

**Государственное бюджетное учреждение дополнительного
профессионального образования Республики Адыгея
«Адыгейский республиканский институт повышения квалификации»**

П Р И К А З
28.12.2024 г. № 146 - од
г. Майкоп

О персональных данных

В связи с кадровыми изменениями и переименованием структурных подразделений в Государственном бюджетном учреждении дополнительного профессионального образования Республики Адыгея «Адыгейский республиканский институт повышения квалификации»

ПРИКАЗЫВАЮ:

1. Изложить приказ, а также приложения к нему в новой редакции.

2. Назначить ответственными за организацию обработки персональных данных в Государственном бюджетном учреждении дополнительного профессионального образования Республики Адыгея «Адыгейский республиканский институт повышения квалификации» (далее – ГБУ ДПО РА «АРИПК»):

- Праток С.М., начальника отдела документального и кадрового обеспечения (обработка персональных данных сотрудников ГБУ ДПО РА «АРИПК»);

- Нагоеву Д.У., заместителя директора (обработка персональных данных в ФИС ФРДО, Постановление Правительства РФ от 26.08.2013г. № 729 «О федеральной системе «Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об образовании»);

- Хариеву Д.С., заместителя директора (обработка персональных данных лиц, привлекаемых к проведению конкурсов, конференций, семинаров, круглых столов и т.п.);

- Индрисову Р.А., начальника ОПиОУД (обработка персональных данных слушателей КПК и ИП).

1.1. Утвердить Инструкцию ответственных лиц за обработку персональных данных в АРИПК (приложение № 1).

1.2. Возложить на ответственных за организацию обработки персональных данных в ГБУ ДПО РА «АРИПК» следующие обязанности:

- предоставление на утверждение списков, доступ которых к персональным данным, обрабатываемым в ГБУ ДПО РА «АРИПК» необходим для выполнения служебных (трудовых) обязанностей, а также изменений к нему;

- осуществление внутреннего контроля за соблюдением работниками АРИПК законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

- доведение до сведения работников (оператора) положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

- организация приема и обработка обращений субъектов персональных данных или их представителей и осуществление контроля за приемом и обработкой таких обращений.

2. Утвердить список сотрудников ГБУ ДПО РА «АРИПК», доступ которых к персональным данным необходим для выполнения служебных обязанностей.

2.1. Разрешить внутренний доступ ко всем персональным данным следующим сотрудникам:

- Тхаговой Ф.Р.	- Кайтмесовой Н.Х.	- Варельджан К.С.	Левченко С.В.
- Нагоевой Д.У.	- Нагороковой З.А.	- Индрисовой Р.А.	Сергеевой Т.В.
- Шоровой Ж.К.	- Нинуху Н.С.	- Кемечевой Э.Н.	Борокову Т.Н.

- | | | | |
|-------------------|--------------------|--------------------|---------------------|
| - Хариевой Д.С. | - Шефруковой З. А. | -Сухомлиновой Т.А. | - Джаримовой Р.Н. |
| - Праток С.М. | - Кесебежевой Л.А. | Берестовой Л.Ю. | - Клепальченко О.В. |
| - Максименко У.В. | - Тумовой С.Н. | Казакову О.А. | - Филлипову А.В. |
| | - Леоновой М.Н. | | |

2.2. Разрешить внутренний доступ к сведениям о слушателях следующим сотрудникам:

- | | | | | |
|-------------------|--------------------|-------------------|-------------------|--------------------|
| - Тхаговой Ф.Р. | -Клепальченко О.В. | - Кардановой Ф.Г. | - Хатляковой С.К. | -Варельджан К.С. |
| - Нагоевой Д.У. | -Кайтмесовой Н.Х. | - Мамий Р.Х. | - Хатхоху С.Х. | Сергеевой Т.В. |
| - Шоровой Ж.К. | - Нинуху Н.С. | - Сет Ж.К. | - Яхутль Н.Ш. | -Кемечевой Э.Н. |
| - Хариевой Д.С. | -Шефруковой З. А. | - Ситимовой А.Х. | Нагорокова З.А. | -Сухомлиновой Т.А. |
| - Праток С.М. | - Апазаовой М. Н. | - Татлок М.С. | Винограденко П.В. | Берестовой Л.Ю. |
| - Индрисовой Р.А. | - Булгакову С.Ю. | - Тлюповой З.Х. | Шарова Е.И. | Казакову О.А. |
| - Джаримовой Р.Н. | - Говоровой Т.В. | - Стаценко И.А. | - Леоновой М.Н. | Левченко С.В. |
| - Максименко У.В. | - Дышековой А.А. | - Тумовой С.Н. | - Филлипову А.В. | Борокову Т.Н. |

2.3. Разрешить внутренний доступ к сведениям о служебном положении, составе семьи работников, а также к сведениям, имеющим отношение к начислению заработной платы, налогов и иных обязательных платежей сотрудников, бухгалтеру Магдалевич С.В.

2.4. Допустить указанных сотрудников к обработке персональных данных.

3. Утвердить Регламент допуска работников к обработке персональных данных (приложение № 2).

4. Утвердить Порядок доступа работников ГБУ ДПО РА «АРИПК» в помещения, в которых ведется обработка персональных данных (приложение № 3).

5. Утвердить Политику обработки персональных данных и реализуемых требований к защите персональных данных для слушателей и работников ГБУ ДПО РА «АРИПК» (приложение № 4).

6. Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУ ДПО «АРИПК» (приложение № 5).

7. Утвердить:

7.1. Положение об организации и проведении работ в ГБУ ДПО РА «АРИПК» по обеспечению безопасности персональных данных при их обработке (приложение № 6).

7.2. Типовые формы журналов:

7.2. Типовые формы журналов:

- учета установленных средств защиты информации (приложение № 7);
- журнала учета машинных носителей (приложение № 8);
- журнала периодического тестирования средств защиты (приложение № 9);
- журнала учета нештатных ситуаций информационных систем персональных данных (далее-ИСПДн), выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн (приложение № 10);
- журнала учета пользователей, допущенных к информационным системам персональных данных (приложение № 11);
- журнала проверок электронных журналов (приложение № 12);
- журнала учета обращений субъектов персональных данных (далее-ПДн) о выполнении их законных прав (приложение № 13);
- журнала учета хранилищ (приложение № 14).

7.3. Ответственным за организацию обработки персональных данных в ГБУ ДПО РА «АРИПК» завести журналы согласно типовым формам.

8. Утвердить список помещений, предназначенных для обработки персональных данных без использования средств автоматизации, (приложение № 15) к настоящему приказу.

8.1. Руководителям структурных подразделений:

- разместить списки лиц, имеющих право самостоятельного доступа в указанные помещения на дверях помещений, предназначенных для обработки персональных данных без использования средств автоматизации с внутренней стороны;

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

- запретить нахождение в указанных помещениях посторонних лиц без сопровождения лиц, имеющих право самостоятельного доступа;

- в нерабочее время указанные помещения должны закрываться на ключ и сдаваться под охрану;

- возложить ответственность за соблюдение режима доступа в защищаемые помещения на лиц, постоянно работающих в помещениях, и руководителей структурных подразделений;

- возложить на ответственных за организацию обработки персональных данных в ГБУ ДПО РА «АРИПК» контроль за списками лиц, допущенных для работы в защищаемых помещениях.

9. Утвердить Правила рассмотрения запросов субъектов ПДн в ГБУ ДПО РА «АРИПК» (приложение №17).

10. Границами контролируемой зоны ГБУ ДПО РА «АРИПК» считать периметр ограждающих конструкций главного здания учреждения по адресу ул. Ленина 15.

10.1. Утвердить порядок доступа работников в помещения АРИПК, в которых ведется обработка персональных данных (приложение № 11).

11. Утвердить Положение о порядке уничтожения персональных данных в ГБУ ДПО РА «АРИПК» (приложение №18).

12. Утвердить в ГБУ ДПО РА «АРИПК» состав Комиссии по уничтожению персональных данных в составе:

Председатель комиссии - Нагоева Джаншир Умаровна, заместитель директора по УРиОКО.

Члены комиссии:

- Праток Саняйт Мадиновна, начальник отдела документального и кадрового обеспечения;

- Индрисова Роза Азметовна, начальник ОПиОУД;

- Нагорокова Залина Ауэсовна, заведующий кафедрой;

- Говорова Татьяна Владимировна, архивариус.

13. Утвердить форму акта уничтожения персональных данных (далее – Акт) (приложение №19).

13.1. Комиссии по уничтожению персональных данных производить уничтожение персональных данных и носителей персональных данных в ГБУ ДПО «АРИПК» по мере возникновения необходимости. Действия по уничтожению персональных данных оформлять актом уничтожения по форме. Акты уничтожения персональных данных, оформленные и подписанные членами комиссии хранить в отдельно выделенном деле.

14. Утвердить форму согласия на обработку персональных данных слушателей (Приложение 20).

15. Форма согласия на обработку персональных данных работников АРИПК (Приложение 21).

16. Контроль за выполнением настоящего приказа оставляю за собой.

Директор



Ф.Р. Тхагова

ИНСТРУКЦИЯ

ответственного за организацию обработки персональных данных в АРИПК

I. Общие положения

1.1. Настоящая должностная инструкция определяет права, ответственность и обязанности ответственного (далее - Ответственный) за организацию обработки персональных данных (далее - ПДн) в АРИПК.

1.2. Методическое руководство и контроль работы должностных лиц в АРИПК осуществляет ответственный за организацию обработки персональных данных.

II. Обязанности ответственного за организацию обработки персональных данных

2.1. Должностное лицо, ответственное за организацию обработки ПДн в АРИПК обязано:

- знать и выполнять требования действующего законодательства РФ, а также внутренних инструкций и положений, регламентирующих деятельность по обработке и защите ПДн;
- документы, определяющие политику Оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;
- отслеживать изменения действующего законодательства РФ по вопросам защиты и обработки ПДн;
- участвовать в проведении служебных расследований по фактам нарушения функционирования информационной системы персональных данных, а также других случаев нарушения правил обработки и защиты ПДн в соответствующем структурном подразделении;
- организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов;
- организовать ведение журнала учета обращений субъектов ПДн;
- методы применения правовых, организационных и технических мер по обеспечению безопасности персональных данных;
- организовать инструктаж должностных лиц, уполномоченных на обработку персональных данных.

III. Права ответственного за организацию обработки персональных данных

3.1. Должностное лицо, ответственное за организацию обработки ПДн в АРИПК имеет право:

- требовать от должностных лиц, уполномоченных на обработку персональных данных, безусловного соблюдения установленных правил обработки и защиты ПДн;
- требовать от должностных лиц, уполномоченных на обработку персональных данных прекращения обработки ПДн, в случаях их неправомерного использования и нарушения установленного порядка обработки;
- доступа во все помещения соответствующего структурного подразделения, где осуществляется обработка ПДн.

IV. Ответственность

4.1. Должностное лицо, ответственное за организацию обработки ПДн в АРИПК несет

ответственность:

- за качество и полноту проводимых им работ по организации обработки ПДн в соответствии с функциональными обязанностями, определенными настоящей Инструкцией;
- за сохранность сведений ограниченного распространения в соответствии с требованиями законодательства в области защиты ПДн.

