УТВЕРЖДАЮ

И.о. директора ИСЗФ СО РАН,
Д. ф.-м. н.

_____ В.И. Куркин

«24» декабря 2014г.

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Иркутск 2014

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения:

1) *персональные данные* — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2) *оператор* — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

3) *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;

4) *автоматизированная обработка персональных данных* — обработка персональных данных с помощью средств вычислительной техники;

5) *распространение персональных данных* — действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) *предоставление персональных данных* — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) *блокирование персональных данных* — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) *уничтожение персональных данных* — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

9) *обезличивание персональных данных* — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) *информационная система персональных данных* — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

11) *трансграничная передача персональных данных* — передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1.Настоящее Положение определяет порядок и условия обработки ПДн в ИСЗФ СО РАН (далее Институте), включая порядок передачи ПДн третьим лицам, случаи взимания согласий субъектов ПДн и уведомления органа по защите прав субъектов ПДн, особенности автоматизированной и неавтоматизированной обработки ПДн, порядок доступа к ПДн, систему защиту ПДн, порядок организации внутреннего контроля и ответственность за нарушения при обработке ПДн, иные вопросы.

1.2. Действие настоящего Положения распространяется на все процессы по сбору, систематизации, накоплению, хранению, уточнению, использованию, распространению (в том числе передачу), обезличиванию, блокированию, уничтожению ПДн, осуществляемых с использованием средств автоматизации и без их использования.

1.3. Порядок ввода в действие и изменения Положения.

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

1.3.2. Все изменения в Положение вносятся приказом

1.3.3. Все работники Института должны быть ознакомлены с настоящим Положением под роспись.

2. ЦЕЛИ ОБРАБОТКИ ПДн

2.1. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

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

2.3. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

2.4. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

2.5. Целями обработки персональных данных является оказание услуг клиентам Организации, а также ведение кадрового делопроизводства.

2.6. Обработка персональных данных работников Института 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 Института.

3. ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Защита ПДн представляет собой процесс, организуемый и поддерживаемый в Институте, с целью предупреждения несанкционированного доступа к охраняемой информации и исключения ее разглашения и утечки через различные каналы.

3.2. Защита ПДн предусматривает:

— определение класса ПДн и мероприятий по их защите;
— ограничение свободного доступа к ПДн, путем установления порядка обращения с этой информацией и осуществление контроля за его соблюдением;
— договорное регулирование отношений с контрагентами по вопросам условий передачи и использования ПДн;
— применение при необходимости средств и методов технической защиты конфиденциальности ПДн;
— принятие иных мер, не противоречащих законодательству Российской Федерации.

3.3. Обеспечение защиты ПДн предусмотрено действующим законодательством

Российской Федерации и является обязательной неотъемлемой составной частью деятельности как Института в целом, так и всех его отделов и работников.

3.4. Защита ПДн от несанкционированного доступа или утечки по техническим каналам, обеспечение сохранности информации, создаваемой, обрабатываемой, передаваемой и хранящейся в электронном виде в информационно-вычислительных сетях Института осуществляется в соответствии с действующим законодательством Российской Федерации.

3.5. Работа с документами, содержащими ПДн, не допускает их свободной рассылки, публикации в СМИ, размещения в информационных системах общего пользования, в том числе в сети Интернет, разглашения сторонним юридическим и физическим лицам без согласия владельца ПДн.

3.6. Обезличивание или уничтожение ПДн производится по достижению целей обработки ПДн. Обезличивание или уничтожение ПДн производится ответственным за организацию обработки ПДн

4. ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ОБРАБАТЫВАЕМЫЕ В ИНСТИТУТЕ

4.1. В Институте обрабатываются ПДн следующих субъектов ПДн:
— работники Института
— кандидаты для приема на работу;.

5. УВЕДОМЛЕНИЕ В РОСКОМНАДЗОР ОБ ОБРАБОТКЕ ПДн

5.1. В соответствии с Законом РФ «О персональных данных» Институт является оператором ПДн.

