Правилами.

7.7. Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки ПДн, а также требований к защите ПДн, установленных Федеральным законом «О персональных данных», подлежит возмещению в соответствии с законодательством Российской Федерации.

7.8. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом ПДн убытков.

Приложение №2
к приказу ГПОАУ АО «Амурский аграрный колледж»
от «_27_»_сентября 2019 г._ №__27092-од__

**ПРАВИЛА**
**рассмотрения запросов субъектов персональных данных или их представителей в ГПОАУ АО «Амурский аграрный колледж»**

1.Общие положения

1.1. Настоящие правила рассмотрения запросов субъектов персональных данных или их представителей (далее – Правила) в ГПОАУ АО «Амурский аграрный колледж» (далее – Учреждение), обработка персональных данных (далее – ПДн), которых необходима для предоставлении государственных услуг и для обеспечения кадровой и бухгалтерской деятельности в Учреждении, определяют порядок учета (регистрации) и рассмотрения запросов субъектов ПДн или их уполномоченных представителей (далее – запросы).

1.2. Настоящие Правила разработаны на основании Федерального закона РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федерального закона РФ от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», Федерального закона РФ от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» и в соответствии с частью 1 «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», утвержденных постановлением Правительства РФ от 21 марта 2012 г. № 211.

1.3. Субъектами ПДн (далее – субъекты) являются сотрудники Учреждения, обработка ПДн которых необходима для обеспечения кадровой и бухгалтерской деятельности в соответствии с Трудовым кодексом РФ, а также заявители – физические лица и уполномоченные представители физических или юридических лиц, обратившиеся в Учреждение с запросом о предоставлении государственных услуг,а также физические лица, обработка ПДн которых необходима для предоставления государственных услуг заявителям или их уполномоченным представителям.

1.4. Оператором ПДн (далее – оператор), организующим и осуществляющим обработку ПДн субъектов для предоставления государственных услуг заявителям или их уполномоченным представителям, а также для обеспечения кадровой и бухгалтерской деятельности, является специалист по защите ПД.

2.Права субъекта

2.1. Субъект имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

2.1.1 подтверждение факта обработки ПДн оператором;

2.1.2 правовые основания и цели обработки ПДн;

2.1.3 цели и применяемые оператором способы обработки ПДн;

2.1.4 наименование и место нахождения оператора, сведения о лицах (за исключением сотрудников оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании федерального закона;

2.1.5 обрабатываемые ПДн, относящиеся к соответствующему субъекту; источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

2.1.6 сроки обработки ПДн, в том числе сроки их хранения;

2.1.7 наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению директора Учреждения, если обработка поручена или будет поручена такому лицу.

2.2. Субъект вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений и ознакомления с такими ПДн не ранее чем через 30 (тридцать) 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.

2.3. Субъект имеет право требовать от оператора уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

## 3.Предоставление сведений субъекту

3.1. Сведения должны быть предоставлены субъекту оператором в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

3.2. Сведения, указанные в пункте 2.1 настоящих Правил, предоставляются субъекту или его уполномоченному представителю оператором при обращении, либо при получении запроса субъекта или его уполномоченного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта или его уполномоченного представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн оператором, подпись субъекта или его уполномоченного представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

3.3. Рассмотрение запросов является служебной обязанностью директора, заместителя директора и уполномоченных должностных лиц, в чьи обязанности входит обработка ПДн.

## 4.Права оператора

4.1. Оператор вправе отказать субъекту в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 2.2 и 3.2 настоящих Правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

4.2. Оператор в праве ограничить доступ субъекта к его ПДн в соответствии с федеральными законами, в том числе если:

4.2.1. обработка ПДн, включая ПДн, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

4.2.2.обработка ПДн осуществляется органами, осуществившими задержание субъекта по подозрению в совершении преступления, либо предъявившими субъекту обвинение по уголовному делу, либо применившими к субъекту меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным

законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими ПДн;

4.2.3. обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

4.2.4. доступ субъекта к его ПДн нарушает права и законные интересы третьих лиц;

4.2.5. обработка ПДн осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

## 5.Обязанности оператора

Обязанности оператора при обращении к нему субъекта, либо при получении запроса субъекта или его уполномоченного представителя, а также уполномоченного органа по защите прав субъектов ПДн.