РЕГЛАМЕНТ

допуска работников к обработке персональных данных

1. Общие положения

1.1. Регламент допуска работников к обработке персональных данных других работников ГБУ ДПО РА «Адыгейский республиканский институт повышения квалификации» (далее - ГБУ ДПО РА «АРИПК») разработан в соответствии с Трудовым кодексом, Федеральным законом от 27.07.2006 г. № 152-ФЗ и иными нормативно - правовыми актами, действующими на территории РФ.

1.2. Настоящий Регламент определяет порядок допуска работников к обработке персональных данных других работников и гарантии конфиденциальности сведений о работнике, предоставленных работником работодателю.

1.3. Цель настоящего Регламента – защита персональных данных работников и слушателей ГБУ ДПО РА «АРИПК» от несанкционированного доступа и разглашения. Персональные данные работников являются конфиденциальной, строго охраняемой информацией.

1.4. Настоящий Регламент вступает в силу с «28» декабря 2024 года.

2 Виды допуска к обработке персональных данных работников

2.1. Допуск работников к обработке персональных данных других работников подразделяется на полный и частичный.

2.2. Полный допуск к обработке персональных данных работников имеют директор ГБУ ДПО РА «АРИПК», его заместитель, главный бухгалтер, а также работники отдела кадров.

2.3. Частичный допуск к обработке персональных данных работников имеют:

- работники ГБУ ДПО РА «АРИПК», допущенные к обработке тех данных, которые необходимы для выполнения их непосредственных должностных обязанностей.

2.4. Лицам, не указанным в п. 2.3 настоящего Регламента, частичный допуск к обработке персональных данных других работников может быть предоставлен на основании письменного разрешения директора ГБУ ДПО РА «АРИПК» или его заместителя.

3. Порядок допуска работников к обработке персональных данных

3.1. Лица, указанные в п. 2.2, 2.3 настоящего Регламента, допускаются к обработке персональных данных других работников с соблюдением общей процедуры оформления работы с персональными данными, предусмотренной действующим законодательством и локальными актами ГБУ ДПО РА «АРИПК», без дополнительного оформления.

3.2. Лица, указанные в п. 2.4 настоящего Регламента, заинтересованные в частичном допуске к обработке персональных данных других работников, направляют директору ГБУ ДПО РА «АРИПК» или его заместителю мотивированное ходатайство, в котором излагают:

-цель допуска к обработке персональных данных других работников;

-перечень персональных данных, допуск к обработке которых необходим;

-обоснование необходимости и целесообразности допуска к обработке персональных данных других работников.

3.3. Ходатайство подлежит рассмотрению в течение трех рабочих дней. По

Результатам рассмотрения ходатайства директор ГБУ ДПО РА «АРИПК» или его заместитель издает распоряжение о допуске работника к обработке персональных данных других работников либо принимает решение об отказе в допуске с указанием причин отказа.

4. Порядок прекращения допуска работников к обработке персональных данных

4.1. Допуск к обработке персональных данных работников прекращается:

- при увольнении работника, имеющего допуск;
- при переводе работника, имеющего допуск, на должность, выполнение работ по которой уже не требует допуска к обработке персональных данных.

4.2. Допуск к обработке персональных данных у лиц, указанных в п. 2.4 настоящего Регламента, может быть дополнительно прекращен по письменному решению директора ГБУ ДПО РА «АРИПК» или его заместителя.

5. Заключительные положения

5.1. В случае изменения действующего законодательства РФ, внесения изменений в нормативные документы по защите персональных данных настоящий Регламент действует в части, не противоречащей действующему законодательству до приведения в соответствие.

ПОРЯДОК
доступа работников ГБУ ДПО РА «АРИПК» в помещения, в
которых ведется обработка персональных данных

1. Настоящий Порядок доступа работников в помещения АРИПК, в которых ведется обработка персональных данных (далее – Порядок) разработан в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

2. Персональные данные относятся к конфиденциальной информации. Должностные лица, уполномоченные на обработку персональных данных, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3. Размещение информационных систем, в которых обрабатываются персональные данные, осуществляется в охраняемых помещениях, исключая возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

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

5. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только должностные лица, уполномоченные на обработку персональных данных приказом директора.

6. Ответственными за организацию доступа в помещения, в которых ведется обработка персональных данных, являются руководители структурных подразделений ГБУ ДПО РА «АРИПК».

7. Нахождение лиц, в помещениях ГБУ ДПО РА «АРИПК» предназначенных для обработки персональных данных, не являющихся уполномоченными на обработку персональных данных, возможно только в сопровождении сотрудника, уполномоченного на обработку персональных данных на время, обусловленное производственной необходимостью.

8. Внутренний контроль за соблюдением порядка доступа в помещения, в которых ведется обработка персональных данных, осуществляется ответственным за организацию обработки персональных данных и ответственным за безопасность персональных данных

**Политика обработки персональных данных
и реализуемых требований к защите персональных данных
в Государственном бюджетном учреждении дополнительного
профессионального образования Республики Адыгея
«Адыгейский республиканский институт повышения квалификации»
(АРИПК)**

1. Общие положения

1.1. Настоящая Политика обработки персональных данных и реализуемых требований к защите персональных данных в Государственном бюджетном учреждении дополнительного профессионального образования Республики Адыгея «Адыгейский республиканский институт повышения квалификации» (АРИПК) (далее - Политика) разработана в соответствии со следующими нормативными правовыми актами:

- [Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»](#);
- Указ Президента Российской Федерации от 06 марта 1997г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;
- Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказ Роскомнадзора от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;
- иные нормативные правовые акты Российской Федерации и нормативные документы уполномоченных органов государственной власти.

1.2. Настоящая Политика определяет основные вопросы, связанные с обработкой, получением, учетом, обработкой, накоплением, хранением и защитой сведений, отнесенных к персональным данным работников и слушателей в АРИПК размещенных и/или доступных в сети Интернет по адресу: <http://aripk.ru> с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств.

1.3. Цель настоящего Положения – определение порядка обработки персональных данных работников и слушателей АРИПК, нормативное закрепление системы организационно-правовых и технических средств защиты персональных данных работников и слушателей от несанкционированного доступа и разглашения, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований, регулирующих получение, учет, обработку и защиту персональных данных.

1.4. Настоящее Положение вступает в силу с момента его утверждения директором АРИПК и действует бессрочно, до замены его новым Положением.

1.5. Все изменения в Положение вносятся приказом.

1.6. Все работники АРИПК должны быть ознакомлены с настоящим Положением под роспись.

1.7. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении 75 лет срока их хранения, или

продлевается на основании заключения экспертной комиссии АРИПК, если иное не определено законом.

1.8. Использование Пользователем Сайта означает согласие с настоящей Политикой конфиденциальности и на условия обработки персональных данных.

1.9. В случае несогласия с условиями Политики конфиденциальности Пользователь должен прекратить использование сайта АРИПК.

1.10. Персональные данные являются конфиденциальной, охраняемой информацией и на них распространяются все требования, установленные внутренними документами АРИПК к защите конфиденциальной информации.

1.11. Основные понятия, используемые в настоящем Положении:

- **персональные данные слушателя** — любая информация, относящаяся к определенному или определяемому на основании такой информации слушателю, определяемая нормативно - правовыми актами Российской Федерации в области образования, нормативными и распорядительными документами Минобрнауки России, Рособразования и Рособрнадзора, а также локальными нормативными документами АРИПК;

- **обработка персональных данных** — сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных;

- **конфиденциальность персональных данных** — обязательное для соблюдения ответственным лицом, получившим доступ к персональным данным слушателя АРИПК, требование не допускать их распространения без согласия слушателя или наличия иного законного основания;

- **распространение персональных данных** — действия, направленные на передачу персональных данных слушателя определенному кругу лиц или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных слушателя в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным слушателя каким-либо иным способом;

- **использование персональных данных** — действия (операции) с персональными данными, совершаемые специалистами АРИПК, в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении слушателя либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

- **блокирование персональных данных** — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных слушателя АРИПК, в том числе их передачи;

- **уничтожение персональных данных** — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных слушателя АРИПК или в результате которых уничтожаются материальные носители персональных данных слушателя;

- **обезличивание персональных данных** — действия, в результате которых невозможно определить принадлежность персональных данных конкретному слушателю;

- **общедоступные персональные данные** — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия слушателя или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

2. Понятие и состав персональных данных

2.1. Под персональной информацией в настоящей Политике понимается:

- информация, которую Пользователь предоставляет о себе самостоятельно при

регистрации на курсы или авторизации на сайте, а также в процессе дальнейшего использования Сайта АРИПК, включая персональные данные Пользователя;

- информация, предоставляемая кандидатами при приеме на работу и работниками АРИПК.

2.2. АРИПК обрабатывает персональные данные следующих категорий субъектов персональных данных:

- персональные данные работников АРИПК - информация, необходимая Организации в связи с трудовыми отношениями;
- персональные данные обучающихся (слушателей), а также персональные данные руководителя или сотрудника юридического лица, являющегося клиентом или контрагентом (потенциальным клиентом, партнером, контрагентом) АРИПК - информация, необходимая АРИПК для выполнения своих обязательств в рамках договорных отношений, находящаяся как на серверах сайта АРИПК, так и на бумажных носителях;

-

3. Цели и случаи обработки персональных данных

3.1. Целями обработки персональных данных являются:

- организация кадрового учета, ведение кадрового делопроизводства, содействие работникам в трудоустройстве, обучении и продвижении по службе, исполнение налогового законодательства РФ в связи с исчислением и уплатой НДФЛ, а также пенсионного законодательства РФ при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение, заполнение первичной статистической документации;
- идентификации Пользователя, зарегистрированного на сайте АРИПК, для оформления и (или) заключения Договора предоставления Услуги дистанционным способом;
- записи на курсы повышения квалификации и переподготовки;
- установления с Пользователем обратной связи, включая направление уведомлений, запросов, касающихся использования Сайта АРИПК, оказания услуг, обработка запросов и заявок от Пользователя.
- заключение, исполнение и прекращение гражданско-правовых договоров;
- подтверждения достоверности и полноты персональных данных, предоставленных Пользователем.

