МИНОБРНАУКИ России

Федеральное государственное бюджетное учреждение науки
«Крымская астрофизическая обсерватория РАН»

(ФГБУН «КрАО РАН»)

ПРИКАЗ

« 29 » сентября 2023 г. № 90

пгт. Научный Бахчисарайского района, Республика Крым

О персональных данных

С целью приведения в соответствие требованиям Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» обработки и защиты персональных данных в ФГБУН «КрАО РАН»

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие:
   - Положение об обработке персональных данных (Приложение 1);
   - Политику в отношении обработки персональных данных (Приложение 2);
   - Перечень обрабатываемых персональных данных (Приложение 3);
   - Перечень должностей, замещение которых требует в соответствии с должностной инструкцией доступа к персональным данным (Приложение 4);
   - Перечень должностных лиц, допущенных к обработке персональных данных (Приложение 5);
   - Перечень информационных систем персональных данных (ИСПДн) (Приложение 6);
   - Систему разграничения доступа к ресурсам ИСПДн (Приложение 7);
   - План внутреннего контроля соблюдения законодательства и локальных нормативных актов в области персональных данных (Приложение 8);

2. Автоматизированную обработку персональных данных осуществлять исключительно в ИСПДн. При обработке и защите персональных данных должностным лицам руководствоваться:
   - Инструкцией пользователя ИСПДн;
   - Инструкцией по осуществлению парольной защиты;
   - Инструкцией по осуществлению антивирусного контроля;
   - Инструкция по учету машинных носителей персональных данных;
   - Инструкцией по резервированию и восстановлению персональных данных;
   - Инструкцией администратора безопасности ИСПДн.

3. Обработку персональных данных без использования средств автоматизации и их хранение осуществлять в соответствии с Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным Постановлением Правительства от 15 сентября 2008 № 687.

4. По достижении целей обработки персональных данных или в случае утраты необходимости в достижении целей обработки персональных данных при условии отсутствия законных оснований для продолжения обработки персональных данных

прекратить обработку таких персональных данных и уничтожить их в тридцатидневный срок, о чем составить соответствующий акт.

5. Обращения субъектов персональных данных об исполнении их законных прав регистрировать в журнале учета обращений.

6. Отделу кадров (начальник Семенова А.С.):
- внести дополнения в должностные инструкции работников, допущенных к обработке персональных данных, ответственного за организацию обработки персональных данных, администратора безопасности;
- подписать обязательство о неразглашении персональных данных с работниками, допущенными к обработке персональных данных и ранее не подписывавшими данное обязательство
- при замещении должностей в перечне (приложение 4) вносить вновь принятых сотрудников в список (приложение 5) и получать от них обязательство о неразглашении персональных данных;
- ежегодно, до 15 января, обновлять списки (приложение 5).

7. Ведущему юрисконсульту ПИТКЕВИЧ Денису Николаевичу ежегодно знакомить сотрудников, непосредственно осуществляющих обработку персональных данных (приложение 5), с положениями законодательства Российской Федерации о персональных данных, с документами ФГБУН КрАО «РАН», определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

8. Утвердить и ввести в действие план работ по внутреннему контролю соблюдения законодательства и локальных актов в области персональных данных.

9. Приказ от 30.03.2023 № 32 и от 31.03.2023 № 34 считать утратившими силу

10. Контроль за исполнением настоящего приказа оставляю за собой.

Директор А.Н. Ростопчина-Шаховская

Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное учреждение науки
«КРЫМСКАЯ АСТРОФИЗИЧЕСКАЯ ОБСЕРВАТОРИЯ РАН»
(ФГБУН «КрАО РАН»)

Приложение 1

УТВЕРЖДЕНО
Приказом директора
ФГБУН «КрАО РАН»
от 29.09.2023 № 90

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
в ФГБУН «КрАО РАН»

пгт. Научный 2023

Положение
об обработке и защите персональных данных
в ФГБУН «КрАО РАН»

1. Общие положения

1.1. Настоящее Положение устанавливает порядок получения, учета, обработки и защиты персональных данных федерального государственного бюджетного учреждения науки «Крымская астрофизическая обсерватория РАН» (далее – КрАО РАН, Работодатель) с целью обеспечения защиты прав и свобод физических лиц при обработке их персональных данных, а также установления ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований законодательства и локальных актов в области персональных данных.

1.2. Основанием для разработки настоящего Положения являются Конституция Российской Федерации, Трудовой кодекс Российской Федерации, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», 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», Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и другие действующие нормативные правовые акты Российской Федерации.

1.3. Настоящее Положение и изменения к нему утверждаются руководителем Работодателя и вводятся приказом. Все работники должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

1.4. Настоящее Положение является обязательным для исполнения всеми работниками ФГБУН «КрАО РАН», которые имеют или могут получить доступ к персональным данным в связи с исполнением служебных обязанностей.

1.5. Персональные данные относятся к категории конфиденциальной информации и должны быть защищены от несанкционированного, в том числе случайного, доступа к ним.

Режим конфиденциальности персональных данных снимается в случаях их обезличивания, по истечении срока их хранения, либо продлевается на основании заключения комиссии ФГБУН «КрАО РАН», если иное не предусмотрено законодательством.

2. Основные понятия в области персональных данных и состав персональных данных

2.1. Под персональными данными понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу, в том числе:

- фамилия, имя, отчество;
- дата и место рождения;
- адрес регистрации, место проживания;

- семейное, социальное, имущественное положение;
- образование, профессия, доходы;
- любая другая информация.

2.2. В настоящем Положении используются следующие понятия:

Оператор персональных данных – юридическое лицо самостоятельно или совместно с третьими лицами организующие и осуществляющие обработку персональных данных, а также определяющие цели обработки, состав персональных данных и действия с ними;

Субъект персональных данных – физическое лицо, персональные данные которого обрабатываются оператором персональных данных.

Работники – лица, заключившие трудовой договор с Работодателем.

Обработка персональных данных – любое действие, совершаемое с персональными данными, в том числе сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

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

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

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.3. Персональными данными, разрешенными субъектом персональных данных для распространения, являются персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

2.3. Состав персональных данных работника:

- фамилия, имя, отчество;
- пол, возраст;
- год, месяц, дата и место рождения, а также иные данные, содержащиеся в удостоверении личности работника;
- сведения об образовании, квалификации, профессиональной подготовке,

повышении квалификации;

- место жительства;
- семейное положение, наличие детей, состав семьи, родственные связи;
- данные медицинского характера, в случаях, предусмотренных законодательством;
- факты биографии и предыдущая трудовая деятельность (в том числе место работы, судимость, служба в армии, работа на выборных должностях, на государственной службе и др.);
- данные о месте жительства, почтовый адрес, телефон работника, а также членов его семьи;
- финансовое положение, сведения о заработной плате;
- паспортные данные;
- сведения о воинском учете;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- размер заработной платы;
- наличие судимостей;
- содержание трудового договора;
- подлинники и копии приказов по личному составу;
- личные дела, трудовые книжки и сведения о трудовой деятельности;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемых в органы статистики;
- сведения о результатах медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- фотографии и иные сведения, относящиеся к персональным данным работника;
- принадлежность лица к конкретной нации, этнической группе, расе;
- религиозные и политические убеждения (принадлежность к религиозной конфессии, членство в политической партии, участие в общественных объединениях, в том числе в профсоюзе, и др.);
- деловые и иные личные качества, которые носят оценочный характер;
- иные персональные данные, при определении объема и содержания которых работодатель руководствуется настоящим Положением и законодательством РФ.

Из указанного списка Работодатель вправе получать и использовать только те сведения, которые характеризуют гражданина как сторону трудового договора.

2.4. Сведения, указанные в п. 2.3 настоящего Положения, и документы, их содержащие, являются конфиденциальными. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 50 лет срока хранения, если иное не определено законом.

2.5. Документами, содержащими персональные данные работников, являются:

- комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении;
- комплекс материалов по анкетированию, тестированию, проведению собеседований с кандидатом на должность;

- подлинники и копии приказов (распоряжений) по кадрам;
- личные дела, трудовые книжки, сведения о трудовой деятельности работников;
- дела, содержащие материалы аттестаций работников;
- дела, содержащие материалы внутренних расследований;
- справочно-информационный банк данных по персоналу (картотеки, журналы);
- копии отчетов, направляемых в государственные контролирующие органы.

2.6. Перечень персональных данных, обрабатываемых в ФГБУН «КрАО РАН» в связи с деятельностью внебюджетных подразделений, утверждается отдельным локальным нормативным актом.