5.1. Оператор обязан сообщить в порядке, предусмотренном статьей 14 Федерального закона РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных», субъекту или его уполномоченному представителю информацию о наличии ПДн, относящихся к соответствующему субъекту, а также предоставить возможность ознакомления с этими ПДн, при обращении субъекта или его уполномоченного представителя в течение 30 (тридцати) дней с даты получения запроса субъекта или его уполномоченного представителя.

5.2. В случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте, или отказа в предоставлении ПДн субъекту или его уполномоченному представителю, при их обращении, либо при получении запроса, оператор обязан дать мотивированный ответ в письменной форме, содержащий ссылку на положение части 8 статьи 14 Федерального закона РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 (тридцати) дней со дня обращения субъекта или его уполномоченного представителя, либо с даты получения запроса субъекта или его уполномоченного представителя.

5.3. Оператор обязан предоставить безвозмездно субъекту или его уполномоченному представителю возможность ознакомления с ПДн, относящимися к этому субъекту.

5.4. В срок, не превышающий 7 (семи) рабочих дней со дня предоставления субъектом или его уполномоченным представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения.

5.5. В срок, не превышающий 7 (семи) рабочих дней со дня представления субъектом или его уполномоченным представителем сведений, подтверждающих, что ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие ПДн.

5.6. Оператор обязан уведомить субъекта или его уполномоченного представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.

5.7. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию в течение 30 (тридцати) дней с даты получения такого запроса.

Приложение №3
к приказу ГПОАУ АО «Амурский аграрный колледж»
от «_27_»_сентября 2019 г._ №__27092-од__

**ПРАВИЛА**
**осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГПОАУ АО «Амурский аграрный колледж»**

1.Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) в ГПОАУ АО «Амурский аграрный колледж» (далее – Учреждение) определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее – ПДн), основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки ПДн, необходимой для предоставления государственных и муниципальных услуг, требованиям к защите ПДн.

1.2. Настоящие Правила разработаны на основании Федерального закона РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федерального закона РФ от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» и в соответствии с частью 1 «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», утвержденных постановлением Правительства РФ от 21 марта 2012 г. № 211.

1.3. Для обработки ПДн, необходимых для предоставления государственных услуг в Учреждении, используется информационная система персональных данных (далее – ИСПДн), предназначенная для осуществления деятельности Учреждения согласно законодательству РФ.

1.4. Для обработки ПДн сотрудников, необходимых для обеспечения кадровой и бухгалтерской деятельности в Учреждении в соответствии с Трудовым кодексом Российской Федерации, используется ИСПДн и ИСПДн.

1.5. Пользователем ИСПДн (далее – Пользователь) является сотрудник Учреждения, участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, ПО, данным и средствам защиты информации (далее – СЗИ) ИСПДн.

1.6. Контрольные мероприятия за обеспечением уровня защищенности персональных данных и соблюдений условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в ИСПДн Учреждения проводятся в следующих целях:

1.6.1. проверка выполнения требований организационно-распорядительной документации по защите информации в Учреждении и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

1.6.2. оценка уровня осведомленности и знаний работников Учреждения в области обработки и защиты персональных данных;

1.6.3. оценка обоснованности и эффективности применяемых мер и средств защиты.

2.Тематика внутреннего контроля

Тематика внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн:

2.1. Проверки соответствия обработки ПДн установленным требованиям в Учреждении разделяются на следующие виды:

регулярные;

плановые;

внеплановые.

2.2. Регулярные контрольные мероприятия проводятся Администратором АИС периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План, приложение 1) и предназначены для осуществления контроля выполнения требований в области защиты информации в Учреждении.

2.3. Плановые контрольные мероприятия проводятся постоянной комиссией периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План, приложение 1) и направлены на постоянное совершенствование системы защиты персональных данных ИСПДн Учреждения.

2.4. Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности (создается на период проведения мероприятий). Решение о проведении внеплановых контрольных мероприятий и созданию комиссии по информационной безопасности может быть принято в следующих случаях:

2.4.1. по результатам расследования инцидента информационной безопасности;

2.4.2. по результатам внешних контрольных мероприятий, проводимых регулирующими органами;

2.4.3. по решению директора Учреждения.