3.2. Состав персональных данных работника:

- фамилия, имя, отчество (в т.ч. прежние), дата и место рождения;
- паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ);
- сведения о гражданстве;
- адрес и дата регистрации по месту жительства или по месту пребывания;
- сведения из разрешения на временное проживание;
- сведения из заключений медицинских организаций о прохождении предварительного/периодического осмотра;
- сведения из справки о наличии/отсутствии судимостей;
- номера телефонов, в случае их регистрации на субъекта персональных данных или по адресу его места жительства;
- адрес электронной почты;
- сведения об образовании, квалификации и о наличии ученой степени, ученого звания, специальных знаний или специальной подготовки;

- сведения о повышении квалификации и переподготовке;
- сведения о трудовой деятельности (данные о трудовой занятости на текущее текущее время с полным указанием должности, подразделения, организации и ее наименования, ИНН, адреса и телефонов, а также реквизитов других организаций с полным наименованием занимаемых ранее в них должностей и времени работы в этих организациях, о стаже работы, об опыте работы, а также другие сведения);
- сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней;
- содержание и реквизиты трудового договора с работником университета или гражданско-правового договора с гражданином;
- сведения о заработной плате (в том числе номера счетов для расчета с работниками, данные зарплатных договоров с клиентами, данные по окладу, надбавкам, налогам и другие сведения);
- сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер подтверждающего регистрацию в системе индивидуального (персонифицированного) учета, дата выдачи, наименование органа, выдавшего военный билет, военно-учетная специальность, воинское звание, данные о принятии/снятии на(с) учет(а) и другие сведения);
- сведения о семейном положении (состояние в браке, данные свидетельства о заключении брака, фамилия, имя, отчество супруга(и), паспортные данные супруга(и), данные справки по форме 2-НДФЛ супруга(и), степень родства, фамилии, имена, отчества и даты рождения других членов семьи, иждивенцев и другие сведения);
- сведения об имуществе (имущественном положении);
- сведения о номере и серии страхового свидетельства обязательного пенсионного страхования;
- сведения об идентификационном номере налогоплательщика;
- сведения из страхового полиса обязательного (добровольного) медицинского страхования;
- сведения, указанные в оригиналах и копиях приказов по личному составу университета и основаниях к ним;
- сведения о государственных и ведомственных наградах, почетных и специальных званиях, поощрениях (в том числе наименование ил название награды, звания или поощрения, дата и вид нормативного акта о награждении или дата поощрения) работников университета;
- материалы по аттестации и оценке работников АРИПК;
- материалы по внутренним служебным расследованиям в отношении работников АРИПК;
- внутренние материалы по расследованию и учету несчастных случаев на производстве и профессиональным заболеваниям в соответствии с Трудовым кодексом Российской Федерации, другими федеральными законами;
- сведения о временной нетрудоспособности работников АРИПК;
- сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса) и другие сведения, связанные с предоставлением социальных льгот и гарантий;
- биометрические сведения, к которым относятся физиологические данные, а также иные физиологические или биологические характеристики человека, в том числе изображения (фотографии, видеозаписи систем контроля доступа), которые позволяют установить личность.

При определении объема и содержания обрабатываемых персональных данных АРИПК руководствуется нормативно-правовыми актами Российской Федерации,

касающимися получения, обработки и хранения персональных данных.

3.3. Обработка персональных данных в АРИПК допускается в случаях:

- если обработка персональных данных осуществляется с согласия субъекта персональных данных;
- если обработка персональных данных необходима для исполнения трудового договора, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
- если обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- если обработка персональных данных необходима для осуществления прав и законных интересов АРИПК или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- если обработка персональных данных необходима для осуществления научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;
- если осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;
- если осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законом.

4. Основные принципы обработки персональных данных

4.1. Обработка персональных данных возможна только в соответствии с целями, определившими их получение.

4.2. Работник АРИПК предоставляет начальнику отдела документального и кадрового обеспечения АРИПК достоверные сведения о себе. Начальник отдела документального и кадрового обеспечения проверяет достоверность сведений, сверяя данные, предоставленные работником, с имеющимися у работника документами.

4.3. В соответствии со ст. 86, гл. 14 ТК РФ в целях обеспечения прав и свобод человека и гражданина директор АРИПК и его представители при обработке персональных данных работника должны соблюдать следующие общие требования:

- Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
- При определении объема и содержания, обрабатываемых персональных данных Работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами;
- При принятии решений, затрагивающих интересы работника, Работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;
- Защита персональных данных работника от неправомерного их

использования или утраты обеспечивается Работодателем за счет его средств, в порядке, установленном федеральным законом;

- Работники и их представители должны быть ознакомлены под расписку с документами АРИПК, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;

- Во всех случаях отказ работника от своих прав на сохранение и защиту тайны недействителен.

4.4. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4.5. Право доступа для обработки персональных данных имеют сотрудники АРИПК в соответствии с возложенными на них функциональными обязанностями.

4.6. При обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к заявленным целям их обработки.

4.7. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных.

4.8. Обработываемые персональные данные уничтожаются или обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено [Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»](#);

4.9. Сроки хранения персональных данных определяются в соответствии со сроком действия гражданско-правовых отношений между субъектом персональных данных и АРИПК, сроком исковой давности, сроками хранения документов на бумажных носителях и документов в электронных базах данных, иными требованиями законодательства РФ, а также сроком действия согласия субъекта на обработку его персональных данных.

4.10. Персональные данные слушателя получают сотрудники АРИПК, список сотрудников, имеющих доступ к персональным данным, утверждается приказом директора АРИПК. Слушатель заполняет заявление, представляющее собой перечень вопросов о персональных данных, подтверждая согласие на их сбор Согласием на обработку персональных данных (проставление галочки). Заявление заполняется слушателем самостоятельно. При заполнении заявления слушатель должен заполнять все ее графы, на все вопросы давать полные ответы в точном соответствии с записями, которые содержатся в его личных документах, не допускать при этом исправлений, зачеркиваний, прочерков, помарок.

4.11. Если персональные данные слушателя возможно получить только у третьей стороны, то слушатель должен быть уведомлен о соответствующем запросе заранее и от него должно быть получено на это письменное согласие. Сотрудники АРИПК должны сообщить слушателю о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа слушателя дать письменное согласие на их получение.

4.12. Слушатель должен предоставлять сотрудникам АРИПК достоверные сведения о себе. Сотрудники АРИПК вправе сверять достоверность сведений, предоставленных слушателем, с имеющимися у него документами.

4.13. Специалисты АРИПК не имеют права получать и обрабатывать персональные данные слушателя о его политических, религиозных и иных убеждениях, частной жизни, здоровье.

4.14. АРИПК не вправе без письменного согласия субъекта персональных данных передавать обрабатываемые персональные данные третьим лицам, за исключением случаев, предусмотренных законодательством Российской Федерации.

4.15. Письменное согласие слушателя на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие слушателя;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых специалистами АРИПК способов обработки этих данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

4.16. Сотрудники АРИПК не имеют права получать и обрабатывать персональные данные слушателя о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством Российской Федерации и настоящим Положением.

4.17. При принятии решений, затрагивающих интересы слушателя, специалисты АРИПК не имеют права основываться на персональных данных слушателя, полученных исключительно в результате их автоматизированной обработки.

4.18. АРИПК также не вправе принимать решения, затрагивающие интересы слушателя, основываясь на персональных данных, допускающих двойное толкование. В случае, если на основании имеющихся персональных данных слушателя невозможно достоверно установить какой-либо факт, АРИПК предлагает слушателю представить письменные объяснения о причинах расхождения персональных данных.

4.19. Персональные данные защищаются от несанкционированного доступа в соответствии с нормативно-правовыми актами Российской Федерации.

4.20. Слушатели не должны отказываться от своих прав на сохранение и защиту тайны

4.21. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4.22. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных.

4.23. Обрабатываемые персональные данные слушателей уничтожаются или обезличиваются по достижении целей обработки или в случае утраты необходимости в

достижении этих целей, если иное не предусмотрено [Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»](#);

4.24. При зачислении слушатель заполняет заявление и согласие на обработку персональных данных.

4.25. Заявление и согласие, содержащее сведения о персональных данных слушателя, должны храниться в личном деле слушателя на протяжении всего периода обучения. В личном деле также хранятся иные документы персонального учета, относящиеся к персональным данным слушателя.

4.26. Персональные данные слушателя могут также храниться в электронном виде в локальной компьютерной сети.

4.27. Передача персональных данных через сотрудников АРИПК, имеющих право в соответствии с настоящим Положением на ознакомление с персональными данными, не допускается.

4.28. АРИПК являющаяся организацией, осуществляющей образовательную деятельность, обязано передавать, согласно Постановлению Правительства РФ от 26 августа 2013г. № 729 «О федеральной информационной системе «Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении», сведения о Слушателях и полученных ими документах об образовании в ФИС ФРДО.

4.29. АРИПК не вправе сообщать персональные данные слушателя третьей стороне без письменного согласия слушателя, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью слушателя, а также в других случаях, предусмотренных федеральными законами. В случае, если лицо, обратившееся с запросом, не уполномочено федеральным законом или настоящим Положением на получение информации, относящейся к персональным данным слушателя, АРИПК обязан отказать лицу в выдаче информации; при этом лицу, обратившемуся с запросом, выдается уведомление об отказе в выдаче информации с указанием мотивов отказа, копия которого хранится в структурном подразделении АРИПК которое осуществляет обращение с персональными данными.

4.30. На АРИПК лежит обязанность предупредить лиц, получающих персональные данные слушателя, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило будет соблюдено. Лица, получающие персональные данные слушателя, обязаны соблюдать режим конфиденциальности указанной информации.

4.30.1. В целях обеспечения защиты персональных данных, хранящихся в АРИПК слушатели имеют право на получение полной информации об их персональных данных и обработке этих данных, свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные слушателя, за исключением случаев, предусмотренных федеральным законодательством.

5. Передача и хранение персональных данных

При передаче персональных данных работника Работодатель должен соблюдать следующие требования:

5.1. Не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях

предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом.

5.2. Предупредить лиц, получивших персональные данные работника, о том, эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получившие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное Положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами.

5.3. Осуществлять передачу персональных данных работников в пределах АРИПК в соответствии с настоящим Положением.

5.4. Разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретной функции.

5.5. Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

5.6. Передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функции.

6. Хранение и использование персональных данных работников:

6.1. Персональные данные работников обрабатываются и хранятся в отделе документального и кадрового обеспечения.

6.2. Персональные данные работников могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде - локальной компьютерной сети и компьютерной программе «1С: Зарплата и кадры».

6.3. При получении персональных данных не от работника (за исключением случаев, если персональные данные были предоставлены работодателю на основании федерального закона или если персональные данные являются общедоступными) работодатель до начала обработки таких персональных данных обязан предоставить работнику следующую информацию:

- наименование (фамилия, имя, отчество) и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные настоящим Федеральным законом права субъекта персональных данных.

6.2.1. Персональные данные слушателей обрабатываются в целях осуществления исполнения договора, одной из сторон которого является субъект персональных данных.

6.2.2. Документы, содержащие персональные данные, создаются путем: копирования оригиналов; внесения сведений в учетные формы (на бумажных и электронных носителях); получения оригиналов необходимых документов.

6.2.3. Информация о персональных данных слушателей может храниться на бумажных и на электронных носителях, а также в информационно-телекоммуникационных сетях и иных информационных системах.

6.2.4. Хранение персональных данных в АРИПК осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют

цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом или договором, стороной которой является субъект персональных данных.

6.2.5. Общий срок обработки персональных данных определяется периодом времени, в течение которого АРИПК осуществляет действия (операции) в отношении персональных данных, обусловленные заявленными целями их обработки, в том числе хранение персональных данных.

6.2.6. По истечении сроков хранения документов, содержащих персональные данные слушателей, они подлежат уничтожению.

7. Меры по обеспечению безопасности персональных данных

7.1. При обработке персональных данных АРИПК принимает необходимые правовые, организационные и технические меры защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

7.2. Ответственный за обработку ПД совместно с Пользователем принимает все необходимые меры по предотвращению убытков или иных отрицательных последствий, вызванных утратой или разглашением персональных данных Пользователя.

7.3. При утрате или разглашении персональных данных Ответственный за обработку персональных данных информирует Пользователя об утрате или разглашении персональных данных.