3. Обязанности Работодателя

3.1. В целях обеспечения прав и свобод человека и гражданина Работодатель и его представители при обработке персональных данных субъекта персональных данных обязаны соблюдать следующие общие требования:

3.1.1. Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия субъекту персональных данных в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы, оплаты труда, пользования льготами, предусмотренными законодательством РФ и актами работодателя, обеспечения сохранности имущества.

3.1.2. При определении объема и содержания обрабатываемых персональных данных Работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.

3.1.3. 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.

3.1.4. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена Работодателем за счет его средств в порядке, установленном федеральным законом.

3.1.5. Работники и их представители должны быть ознакомлены под подпись с локальными актами Работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

3.1.6. Работники не должны отказываться от своих прав на сохранение и защиту тайны.

3.2. ***Сбор персональных данных.***

3.2.1. Персональные данные следует получать непосредственно у самого субъекта персональных данных. Если предоставление персональных данных является обязательным в соответствии с законодательством, субъекту персональных данных должны быть разъяснены юридические последствия отказа в предоставлении таких

данных.

3.2.2. Получение персональных данных у третьей стороны возможно только при наличии законных оснований. При получении персональных данных у третьей стороны необходимо уведомить об этом субъекта. В этом случае субъекту персональных данных сообщаются сведения о цели обработки его персональных данных, правовое основание обработки, права субъекта, предполагаемые пользователи персональных данных, а также источник их получения.

3.2.3. Работодатель не имеет права получать и обрабатывать персональные данные субъекта персональных данных (работника) о его расовой, национальной принадлежности, политических, религиозных и иных убеждениях, частной жизни, состоянии здоровья, за исключением случаев, предусмотренных Трудовым кодексом Российской Федерации и другими федеральными законами. В случаях, непосредственно связанных с вопросами трудовых отношений или договорных обязательств, в соответствии со ст. 24 Конституции Российской Федерации они могут быть получены и обработаны только с письменного согласия самого субъекта или его законного представителя.

3.2.4. Работодатель не имеет права получать и обрабатывать персональные данные субъекта персональных данных (работника) о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

3.2.5. Работник представляет Работодателю достоверные сведения о себе. Работодатель проверяет достоверность сведений, сверяя данные, представленные работником, с имеющимися у работника документами. Представление работником подложных документов или ложных сведений при поступлении на работу является основанием для расторжения трудового договора.

3.2.6. При поступлении на работу работник заполняет анкету и автобиографию (на определенные должности).

3.2.7. Анкета представляет собой перечень вопросов о персональных данных работника.

Анкета заполняется работником самостоятельно. При заполнении анкеты работник должен заполнять все ее графы, на все вопросы давать полные ответы, не допускать исправлений или зачеркиваний, прочерков, помарок в строгом соответствии с записями, которые содержатся в его личных документах.

3.2.8. Автобиография - документ, содержащий описание в хронологической последовательности основных этапов жизни и деятельности принимаемого работника. Автобиография составляется в произвольной форме, без помарок и исправлений.

3.2.9. Анкета и автобиография работника должны храниться в личном деле работника. В личном деле также хранятся иные документы персонального учета, относящиеся к персональным данным работника.

3.2.10. Личное дело работника оформляется после издания приказа о приеме на работу.

Все документы личного дела подшиваются в обложку образца, установленного Работодателем. На ней указываются фамилия, имя, отчество работника, номер личного дела.

К каждому личному делу прилагаются две цветные фотографии работника размером 4х6.

Все документы, поступающие в личное дело, располагаются в хронологическом порядке. Листы документов, подшитых в личное дело, нумеруются.

Личное дело ведется на протяжении всей трудовой деятельности работника. Изменения, вносимые в личное дело, должны быть подтверждены соответствующими документами.

3.3. ***Обработка персональных данных.***

3.3.1. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных работника.

3.3.2. Обработка персональных данных возможна в следующих случаях:

- получено согласие субъекта на обработку его персональных данных;
- обработка персональных данных необходима для осуществления и выполнения возложенных законодательством РФ на оператора функций, полномочий и обязанностей;
- обработка персональных данных необходима для исполнения договора, стороной которого является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта;
- обработка персональных данных осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных;
- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (общедоступные персональные данные);
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством.

3.3.2. Обработка персональных данных может осуществляться исключительно в целях соблюдения законов и нормативных правовых актов Российской Федерации, заключения договоров и исполнения договорных обязательств.

3.3.3. Обработку персональных данных могут осуществлять только работники оператора, допущенные руководством в установленном порядке. Лица, получившие доступ к персональным данным, должны быть предупреждены о факте обработки ими

таких данных.

3.3.4. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда, затруднения реализации прав и свобод граждан.

3.3.5. Обработка персональных данных, разрешенных для распространения, из числа специальных категорий персональных данных, указанных в ч. 1 ст. 10 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных", допускается, если соблюдаются запреты и условия, предусмотренные ст. 10.1 указанного Закона.

3.3.6. Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами.

3.3.7. Обработка персональных данных субъекта Работодателем возможна только с его согласия. Исключение составляют случаи, предусмотренные законодательством Российской Федерации (в частности, согласие не требуется при наличии оснований и соблюдении условий, перечисленных в п. п. 2 - 11 ч. 1 ст. 6, п. п. 2.1 - 10 ч. 2 ст. 10, ч. 2 ст. 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»).

3.3.8. Письменное согласие субъекта на обработку своих персональных данных должно включать в себя, в частности, сведения, указанные в п. п. 1 - 9 ч. 4 ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

3.3.9. Письменное согласие субъекта на обработку персональных данных, разрешенных для распространения, оформляется отдельно от других согласий на обработку его персональных данных. При этом соблюдаются условия, предусмотренные, в частности, ст. 10.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Требования к содержанию такого согласия устанавливаются уполномоченным органом по защите прав субъектов персональных данных.

3.3.10. Письменное согласие на обработку персональных данных, разрешенных для распространения, субъект предоставляет Работодателю лично.

Работодатель обязан не позднее трех рабочих дней с момента получения указанного согласия опубликовать информацию об условиях обработки, о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных для распространения.

Согласие на обработку персональных данных, разрешенных для распространения, прекращает свое действие с момента поступления Работодателю требования, указанного в п. 5.2.7. настоящего Положения.

3.3.11. В соответствии со ст. 86 Трудового кодекса Российской Федерации в целях обеспечения прав и свобод человека и гражданина Работодатель и его представители при обработке персональных данных субъекта персональных данных должны соблюдать, в частности, следующие общие требования:

- при определении объема и содержания обрабатываемых персональных данных субъекта 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, полученных исключительно в результате их автоматизированной обработки или электронного получения;

- защита персональных данных работника от неправомерного их использования, утраты обеспечивается Работодателем за счет его средств в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами.

- работники и их представители должны быть ознакомлены под подписку с документами Работодателя, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

- работники не должны отказываться от своих прав на сохранение и защиту тайны.

3.4. ***Хранение персональных данных.***

3.4.1. Персональные данные хранятся в пределах установленных помещений на материальных (бумажных) носителях или в электронном виде (в информационных системах персональных данных, на машинных носителях). Машинные носители информации (диски, дискеты, флеш-накопители) должны быть учтены в соответствии с Инструкцией по учету машинных носителей персональных данных.

3.4.2. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен законодательством либо договором, стороной которого является субъект персональных данных.

3.4.3. Хранение персональных данных должно осуществляться с учетом обеспечения режима их конфиденциальности.

3.4.4. Персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством.

3.5. ***Передача и распространение персональных данных.***

3.5.1. Передача персональных данных третьему лицу возможна только с письменного согласия субъекта персональных данных за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, прямо предусмотренных законодательством.

3.5.2. Не допускается сообщать персональные данные третьему лицу без письменного согласия соответствующего субъекта, за исключением случаев, когда это необходимо для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных.

3.5.3. Вне зависимости от наличия согласия субъекта, не допускается раскрытие сведений о субъекте, его задолженности и любых других персональных данных неограниченному кругу лиц, в том числе путем размещения таких сведений в сети Интернет или в (на) жилом помещении, доме, любом другом здании, строении, сооружении, а также сообщении по месту работы субъекта.

3.5.4. Запрещено сообщать персональные данные третьему лицу в коммерческих целях без письменного согласия соответствующего субъекта. Обработка персональных данных в целях политической агитации возможна только при условии предварительного согласия на это субъекта.

3.5.5. При передаче персональных данных работника Работодатель должен соблюдать следующие требования:

- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать конфиденциальность. Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

- 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 конкретных функций;

- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

- 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 функций.