5.2. В соответствии с п.1 ст.22 ФЗ «О персональных данных» оператор ПДн обязан уведомить уполномоченный орган по защите прав субъектов ПДн (в настоящее время Роскомнадзор) об обработке ПДн. Форма уведомления и порядок заполнения и направления в Роскомнадзор установлены в приложении к настоящему Положению. Форма уведомления разработана в соответствии с Приказом Роскомнадзора от 19 августа 2011 г. N 706

5.3. В случае неполноты или изменения сведений, указанных в уведомлении, Институт обязан уведомить об изменениях уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) в порядке, установленном Роскомнадзором.

5.4. Институт вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

1) обрабатываемых в соответствии с трудовым законодательством;

2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных;

4) сделанных субъектом персональных данных общедоступными;

5) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

7) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;

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

6. СОГЛАСИЕ НА ОБРАБОТКУ ПДн. СЛУЧАИ И ПОРЯДОК ПОЛУЧЕНИЯ СОГЛАСИЯ

6.1. Обработка персональных данных допускается без согласия субъекта ПДН в следующих случаях:

1) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

2) обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее — исполнение судебного акта);

3) обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;

4) обработка персональных данных необходима для исполнения договора (гражданско-правового или трудового), стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по

которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

5) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

6) 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 персональных данных;

7) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

9) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 настоящего Федерального закона, при условии обязательного обезличивания персональных данных;

10) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее — персональные данные, сделанные общедоступными субъектом персональных данных);

11) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

6.2. Соискатели на вакансии Института при заполнении анкет, должны предоставлять согласие на обработку персональных данных, указанных в анкетах, поскольку на момент прохождения собеседования и заполнения анкеты трудовые отношения между Институтом и соискателем еще не возникли.

6.3. Получения согласия на обработку ПДн клиентов по гражданско-правовым договорам не требуется, если персональные данные передаются в момент и после заключения договора. В случае получения от субъекта ПДн заявки на бронирование до момента подтверждения бронирования и заключения договора, договорные отношения между Институтом и субъектом не возникают, в связи с чем необходимо получение согласия на обработку ПДн.

6.4. В случае, если гражданско-правовой договор, заключаемый между ИСЗФ СО РАН и клиентом (субъектом ПДн), предусматривает предоставление услуг иным, кроме клиента, подписавшего договор, лицам (родственники, сопровождающие и т. п.), то должно быть получено согласие от этих физических лиц на обработку ПДн. Клиент обязан оказывать ИСЗФ СО РАН содействие на получение такого согласия на обработку ПДн от указанных лиц.

6.5. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением, в частности следующих случаев (полный перечень установлен п.2 ст. 10 Закона РФ «О защите персональных данных»,

1) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

2.1) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

2.2) обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

6.6. В случае трансграничной передачи ПДн сотрудников или клиентов Института необходимо получать согласие субъектов ПДн на обработку ПДн. Трансграничная обработка осуществляется в соответствии с положениями ст. 12 Закона РФ «О персональных данных».

6.7. Порядок получения согласия на обработку ПДн:

6.7.1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

6.7.2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных, если это необходимо в целях исполнения заключенного договора с субъектом ПДн, а также в иных случаях, установленных в пунктах 2–11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Закона РФ «О персональных данных».

6.7.3. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

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

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

6.8. Получение письменного согласия на обработку ПДн осуществляется сотрудником Института, при получении ПДн от субъекта ПДн, путем оформления письменного согласия по форме, установленной в Институте.

7. ПРАВА СУБЪЕКТА В ОТНОШЕНИИ ПДн, ОБРАБАТЫВАЕМЫХ В ИСЗФ СО РАН

7.1. Субъект персональных данных имеет право на получение информации (далее — сведения), касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

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

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

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

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

7.2. Субъект персональных данных вправе требовать от оператора 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.

7.3. Сведения должны быть предоставлены субъекту персональных данных оператором 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.

7.4. Сведения предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта

персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации. Срок ответа на запрос — 30 дней.