7.4. Обеспечение безопасности персональных данных достигается, в частности:

- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности персональных данных;

- обнаружением фактов несанкционированного доступа к персональным данным и принятием необходимых мер;

- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационной системы персональных данных.

8. Доступ к персональным данным работников и слушателей:

8.1. Право доступа к персональным данным работников имеют:

- директор АРИПК;
- сотрудники отдела документального и кадрового обеспечения;
- сотрудники бухгалтерии;
- сотрудники секретариата (информация о фактическом месте проживания и контактные телефоны работников);

- сотрудники, привлеченные в качестве ответственных приказом Директора.

Приложение № 5
к приказу ГБУ ДПО РА «АРИПК»
от 28.12.2024 г. №_146-од

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУ ДПО «АРИПК»

1. Общие положения

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУ ДПО «АРИПК» (далее – Правила) устанавливают основания, порядок и формы проведения внутреннего контроля соответствия обработки и защиты персональных данных (далее - ПД) требованиям, установленным в ГБУ ДПО «АРИПК» (далее – ГБУ ДПО «АРИПК»).

1.2. Настоящие Правила разработаны в соответствии с законодательством Российской Федерации в области обработки и защиты ПД и иными правовыми актами, принимаемыми в соответствии с данным законодательством (далее – законодательство в сфере персональных данных).

1.3. Целями осуществления внутреннего контроля являются:

- оценка общего состояния выполнения в процессах ГБУ ДПО «АРИПК» требований по обработке и защите ПД, закрепленных законодательно, а также в локальных актах ГБУ ДПО «АРИПК»;

- выявление и предотвращение нарушений законодательства в сфере персональных данных.

1.4. Проверки проводятся Комиссией по обеспечению безопасности ПД, создаваемой приказом ГБУ ДПО «АРИПК» (далее – Комиссией).

1.5. В состав Комиссии могут входить государственные служащие Министерства образования и науки РА и работники подведомственных организаций. В проведении проверки не может участвовать государственный гражданский служащий Министерства образования и науки РА, прямо или косвенно заинтересованный в ее результатах.

1.6. Члены Комиссии, получившие доступ к ПД субъектов ПД в ходе проведения проверки, обеспечивают конфиденциальность ПД субъектов ПД, не раскрывают третьим лицам и не распространяют ПД без согласия субъекта ПД.

2. Порядок осуществления внутреннего контроля

2.1. Внутренний контроль соответствия обработки ПД установленным требованиям (далее – внутренний контроль) осуществляется ГБУ ДПО РА «АРИПК» путем проведения проверок соблюдения требований законодательства в сфере ПД.

2.2. Проверки разделяются на:

- плановые;
- внеплановые.

2.3. Плановые проверки проводятся не реже одного раза в год.

2.4. Непосредственно перед началом проведения плановой проверки, за 10 (десять) рабочих дней, ответственным за организацию обработки ПД направляются уведомления

руководителям структурных подразделений, в которых планируется проведение внутреннего контроля.

2.5. Внеплановые внутренние проверки могут проводиться в следующих случаях:

- по результатам расследования выявленных нарушений требований законодательства в сфере ПД;
- по результатам внешних контрольных мероприятий, проводимых, уполномоченным органом по защите прав субъектов ПД.

2.6. Проверка представляет собой комплекс мероприятий, который состоит из следующих этапов:

- подготовка к проведению проверки;
- сбор свидетельств проверки;
- анализ соответствия контрольным параметрам;
- подготовка заключения по проверке.

2.7. В ходе подготовки к проведению проверки Комиссия определяет:

- границы и описание области, подвергающейся проверки;
- перечень контрольных параметров;
- объекты контроля (процессы, подразделения, информационные системы ПД и т.п.);
- состав участников, привлекаемых для проведения проверки;
- сроки и этапы проведения проверки.

2.8. Типовой перечень контрольных параметров приведен в приложении к настоящим Правилам (Приложение 1).

2.9. Сбор свидетельств проверки включает:

- анализ организационно-распорядительных и регламентирующих документов по обработке и защите ПД;
- опрос персонала, участвующего в процессах обработки ПД, обслуживании и эксплуатации информационных систем ПД.

2.10. Проверки проводятся Комиссией непосредственно на месте обработки ПД путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки ПД.

2.11. Свидетельства проверки сопоставляются с контрольными параметрами для формирования заключения по проверке.

2.12. Общий срок проверки не должен превышать 20 (двадцати) рабочих дней. При необходимости срок проведения проверки может быть продлен, но не более чем на 10 (десять) рабочих дней.

3. Права Комиссии при проведении проверки

3.1. Комиссия для реализации своих полномочий имеет право:

- привлекать к проведению проверок служащих ГБУ ДПО РА «АРИПК» и работников подведомственных ГБУ ДПО «АРИПК» организаций;
- запрашивать у сотрудников ГБУ ДПО РА «АРИПК» и подведомственных ГБУ ДПО «АРИПК» организаций необходимую информацию;
- принимать меры по устранению выявленных нарушений выполнения требований к защите ПД в ГБУ ДПО РА «АРИПК»;
- вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности ПД при их обработке;
- вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки ПД.

3.2. Проверки могут проводиться с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

4. Порядок фиксирования результатов проверки

3

4.1. Факт проведения проверок и результаты проверки фиксируются в журнале проведения проверок (Приложение 2).

4.2. По результатам проверки Комиссией, при необходимости, проводится заседание.

Решения, принятые на заседаниях Комиссии, оформляются протоколом.

4.3. В целях контроля устранения выявленных нарушений Комиссия проводит повторную проверку.

Приложение № 1
к Правилам осуществления
внутреннего контроля
соответствия
обработки персональных
данных требованиям к
защите
персональных данных
в ГБУ ДПО «АРИПК»

ПЕРЕЧЕНЬ
контрольных параметров проверок в области обработки и обеспечения
безопасности персональных данных
(типовой)

№ п/п	Контрольные параметры и объекты проверок
1.	Соответствие установленных в перечне персональных данных категорий персональных данных фактически обрабатываемым в [Наименование ОИВ, организации, учреждения]
2.	Соответствие установленных прав доступа к персональным данным полномочиям в рамках трудовых обязанностей работников
3.	Подтверждение факта ознакомления с локальными актами [Наименование ОИВ, организации, учреждения] в области обработки и обеспечения безопасности персональных данных
4.	Наличие в договорах с третьими лицами положений, касающихся обеспечения конфиденциальности и безопасности персональных данных
5.	Наличие законных целей и оснований обработки всех категорий персональных данных
6.	Выборочные проверки сотрудников на предмет знания организационно-распорядительных документов в области обработки и обеспечения безопасности персональных данных
7.	Соблюдение сроков хранения и порядка уничтожения персональных данных
8.	Соблюдение процедур и сроков подготовки ответов на обращения субъектов персональных данных
9.	Необходимость актуализации Уведомления уполномоченного органа по защите прав субъектов персональных данных

Приложение № 2
к Правилам осуществления внутреннего контроля
соответствия обработки персональных данных
требованиям к защите персональных данных
в ГБУ ДПО «АРИПК»

ЖУРНАЛ
проведения внутреннего контроля соответствия обработки персональных данных
требованиям к защите персональных данных

№ п/п	Дата проведения проверки	Основание проверки	Заключение по проверке (кратко)	Подпись председателя Комиссии	Примечание

ПОЛОЖЕНИЕ

об организации и проведении работ по обеспечению безопасности персональных данных обрабатываемых в информационных системах персональных данных и/или без использования средств автоматизации.

1. Общие положения.

1.1. Данное «Положение об организации и проведении работ в ГБУ ДПО РА «АРИПК» по обеспечению безопасности персональных данных при их автоматизированной обработке и/или без использования средств автоматизации в информационных системах персональных данных» (далее – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», методическими рекомендациями ФСТЭК России и ФСБ России в целях обеспечения безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн).

1.2. Положение определяет порядок работы пользователей и администраторов ИСПДн, сотрудников, ответственных за техническое обеспечение, обеспечение безопасности ПДн при их обработке, порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления, порядок обучения персонала практике работы в ИСПДн, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок охраны и допуска посторонних лиц в помещения ИСПДн, а также порядок обезличивания ПДн.

1.3. При обеспечении безопасности персональных данных в ИСПДн с использованием криптографических средств защиты информации все сотрудники обязаны выполнять требования, изложенные в документе «Типовые требования 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» (ФСБ России, № 149/6/6-622, 2008).

1. Порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации.

1.1. Допуск пользователей для работы на компьютерах ИСПДн осуществляется на основании приказа, который издается директором АРИПК, и в соответствии со списком лиц, допущенных к работе в ИСПДн. С целью контроля выполнения необходимых мероприятий по обеспечению безопасности назначается ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн.

1.2. Пользователь имеет право в отведенное ему время решать поставленные

задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники (СВТ), входа в систему и все действия при работе в ИСПДн.

Вход пользователя в систему может осуществляться по выдаваемому ему электронному идентификатору или по персональному паролю.

При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на компьютерах ИСПДн. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения.

Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ в помещение, в котором производится обработка ПДн, аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и **обязан**:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах ИСПДн;
- хранить в тайне свой пароль (пароли) и с установленной периодичностью менять свой пароль (пароли);
- хранить в установленном порядке свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе, или ящике, закрывающемся на ключ;

Немедленно известить ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн и (или) ответственного за обработку персональных данных в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

- нарушений целостности пломб (наклеек, нарушений или несоответствии номеров печатей) на составляющих узлах и блоках СВТ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к данным защищаемым СВТ;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;
- некорректного функционирования установленных на компьютеры технических средств защиты;
- непредусмотренных отводов кабелей и подключенных устройств.

1.3. Пользователю категорически **запрещается**:

- использовать компоненты программного и аппаратного обеспечения персонального компьютера в неслужебных целях;
- вносить какие-либо изменения в конфигурацию аппаратных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;
- осуществлять обработку ПДн в присутствии посторонних (не допущенных данной информации) лиц;
- оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
- оставлять без личного присмотра свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);
- размещать средства ИСПДн так, чтобы существовала возможность визуального считывания информации.

1.4. Лица, ответственные за защиту персональных данных в АРИПК.

Ответственный за организацию обработки ПДн - штатный сотрудник определяющий уровень доступа и ответственность лиц участвующих в обработке ПДн. Назначается приказом по учреждению.

Ответственный за обеспечение безопасности персональных данных – штатный сотрудник (или подразделение) отвечающий за проведение мероприятий, связанных с защитой ПДн (организационных и технических), а также осуществляющий контроль за соблюдением требований по защите ПДн в подразделениях. Назначается приказом по учреждению.

Администратор информационной безопасности – штатный сотрудник, ответственный за защиту автоматизированной системы (АС) от несанкционированного доступа (НСД) к информации. Назначается приказом по учреждению.