## 3.Планирование контрольных мероприятий

3.1. Для проведения плановых внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности персональных данных, разрабатывает План внутренних контрольных мероприятий на текущий год.

3.2. План проведения внутренних контрольных мероприятий включает следующие сведения по каждому из мероприятий:

3.2.1 цели проведения контрольных мероприятий;

3.2.2 задачи проведения контрольных мероприятий,

3.2.3 объекты контроля (процессы, подразделения, информационные системы и т.п.);

3.2.4 состав участников, привлекаемых для проведения контрольных мероприятий;

3.2.5 сроки и этапы проведения контрольных мероприятий.

3.3. Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Отчете, выполняемом по результатам проведенных контрольных мероприятий.

## 4.Оформление результатов контрольных мероприятий

4.1. По итогам проведения регулярных контрольных мероприятий результаты проверок фиксируется в Журнале учета событий информационной безопасности.

4.2. По итогам проведения плановых и внеплановых контрольных мероприятий лицо, комиссия, разрабатывает отчет, в котором указывается:

4.2.1 описание проведенных мероприятий по каждому из этапов;

4.2.2 перечень и описание выявленных нарушений;

4.2.3 рекомендации по устранению выявленных нарушений;

4.2.4 заключение по итогам проведения внутреннего контрольного мероприятия.

4.3. отчет передается на рассмотрение директору Учреждения.

4.4. Общая информации о проведенном контрольном мероприятий фиксируется в Журнале учета событий информационной безопасности.

4.5. Результаты проведения мероприятий по внеплановому контролю заносятся в протокол проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в Учреждении.

## 5.Порядок проведения плановых и внеплановых контрольных мероприятий

5.1. Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственному за обеспечение безопасности ПДн, также по его ходатайству к проведению контрольных мероприятий могут привлекаться администраторы АИС, и ответственный за обеспечение безопасности персональных данных информационных систем персональных данных Учреждения.

5.2. Лицо, ответственное за обеспечение безопасности ПДн, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех руководителей подразделений, в которых планируется проведение контрольных мероприятий, и направляет им для ознакомления План проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

5.3. Во время проведения контрольных мероприятий, в зависимости от целей мероприятий, могут выполнятся следующие проверки:

- соответствие полномочий Пользователя правилам доступа.
- Соблюдение Пользователями требований инструкций по организации антивирусной и парольной политики, инструкции по обеспечению безопасности ПДн.
- Соблюдение Администраторами инструкций и регламентов по обеспечению безопасности информации в Учреждении.
- Соблюдение Порядка доступа в помещения Учреждения, где ведется обработка персональных данных.
- Знание Пользователей положений Инструкции пользователя по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций.
- Знание Администраторами инструкций и регламентов по обеспечению безопасности информации в Учреждении.
- Порядок и условия применения средств защиты информации.
- Состояние учета машинных носителей персональных данных.
- Наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер.
- Проведенные мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
- Технические мероприятия, связанные с штатным и нештатным функционированием средств защиты.
- Технические мероприятия, связанные с штатным и нештатным функционированием подсистем системы защиты информации.

Приложение 1

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

# ПЛАН

внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных

| **Мероприятие** | **Периодичность регулярных мероприятий** | **Периодичность плановых мероприятий** | **Исполнитель** |
|---|---|---|---|
| Контроль соблюдения правил доступа к ПДн | Еженедельно | Ежемесячно | Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных |
| Контроль соблюдения режима защиты | Еженедельно | Ежемесячно | Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных |
| Контроль выполнения антивирусной политики | Еженедельно | Ежемесячно | Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных |
| Контроль выполнения парольной политики | Еженедельно | Ежемесячно | Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных |
| Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена | Еженедельно | Ежемесячно | Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных |
| Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн | | Ежемесячно | Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных |
| Контроль обновления ПО и единообразия применяемого ПО на всех элементах АИС СПО | Еженедельно | Ежемесячно | Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных |
| Контроль обеспечения резервного копирования | | Ежемесячно | Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных |
| Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз | | Ежегодно | Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных |
| Поддержание в актуальном состоянии нормативно-организационных документов | | Ежемесячно | Ответственный за организацию обработки ПДн в |
| Контроль запрета на использование беспроводных соединений | Еженедельно | Ежемесячно | |

Приложение

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

ОБРАЗЕЦ

**ПРОТОКОЛ № _____**

проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГПОАУ АмАК

Настоящий Протокол составлен в том, что «__»_____20__ г.