3.6. ***Доступ к персональным данным***

3.6.1. Право доступа к персональным данным, обрабатываемым в ФГБУН «КрАО РАН», имеют:

- директор ФГБУН «КрАО РАН»;
- заместители директора ФГБУН «КрАО РАН»;
- руководитель отдела кадров;
- руководители структурных подразделений по направлению деятельности (доступ к личным данным только работников своего подразделения) по согласованию с руководителем Работодателя;
- при переводе из одного структурного подразделения в другое доступ к персональным данным работника может иметь руководитель нового подразделения по согласованию с руководителем Работодателя;
- работники бухгалтерии, отдела кадров, ПЭО, ученый секретарь, сотрудники Работодателя, на которых возложены определенные функции (охрана труда, защита информации, гражданская оборона и т.п.) - к тем данным, которые необходимы для выполнения конкретных функций;
- другие работники ФГБУН «КрАО РАН», для которых обработка персональных данных необходима в связи с исполнением их должностных обязанностей. Допуск работников к персональным данным осуществляется руководством в установленном порядке;
- сам работник, носитель данных.

3.6.2. Любой субъект, персональные данные которого обрабатываются в ФГБУН «КрАО РАН», имеет право доступа к своим персональным данным, в том числе к следующей информации:

- подтверждение факта обработки его персональных данных;
- правовые основания и цели обработки его персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах, которые имеют доступ к персональным данным (за исключением работников оператора) или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании законодательства;
- перечень обрабатываемых персональных данных, относящиеся к соответствующему субъекту, и источник их получения;
- сроки обработки персональных данных и сроки их хранения;
- порядок осуществления субъектом прав, предусмотренных законодательством;
- наименование лица, осуществляющего обработку персональных данных по поручению оператора, в случае если обработка поручена третьему лицу.

3.6.3. Работодатель вправе осуществлять передачу персональных данных работника третьим лицам, в том числе в коммерческих целях, только с его предварительного письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных действующим законодательством Российской Федерации.

Перед передачей персональных данных Работодатель должен предупредить третье лицо о том, что они могут быть использованы только в тех целях, для которых были сообщены. При этом у третьего лица необходимо получить подтверждение того, что такое требование будет им соблюдено.

Не требуется согласие работника на передачу персональных данных:

- третьим лицам в целях предупреждения угрозы жизни и здоровью работника;
- в Социальный фонд России в объеме, предусмотренном действующим законодательством Российской Федерации;
- в налоговые органы;
- в военные комиссариаты;
- по запросу профессиональных союзов в целях контроля за соблюдением трудового законодательства Работодателем;
- по мотивированному запросу органов прокуратуры;
- по мотивированному требованию правоохранительных органов и органов безопасности;
- по запросу от государственных инспекторов труда при осуществлении ими надзорно-контрольной деятельности;
- по запросу суда;
- в органы и организации, которые должны быть уведомлены о тяжелом несчастном случае, в том числе со смертельным исходом;
- в случаях, связанных с исполнением работником должностных обязанностей;
- в кредитную организацию, обслуживающую платежные карты работников.

3.6.4. Сведения о работнике (в том числе уволенном) могут быть предоставлены другой организации только с письменного запроса на бланке организации с приложением

копии заявления работника.

3.6.5. Персональные данные работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого работника.

3.7. ***Защита персональных данных***

3.7.1. При обработке персональных данных принимаются необходимые правовые, организационные и технические меры для 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.

3.7.2. В целях обеспечения безопасности персональных данных в ФГБУН «КрАО РАН» осуществляются следующие мероприятия:

- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах, которые обеспечивают выполнение требований к установленным уровням защищенности;
- применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;
- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных;
- учет машинных носителей персональных данных;
- обнаружение фактов несанкционированного доступа к персональным данным и реагирование на данные инциденты;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных;
- регистрация и учет действий, совершаемых с персональными данными в информационных системах персональных данных;
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных в соответствии с установленным уровнем защищенности персональных данных.

3.7.3. В целях обеспечения сохранности и конфиденциальности персональных данных все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться только работниками отдела кадров, бухгалтерии и другими сотрудниками Работодателя, на которых возложены определенные обязанности, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях.

3.7.4. Общую организацию защиты персональных данных работников осуществляет назначенное приказом (распоряжением) по организации лицо.

3.7.5. Непосредственную организацию защиты персональных данных осуществляет начальник отдела кадров. Начальник отдела кадров обеспечивает:

- ознакомление сотрудника под роспись с настоящим Положением. При наличии иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и защиту персональных данных работника, с данными актами также производится ознакомление сотрудников, имеющих доступ к персональным данным, под подпись;

- истребование с сотрудников, имеющих доступ к персональным данным, письменного обязательства о соблюдении конфиденциальности персональных данных и соблюдении правил их обработки;

- общий контроль за соблюдением сотрудниками работодателя, имеющими доступ к персональным данным, мер по защите персональных данных.

3.7.6. Организацию и контроль за защитой персональных данных субъектов персональных данных в структурных подразделениях работодателя, сотрудники которых имеют доступ к персональным данным, осуществляют их непосредственные руководители.

3.7.7. Защите подлежит:

- информация о персональных данных;
- документы, содержащие персональные данные;
- персональные данные, содержащиеся на электронных носителях.

3.7.8. Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной форме на бланке Работодателя и в том объеме, который позволяет не разглашать излишний объем персональных данных.

3.7.9. Передача информации, содержащей сведения о персональных данных, по телефону, факсу, электронной почте без письменного согласия субъекта персональных данных запрещается.

3.7.10. Личные дела и документы, содержащие персональные данные, хранятся в запирающихся шкафах (сейфах), обеспечивающих защиту от несанкционированного доступа.

3.7.11. Персональные данные работника в отделе кадров и бухгалтерии хранятся также в электронном виде в локальной компьютерной сети. Доступ к электронным базам данных, содержащим персональные данные работников, обеспечиваются системой паролей. Пароли устанавливаются сотрудником, имеющим доступ к персональным данным работников, и не подлежат разглашению.

3.7.12. Хранение персональных данных в иных структурных подразделениях работодателя, сотрудники которых имеют право доступа к персональным данным, осуществляется в порядке, исключающим к ним доступ третьих лиц.

3.7.13. Персональные компьютеры, в которых содержатся персональные данные, должны быть защищены паролями доступа. Защита сведений, хранящихся в электронных базах данных Работодателя, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий, обеспечивается разграничением прав доступа с использованием учетной записи и системы паролей.

3.7.14. Сотрудник работодателя, имеющий доступ к персональным данным в связи с исполнением трудовых обязанностей:

- обеспечивает хранение информации, содержащей персональные данные, исключающее доступ к ним третьих лиц. В отсутствие сотрудника на его рабочем месте не должно быть документов, содержащих персональные данные (соблюдение "политики чистых столов").

- при уходе в отпуск, служебной командировке и иных случаях длительного отсутствия работника на своем рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные работников лицу, на которое локальным актом Организации (приказом, распоряжением) будет возложено исполнение его трудовых обязанностей. В случае если такое лицо не назначено, то документы и иные носители, содержащие персональные данные, передаются другому сотруднику, имеющему доступ к персональным данным по указанию руководителя структурного подразделения.

При увольнении сотрудника, имеющего доступ к персональным данным, документы и иные носители, содержащие персональные данные, передаются другому сотруднику, имеющему доступ к персональным данным, по указанию руководителя структурного подразделения.

3.7.15. Доступ к персональным данным работника имеют сотрудники работодателя, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей.

3.7.16. В случае если работодателю оказывают услуги юридические и физические лица на основании заключенных договоров (либо иных оснований) и в силу данных договоров они должны иметь доступ к персональным данным работников, то соответствующие данные предоставляются работодателем только после подписания с ними соглашения о неразглашении конфиденциальной информации либо при наличии в договорах пунктов о неразглашении конфиденциальной информации, в том числе предусматривающих защиту персональных данных работника.

3.7.17. Процедура оформления доступа к персональным данным включает в себя:

- ознакомление работника под роспись с настоящим Положением. При наличии иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и защиту персональных данных работника, с данными актами также производится ознакомление работника под роспись.

- истребование с сотрудника (за исключением директора) письменного обязательства о соблюдении конфиденциальности персональных данных работника и соблюдении правил их обработки, подготовленного по установленной форме.

3.7.18. Сотрудники работодателя, имеющие доступ к персональным данным, имеют право получать только те персональные данные, которые необходимы им для выполнения конкретных трудовых функций.