1.5. Администратор информационной безопасности обязан:

- знать состав основных и вспомогательных технических систем и средств (далее - ОТСС и ВТСС) установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения (далее - ПО) в ИСПДн;
- контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, защищенных СВТ и других устройствах;
- производить необходимые настройки подсистемы управления доступом установленных в ИСПДн СЗИ от НСД и сопровождать их в процессе эксплуатации, при этом:
 - реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);
 - вводить описания пользователей ИСПДн в информационную базу СЗИ от НСД;
 - своевременно удалять описания пользователей из базы данных СЗИ при изменении списка допущенных к работе лиц;
 - контролировать доступ лиц в помещение в соответствии со списком сотрудников, допущенных к работе в ИСПДн;
 - проводить инструктаж сотрудников - пользователей компьютеров по правилам работы с используемыми техническими средствами и системами защиты информации;
 - контролировать своевременное (не реже чем один раз в течение 60 дней) проведение смены паролей для доступа пользователей к компьютерам и ресурсам ИСПДн;
 - обеспечивать постоянный контроль выполнения сотрудниками установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн;
 - осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных;
 - настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе в ИСПДн;
 - вводить в базу данных СЗИ от несанкционированного доступа описания событий, подлежащих регистрации в системном журнале;
 - проводить анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам не реже одного раза в месяц;
 - организовывать печать файлов пользователей на принтере и осуществлять контроль соблюдения установленных правил и параметров регистрации и учета бумажных носителей информации;
 - сопровождать подсистемы обеспечения целостности информации в ИСПДн;
 - периодически тестировать функции СЗИ от НСД, особенно при изменении программной среды и полномочий исполнителей;
 - восстанавливать программную среду, программные средства и настройки СЗИ при сбоях совместно с лицами, ответственными за техническое обеспечение.
 - вести две копии программных средств СЗИ от НСД и контролировать их работоспособность;

- контролировать отсутствие на магнитных носителях остаточной информации по окончании работы пользователей;
- периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядок и правила проведения антивирусного тестирования;
- проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;
- сопровождать подсистему защиты информации от утечки за счет побочных электромагнитных излучений и наводок, контролировать соблюдение требований по размещению и использованию технических средств ИСПДн;
- контролировать соответствие документально утвержденного состава аппаратной и программной части ИСПДн реальным конфигурациям ИСПДн, вести учет изменений аппаратно-программной конфигурации;
- обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИСПДн и отправке его в ремонт (контролировать затирание конфиденциальной информации на магнитных носителях с составлением соответствующего акта);
- присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;
- вести журнал учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн;
- поддерживать установленный порядок проведения антивирусного контроля согласно требованиям настоящего Положения;
- в случае отказа средств и систем защиты информации принимать меры по их восстановлению;
- докладывать ответственному за обработку персональных данных о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;
- вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

1.6. Администратор информационной безопасности и ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн имеют право:

- требовать от сотрудников - пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности и защите информации в ИСПДн;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов ИСПДн;
- требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;
- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

2. Порядок обработки персональных данных без использования средств автоматизации.

2.1. Обработка персональных данных без использования средств автоматизации может осуществляться в виде документов на бумажных носителях. 3

2.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

2.3. При неавтоматизированной обработке персональных данных на бумажных

носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;
- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;
- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

2.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

2.4.1. типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, 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;

2.4.2. типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

2.4.3. 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;

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

2.5. 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.

3. Порядок контроля защиты информации в ИСПДн и приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления. Порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации и принятие мер по предотвращению возможных опасных последствий.

3.2. Основными задачами контроля являются:

- проверка организации выполнения мероприятий по защите информации в учреждении, учёта требований по защите информации в разрабатываемых плановых и распорядительных документах;
- выявление демаскирующих признаков объектов ИСПДн;
- уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;
- проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;
- проверка выполнения требований по защите ИСПДн от несанкционированного доступа;
- проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;
- проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;
- оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн;
- разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

3.3. Контроль защиты информации проводится с учетом реальных условий по всем физическим полям, по которым возможен перехват информации, циркулирующей в ИСПДн учреждения, и осуществляется по объектовому принципу, при котором на объекте одновременно проверяются все вопросы защиты информации.

Перечень каналов утечки устанавливается в соответствии с моделью угроз.

3.4. В ходе контроля проверяются:

- соответствие принятых мер по обеспечению безопасности персональных данных (далее – ОБ ПДн);
- своевременность и полнота выполнения требований настоящего Положения и других руководящих документов ОБ ПДн;
- полнота выявления демаскирующих признаков охраняемых сведений об объектах защиты и возможных технических каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;
- эффективность применения организационных и технических мероприятий по защите информации;
- устранение ранее выявленных недостатков.

Кроме того, могут проводиться необходимые измерения и расчеты приглашенными для этих целей специалистами организации, имеющей соответствующие лицензии ФСТЭК России.

3.5. Основными видами технического контроля являются визуально-оптический контроль, контроль эффективности защиты информации от утечки по техническим каналам, контроль несанкционированного доступа к информации и программно-технических воздействий на информацию.

3.6. Полученные в ходе ведения контроля результаты обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер защиты информации и выявления нарушений. При обнаружении нарушений норм и требований по защите информации администратор безопасности докладывает руководителю для принятия ими решения о прекращении обработки информации и проведения, соответствующих организационных и технических мер по устранению нарушения. Результаты контроля защиты информации оформляются актами либо в соответствующих журналах учета результатов контроля.

3.7. Невыполнение предписанных мероприятий по защите ПДн, считается предпосылкой к утечке

информации (далее – предпосылка). По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по указанию руководителя или ответственного за защиту информации проводится расследование. Для проведения расследования назначается комиссия с привлечением администратора безопасности. Комиссия обязана установить, имела ли место утечка сведений, и обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования руководитель принимает решение о наказании виновных лиц и необходимых мероприятиях по устранению недостатков.

3.8. Ведение контроля защиты информации осуществляется путём проведения периодических, плановых и внезапных проверок объектов защиты. Периодические, плановые и внезапные проверки объектов учреждения проводятся, как правило, силами администратора безопасности и (или) ответственного за защиту информации, в соответствии с утвержденным планом или по согласованию с руководителем.

3.9. Одной из форм контроля защиты информации является обследование объектов ИСПДн. Оно проводится не реже одного раза в год рабочей группой в составе администратора безопасности, ответственного за защиту информации, ответственного за эксплуатацию объекта. Для обследования ИСПДн может привлекаться организация, имеющая лицензию ФСТЭК России на деятельность по технической защите информации.

3.10. Обследование ИСПДн проводится с целью определения соответствия помещений, технических и программных средств требованиям по защите информации, установленным в «Аттестате соответствия» и(или) требованиям по безопасности персональных данных.

3.11. В ходе обследования проверяется:

- соответствие текущих условий функционирования обследуемого объекта

3.12. Классификация нарушений защиты ПДн. Нарушения, связанные с выполнением требований руководящих документов по безопасности информации, с применением средств защиты информации и разграничением доступа, использованием технического, программного обеспечения информационных систем, по степени их опасности целесообразно разделить на:

- нарушения 1 - ой категории;
- нарушения 2 - ой категории;
- некатегоризированные нарушения.

К нарушениям 1-ой категории относятся нарушения, повлекшие за собой разглашение (утечку) защищаемых сведений, утрату бумажных документов и магнитных носителей информации, уничтожение (искажение) информационного и программного обеспечения, выведение из строя технических средств.

К нарушениям 2-ой категории относятся нарушения, в результате которых возникает возможность разглашения (утечки) защищаемых сведений или утраты бумажных документов и магнитных носителей информации, уничтожения (искажения) информационного и программного обеспечения, выведения из строя технических средств.

Остальные нарушения, не вошедшие в первую и вторую категории, относятся к некатегоризированным нарушениям.

Нарушения 1-ой категории:

- утрата бумажных документов и магнитных носителей информации, содержащих охраняемые (конфиденциальные) сведения; – действия работников структурных подразделений, приведшие к искажению или разрушению охраняемых сведений или иных защищаемых ресурсов

- умышленная разработка, использование и распространение вредоносных программ (программ - вирусов и т. п.), а также непреднамеренные (по халатности) виновные действия, приведшие к использованию и распространению таких программ;

- несанкционированная корректировка адресной информации маршрутов и путей коммутации технических средств пользователей данных и сообщений в информационных сетях;

- компрометация средств защиты информации;

- несанкционированный доступ к защищаемой информации;

- несанкционированные действия работников, направленные на сбор, накопление и обобщение охраняемых сведений. Нарушения 2-ой категории:

- компрометация паролей;

- несвоевременная замена паролей и идентификаторов при их компрометации;

– вывод информации, содержащей охраняемые сведения, на неучтенные носители информации и машинные документы; – несанкционированное внесение изменений в программное информационное обеспечение информационных систем;

– несанкционированное отключение средств защиты информации;

– самовольное отключение средств антивирусной защиты; – несанкционированное подключение к вычислительной сети штатных технических средств обработки информации (например, личных портативных компьютеров и т.п.);

– вход в систему в обход системы защиты (загрузка ОС с флэш-карты или загрузочного CD);

– отсутствие разграничения доступа к информации, содержащей охраняемые сведения и обрабатываемой в многопользовательском режиме, при работе по технологии "Клиент-Сервер", а также доступа из других информационно - вычислительных сетей по каналам корпоративной или открытой сети;

– нарушение порядка учета, хранения и обращения со средствами разграничения доступа к информации. Перечень категоризированных нарушений должен ежегодно корректироваться и доводиться до всех работников, работающих с защищаемыми ресурсами.

3.13. Оперативная реакция на нарушения режима безопасности:

– работники обязаны немедленно уведомлять непосредственных руководителей и ответственного за обеспечение безопасности ПДн лица о случаях нарушения защиты или об обнаруженных уязвимостях (слабостях) в информационных системах и средствах защиты;

– функции своевременной и адекватной реакции на выявленные нарушения защиты ПДн, требующих оперативного реагирования, например, таких как обнаружение и нейтрализация вторжений хакеров или внедрение программных вирусов, возлагаются на Администратора ИСПДн и Администратора безопасности ИСПДн. Эти работники должны быть доступны в течение рабочего времени (лично, по телефону или электронной почте);

– работники учреждения должны обращаться к ним при обнаружении признаков нарушения защиты ПДн в соответствии с установленной процедурой.

3.14. Расследование инцидентов, связанных с нарушениями защиты ПДн: По каждому инциденту, связанному с нарушением защиты ПДн в учреждении, должно проводиться расследование. Ответственность за проведение расследования возлагается на лиц ответственных за обеспечение безопасности ПДн. В результате расследования необходимо определить:

– нарушителя (нарушителей) защиты ПДн;

– категорию нарушения и величину нанесенного ущерба (если он есть);

– причины, приведшие к нарушению;

– меры и средства, необходимые для ликвидации нежелательных последствий;

– меры и средства, необходимые для ликвидации или ослабления причин, приведших к нарушению, чтобы подобные нарушения не повторялись в будущем. Результаты расследования должны оформляться документально.

Вид нарушения, если такового не было ранее, должен быть включен в перечень категоризированных нарушений по защите ПДн.

4. Порядок обучения персонала практике работы в ИСПДн в части обеспечения безопасности персональных данных.

4.1. Перед началом работы в ИСПДн пользователи должны ознакомиться с инструкциями по использованию программных и технических средств, по использованию средств защиты информации под роспись.

4.2. Пользователи, демонстрирующие недостаточные знания и умения для обеспечения безопасности персональных данных в соответствии с требованиями настоящего положения, к работе в ИСПДн не допускаются.