7.5. В случае, если сведения, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 настоящей статьи, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

7.6.Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

7.7. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого

7.8. Если персональные данные были получены не от субъекта персональных данных, за исключением случаев, если персональные данные были предоставлены Институту на основании федерального закона или если персональные данные являются общедоступными, Институт до начала обработки таких персональных данных обязана предоставить субъекту персональных данных следующую информацию:

— наименование (фамилия, имя, отчество) и адрес Института или его представителя;
— цель обработки персональных данных и ее правовое основание;
— предполагаемые пользователи персональных данных;

— установленные настоящим Федеральным законом права субъекта персональных данных.

7.9. Если обязанность предоставления персональных данных установлена федеральным законом, Организация обязана разъяснить субъекту персональных данных юридические последствия отказа предоставить свои персональные данные.

8. ПОРЯДОК ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Институт обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие 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.

8.2. В Институте в соответствии с Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных сисстемах персональных данных» осуществлена классификация ИСПДн Института, на основании которой определён уровень защищённости ИСПДн.

8.3. Для разработки требований по обеспечению безопасности и внедрения системы обеспечения безопасности ПДн в Институте разработана типовая модель угроз на основе нормативно-методического документа ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

8.4. В Организации в соответствии с нормативно-методическим документом ФСТЭК России «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» разработан и внедрен комплекс мер по защите и обеспечению безопасности ПДн.

8.5. Требования к работникам в связи с обработкой ПДн

8.5.1. Должностные обязанности работников установлены в должностных инструкциях, руководствах пользователей.

8.5.2. Обеспечение конфиденциальности ПДн, обрабатывающихся в Институте, является обязательным требованием для всех сотрудников Института, которым ПДн стали известны.

8.5.3. Все лица, допущенные к работе с ПДн, а также связанные с эксплуатацией и техническим сопровождением ИСПДн должны быть под роспись ознакомлены с требованиями настоящего Положения, а также должны подписать «Соглашение об обеспечении конфиденциальности персональных данных сотрудниками Института», приведенного в Приложении к настоящему Положению.

8.5.4. В Институте организован процесс обучения использования средств защиты ПДн, эксплуатируемых в организации. Обучение по данному направлению рекомендовано лицам, имеющим постоянный доступ к ПДн, и лицам, эксплуатирующим технические и программные средства ИСПДн и средств защиты ИСПДн. В обязательном порядке

обучение должны проходить лица, ответственные за эксплуатацию средств защиты информации ИСПДн.

8.5.5. ПДн поступают в Институт при приеме новых сотрудников, заключении договоров, проведении собеседований, а также в иных случаях.

Сотрудники Института, осуществляющие оформление документов, обязаны получать в установленных случаях согласие субъектов ПДн на обработку.

8.5.6. В случае нарушения установленного порядка обработки ПДн работники Института несут ответственность в соответствии с разделом 12 настоящего Положения.

8.6. Доступ к ПДн.

8.6.1. В Институте установлен разрешительный порядок доступа к ПДн. Сотрудникам Института предоставляется доступ к работе с ПДн исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей на основании решения Генерального директора.

8.6.2. Сотрудники Института, которые в силу выполняемых служебных обязанностей постоянно работают с ПДн, получают допуск к необходимым категориям ПДн на срок выполнения ими соответствующих должностных обязанностей на основании перечня лиц, допущенных к работе с ПДн, который утверждается директором Института

8.6.3. Список лиц, имеющих доступ к ПДн для информационной системы, должен поддерживаться в актуальном состоянии.

8.6.4. Временный или разовый допуск к работе с ПДн в связи со служебной необходимостью может быть получен сотрудником Института по согласованию директора или ответственного за организацию обработки ПДн Института.

8.6.5. Доступ к ПДн третьих лиц, не являющихся сотрудниками Института, без согласия субъекта ПДн, запрещен, за исключением доступа сотрудников органов исполнительной власти, осуществляемого в рамках мероприятий по контролю и надзору за исполнением законодательства, реализации функций и полномочий соответствующих органов государственной власти. Предоставление информации по запросу или требованию органа государственной власти осуществляется с ведома директора института.