3.7.19. Доступ к персональным данным без специального разрешения имеют работники, занимающие в организации следующие должности:

- руководитель Организации;

- заместители руководителя Организации;

- главный бухгалтер;
- заместитель главного бухгалтера;
- работники отдела кадров;
- ученый секретарь;
- инженеры-программисты отдела информатизации и защиты информации;
- начальники структурных подразделений – в отношении персональных данных работников, числящихся в соответствующих структурных подразделениях.

3.7.20. Допуск к персональным данным других сотрудников работодателя, не имеющих надлежащим образом оформленного доступа, запрещается.

3.8. ***Обработка персональных данных соискателей на замещение вакантных должностей.***

3.8.1. Обработка персональных данных соискателей на замещение вакантных должностей в рамках правоотношений, урегулированных Трудовым кодексом РФ, предполагает получение согласия соискателей на замещение вакантных должностей на обработку их персональных данных на период принятия работодателем решения о приеме либо отказе в приеме на работу.

3.8.2. Согласие соискателя на замещение вакантных должностей не требуется, когда от имени соискателя действует кадровое агентство, с которым данное лицо заключило соответствующий договор, а также при самостоятельном размещении соискателем своего резюме в сети Интернет, доступного неограниченному кругу лиц.

3.8.3. При получении резюме соискателя по каналам электронной почты, факсимильной связи дополнительно проводятся мероприятия, направленные на подтверждение факта направления указанного резюме самим соискателем. При поступлении в адрес работодателя резюме, составленного в произвольной форме, при которой однозначно определить физическое лицо его направившее не представляется возможным, данное резюме подлежит уничтожению в день поступления.

3.8.4. В случае, если сбор персональных данных соискателей осуществляется посредством типовой формы анкеты соискателя, утвержденной оператором, то данная типовая форма анкеты должна соответствовать требованиям п. 7 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687, а также содержать информацию о сроке ее рассмотрения и принятия решения о приеме либо отказе в приеме на работу. Типовая форма анкеты соискателя может быть реализована в электронной форме на сайте организации, где согласие на обработку персональных данных подтверждается соискателем путем проставления отметки в соответствующем поле, за исключением случаев, когда работодателем запрашиваются сведения, предполагающие получение согласия в письменной форме.

3.8.5. В случае отказа в приеме на работу сведения, предоставленные соискателем, должны быть уничтожены в течение 30 дней, за исключением случаев, предусмотренных законодательством о государственной гражданской службе, где срок хранения персональных данных соискателя определен в течение 3 лет.

3.8.6. Получение согласия также является обязательным условием при направлении работодателем запросов в иные организации, в том числе, по прежним местам работы, для уточнения или получения дополнительной информации о соискателе.

3.9. ***Ответственность за разглашение информации, связанной с персональными данными работника.***

3.9.1. За нарушение требований, установленных законодательством РФ, настоящим Положением и другими локальными актами ФГБУН «КрАО РАН», работники и иные лица, получившие доступ к персональным данным, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с федеральными законами РФ.

3.9.2. Разглашение персональных данных (передача их посторонним лицам, в том числе, работникам Организации, не имеющим к ним доступа), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные, а также иные нарушения обязанностей по их защите и обработке, установленные настоящим Положением, локальными нормативными актами (приказами, распоряжениями) Организации, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарного взыскания – замечания, выговора, увольнения.

3.9.3. Сотрудники, имеющие доступ к персональным данным и совершившие указанный дисциплинарный проступок, несут полную материальную ответственность в случае причинения их действиями ущерба работодателю (п.7 ст. 243 Трудового кодекса РФ).

3.9.4. Сотрудники, имеющие доступ к персональным данным, виновные в незаконном разглашении или использовании персональных данных без согласия субъекта персональных данных из корыстной или иной личной заинтересованности и причинившие крупный ущерб, несут уголовную ответственность в соответствии со ст. 183 Уголовного кодекса РФ.

4. Обязанности субъекта персональных данных (работника)

Субъект персональных данных обязан:

4.1. Передавать Работодателю или его представителю комплекс достоверных документированных персональных данных, перечень которых установлен Трудовым кодексом Российской Федерации или иными законами РФ.

4.2. Своевременно в разумный срок, не превышающий 5 рабочих дней, сообщать Работодателю об изменении своих персональных данных.

5. Права работодателя и работника

5.1. Работодатель имеет право проверять достоверность сведений, предоставленных субъектом персональных данных, сверяя данные, предоставленные субъектом персональных данных с имеющимися у субъекта документами.

5.2. Субъект персональных данных имеет право:

5.2.1. На полную информацию о своих персональных данных и обработке этих данных.

5.2.2. На свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные сотрудника, за исключением случаев, предусмотренных законодательством Российской Федерации.

5.2.3. Требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований, определенных трудовым законодательством. При отказе Работодателя исключить или исправить персональные данные сотрудника он имеет право заявить в письменной форме Работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения.

5.2.4. Требовать извещения Работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.2.5. Обжаловать в суд любые неправомерные действия или бездействие Работодателя при обработке и защите его персональных данных.

5.2.6. Определять своих представителей для защиты своих персональных данных.

5.2.7. Требовать прекратить в любое время передачу (распространение, предоставление, доступ) персональных данных, разрешенных для распространения. Требование оформляется в письменном виде. Оно должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) работника, а также перечень персональных данных, обработка которых подлежит прекращению.

Приложение 2

УТВЕРЖДЕНО:

Приказом директора

ФГБУН «КрАО РАН»

от «_29__» «09» 2023 г. № 90

ПОЛИТИКА
В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
ФГБУН «КрАО РАН»

1. Общие положения

Политика в отношении обработки персональных данных ФГБУН «КрАО РАН» разработана в соответствии с частью 2 статьи 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и предназначена для предоставления неограниченного доступа к информации в отношении обработки персональных данных, а также к сведениям о реализуемых требованиях к защите персональных данных в ФГБУН «КрАО РАН».

Настоящая Политика является выдержкой из Положения об обработке и защите персональных данных ФГБУН «КрАО РАН» и описывает порядок обработки и защиты персональных физических лиц в связи с реализацией трудовых отношений, заключением договоров и исполнением договорных обязательств ФГБУН «КрАО РАН».

Персональные данные относятся к категории конфиденциальной информации и защищены от несанкционированного, в том числе случайного, доступа к ним.

2. Основные понятия в области персональных данных

Под персональными данными понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу, в том числе:

- фамилия, имя, отчество;
- дата и место рождения;
- адрес регистрации, место проживания;
- семейное, социальное, имущественное положение;
- образование, профессия, доходы и т.п.

Также в настоящей Политике используются следующие понятия:

Оператор персональных данных – юридическое лицо самостоятельно или совместно с третьими лицами организующие и осуществляющие обработку персональных данных, а также определяющие цели обработки, состав персональных данных и действия с ними;

Субъект персональных данных – физическое лицо, персональные данные которого обрабатываются оператором персональных данных.

Обработка персональных данных – любое действие, совершаемое с персональными данными, в том числе сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

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

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

3. Обработка персональных данных

Сбор персональных данных осуществляется непосредственно у самого субъекта персональных данных. Если предоставление персональных данных является обязательным в соответствии с законодательством, субъекту персональных данных разъясняются юридические последствия отказа в предоставлении таких данных.

Получение персональных данных у третьей стороны возможно только при наличии законных оснований. При получении персональных данных у третьей стороны субъект уведомляется об этом.

Получение и обработка персональных данных физического лица о его политических, религиозных убеждениях и частной жизни не допускается. В случаях, когда обработка таких сведений необходима в связи с исполнением договорных обязательств, они могут быть получены и обработаны только с письменного согласия самого физического лица или его законного представителя.

Обработка персональных данных осуществляется в случаях, когда получено согласие субъекта на обработку его персональных данных или в иных случаях, предусмотренных законодательством.

Обработка персональных данных осуществляется исключительно в целях соблюдения законов и нормативных правовых актов Российской Федерации, заключения договоров и исполнения договорных обязательств.

Обработку персональных данных осуществляют только работники оператора, допущенные руководством в установленном порядке.

Персональные данные обрабатываются как на материальных (бумажных) носителях, так и в электронном виде (в информационных системах персональных данных, на машинных носителях).

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 законодательством либо договором, стороной которого является субъект персональных данных.

Хранение персональных данных осуществляется с учетом обеспечения режима их конфиденциальности.

Персональные данные уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством.

Передача персональных данных третьему лицу осуществляется только с согласия субъекта персональных данных или в случаях, прямо предусмотренных законодательством.

Раскрытие персональных данных третьему лицу без письменного согласия соответствующего субъекта не допускается, за исключением случаев, когда это необходимо для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных.