4.3. Ответственным за организацию обучения и оказание методической помощи в ГБУ ДПО РА «АРИПК» являются ответственные за обработку персональных данных.

4.4. Для проведения занятий, семинаров и совещаний могут привлекаться специалисты по программному и техническому обеспечению, а также специалисты органов по аттестации объектов ИСПДн, организаций-лицензиатов ФСТЭК России и ФСБ России.

5. Правила антивирусной защиты.

5.1. На каждом компьютере ИСПДн должны быть установлены лицензионные антивирусные средства.

5.2. Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется специалистами, ответственными за техническое обеспечение информационных систем учреждения.

5.3. Специалисты, ответственные за техническое обеспечение информационных систем учреждения, осуществляют периодическое обновление антивирусных пакетов и контроль их работоспособности.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.).

5.4. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, администратором информационной безопасности должна быть выполнена антивирусная проверка ИСПДн.

5.5. На компьютеры запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

5.6. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно (или вместе с администратором информационной безопасности) должен провести внеочередной антивирусный контроль компьютера.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить обработку данных в ИСПДн;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора информационной безопасности, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ возможности, дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

5.7. Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями настоящего Положения возлагается на ответственного за обработку персональных данных.

6. Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на специалистов по техническому обеспечению.

6.1. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно (или вместе с администратором информационной безопасности) должен провести внеочередной антивирусный контроль компьютера.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить обработку данных в ИСПДн;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора информационной безопасности, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ возможности, дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

6.2. Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями настоящего Положения возлагается на ответственного за обработку персональных данных.

7. Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на специалистов по техническому обеспечению.

8. Правила парольной защиты.

8.1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль действий пользователей при работе с паролями возлагается на администратора информационной безопасности.

8.2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями объекта вычислительной техники самостоятельно с учетом следующих требований:

- пароль должен быть не менее 6 символов;
- в числе символов пароля **обязательно** должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, \$, &, *, % и т.п.);
- символы паролей для рабочих станций, на которых установлено средство защиты информации от несанкционированного доступа, должны вводиться в режиме латинской раскладки клавиатуры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.).

8.3. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры по восстановлению парольной защиты.

8.4. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в течение 360 дней.

8.5. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри учреждения т.п.) должна производиться администратором безопасности (либо новым постоянным пользователем) немедленно после окончания последнего сеанса работы данного пользователя с системой на основании указания начальника отдела.

8.6. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри учреждения и другие обстоятельства) администратора безопасности.

9. Управление учетными записями пользователей.

9.1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе на компьютерах конкретной ИСПДн, должна быть создана уникальная учетная запись пользователя.

9.2. Работу в ИСПДн сотрудник должен осуществлять только с использованием своего уникального имени пользователя. Работа в ИСПДн под чужой учетной записью, кроме случаев, описанных в п.9.5, **запрещена**.

10. Порядок контроля соблюдения условий использования средств защиты информации, в том числе криптографических.

10.1. Данный раздел Положения определяет порядок контроля соблюдения условий использования средств защиты информации (далее - СЗИ).

10.2. Технические средства защиты информации являются важным компонентом ОБ ПДн.

10.3. Порядок работы с техническими СЗИ определен в соответствующих руководствах по настройке и использованию СЗИ обязательных для исполнения, как сотрудниками обрабатывающими конфиденциальную информацию, так и администратором информационной безопасности. Право проверки соблюдения условий использования средств защиты информации имеют:

- руководитель;
- ответственный за обработку персональных данных;
- администратор информационной безопасности.

10.4. Пользователю ИСПДн категорически запрещается:

- отключать СЗИ;
- производить обработку конфиденциальной информации в случае неработоспособности средств ее защиты (СЗИ);
- менять настройки СЗИ.

10.5. Криптографические средства защиты информации должны использоваться в соответствии с технической и эксплуатационной документацией на них, а также в соответствии с правилами пользования ими.

11. Порядок охраны и допуска посторонних лиц в защищаемые помещения.

11.1. Данный раздел Положения устанавливает порядок охраны помещений ИСПДн.

11.2. Вскрытие и закрытие помещений осуществляется сотрудниками, работающими в данных помещениях.

Список сотрудников, имеющих право вскрывать (сдавать под охрану) и опечатывать помещения утверждается руководителем и передаётся на пост охраны.

11.3. При отсутствии сотрудников, ответственных за вскрытие помещений, данные помещения могут быть вскрыты комиссией, созданной на основании приказа. Комиссией составляется акт вскрытия.

11.4. При закрытии помещений сотрудники, ответственные за помещения, проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и носители информации, на которых содержится конфиденциальная информация, убирают для хранения в опечатываемый сейф (металлический шкаф). Закрываемое помещение опечатывается личной печатью сотрудника, ответственного за помещение.

11.5. Постановка и снятие помещений под охрану производится охранником после окончания и перед началом рабочего дня соответственно.

11.6. Сотрудник, имеющий право на вскрытие помещений:

- производит проверку оттиска печати на двери помещения и исправность запоров;
- вскрывает помещение.

11.7. При обнаружении нарушений целостности оттисков печатей, повреждения запоров или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не вскрывается, а составляется акт, в присутствии охранника. О происшествии немедленно сообщается руководителю и (или) ответственному за обеспечение безопасности персональных данных при их обработке в ИСПДн.

Одновременно принимаются меры по охране места происшествия и до прибытия должностных лиц в помещение никто не допускается.

11.8. Руководитель, ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн и ответственный за обработку персональных данных организуют проверку ИСПДн на предмет несанкционированного доступа к конфиденциальной информации и наличие документов и машинных носителей информации.

11.9. Порядок пребывания посторонних лиц на территории ГБУ ДПО РА «АРИПК» устанавливается соответствующим приказом.

12. Порядок стирания защищаемой информации и уничтожения носителей защищаемой информации.

12.1. В обязательном порядке уничтожению подлежат поврежденные, выводимые из эксплуатации носители, содержащие защищаемую информацию, использование которых не предполагается в дальнейшем. Стиранию подлежат носители, содержащие защищаемую информацию, которые выводятся из эксплуатации в составе ИСПДн. Не допускается стирание неисправных носителей и передача их в сервисный центр для ремонта. Такие носители должны уничтожаться в соответствии с настоящим порядком.

12.2. Стирание должно производиться по технологии, предусмотренной для данного типа носителя.

12.3. Уничтожение носителей производится путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления информации (перед уничтожением, если носитель исправен, должно быть произведено

гарантирование стирание информации на носителе). Непосредственные действия по уничтожению конкретного типа носителя должны быть достаточны для исключения возможности восстановления информации.

12.4. Бумажные и прочие сгораемые носители (конверты с неиспользуемыми более паролями) уничтожают путем сжигания или с помощью любых бумагорезательных машин.

12.5. По факту уничтожения или стирания носителей составляется акт, в журналах учета делаются соответствующие записи.

12.6. Процедуры стирания и уничтожения осуществляются комиссией, в которую входит ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн.

13. Обезличивание персональных данных.

13.1. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

13.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

- метод введения идентификаторов;
- метод изменения состава или семантики;
- обобщение (понижение точности некоторых сведений);
- метод декомпозиции (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств;
- метод перемешивания (перестановка отдельных записей, а также групп записей в массиве персональных данных).

13.3. Для обезличивания персональных данных используются способы обезличивания, определенные приказом Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных» в соответствии с рекомендациями по использованию этих методов.

13.4. Решение о необходимости обезличивания персональных данных принимает директор АРИПК.

13.5. Сотрудники подразделений, обслуживающих базы данных с персональными данными, осуществляют непосредственное обезличивание выбранным способом.

13.6. Порядок работы с обезличенными персональными данными:

13.6.1. Обезличенные персональные данные не подлежат разглашению.

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

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

- парольной политики;
- антивирусной политики;
- правил работы со съемными носителями (если они используется);
- правил доступа в помещения, где расположены элементы информационных систем;

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

- правил хранения бумажных носителей;
- правил доступа к ним и в помещения, где они хранятся.

14. Порядок проверки электронного журнала обращений к ИСПДн

14.1. Настоящий раздел Положения определяет порядок проверки электронных журналов обращений к ресурсам ИСПДн.

3

14.2. Проверка электронного журнала обращений проводится с целью выявления несанкционированного доступа к защищаемой информации в ИСПДн.

14.3. Право проверки электронного журнала обращений имеют:

- администратор безопасности; – ответственный за обеспечение безопасности ПДн;
- руководитель образовательной организации.

14.4. На технических средствах ИСПДн, на которых установлены специализированные средства защиты информации (далее – СЗИ) проверка электронного журнала производится в соответствии с прилагаемым к указанным СЗИ Руководством.

14.5. Если в ходе периодических, плановых или внезапных проверок ИСПДн выявлены случаи НСД к информации конфиденциального характера, то вступает в силу п.п. 3.6., 3.7. данного Положения.

14.6. Проверке подлежат все электронные журналы ИСПДн.

14.7. Проверка должна проводиться не реже, чем один раз в месяц с целью своевременного выявления фактов нарушения требований настоящего Положения.

14.8. Факты проверок электронных журналов отражаются в специальном журнале проверок электронных журналов. После каждой проверки Администратор безопасности делает соответствующую отметку в журнале и ставит свою подпись.

ТИПОВАЯ ФОРМА
журнала учета установленных средств защиты информации

№ п/п	Регистрационный номер	Наименование	Сведения об установке средств защиты информации			Сведения об изъятии/удалении средства защиты информации			Примечание
			Дата установки	Место установки (использования)	ФИО проводившего установку, подпись	Дата изъятия/ удаления	ФИО проводившего изъятие/ удаление, подпись	Причина изъятия/ удаления	

ТИПОВАЯ ФОРМА
журнала учета машинных носителей информации

№ п/п	Регистрационный (учетный) номер носителя	Вид носителя	Тип носителя и его емкость	Дата поступления
1	2	3	4	5

Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения	Дата и номер акта об уничтожении	Примечание
6	7	8	9	10

ТИПОВАЯ ФОРМА
журнала периодического тестирования средств защиты информации

№ п/п	Наименование средства защиты информации от НСД или криптосредства	Регистрационные номера СЗИ от НСД или криптосредства	Дата тестирования	Фамилия и подпись ответственного пользователя, проводившего тестирование
1	2	3	4	5

Наименование теста, используемые средства для проведения теста	Результат тестирования (успешный/неуспешный), комментарий	Дата очередного тестирования
6	7	8

Приложение №10
к приказу ГБУ ДПО РА «АРИПК»
от 28.12.2024 г. № 146-од

ТИПОВАЯ ФОРМА
журнала учета нештатных ситуаций ИСПДн, выполнения профилактических работ,
установки и модификации программных средств на компьютерах ИСПДн

№ п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	ФИО исполнителей и их подписи
1	2	3	4

ФИО ответственного за эксплуатацию ПЭВМ, подпись	Подпись специалиста по защите информации	Примечание (ссылка на заявку)
5	6	7

Приложение № 11
к приказу ГБУ ДПО РА «АРИПК»
от 28.12.2024 г. № 146-од

ТИПОВАЯ ФОРМА
журнала учета пользователей, допущенных к информационным системам
персональных данных