_____ (комиссией)

(должность, Ф.И.О. сотрудника)

проведена проверка _____

(тема проверки)

Проверка осуществлялась в соответствии с требованиями:

_____

(название документа)

_____

В ходе проверки проверено:

_____

_____

_____

_____

_____

_____

_____

Выявленные нарушения:

_____

_____

_____

_____

_____

_____

_____

Меры по устранению нарушений:

_____

_____

_____

_____

_____

_____

_____

_____

_____

Срок устранения нарушений: _____

Председатель комиссии:

*фамилия и инициалы / подпись / должность*

Члены комиссии:

*фамилия и инициалы / подпись / должность*
*фамилия и инициалы / подпись / должность*

Приложение №4
к приказу ГПОАУ АО «Амурский аграрный колледж»
от «_27_»_сентября 2019 г._ №__27092-од__

# Порядок доступа сотрудников в помещения, в которых ведется обработка ПД

## 1.Общие положения

1.1. Настоящие порядок доступа (далее – Порядок) сотрудников ГПОАУ АО «Амурский аграрный колледж» (далее – Учреждения) в помещения, в которых ведется обработка персональных данных (далее – ПДн) в информационных системах персональных данных (далее – ИСПДн),устанавливает единые требования к доступу сотрудников Учреждения в служебные помещения в целях предотвращения нарушения прав субъектов ПДн, обработка ПДн которых необходима для оказания государственных услуг и обеспечения кадровой и бухгалтерской деятельности в Учреждении, а также в целях обеспечения соблюдения требований законодательства РФ в области ПДн.

1.2. Настоящий Порядок разработан в соответствии с частью 1 «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», утвержденных постановлением Правительства РФ от 21 марта 2012 г. № 211, и на основании «Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденных приказом ФСТЭК России от 11 февраля 2013г. № 17, и «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных ФСБ России 21 февраля 2008 г. № 149/6/6-622.

1.3. Контролируемая зона (далее – контролируемая зона) – пространство (территория, здание, часть здания, помещение), в котором расположены средства автоматизации и защиты ИСПДн, в том числе автоматизированные рабочие места (далее – АРМ), на которых ведется обработка ПДн.

1.4. Перечень помещений, в которых ведется обработка ПДн, и их границы устанавливаются приказом Учреждения «Об определении границ контролируемой зоны и требований к ее безопасности».

1.5. Настоящий Порядок обязателен для применения и исполнения всеми сотрудниками Учреждения.

1.6. Ответственность за соблюдение положений настоящего Порядка несут сотрудники структурных подразделений Учреждения, обрабатывающие ПДн, а также руководители данных структурных подразделений.

1.7. Контроль соблюдения требований настоящего Порядка обеспечивает ответственный за организацию обработки ПДн в Учреждении.

## 2.Требования к помещениям контролируемой зоны

2.1. Бесконтрольный доступ сторонних лиц в помещения контролируемой зоны должен быть исключён.

2.2. Все помещения контролируемой зоны должны быть оборудованы охранной сигнализацией, либо предусматривать круглосуточное дежурство.

2.3. Ограждающие конструкции помещений контролируемой зоны должны предполагать существенные трудности для нарушителя по их преодолению.
2.4. К помещениям контролируемой зоны, в которых установлены криптографические средства защиты ПДн (далее – криптосредства) или хранятся ключевые документы к ним, (далее – режимные помещения), предъявляются ужесточённые требования по безопасности, указанные в разделе 5 настоящих Правил.

## 3.Доступ в помещения контролируемой зоны

3.1. Доступ посторонних лиц в помещения контролируемой зоны должен осуществляется только ввиду служебной необходимости.
3.2. На момент присутствия посторонних лиц в помещении контролируемой зоны, должны быть приняты меры по недопущению ознакомления посторонних лиц с ПДн (например: мониторы повёрнуты в сторону от посетителей, документы убраны в стол, либо находятся в непрозрачной папке или накрыты чистыми листами бумаги).
3.3. Допуск сотрудников в помещения контролируемой зоны оформляется после подписания сотрудником Обязательства о неразглашении информации, содержащей персональные данные, и инструктажа ответственным за организацию обработки ПДн в Учреждении, либо ответственным за обеспечение безопасности персональных данных информационных систем персональных данных Учреждения.
3.4. В нерабочее время помещения контролируемой зоны должны ставиться на охрану. При этом все окна и двери в смежные помещения должны быть надёжно закрыты, материальные носители ПДн должны быть убраны в запираемые шкафы (сейфы), АРМ выключены или заблокированы.