Вне зависимости от наличия согласия субъекта, не допускается раскрытие сведений о субъекте, его задолженности и любых других персональных данных неограниченному кругу лиц, в том числе путем размещения таких сведений в сети Интернет или в (на) жилом помещении, доме, любом другом здании, строении, сооружении, а также сообщение по месту работы субъекта.

Раскрытие персональных данных третьему лицу в коммерческих целях без письменного согласия соответствующего субъекта запрещено. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации осуществляется только при условии предварительного согласия на это субъекта.

Право доступа к персональным данным, обрабатываемым для ФГБУН «КрАО РАН», имеют:

- директор ФГБУН «КрАО РАН»;
- другие работники ФГБУН «КрАО РАН», для которых обработка персональных данных необходима в связи с исполнением их должностных обязанностей. Допуск работников к персональным данным осуществляется руководством в установленном порядке.

Любой субъект, персональные данные которого обрабатываются для ФГБУН «КрАО РАН», имеет право доступа к своим персональным данным, в том числе к следующей информации:

- подтверждение факта обработки его персональных данных;
- правовые основания и цели обработки его персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах, которые имеют доступ к персональным данным (за исключением работников оператора) или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании законодательства;
- перечень обрабатываемых персональных данных, относящиеся к соответствующему субъекту, и источник их получения;
- сроки обработки персональных данных и сроки их хранения;
- порядок осуществления субъектом прав, предусмотренных законодательством;

- наименование лица, осуществляющего обработку персональных данных по поручению оператора, в случае если обработка поручена третьему лицу.

4. Защита персональных данных

При обработке персональных данных принимаются необходимые правовые, организационные и технические меры для 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, в соответствии с требованиями ст.19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

5. Ответственность

За нарушение требований, установленных законодательством РФ, Положением и другими локальными актами ФГБУН «КрАО РАН», работники и иные лица, получившие доступ к персональным данным, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с федеральными законами РФ.

6. Заключительные положения

Настоящая Политика вступает в силу с момента её утверждения и действует бессрочно. Изменения в Политику вносятся отдельными актами ФГБУН «КрАО РАН».

К настоящей политике обеспечен неограниченный доступ всех заинтересованных лиц, в том числе субъектов персональных данных и органов власти, осуществляющих контрольно-надзорную функцию в области персональных данных.

Приложение 3

УТВЕРЖДЕНО

Приказом директора ФГБУН «КрАО РАН»

от 29.09.2023 № 90

ПЕРЕЧЕНЬ
ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ
ФГБУН «КрАО РАН»

№ п/п	Субъекты персональных данных	Персональные данные	Цель обработки	Основания для обработки	Условия прекращения обработки, сроки хранения
1.	Сотрудники ФГБУН «КрАО РАН»	1) Фамилия, имя, отчество, пол 2) Дата и место рождения 3) Сведения о гражданстве 4) Сведения об образовании 5) Профессия, квалификация, должность, звания 6) Сведения о семейном положении, составе семьи, наличии детей, родственные связи, которые могут понадобиться работодателю для предоставления льгот, предусмотренных трудовым и налоговым законодательством либо ограничения на замещение должностей, предусмотренных законодательством о коррупции 7) Паспортные данные, а также иные данные, содержащиеся в удостоверении личности работника 8) Адрес регистрации, адрес фактического проживания	Обеспечение соблюдения законов и иных НПА, содействие работникам в трудоустройстве, обучении и продвижении по службе, обеспечение личной безопасности работников, контроль количества и качества выполняемой работы, обеспечение сохранности имущества	Трудовой кодекс РФ, Налоговый Кодекс РФ, Федеральный закон от 01.04.1996 №27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», Договор, Согласие	Прекращение действия трудового договора, 75 лет ЭПК

		9) Номер телефона (домашний, мобильный) 10) Сведения о воинском учете 11) Данные документов об образовании, специальности, квалификации, профессиональной подготовке, переподготовке, сведения о повышении квалификации 12) Данные пенсионного, медицинского страхования, СНИЛС, ИНН 13) Доходы, суммы отчислений 14) Информация об отпусках 15) Ученая степень, ученое звание 16) Факты биографии и предыдущая трудовая деятельность (в том числе сведения о трудовом стаже, местах работы, судимости, службе в армии, работе на выборных должностях, на государственной службе и др.), 17) Личное фото 18) Сведения о результатах медицинского обследования на предмет годности к осуществлению трудовых обязанностей 19) Сведения о доходах с предыдущих мест работы за два предшествующих календарных года 20) Принадлежность к профессиональному союзу (для начисления взносов) 21) Сведения о наградах, поощрениях, почетных званиях 22) Занимаемая должность 23) Размер заработной платы			
2.	Близкие родственники	1) Фамилия, имя, отчество 2) Степень родства	Обеспечение соблюдения законов и иных НПА	Трудовой кодекс РФ	Прекращение действия трудового договора, 75

	сотрудников ФГБУН «КрАО РАН»	3) Год рождения			лет ЭПК
3.	Работники ФГБУН «КрАО РАН» по договору ГПХ (внештатные)	1) Фамилия, имя, отчество, пол; 2) Дата и место рождения; 3) Сведения о гражданстве; 4) Сведения об образовании; 5) Профессия, квалификация, должность; 6) Паспортные данные, а также иные данные, содержащиеся в удостоверении личности; 7) Адрес регистрации, адрес фактического проживания, телефон; 8) Данные пенсионного, медицинского страхования, ИНН, СНИЛС; 9) Доходы, суммы отчислений	Заключение договоров гражданско-правового характера (ГПХ) и исполнение договорных обязательств	Договор ГПХ, Согласие	Прекращение действия договора ГПХ, 1 год
4.	Физические лица (получатели услуг)	1) Фамилия, имя, отчество 2) Дата, место рождения 3) Адрес регистрации, адрес фактического проживания 4) Паспортные данные, а также иные данные, содержащиеся в удостоверении личности 5) Контактные данные (телефон, e-mail) 6) Миграционная карта 7) Паспорт иностранного гражданина	Исполнение договорных обязательств на оказание услуг, в том числе гостиничных, на базе отдыха, при проживании в общежитии или служебном жилье	Договор, Согласие	Прекращение действия договора, отзыв согласия, 3 года

Приложение 4

УТВЕРЖДЕНО:

Приказом директора

ФГБУН «КрАО РАН»

от «_29__» «09» 2023 г. № 90

Перечень
должностей, замещение которых требует в соответствии с должностной инструкцией доступа к персональным данным:

I. Работников ФГБУН «КрАО РАН»:
- директор;
- заместитель директора по научной работе;
- заместитель директора по общим вопросам;
- учёный секретарь;
- главный бухгалтер;
- заместитель главного бухгалтера;
- бухгалтер (ведущий, 1 категории, 2 категории), ведущие учёт и начисление зарплаты;
- начальник Отдела кадров;
- специалисты по кадрам (ведущий, 1 категории, 2 категории);
- ведущий юрисконсульт;
- ведущий специалист по охране труда;
- заведующий хозяйственным подразделением 2.
- начальник ПЭО;
- ведущий экономист.

II. К персональным данным получателей услуг:
- администратор;
- бухгалтер (гостиница);
- заведующий хозяйством (база отдыха);
- делопроизводитель;
- дежурный хозяйственного подразделения 2;
- дежурный главного здания.

III К персональным данным авторов, рецензентов и зарегистрированных читателей журналов издаваемых ФГБУН «КрАО РАН»:
- Главный редактор;
- Заместители главного редактора;
- Ответственный секретарь редколлегии;
- Научный редактор

Приложение 5

УТВЕРЖДЕНО

Приказом директора ФГБУН «КрАО РАН»

от 29.09.2023 № 90

Перечень должностных лиц, допущенных к обработке персональных данных ФГБУН «КрАО РАН»

№ п/п	Должность	Основание для обработки	Допуск в ИСПДн и помещения	Примечание
1	Директор	Трудовой кодекс РФ, Налоговый Кодекс РФ, Федеральный закон от 01.04.1996 №27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», Договор, Согласие	Неограниченный допуск в помещения и ИСПДн	Автоматизированная и неавтоматизированная обработка
2	Заместитель директора по научной работе	Доверенность, Договор, Согласие	Неограниченный допуск в помещения и ИСПДн	Автоматизированная и неавтоматизированная обработка
3	Заместитель директора по общим вопросам	Доверенность, Договор, Согласие	Неограниченный допуск в помещения и ИСПДн	Автоматизированная и неавтоматизированная обработка
4	Главный бухгалтер	Договор, Согласие	ИСПДн №1 «Бухгалтерия и кадры», Республика Крым, Бахчисарайский район, пгт. Научный, д. 42, каб. 105, 106, 108	Автоматизированная и неавтоматизированная обработка
5	Заместитель главного бухгалтера	Договор, Согласие	ИСПДн №1 «Бухгалтерия и кадры», Республика Крым, Бахчисарайский район, пгт. Научный, д. 42, каб. 105, 106, 108	Автоматизированная и неавтоматизированная обработка
6	Начальник отдела кадров	Договор, Согласие	ИСПДн №1 «Бухгалтерия и кадры», Республика Крым, Бахчисарайский район, пгт. Научный, д. 42, каб. 104	Автоматизированная и неавтоматизированная обработка
7	Сотрудники отдела кадров	Договор, Согласие	ИСПДн №1 «Бухгалтерия и кадры», Республика	Автоматизированная и