№ п/п	Дата	Фамилия, имя, отчество пользователя	Наименование ИСПДн
1	2	3	4

Подпись пользователя об ознакомлении с Положением и Требованиями по безопасности	Подпись администратора безопасности о готовности пользователя к работе в ИСПДн	Примечание
5	6	7

Приложение № 12
к приказу ГБУ ДПО РА «АРИПК»
от 28.12.2024 г. № 146-од

ТИПОВАЯ ФОРМА
Журнала проверок электронных журналов

№ п/п	Дата проверки	Наименование ИСПДн, компьютера, технического средства	Наименование проверяемого журнала
1	2	3	4

Выявленные нарушения требований безопасности, нестандартные ситуации	Подпись администратора безопасности	Примечание
5	6	7

ТИПОВАЯ ФОРМА
Журнала учета обращений субъектов ПДн о выполнении их законных прав

№ п / п	Ф.И.О	Дата	Цель обращения	Регистрационный номер обращения
1	2	3	4	5

ЖУРНАЛ
УЧЕТА ХРАНИЛИЩ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

Дата начала ведения журнала: _____

Дата окончания ведения журнала: _____

Количество листов: _____

[illegible]

Приложение № 15
к приказу ГБУ ДПО РА «АРИПК»
от 28.12.2024 г. № 146-од

Список помещений,
предназначенных для обработки персональных данных без
использования средств автоматизации

№ п/п	Наименование помещения	Место хранения носителей персональных данных	Адрес расположения помещения
1			г. Майкоп ул. Ленина, 15
2			

Правила рассмотрения запросов субъектов персональных данных или их представителей в ГБУ ДПО РА «АРИПК»

1. Настоящие Правила устанавливают порядок рассмотрения запросов субъектов персональных данных или их представителей в целях предотвращения нарушений законодательства Российской Федерации при обработке персональных данных, в том числе Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» (далее – Правила).

2. В ГБУ ДПО РА «АРИПК» в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» является оператором, осуществляющим обработку персональных данных, а также определяющим цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (далее – оператор персональных данных).

3. Субъектами персональных данных являются сотрудники и слушатели ГБУ ДПО РА «АРИПК», граждане Российской Федерации (далее – субъекты персональных данных).

4. Субъект персональных данных или его представитель имеет право на получение следующей информации:

а) подтверждение факта обработки персональных данных оператором персональных данных;

б) правовые основания, цели и способы обработки персональных данных оператором персональных данных;

г) наименование и место нахождения оператора персональных данных, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором персональных данных или на основании Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон);

д) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;

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

ж) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом;

з) название или фамилию, имя, отчество (если имеется) и адрес лица, осуществляющего обработку персональных данных по поручению оператора персональных данных, если обработка поручена или будет поручена такому лицу;

и) иные сведения, предусмотренные Федеральным законом.

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

а) оператор персональных данных обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя в течение 10 рабочих дней с даты получения запроса субъекта персональных данных или его представителя;

б) в случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор персональных данных обязан дать в письменной форме мотивированный ответ, с указанием основания для такого отказа, в срок, не превышающий 10 рабочих дней со дня обращения субъекта персональных данных или его представителя либо от даты получения запроса субъекта персональных данных или его представителя.

в) прекратить обработку персональных данных по требованию субъекта персональных данных.

г) разъяснять субъекту персональных данных юридические последствия отказа предоставить персональные данные и/или дать согласие на их обработку, если предоставление этих персональных данных или согласие являются обязательными;

д) предоставлять субъекту персональных данных информацию о том, какие данные о нем он будет обрабатывать, если эти персональные данные получены не от субъекта персональных данных;

ж) уведомлять Роскомнадзор в течение 24 часов о факте неправомерной или случайной передачи персональных данных, повлекшей нарушение прав субъектов персональных данных, а также о предполагаемых причинах и вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий инцидента;

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

8. Запрашиваемые сведения должны быть предоставлены субъекту персональных данных или его представителю оператором персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

В случае если запрашиваемые сведения, а также обрабатываемые персональные данные не были предоставлены субъекту персональных данных для ознакомления в полном объеме, субъект персональных данных вправе обратиться повторно к оператору персональных данных или направить ему повторный запрос в целях получения дополнительных сведений и ознакомления с такими персональными данными не ранее чем через 10 рабочих дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных. Повторный запрос должен содержать обоснование направления

повторного запроса.

Оператор персональных данных вправе отказать субъекту персональных данных в выполнении запроса, не соответствующего условиям, предусмотренным Правилами. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении запроса лежит на операторе персональных данных.

ПОРЯДОК
доступа работников ГБУ ДПО РА «АРИПК» в помещения, в
которых ведется обработка персональных данных

1. Настоящий Порядок доступа работников в помещения ГБУ ДПО РА «АРИПК», в которых ведется обработка персональных данных (далее – Порядок) разработан в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

2. Персональные данные относятся к конфиденциальной информации. Должностные лица, уполномоченные на обработку персональных данных, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3. Размещение информационных систем, в которых обрабатываются персональные данные, осуществляется в охраняемых помещениях, исключая возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

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

5. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только должностные лица, уполномоченные на обработку персональных данных приказом директора АРИПК.

6. Ответственными за организацию доступа в помещения, в которых ведется обработка персональных данных, являются руководители структурных подразделений АРИПК.

7. Нахождение лиц, в помещениях предназначенных для обработки персональных данных, не являющихся уполномоченными на обработку персональных данных, возможно только в сопровождении сотрудника, уполномоченного на обработку персональных данных на время, обусловленное производственной необходимостью.

8. Внутренний контроль за соблюдением порядка доступа в помещения, в которых ведется обработка персональных данных, осуществляется ответственным за организацию обработки персональных данных и ответственным за безопасность персональных данных.

Положение о порядке уничтожения персональных данных в ГБУ ДПО РА «Адыгейский республиканский институт повышения квалификации»

1. Общие положения

1.1. Настоящее Положение о порядке уничтожения персональных данных в ГБУ ДПО РА «Адыгейский республиканский институт повышения квалификации» (далее – ГБУ ДПО РА «АРИПК») устанавливает периодичность и способы уничтожения носителей, содержащих персональные данные субъектов персональных данных.

1.2. Целью настоящего Положения является обеспечение защиты прав и свобод обучающихся и работников при обработке их персональных данных в ГБУ ДПО РА «АРИПК».

2. Правила уничтожения носителей, содержащих персональные данные

2.1. Уничтожение носителей, содержащих персональные данные субъектов персональных данных, должно соответствовать следующим правилам:

- быть конфиденциальным, исключая возможность последующего восстановления;
- оформляться юридически, в частности, актом о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению и актом об уничтожении носителей, содержащих персональные данные субъектов персональных данных;
- должно проводиться комиссией по уничтожению персональных данных;
- уничтожение должно касаться только тех носителей, содержащих персональные данные субъектов персональных данных, которые подлежат уничтожению в связи с истечением срока хранения, достижением цели обработки указанных персональных данных либо утратой необходимости в их достижении, не допуская случайного или преднамеренного уничтожения актуальных носителей.

3. Порядок уничтожения носителей, содержащих персональные данные

3.1. Персональные данные субъектов персональных данных хранятся не дольше, чем этого требуют цели их обработки, и подлежат уничтожению по истечении срока хранения, достижении целей обработки или в случае утраты необходимости в их достижении.

3.2. Носители, содержащие персональные данные субъектов персональных данных, уничтожаются комиссией по уничтожению персональных данных, утвержденной приказом директора ГБУ ДПО РА «АРИПК» (далее – Комиссия).

3.3. Носители, содержащие персональные данные субъектов персональных данных, уничтожаются Комиссией в срок, не превышающий 10 дней с даты достижения целей обработки персональных данных либо утраты необходимости в их достижении, а также в случае, если истек срок их хранения.

3.4. Комиссия производит отбор бумажных носителей персональных данных, подлежащих уничтожению, с указанием оснований для уничтожения.

3.5. На все отобранные к уничтожению документы составляется акт о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению.

3.6. В актах о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению и актах об уничтожении носителей, содержащих персональные данные субъектов персональных данных, исправления не допускаются.

3.7. Комиссия проверяет наличие всех документов, включенных в акт о выделении носителей, содержащих персональные данные субъектов персональных данных, к уничтожению.

3.8. По окончании сверки акт о выделении документов, содержащих персональные

данные субъектов персональных данных, к уничтожению подписывается всеми членами Комиссии и утверждается директором.

3.9. Носители, содержащие персональные данные субъектов персональных данных, отобранные для уничтожения и включенные в акт, после проверки их Комиссией передаются ответственному за уничтожение документов в помещение отдела документального и кадрового обеспечения.

3.10. Уничтожение носителей, содержащих персональные данные субъектов персональных данных, производится после утверждения акта в присутствии всех членов Комиссии, которые несут персональную ответственность за правильность и полноту уничтожения перечисленных в акте носителей.

3.11. Уничтожение 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).

3.12. Уничтожение носителей, содержащих персональные данные, осуществляется в следующем порядке:

- уничтожение персональных данных, содержащихся на бумажных носителях, осуществляется путем измельчения на мелкие части, исключающие возможность последующего восстановления информации. Измельчение осуществляется с использованием shreddera (уничтожителя документов), установленного в помещении отдела документального и кадрового обеспечения, либо документы передаются на переработку (утилизацию) организациям, собирающим вторсырье (пункты приема макулатуры);

- уничтожение персональных данных, содержащихся на машиночитаемых носителях, осуществляется путем нанесения им неустраняемого физического повреждения, исключающего возможность их использования, а также восстановления данных. Вышеуказанное достигается путем деформирования, нарушения единой целостности носителя;

- подлежащие уничтожению файлы с персональными данными субъектов персональных данных, расположенные на жестком диске, удаляются средствами операционной системы компьютера с последующим «очищением корзины»;

- в случае допустимости повторного использования носителя CD-RW, DVD-RW применяется программное удаление («затирание») содержимого диска путем его форматирования с последующей записью новой информации на данный носитель.

4. Порядок сдачи макулатуры

4.1. Документы по истечении срока хранения, достижении целей обработки или в случае утраты необходимости в их достижении подлежат уничтожению путем сдачи организациям, собирающим вторсырье (пункты приема макулатуры).

4.2. Выделенные документы по акту о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению передаются к уничтожению в упакованном виде.

4.3. Документы, подлежащие вывозу, не должны содержать бумагу и картон, не пригодные для переработки; бумагу и картон, покрытые полиэтиленом и другими полимерными пленками; материал, выделяющий ядовитые и токсичные вещества.

4.4. Документы, подлежащие вывозу, не должны содержать:

- тряпье, веревку, шпагат из лубяных волокон и полимеров;
- металлические и деревянные изделия, кусочки стекла и керамики, камень, уголь, слюду, целлофан, целлулоид, полимерные материалы в виде изделий (пленок, гранул), пенопласт, искусственную и натуральную кожу, клеенку, битум, парафин, остатки химических и минеральных веществ и красок;

- влажность документов, подлежащая вывозу, должна быть не более 10 процентов.

4.5. Сдача оформляется приемо-сдаточными накладными, данные которых (дата сдачи, номер накладной, вес сданной макулатуры) указываются в акте о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению.

4.6. Погрузка и вывоз документов осуществляются под контролем лица, ответственного за обеспечение сохранности документов структурного подразделения.