## 4.Доступ в серверные помещения контролируемой зоны

4.1. Доступ в серверные помещения контролируемой зоны разрешён только администратору ИСПДн, ответственному за обеспечение безопасности персональных данных информационных систем персональных данных Учреждения и ответственному за организацию обработки ПДн в Учреждении.
4.2. Уборка серверных помещений происходит только при строгом контроле лиц, указанных в пункте 4.1 настоящих Правил
4.3. Серверные помещения контролируемой зоны в обязательном порядке оснащается охранной сигнализацией, системой видеонаблюдения и системой автономного питания средств охраны.
4.4. Доступ в серверные помещения контролируемой зоны посторонних лиц допускается строго по согласованию с ответственным за организацию обработки ПДн в Учреждении.
4.5. Нахождение в серверных помещениях контролируемой зоны посторонних лиц без сопровождающего не допустимо.

## 5.Требования к режимным помещениям

5.1. Режимные помещения выделяют с учётом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к криптосредствам. Помещения должны иметь прочные входные двери с замками, гарантирующими надёжное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, необходимо оборудовать металлическими решётками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

5.2. Размещение, специальное оборудование, охрана и организация режима в режимных помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

5.3. Для предотвращения просмотра извне режимных помещений их окна должны быть защищены.

5.4. Режимные помещения должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации. Исправность сигнализации периодически необходимо проверять ответственному за организацию обработки ПДн в совместно с представителем службы охраны или дежурным по организации с отметкой в соответствующих журналах.

5.5. Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих криптосредства носителей должно быть предусмотрено необходимое число надёжных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у ответственного за организацию обработки ПДн в Учреждении.

5.6. По окончании рабочего дня режимное помещение и установленные в нем хранилища должны быть закрыты, хранилища опечатаны.

5.7. Ключи от режимных помещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ режимного помещения, в опечатанном виде должны быть сданы под расписку в соответствующем журнале службы охраны или дежурному по организации одновременно с передачей под охрану самих режимных помещений. Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей криптосредств, ответственных за эти хранилища.

5.8. При утрате ключа от хранилища или от входной двери в режимное помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает ответственный за организацию обработки ПДн в Учреждении.

5.9. В обычных условиях режимные помещения, находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями криптосредств или ответственным за организацию обработки ПДн в Учреждении. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному за организацию обработки ПДн в Учреждении. Прибывший ответственный за организацию обработки ПДн в Учреждении должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации персональных данных и к замене скомпрометированных криптоключей.

5.10. Размещение и монтаж криптосредств, а также другого оборудования, функционирующего с криптосредствами, в режимных помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

5.11. На время отсутствия пользователей криптосредств указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с ответственным за организацию обработки ПДн в Учреждении необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

Приложение №5
к приказу ГПОАУ АО «Амурский аграрный колледж»
от «_27_»_сентября 2019 г._ №__27092-од__

# Положение о разрешительной системе допуска к ресурсам информационной системы персональных данных

## 1. Общие положения

1.1. Настоящее Положение разработано на основании:
Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
1.2. Настоящее Положение устанавливает порядок предоставления допуска к ресурсам информационной системы персональных данных ГПОАУ АО «Амурский аграрный колледж» (далее – информационная система, Учреждение).
1.3. К персональным данным относятся:
- анкетные и биографические данные гражданина, включая адрес места жительства;
- паспортные данные или данные иного документа, удостоверяющего личность и гражданство, включая серию, номер, дату выдачи, наименование органа, выдавшего документ);
- сведения об образовании, квалификации, наличии специальных знаний или специальной подготовки;
- сведения о трудовой деятельности, опыте работы, занимаемой должности, трудовом стаже, повышении квалификации и переподготовки;
- сведения о составе семьи, а также сведения о месте работы или учёбы членов семьи;
- сведения о состоянии здоровья и наличии заболеваний;
- сведения об отношении к воинской обязанности;
- сведения о доходах и обязательствах имущественного характера, в том числе членов семьи;
- сведения об идентификационном номере налогоплательщика;
- реквизиты расчетных счетов в банках;
- сведения о социальных льготах и о социальном статусе гражданина и членов его семьи;
- сведения о решениях судебных органов, органов опеки в отношении гражданина и членов его семьи.