			Крым, Бахчисарайский район, пгт. Научный, д. 42, каб. 104	неавтоматизированная обработка
8	Сотрудники бухгалтерии	Договор, Согласие	ИСПДн №1 «Бухгалтерия и кадры», Республика Крым, Бахчисарайский район, пгт. Научный, д. 42, каб. 106, 108	Автоматизированная и неавтоматизированная обработка
9	Ведущий специалист по охране труда	Договор, Согласие	Республика Крым, Бахчисарайский район, пгт. Научный, д. 42, каб. 104, 106	Автоматизированная и неавтоматизированная обработка
10	Бухгалтер внебюджетного подразделения	Договор, Согласие	ИСПДн №1 «Бухгалтерия и кадры» Республика Крым, каб. 106	Автоматизированная и неавтоматизированная обработка
11	Администратор	Договор, Согласие	ИСПДн №2 «Гостиница» Бахчисарайский район, пгт. Научный, гостиница, каб. Администратора, каб. Дежурной	Автоматизированная и неавтоматизированная обработка
12	Заведующий хозяйством (база отдыха)	Договор, Согласие	ИСПДн №3 «Гости» г. Ялта, пгт. Кацивели, ул. Шулейкина 1, лит. Б	Неавтоматизированная обработка
13	Делопроизводитель	Договор, Согласие	ИСПДн №3 «Гости» г. Ялта, пгт. Кацивели, ул. Шулейкина 19, каб. 22	Автоматизированная и неавтоматизированная обработка

Приложение 6

УТВЕРЖДЕНО

Приказом директора ФГБУН «КрАО РАН»

от 29.09.2023 № 90

Перечень

информационных систем персональных данных

ФГБУН «КрАО РАН»

№ п/п	Наименование ИСПДн	Территориальное расположение	Структура ИСПДн	Подключение к сетям общего доступа	Режим обработки ПДн	Ответственный за ИСПДн
1	ИСПДн №1 «Бухгалтерия и кадры»	АРМ: Республика Крым, Бахчисарайский район, пгт. Научный д. 42 каб. 104, 105, 106, 108 ЦОД: г. Москва Селезневская ул., д.34	Распределенная ИСПДн на базе Сервера ЦОД и АРМ Инв. №: 28743 1С Бухгалтерия	Имеет подключение	Многопользовательский	Главный бухгалтер
2	ИСПДн №2 «Гостиница»	АРМ: Бахчисарайский район, пгт. Научный, гостиница, кабинет администратора ЦОД: Свердловская обл., г. Екатеринбург, ул. Циолковского, 27	Распределенная ИСПДн на базе Сервера ЦОД и АРМ Инв. №: 27828 АО "ПФ "СКБ Контур"	Имеет подключение	Многопользовательский, без разграничения прав доступа	Администратор гостиницы
3	ИСПДн №3 «Гости»	АРМ: г. Ялта, пгт. Кацивели, ул. Шулейкина 19, каб.22 ЦОД: Свердловская обл., г. Екатеринбург, ул. Циолковского, 27	Распределенная ИСПДн на базе Сервера ЦОД и АРМ Инв. №: 10400230 АО "ПФ "СКБ Контур"	Имеет подключение	Многопользовательский, без разграничения прав доступа	Делопроизводитель

Приложение 7

УТВЕРЖДЕНО:

Приказом директора

ФГБУН «КрАО РАН»

от «_29__» «09» 2023 г. № 90

Система разграничения доступа к ресурсам ИСПДн ФГБУН «КрАО РАН»

В ФГБУН «КрАО РАН» выделяются следующие группы доступа к ИСПДн:

Группы доступа	Уровень доступа к ПДн в ИСПД	Разрешенные действия
Администратор	Доступ на правах администратора к ПДн, ТС, прикладному ПО, системам защиты информации.	1) модернизация, настройка и мониторинг работоспособности комплекса ТС (серверов, АРМ); 2) установка, модернизация, настройка и мониторинг работоспособности системного и базового ПО; 3) установка, настройка и мониторинг прикладного ПО; 4) соблюдение правил, оговоренных в инструкции администратора 5) управление системой защиты информации ИСПДн; 6) выявление инцидентов и реагирование на них; 7) управление конфигурацией ИСПДн и ее системы защиты; 8) контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в ИСПДн; 9) управление правами доступа пользователей к функциям системы; 10) проверка состояния используемых СЗИ от НСД, проверка правильности их настройки; 11) обеспечение функционирования и поддержание работоспособности СЗИ; 12) проведение инструктажа пользователей по правилам работы с используемыми СЗИ; 13) контроль и предотвращение несанкционированного изменения целостности ресурсов; 14) контроль аппаратной конфигурации защищаемых компьютеров и предотвращение попытки ее несанкционированного изменения.
Администратор резервного копирования	Доступ на правах администратора к прикладному ПО. Без доступа на изменение ПДн, ТС и СЗИ	1) настройка и контроль работы процедуры резервного копирования; 2) изготовление резервных копий информации; 3) анализ объемов данных резервного копирования;

		4) контроль состояния оборудования системы резервного копирования; 5) замена неработоспособных или выработавших свой ресурс носителей резервной информации или оборудования системы резервного копирования; 6) восстановление программ и данных из резервных копий в случае порчи или утери данных
Ответственный по защите персональных данных	Доступ на правах пользователя к ПДн, ТС, прикладному ПО и СЗИ. Без доступа на изменение ПО, СЗИ и ТС	1) разработка, управление и реализация эффективной политики информационной безопасности системы; 2) выявление инцидентов и реагирование на них; 3) управление конфигурацией ИСПДн и ее системы защиты; 4) контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в ИСПДн; 5) управление правами доступа пользователей к функциям системы; 6) проверка состояния используемых СЗИ от НСД, проверка правильности их настройки; 7) контроль и предотвращение несанкционированного изменения целостности ресурсов
Пользователь	Доступ на правах пользователя к ПДн, ТС, прикладному ПО и СЗИ. Без доступа на изменение ПО, СЗИ и ТС	Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, предоставление, уничтожение записей, содержащих ПДн

Разграничение доступа пользователей к ИСПДн

Должность	**Группа доступа**	**ИСПДн**
	Администратор	ИСПДн №1 «Бухгалтерия и кадры» ИСПДн №2 «Гостиница» ИСПДн №3 «Гости»
	Администратор резервного копирования	ИСПДн №1 «Бухгалтерия и кадры»
	Ответственный по защите персональных данных	ИСПДн №1 «Бухгалтерия и кадры» ИСПДн №2 «Гостиница» ИСПДн №3 «Гости»
Главный бухгалтер, заместитель главного бухгалтера, ведущий бухгалтер, бухгалтер 1 категории, бухгалтер 2 категории	Пользователь	ИСПДн №1 «Бухгалтерия и кадры»
Начальник отдела кадров, ведущий специалист по кадрам	Пользователь	ИСПДн №1 «Бухгалтерия и кадры»
Администратор гостиницы	Пользователь	ИСПДн №2 «Гостиница»
Делопроизводитель	Пользователь	ИСПДн №3 «Гости»

Приложение 8

УТВЕРЖДЕНО:

Приказом директора

ФГБУН «КрАО РАН»

от «_29__» «09» 2023 г. № 90

ПЛАН ВНУТРЕННЕГО КОНТРОЛЯ

соблюдения законодательства и локальных актов

в области персональных данных для ФГБУН «КрАО РАН»

№ п/п	Наименование мероприятия	Периодичность	Ответственный
1.	Контроль за соблюдением режима обработки и защиты персональных данных	Не реже 1 раза в квартал	Председатель комиссии по внутреннему контролю
2.	Контроль за выполнением антивирусной защиты и обновлением антивирусных баз в ИСПДн	Не реже 1 раза в месяц	Начальник ОИЗИ А.О. Махин
3.	Контроль резервного копирования персональных данных в ИСПДн	Не реже 1 раза в месяц	Начальник ОИЗИ А.О. Махин
4.	Контроль работоспособности средств обеспечения безопасности персональных данных в ИСПДн	Не реже 1 раза в месяц	Начальник ОИЗИ А.О. Махин
5.	Анализ изменения режима обработки и защиты персональных данных и актуализация локальных актов в области персональных данных	Не реже 1 раза в год	Лицо, ответственное за обработку персональных данных
6.	Анализ и пересмотр угроз безопасности персональных данных с учетом возможного появления новых ранее неизвестных угроз	Не реже 1 раза в год	Лицо, ответственное за обработку персональных данных
7.	Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных при их обработке в ИСПДн	Не реже 1 раза в 3 года	Лицо, ответственное за обработку персональных данных

УТВЕРЖДЕНО:

Приказом директора

ФГБУН «КрАО РАН»

от «_29__» «09» 2023 г. № 90

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ

информационной системы персональных данных

ФГБУН «КрАО РАН»

1. Общие положения

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

1.2. Пользователем является сотрудник ФГБУН «КрАО РАН», участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и допущенный в установленном порядке к персональным данным, аппаратным средствам, программному обеспечению и средствам защиты информации.