4.7. Отобранные к уничтожению документы перед сдачей на переработку в качестве макулатуры должны в обязательном порядке измельчаться до степени, исключающей возможность прочтения текста.

5. Порядок оформления документов об уничтожении персональных данных

5.1. Об уничтожении носителей, содержащих персональные данные, Комиссия составляет и подписывает акт об уничтожении носителей, содержащих персональные данные субъектов персональных данных, который утверждается директором Общества.

5.2. Акт об уничтожении носителей, содержащих персональные данные субъектов персональных данных, составляется по установленной форме.

В акте указываются:

- дата, место и время уничтожения;
- должности, фамилии, инициалы членов Комиссии;
- вид и количество уничтожаемых носителей, содержащих персональные данные субъектов персональных данных;
- основание для уничтожения;
- способ уничтожения.

5.3. Факт уничтожения носителей, содержащих персональные данные субъектов персональных данных, фиксируется в журнале учета документов, переданных на уничтожение. Данный документ является документом конфиденциального характера и вместе с актами хранится в помещении отдела документального и кадрового обеспечения в течение одного года. По истечении срока хранения акт о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению и акт об уничтожении носителей, содержащих персональные данные субъектов персональных данных, передаются в архив ГБУ ДПО РА «АРИПК» на хранение.

6. Ответственность руководителей структурных подразделений

6.1. Ответственным лицом за организацию хранения документов является начальник отдела документального и кадрового обеспечения.

Акт об уничтожении персональных данных

Комиссия, наделенная полномочиями приказом в ГБУ ДПО «АРИПК» от г. № -од, в составе:

Председатель комиссии - Нагоева Джанцир Умаровна, заместитель директора по УРиОКО.

Члены комиссии:

- Праток Саният Мадиновна, начальник отдела документального и кадрового обеспечения;
- Индрисова Роза Азметовна, начальник ОПиОУД;
- Нагорокова Залина Ауэсовна, заведующий кафедрой;
- Говорова Татьяна Владимировна, архивариус

составила настоящий Акт о том, что информация, зафиксированная на перечисленных в нем носителях информации (электронных, бумажных), подлежит уничтожению путем измельчения и стирания с электронных носителей.

Вид материального носителя персональных данных	Причина уничтожения носителя информации; стирания/обезличивания информации	Тип носителя информации	Производимая операция (стирание, уничтожение, обезличивание)	Дата	Примечание
1	2	3	4	5	6

Правильность произведенных записей в акте проверена.

Возможность дальнейшего использования персональных данных или их восстановления исключена.

Отметки о стирании информации (уничтожении носителей информации) в учетных формах произведены.

(Ф.И.О., подпись, дата)

(Ф.И.О., подпись, дата)(Ф.И.О., подпись, дата)

С приказом ознакомлены:

СОГЛАСИЕ
на обработку персональных данных слушателей

Я (далее – **Субъект**), _____
(фамилия, имя, отчество)
документ, удостоверяющий личность _____ серия _____ № _____
(вид документа)
выдан _____
(кем и когда)

зарегистрированный (ая) по адресу: _____,
даю свое согласие

ГБУ ДПО РА «Адыгейский республиканский институт повышения квалификации» (далее – **Оператор**)

юридический адрес: Российская Федерация, 3875000, Республика Адыгея, г. Майкоп, ул. Ленина д. 15.

на обработку моих персональных данных, на следующих условиях:

1. Оператор осуществляет обработку персональных данных Субъекта исключительно в целях:
 - приёма, обучения и выпуска слушателей по программам повышения квалификации/переподготовки (далее – Курсы) в соответствии с федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» и Уставом Оператора;
 - ведения учёта личных дел слушателей Курсов, а также хранение личных дел в архиве на бумажных и/или электронных носителях, в автоматизированных системах обработки данных;
 - ведения учёта результатов освоения слушателями Курсов по образовательным программам, а также хранение архивов данных об этих результатах на бумажных носителях и/или электронных носителях, в автоматизированных системах обработки данных;
 - выдачи удостоверений/дипломов о повышении квалификации/переподготовке;
 - выдачи справок по запросу Субъекта, работодателей, органов государственного управления и иных сведений в соответствии с законодательством РФ;
 - планирования, организации, регулирования и контроля деятельности образовательного учреждения в целях осуществления государственной политики в области образования;
 - восстановления и выдачи дубликатов документов, подтверждающих образование, в случае их утери.
2. Перечень персональных данных, передаваемых Оператору на обработку:
 - фамилия, имя, отчество;
 - дата рождения (число, месяц, год рождения);
 - место рождения;
 - адрес регистрации (прописки);
 - телефонный номер (мобильный);
 - информация о трудовой деятельности (место работы, должность, период работы, трудовой стаж);
 - информация об образовании (уровень, специальность, профессия, квалификация, наименование образовательного учреждения, форма обучения, дата окончания, сведения о документах, подтверждающих образование: наименование, серия, номер, дата выдачи);
 - информация о месте обучения (программа профессиональной переподготовки, цикл специализации и/или усовершенствования;
 - СНИЛС;
 - e-mail.

3. Субъект дает согласие на обработку Оператором своих персональных данных, в том числе на совершение следующих действий: обработку (включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение персональных данных), а также на передачу такой информации третьим лицам, в случаях:

- обеспечения учебного процесса и выдачи удостоверений/дипломов;
- установленных нормативными документами вышестоящих органов и законодательством РФ.

4. Настоящее согласие действует в течение срока хранения документов, установленных действующим законодательством.

5. Настоящее согласие может быть отозвано Субъектом в любой момент на основании письменного сообщения в произвольной форме, если иное не установлено законодательством РФ.

6. Субъект по письменному запросу имеет право на получение информации, касающейся обработки его персональных данных (в соответствии с п.4 ст.14 Федерального закона от 27.06.2006 № 152-ФЗ) «О персональных данных».

Субъект персональных данных:

на обработку моих персональных данных _____
согласен (согласна) / не согласен (не согласна)

« ____ » _____ 20 ____ г.

Подпись ФИО

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ
работников Государственного бюджетного учреждения дополнительного профессионального образования
республики Адыгея «Адыгейский республиканский институт повышения квалификации»

Я, субъект персональных данных

(ФИО)

зарегистрирован/а

(адрес)

(серия и номер документа, удостоверяющего личность, кем и когда выдан)

в соответствии с Федеральным законом №152-ФЗ «О персональных данных» свободно, в своей воле и в своем интересе даю согласие ГБУ ДПО РА «АРИПК», расположенному по адресу: 385000, г Майкоп, ул.Ленина, д.15, на обработку со следующими условиями:

1. Данное Согласие дается на обработку персональных данных, как без использования средств автоматизации, так и с их использованием.
2. Согласие дается на обработку следующих моих персональных данных:
 - фамилия, имя, отчество (в т.ч. прежние), дата и место рождения;
 - паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ);
 - сведения о гражданстве;
 - адрес и дата регистрации по месту жительства или по месту пребывания;
 - сведения из разрешения на временное проживание;
 - сведения из заключений медицинских организаций о прохождении предварительного/периодического осмотра;
 - номера телефонов, в случае их регистрации на субъекта персональных данных или по адресу его места жительства;
 - адрес электронной почты;
 - сведения об образовании, квалификации и о наличии ученой степени, ученого звания, специальных знаний или специальной подготовки;
 - сведения о повышении квалификации и переподготовке;
 - сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, организации и ее наименования, ИНН, адреса и телефонов, а также реквизитов других организаций с полным наименованием занимаемых ранее в них должностей и времени работы в этих организациях, о стаже работы, об опыте работы, а также другие сведения);
 - сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней;
 - содержание и реквизиты трудового договора с работником университета или гражданско-правового договора с гражданином;
 - сведения о заработной плате (в том числе номера счетов для расчета с работниками, данные зарплатных договоров с клиентами, данные по окладу, надбавкам, налогам и другие сведения);
 - сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер подтверждающего регистрацию в системе индивидуального (персонифицированного учета, дата выдачи, наименование органа, выдавшего военный билет, военно-учетная специальность, воинское звание, данные о принятии/снятии на(с) учет(а) и другие сведения);
 - сведения о семейном положении (состояние в браке, данные свидетельства о заключении брака, фамилия, имя, отчество супруга(и), паспортные данные супруга(и), данные справки по форме 2-НДФЛ супруга(и), степень родства, фамилии, имена, отчества и даты рождения других членов семьи, иждивенцев и другие сведения);
 - сведения о номере и серии страхового свидетельства обязательного

пенсионного страхования;

- сведения об идентификационном номере налогоплательщика;
- сведения из страхового полиса обязательного (добровольного) медицинского медицинского страхования;
- сведения о государственных и ведомственных наградах, почетных и специальных званиях, поощрениях (в том числе наименование и название награды, звания или поощрения, дата и вид нормативного акта о награждении или дата поощрения) работников университета;

- материалы по внутренним служебным расследованиям в отношении работников АРИПК;

- внутренние материалы по расследованию и учету несчастных случаев на производстве и профессиональным заболеваниям в соответствии с Трудовым кодексом Российской Федерации, другими федеральными законами;

- сведения о временной нетрудоспособности работников АРИПК;
- сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса) и другие сведения, связанные с предоставлением социальных льгот и гарантий;

- биометрические сведения, к которым относятся физиологические данные, а также иные физиологические или биологические характеристики человека, в том числе изображения (фотографии, видеозаписи систем контроля доступа), которые позволяют установить личность.

3. Цель обработки персональных данных - исполнение заключенного трудового договора и выполнения возложенных законодательством на стороны трудового договора обязанностей.

4. Основанием для обработки персональных данных является: прием на работу.

5. В ходе обработки с персональными данными будут совершены действия по обработке, передаче в соответствующие органы и хранению персональных данных.

6. Условия обработки Исполнителем персональных данных работников:

- исполнитель по поручению в целях расчета заработной платы, пособий и иных выплат, а также составления и сдачи отчетности в органы ФНС России и внебюджетные фонды совершает все необходимые действия по обработке персональных данных работников.

- исполнитель обязуется соблюдать конфиденциальность полученных при исполнении настоящего договора персональных данных и обеспечивать их безопасность при обработке, принимая все необходимые меры в соответствии с требованиями действующего законодательства.

- по окончании действия настоящего договора Исполнитель обязуется прекратить обработку персональных данных работника, передав ему всю подготовленную во исполнение договора документацию, содержащую такие данные, и удалив их из своих электронных баз данных. Настоящее согласие действует в течение всего срока действия трудового договора и может быть отозвано в письменном виде.

Согласие может быть отозвано субъектом персональных данных или его представителем путем направления письменного заявления в ГБУ ДПО РА «АРИПК», расположенному по адресу: 385000, г Майкоп, ул. Ленина, д.15.

В случае отзыва субъектом персональных данных или его представителем согласия на обработку персональных данных ГБУ ДПО РА «АРИПК» вправе продолжить обработку персональных данных без согласия субъекта персональных данных только при наличии оснований, указанных в п. 2 – 11 ч. 1 ст. 6, ч. 2 ст. 10 и ч. 2 ст. 11 Федерального закона №152-ФЗ «О персональных данных».

«__» _____ 20__ г.

/

(ФИО)

(подпись)