1.4. Пользователями являются сотрудники Учреждения, в силу своих функциональных обязанностей участвующие в процессах обработки персональных данных.
1.5. Методическое руководство работой пользователя осуществляется ответственными лицами, назначенными распоряжения директора Учреждения и в соответствии с установленным порядком.
1.6. Пользователь взаимодействует с ответственными за эксплуатацию информационной системы/ответственными за организацию обработки персональных данных по вопросам обеспечения защиты персональных данных и подчиняется их распоряжениям (далее –

ответственные лица), назначаемыми распоряжением руководителя образовательной организации.
1.7. Перед началом работы пользователи и ответственные лица обязаны изучить настоящее Положение и ознакомиться с ответственностью за выполнение требований Положения под роспись.
1.8. В своей деятельности пользователи и ответственные лица руководствуются настоящим Положением и действующим законодательством в сфере защиты персональных данных.
1.9. Пользователи и ответственные лица несут персональную ответственность за выполнение настоящего Положения в установленном законом порядке.

## 2. Предоставление прав доступа

2.1. Пользователи допускаются к работе с персональными данными на основании приказа директора Учреждения и в соответствии с утвержденным списком лиц, допущенных к работе с персональными данными.
2.2. Состав персональных данных, права при обработке персональных данных (чтение, запись, удаление и т.д.), доступ к которым предоставляется пользователю для выполнения служебных обязанностей, определяются ответственным лицом.
2.3. Необходимость доступа пользователя к персональным данным, состав персональных данных, необходимые права по обработке персональных данных, срок, на который предоставляется доступ, обосновываются ответственным лицом в служебной записке на имя руководителя образовательной организации/руководителя структурного подразделения образовательной организации.
2.4. По распоряжению директора Учреждения/руководителя структурного подразделения образовательной организации ответственное лицо производит необходимые действия по созданию учетной записи пользователя, присвоению ему пароля и заявленных прав доступа к информационной системе, включению его в соответствующие группы пользователей и другие необходимые действия.
2.5. Учетная запись пользователя (уникальное имя), под которым он регистрируется и осуществляет работу в информационной системе, присваивается для обеспечения персональной ответственности пользователя за свои действия.
2.6. В случае производственной необходимости пользователю могут быть сопоставлены несколько учетных записей (уникальных имен).
2.7. Использование несколькими пользователями одной учетной записи запрещается.
2.8. При изменении должностных обязанностей пользователя, связанных с переводом в другое подразделение, переводом на другую должность и т.п., учетная запись подлежит изменению (корректировке), при этом прежние права доступа аннулируются.
2.9. Настройку аппаратно-программного обеспечения рабочего места пользователя выполняют технические специалисты под контролем ответственного лица.

## 3. Порядок изменения, прекращения/приостановления доступа

3.1. Прекращение/приостановление прав доступа пользователя к информационной системе осуществляется на основании служебной записки от ответственного лица на имя директора Учреждения/ руководителя структурного подразделения образовательной организации.
3.2. В случае длительного отсутствия пользователя (по причине отпуска, заболевания, командировки и пр.) ответственное лицо приостанавливает права доступа до фактического возвращения пользователя к исполнению обязанностей.
3.3. При увольнении, изменении должностных обязанностей, переводе в другое подразделение, переводе на другую должность права доступа пользователя аннулируются.
3.4. В случае нарушения пользователем требований по обеспечению безопасности персональных данных и/или правил работы в информационной системе, права доступа

пользователя временно приостанавливаются. Решение о восстановлении или полном прекращении прав доступа принимается в установленном порядке.
3.5. Порядок изменения прав доступа пользователя в сторону их расширения аналогичен порядку их предоставления.
3.6. Порядок изменения прав доступа пользователя в сторону их уменьшения аналогичен порядку их прекращения.
3.7. При удалении учетных записей пользователей/изменении прав доступа ответственное лицо обязано:

- провести смену (удаление) действующих настроек прав доступа на соответствующих средствах защиты информационной системы в соответствии с изменением/прекращением полномочий;
- внести необходимые записи/отметки в соответствующие документы/списки/реестры/матрицы;
- проанализировать целостность персональных данных и состояние программно-аппаратных средств, к которым имел доступ пользователь.