1.3. Пользователь несет персональную ответственность за свои действия в ИСПДн.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, Положением об обработке и защите персональных данных, законами, нормативно-правовыми и локальными актами ФГБУН «КрАО РАН» в области персональных данных.

1.5. Методическое руководство по работе пользователя в ИСПДн осуществляется ответственным за организацию обработки персональных данных.

2. Обязанности пользователя ИСПДн

Пользователь обязан:

2.1. Знать и выполнять требования действующих законов, нормативно-правовых актов и руководящих документов, а также локальных актов (положений, приказов, распоряжений, инструкций и т.п.), регламентирующих порядок обработки и защиты персональных данных.

2.2. Выполнять в ИСПДн только разрешенные к выполнению процедуры.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и передаче машинных носителей, обеспечению безопасности персональных данных.

2.4. Пресекать действия посторонних лиц и работников ФГБУН «КрАО РАН», не имеющих соответствующего допуска, направленные на получение несанкционированного доступа к персональным данным. О таких фактах незамедлительно информировать непосредственного руководителя.

2.5. Хранить в тайне информацию о применяемых методах и средствах защиты персональных данных.

2.6. Соблюдать требования по осуществлению антивирусного контроля и парольной защиты, изложенные в соответствующих инструкциях.

2.7. Соблюдать правила при работе в сети общего доступа и сети международного информационного обмена Интернет, изложенные в разделе 3 настоящей Инструкции.

2.8. Экран монитора во время работы располагать таким образом, чтобы исключить возможность несанкционированного ознакомления с отображаемой информацией посторонними лицами, шторы (жалюзи) в оконных проемах должны быть закрыты.

2.9. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш *Ctrl+Alt+Del* и выбрать опцию *«Блокировать компьютер»*.

2.10. В случае возникновения внештатных или аварийных ситуаций, принимать меры по реагированию с целью ликвидации их последствий в рамках возложенных функций.

2.11. *Пользователю запрещается:*

- разглашать персональные данные третьим лицам;
- копировать персональные данные на внешние носители информации (CD-диски, дискеты, флеш-накопители и т.п.), не учтенные в установленном порядке;
- самостоятельно устанавливать, тиражировать или модифицировать программное и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств ИСПДн;
- несанкционированно открывать общий доступ к папкам на своей рабочей станции.
- подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;
- отключать (блокировать) средства защиты информации;
- обрабатывать в ИСПДн информацию и выполнять другие работы, не предусмотренные правами, установленными Системой разграничения доступа к ресурсам ИСПДн;
- сообщать или передавать посторонним лицам личные ключи, пароли и атрибуты доступа к ресурсам ИСПДн;
- привлекать посторонних лиц для производства ремонта или настройки элементов ИСПДн без согласования с ответственным за организацию обработки персональных данных.

2.12. Обо всех выявленных нарушениях, связанных с безопасностью персональных данных, по вопросам работы и настройки элементов ИСПДн, а также для получения консультаций необходимо обращаться к ответственному за организацию обработки персональных данных.

3. Правила работы в сетях общего доступа и Интернет

3.1. Работа в сети общего доступа (локальная сеть) и сети международного информационного обмена Интернет (далее – Сеть) на элементах ИСПДн, должна проводиться исключительно при служебной необходимости.

3.2. При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирус, персональный межсетевой экран и др.);
- передавать по Сети персональные данные;
- скачивать из Сети программное обеспечение и другие файлы;
- посещать сайты сомнительной репутации, сайты содержащие нелегально распространяемое программное обеспечение и т.п.;
- нецелевое использование подключения к Сети.

УТВЕРЖДЕНО:

Приказом директора

ФГБУН «КрАО РАН»

от «_29__» «09» 2023 г. № 90

ИНСТРУКЦИЯ

по осуществлению парольной защиты в ИСПДн

ФГБУН «КрАО РАН»

1. Общие положения

1.1. Во всех информационных системах персональных данных ФГБУН «КрАО РАН» (далее – ИСПДн) должна быть реализована система парольной защиты информации.

1.2. Личные пароли доступа к элементам ИСПДн выдаются пользователям системным администратором или создаются пользователями самостоятельно.

1.3. Полная плановая смена паролей доступа пользователей в ИСПДн проводится не реже одного раза в полугодие.

2. Правила формирования пароля

2.1. Для каждой учетной записи пользователя должен быть сформирован уникальный пароль. Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.

2.2. Пароль должен состоять не менее чем из шести символов.

2.3. В пароле должны присутствовать символы трех категорий из числа следующих четырех:

- прописные буквы латинского алфавита от A до Z;
- строчные буквы латинского алфавита от a до z;
- десятичные цифры (от 0 до 9);
- символы, не принадлежащие алфавитно-цифровому набору, например !, $, #, %.

2.4. Запрещается использовать простые пароли типа «123», «111», «PASSWORD» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.

2.5. Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

2.6. Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре, например 123456, QWERTY и т.п.;

2.7. Запрещается формировать пароли, которые уже использовались ранее.

3. Правила ввода пароля

3.1. Ввод пароля должен осуществляться с учётом регистра прописных и строчных символов, заданных в процессе формирования пароля.

3.2. Во время ввода пароля необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и т.п.).

4. Правила хранения пароля

4.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

4.2. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

5. Заключительные положения

5.1. При использовании пароля пользователь обязан знать и строго выполнять требования настоящей Инструкции.

5.2. При утере, компрометации, несанкционированном изменении пароля или срока действия пароля пользователь обязан незамедлительно информировать об этом своего непосредственного руководителя и ответственного за организацию обработки персональных данных.

УТВЕРЖДЕНО:

Приказом директора

ФГБУН «КрАО РАН»

от «_29__» «09» 2023 г. № 90

ИНСТРУКЦИЯ

по осуществлению антивирусного контроля в ИСПДн

ФГБУН «КрАО РАН»

1. Общие положения

1.1. Настоящая Инструкция предназначена для пользователей информационных систем персональных данных ФГБУН «КрАО РАН» (далее – ИСПДн).

1.2. В целях обеспечения антивирусной защиты информации, в т.ч. персональных данных, в ИСПДн вводится антивирусный контроль.

1.3. К применению в ИСПДн допускаются исключительно лицензионные антивирусные средства.

1.4. Пользователь несет персональную ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля.

2. Порядок антивирусного контроля

2.1. Ярлык для запуска антивирусной программы должен быть вынесен на «Рабочий стол» операционной системы или в область системных уведомлений.

2.2. Пользователь ИСПДн при работе с внешними носителями (дискеты, CD-диски, флеш-накопители и т.п.) обязан перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.

2.3. Пользователь обязан осуществлять периодическое, не реже одного раза в неделю, обновление антивирусных баз и контроль работоспособности антивирусного средства.

2.4. Пользователь обязан проводить периодическое, не реже одного раза в месяц, тестирование всего программного обеспечения и всех обрабатываемых файлов на предмет отсутствия компьютерных вирусов.

2.5. Системный администратор или ответственный за организацию обработки персональных данных проводит периодический контроль обновления пользователем антивирусных баз и работоспособности антивирусного средства.

2.6. При обнаружении компьютерного вируса пользователь обязан немедленно прекратить какие-либо действия в ИСПДн и поставить в известность системного администратора и ответственного за организацию обработки персональных данных.

2.7. В случае необходимости производится лечение зараженных файлов путем выбора соответствующего пункта меню антивирусной программы. После этого проводится полная антивирусная проверка.