3.8. При удалении учетных записей пользователей/изменении прав доступа удаление или сохранение содержимого почтового ящика, личных локальных и сетевых папок осуществляется в установленном порядке.

## 4. Контроль функционирования разрешительной системы допуска к информационной системе

4.1. Контроль функционирования разрешительной системы допуска к информационной системе проводится в установленном порядке.
4.2. Контроль функционирования разрешительной системы допуска к информационной системе осуществляется ответственными лицами по распоряжению руководителя образовательной организации/ руководителя структурного подразделения образовательной организации.
4.3. Проверка прав доступа пользователей проводится ответственным лицом не реже одного раза в три месяца.

## 5. Ответственность

Пользователи и ответственные лица несут ответственность за:
5.1. Неисполнение или ненадлежащее исполнение своих должностных обязанностей, предусмотренных настоящим Положением, – в пределах, определенных действующим трудовым законодательством Российской Федерации;
5.2. Причинение материального ущерба работодателю – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации;
5.3. Правонарушения, совершенные в процессе осуществления своей деятельности, – в пределах, определенных действующим административным, уголовным, гражданским законодательством Российской Федерации.
5.4. Качество проводимых работ по обеспечению безопасности персональных данных.
5.5. Обеспечение устойчивой работоспособности информационной системы.

Приложение №6
к приказу ГПОАУ АО «Амурский аграрный колледж»
от «_27_»_сентября 2019 г._ №__27092-од__

# Положение о неавтоматизированной обработке персональных данных в ГПОАУ АО «Амурский аграрный колледж»

## 1. Общие положения

1.1. Настоящее Положение разработано на основании:
Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
постановления Правительства Российской Федерации от 15.09.2008№ 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.2. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее – информационная система, персональные данные), 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.

1.3. 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.

1.4. Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации, должны применяться с учетом требований настоящего Положения.

1.5. Настоящее Положение определяет правила неавтоматизированной обработки персональных данных, обязательные для исполнения сотрудниками образовательной организации, в силу своих функциональных обязанностей участвующими (далее – пользователи).

1.6. Допуск пользователей к работе с информационной системой осуществляется на основании приказа директора ГПОАУ АО «Амурский аграрный колледж» (далее – Учреждение) и в соответствии со списком лиц,

допущенных к работе с персональными данными и сведениями конфиденциального характера.

1.7. Методическое руководство работой пользователей осуществляют ответственные лица, назначенные приказом директора Учреждения в соответствии с локальными нормативными актами.

1.8. Требования настоящего Положения обязательны для исполнения всеми пользователями/ответственными лицами и доводятся под роспись.

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

2.1. 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).

2.2. 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.

2.3. 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, 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 способов обработки персональных данных, данные о пользователе;

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 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.

2.4. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в помещение, где проводится обработка персональных данных, должны соблюдаться следующие условия:

необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена локальным актом образовательной организации, 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, где проводится обработка персональных данных, 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, где проводится обработка персональных данных.

2.5. 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 и 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.

2.6. 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).

2.7. Правила, предусмотренные пунктами 2.6 и 2.7. настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

2.8. 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

3.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна проводиться 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.

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

3.3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются локальными нормативными актами образовательной организации.

## 4. Ответственность

Пользователи и ответственные лица несут ответственность за:

4.1. Неисполнение или ненадлежащее исполнение своих должностных обязанностей, предусмотренных настоящим Положением, – в пределах, определенных действующим трудовым законодательством Российской Федерации;

4.2. Причинение материального ущерба работодателю – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации;

4.3. Правонарушения, совершенные в процессе осуществления своей деятельности, – в пределах, определенных действующим административным, уголовным, гражданским законодательством Российской Федерации.