2.8. В случае обнаружения неподдающегося лечению вируса, системный администратор обязан запретить работу в соответствующей ИСПДн и в возможно короткие сроки обновить пакет антивирусных программ и баз сигнатур, после чего провести полную антивирусную проверку.

УТВЕРЖДЕНО:

Приказом директора

ФГБУН «КрАО РАН»

от «_29__» «09» 2023 г. № 90

ИНСТРУКЦИЯ

по учету машинных носителей персональных данных

ФГБУН «КрАО РАН»

1. Общие положения

1.1. Съемные машинные носители информации (съемные жесткие диски, CD-диски, флеш-накопители и т.п.), предназначенные для хранения персональных данных, принимаются на учет ответственным за организацию обработки персональных данных.

1.2. Машинные носители должны быть приняты на учет до записи на них информации, содержащей персональные данные.

2. Учет машинных носителей

2.1. В ходе принятия на учет каждому машинному носителю присваивается уникальный учётный номер.

2.2. Регистрация машинного носителя в Журнале учета носителей персональных данных производится путем заполнения соответствующих полей.

2.3. Учетный номер наносится на машинный носитель механическим путем или красящим веществом, имеющим хорошую механическую стойкость.

2.4. За машинным носителем закрепляется ответственное должностное лицо, которое принимает машинный носитель и расписывается в Журнале учета. Ответственное должностное лицо несет персональную ответственность за сохранность машинного носителя.

3. Использование машинных носителей

3.1. Машинные носители предназначены как для временного использования, так и для длительного хранения персональных данных.

3.2. При временном использовании машинного носителя, например для переноса персональных данных из одной информационной системы в другую, информация должна быть стерта по окончании такого использования.

3.3. Машинные носители должны храниться в сейфе, запираемом шкафу либо иным способом, исключающим несанкционированный доступ к носителю, кражу либо утерю носителя.

3.4. Не допускается выносить машинные носители за пределы здания ФГБУН «КрАО РАН».

3.5. При утере машинного носителя ответственное лицо обязано незамедлительно информировать непосредственного руководителя и ответственного за организацию обработки персональных данных о наличии и составе персональных данных на утерянном машинном носителе.

3.6. При выходе из строя машинный носитель уничтожается, о чем составляется соответствующий акт.

УТВЕРЖДЕНО:

Приказом директора

ФГБУН «КрАО РАН»

от «_29__» «09» 2023 г. № 90

ИНСТРУКЦИЯ

по резервированию и восстановлению персональных данных

ФГБУН «КрАО РАН»

1. Общие положения

1.1. Настоящая Инструкция определяет порядок резервирования и восстановления персональных данных.

1.2. Действие настоящей Инструкции распространяется на пользователей ИСПДн ФГБУН «КрАО РАН».

2. Порядок резервного копирования

2.1. Резервное копирование персональных данных осуществляется исходя из следующих параметров:

- состав и объем резервируемых данных,
- периодичность проведения резервного копирования,
- максимальный срок хранения резервных копий.

2.2. Порядок резервного копирования информации должен обеспечивать сохранность информации, достаточную для поддержания в актуальном состоянии обрабатываемых персональных данных.

2.3. Ответственными за резервное копирование персональных данных являются пользователи ИСПДн.

2.4. Состав резервируемых данных, периодичность резервирования, способ резервирования и срок хранения резервных копий персональных данных определяется администраторами самостоятельно.

2.5. При резервировании информации на машинный носитель информации (CD-диск, флеш-накопитель, съемный жесткий диск) такой носитель должен быть учтен в соответствующем порядке. На машинный носитель наносится пометка «Резервная копия» и дата резервного копирования.

2.6. Контроль результатов резервного копирования производится исполнителем по окончании процедуры резервного копирования. В случае обнаружения ошибок резервное копирование производится повторно.

2.7. Машинный носитель с резервной копией хранится в сейфе, запираемом шкафу либо иным способом, исключающим несанкционированный к нему доступ, кражу либо утерю носителя.

3. Восстановление персональных данных

3.1. Восстановление персональных данных производится в случае потери (незапланированного уничтожения, искажения, фальсификации и т.п.) персональных данных, которая может произойти в результате:

- непреднамеренных действий администраторов;
- преднамеренных действий администраторов и третьих лиц (внешних нарушителей);
- нарушения правил эксплуатации технических средств ИСПДн;
- возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

3.2. При возникновении необходимости восстановления персональных данных администратор сообщает об этом руководителю.

3.3. Восстановление персональных данных из резервных копий производится администратором в максимально сжатые сроки.

УТВЕРЖДЕНО:

Приказом директора

ФГБУН «КрАО РАН»

от «_29__» «09» 2023 г. № 90

ИНСТРУКЦИЯ
администратора безопасности
ФГБУН «КрАО РАН»

1. Общие положения

1.1. Лицо ответственное за обеспечение безопасности персональных данных (администратор безопасности) назначается приказом руководителя ФГБУН «КрАО РАН».

1.2. Администратор в своей работе руководствуется настоящей инструкцией, Положением об обработке и защите персональных данных, законами, нормативно-правовыми и локальными актами ФГБУН «КрАО РАН» в области персональных данных.

1.3. Администратор безопасности является ответственным лицом за поддержание необходимого уровня защищенности информационных систем персональных данных (ИСПДн) на этапах эксплуатации и модернизации.

1.4. Администратор безопасности должен иметь специальное рабочее место, размещенное в помещении, исключающем возможность несанкционированного доступа посторонних лиц и других пользователей.

1.5. Рабочее место Администратора безопасности должно быть оборудовано средствами хранения (сейф, запираемый металлический шкаф или другое), подключением к ИСПДн, а также необходимыми средствами контроля.

1.6. Администратор безопасности осуществляет методическое руководство и консультации пользователей ИСПДн по вопросам обеспечения безопасности персональных данных, эксплуатации ИСПДн и средств защиты информации.

1.7. Администратор безопасности несет персональную ответственность за качество проводимых работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защищенности ИСПДн.

2. Обязанности администратора безопасности

Администратор безопасности обязан:

2.1. Знать и выполнять требования действующих законов, нормативно-правовых актов и руководящих документов, а также локальных актов (концепций, положений, приказов, распоряжений, инструкций и т.п.), регламентирующих порядок обработки и защиты персональных данных.

2.2. Осуществлять настройку и сопровождение средств защиты информации.

2.3. Участвовать в контрольных и тестовых испытаниях, проверках элементов ИСПДн.

2.4. Участвовать в приемке новых программных и технических средств.

2.5. Обеспечивать доступ к персональным данным пользователей ИСПДн согласно их правам, установленным Системой разграничения доступа к ресурсам ИСПДн.

2.6. Уточнять в установленном порядке обязанности пользователей ИСПДн по обработке и защите персональных данных.

2.7. Осуществлять периодический внутренний контроль соблюдения законодательства и локальных актов в области персональных данных, в том числе:

- контроль состояния средств защиты информации, их параметров и режимов работы;
- контроль физической сохранности средств защиты и оборудования ИСПДн;

- контроль исполнения пользователями соответствующих инструкций по работе в ИСПДн, парольной защите, антивирусному контролю, учету машинных носителей и т.д.;
- контроль резервного копирования персональных данных;

2.8. Своевременно осуществлять анализ событий безопасности, регистрируемых средствами защиты информации, с целью выявления возможных нарушений.

2.9. Не допускать установку, использование, хранение и размножение в ИСПДн программных средств и файлов, не связанных с выполнением пользователями должностных обязанностей.

2.10. Не допускать к работе на элементах ИСПДн посторонних лиц.

2.11. Оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам режима безопасности персональных данных.

2.12. При необходимости представлять руководству отчет о состоянии системы защиты ИСПДн, о внештатных ситуациях и допущенных пользователями нарушениях установленных требований в области обработки и защиты персональных данных.

2.13. В случае отказа работоспособности (выхода из строя) элементов ИСПДн осуществлять их ремонт и восстановление силами работников ФГБУН «КрАО РАН».

2.14. В случае невозможности самостоятельного ремонта, передавать технические средства в ремонтную организацию без носителей информации (жестких дисков, CD-дисков, флеш-накопителей) и принимать иные меры по предотвращению доступа посторонних лиц к персональным данным в ходе ремонтных работ. При передаче технических средств в ремонтную организацию с ней должно быть заключено соглашение о конфиденциальности, устанавливающее ответственность за разглашение ставших известными в ходе ремонтных работ персональных данных ФГБУН «КрАО РАН».

2.15. В случае возникновения внештатных или аварийных ситуаций, принимать меры по реагированию с целью ликвидации их последствий.