Приложение №7
к приказу ГПОАУ АО «Амурский аграрный колледж»
от «_27_»_сентября 2019 г._ №__27092-од__

# СВЕДЕНИЯ О РЕАЛИЗУЕМЫХ МЕРАХ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. ГПОАУ АО «Амурский аграрный колледж» (далее – Учреждение) обеспечивает конфиденциальность полученных ПДн путем применения организационных и технических мер для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн. Учреждение обеспечивает, чтобы все реализуемые мероприятия по организационной и технической защите ПДн осуществлялись на законных основаниях, в том числе в соответствии с требованиями законодательства Российской Федерации по вопросам обработки ПДн.

2. Работники Учреждения не раскрывают третьим лицам и не распространяют ПДн субъекта без его согласия, если иное не предусмотрено законодательством Российской Федерации.

3. Все работники Учреждения обеспечивают конфиденциальность ПДн, а также иных сведений, установленных Учреждением, если это не противоречит действующему законодательству Российской Федерации.

4. Применяемые организационные и технические меры по защите ПДн:

– назначение ответственных за организацию обработки ПДн и обеспечение безопасности ПДн;

– издание локальных нормативных актов по вопросам обработки и защиты ПДн, направленных на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

– определение перечня должностей, при замещении которых осуществляется обработка ПДн;

– организация обучения, оказание методической помощи, ознакомление под подпись работников, осуществляющих обработку ПДн, с фактом участия в обработке ПДн, а также с правилами обработки и защиты ПДн;

– обеспечение регистрации и учета совершаемых с ПДн действий;

– ведение учета исполнения обращений субъектов ПДн;

– передача ПДн внутри Учреждения только между лицами, занимающими должности, включенные в перечень должностей, при замещении которых осуществляется обработка ПДн;

– размещение обработки ПДн в границах охраняемой территории, а также организацией физической защиты носителей ПДн, мест и средств их обработки;

– организация доступа в помещения, используемые для обработки ПДн и/или хранения их материальных носителей;

– определение УБПДн, разработка, при необходимости, СЗПДн при обработке ПДн в ИСПДн и установлением правил доступа к ПДн;

– составление типовых форм для сбора ПДн таким образом, чтобы каждый из субъектов ПДн имел возможность ознакомиться со своими ПДн, не нарушая прав и законных интересов иных субъектов ПДн;

– внесение в типовые формы, предусматривающие указание в них ПДн, полей, в которых субъект ПДн имел бы возможность проставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации (при необходимости получения письменного согласия на обработку ПДн);

– применение организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;

– применение прошедших в установленном порядке процедуру оценки соответствия СЗИ;

– оценку эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;

– учет машинных носителей ПДн и контроль за их обращением в целях исключения утраты, хищения, подмены, несанкционированного копирования или уничтожения;

– обнаружение фактов НСД к ПДн и принятие мер;

– восстановление ПДн, модифицированных или уничтоженных вследствие НСД к ним;

– проведение мероприятий, направленных на предотвращение НСД к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;

– своевременное обнаружение фактов НСД к ПДн и принятие необходимых мер;

– недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

– установление правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;

– контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

5. В состав мер по обеспечению безопасности ПДн, реализуемых Учреждением в рамках системы защиты ПДн с учетом актуальных УБПДн и применяемых информационных технологий, входят:

– идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ);

– управление доступом субъектов доступа к объектам доступа (УПД);

– ограничение программной среды (ОПС);

– защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (ЗНИ);

– регистрация событий безопасности (РСБ);

– антивирусная защита (АВЗ);

– контроль (анализ) защищенности персональных данных (АНЗ);

– обеспечение целостности информационной системы и персональных данных (ОЦЛ);

– обеспечение доступности персональных данных (ОДТ);

– защита среды виртуализации (ЗСВ);

– защита технических средств (ЗТС);

– защита информационной системы, ее средств, систем связи и передачи данных (ЗИС);

– выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них (ИНЦ);

– управление конфигурацией информационной системы и системы защиты персональных данных (УКФ).

6. В целях обеспечения соответствия уровня защиты ПДн требованиям законодательства Российской Федерации Учреждение не раскрывает информацию о конкретных применяемых средствах и мерах обеспечения ИБ ПДн.

7. Учреждение обязуется не разглашать полученную от субъектов ПДн информацию. Не считается нарушением предоставление Учреждением информации агентам и третьим лицам, действующим на основании договора с Учреждением, для исполнения обязательств перед субъектом ПДн. Не считается нарушением обязательств разглашение информации в

соответствии с обоснованными и применимыми требованиями законодательства Российской Федерации.