В случае, если сотруднику сторонней организации необходим доступ к ПДн Института, то необходимо, чтобы в договоре со сторонней организацией были прописаны условия конфиденциальности ПДн и обязанность сторонней организации и ее сотрудников по соблюдению требований текущего законодательства в области защиты ПДн. Кроме того, в случае доступа к ПДн лиц, не являющихся сотрудниками Института, должно быть получено согласие субъектов ПДн на предоставление их ПДн третьим лицам. Указанное согласие не требуется, если ПДн предоставляются в целях исполнения гражданско-правового договора, заключенного Организацией с субъектом ПД.

8.6.6. Доступ сотрудника Института к ПДн прекращается с даты прекращения трудовых отношений, либо даты изменения должностных обязанностей сотрудника и/или исключения сотрудника из списка лиц, имеющих право доступа к ПДн. В случае увольнения все носители, содержащие ПДн, которые в соответствии с должностными обязанностями находились в распоряжении работника во время работы в Институте, должны быть переданы соответствующему должностному лицу Института.

8.6.7. Сотрудники обязаны незамедлительно сообщать соответствующему должностному лицу Института об утрате или недостаче носителей информации, составляющей ПДн, а также о причинах и условиях возможной утечки ПДн. В случае попытки посторонних лиц получить от работника ПДн, обрабатываемых в Институте незамедлительно известить об этом соответствующее должностное лицо Института.

8.7. ПДн субъектов на бумажных носителях, обрабатываемых Институтом, хранятся в отделах (у сотрудников), имеющих допуск к обработке соответствующих ПДн. Носители ПДн не должны оставаться без присмотра. При покидании рабочего места, сотрудники, осуществляющие обработку ПДн должны, убирать носители в сейф, запираемый шкаф или иным образом ограничивать несанкционированный доступ к носителям. При утере или порче ПДн осуществляется по возможности их восстановление.

8.7.1. Места хранения документов, содержащих ПДн:

— ПДн сотрудников Института — документы, носители информации (флеш-карты, CD-диски и т.п.) хранятся в сейфе и запираются на ключ. Ответственное лицо, осуществляющее контроль — заведующий отделом кадров.

— Выдача документов для ознакомления осуществляется лицам, допущенным к соответствующей информации в целях исполнения должностных обязанностей, на срок, не более одного рабочего дня.

8.8. При работе с программными средствами автоматизированной системы Института, реализующей функции просмотра и редактирования ПДн, запрещается демонстрация экранных форм, содержащих такие данные, лицам, не имеющим соответствующего допуска.

8.9. При получении персональных данных сотрудником Института, который в соответствии с должностными обязанностями получает ПДн от клиента, сотрудника иного лица в обязательном порядке проводится проверка достоверности ПДн. Ввод персональных данных, полученных Институтом, в автоматизированную систему Института осуществляется сотрудниками имеющими доступ к соответствующим ПДн. Сотрудники, осуществляющие ввод информации, несут ответственность за достоверность и полноту введенной информации.

8.10. Сотрудники, осуществляющие обработку ПДн должны быть ознакомлены с настоящими Правилами.

8.11. Особенности обработки ПДн, содержащихся на бумажных носителях, без использования средств автоматизации (при составлении документов не используется ПЭВМ) установлены в соответствиис Постановлением Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации")

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

8.11.2. 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).

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

а) 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;

б) 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;

в) 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;

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

8.12. 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 федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

8.13. Случаи уничтожения, блокирования и уточнения ПДн.

— В случае выявления недостоверных персональных данных или неправомерных действий с ними Институт при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных обязана осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки. Блокирование осуществляется на основании распоряжения (приказа) директора Института путем прекращения каких-либо действий с ПДн.

— В случае подтверждения факта неточности персональных данных Институт на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные (внести изменения) и снять их блокирование. Снятие блокирования осуществляется на основании приказа директора Института.

— В случае выявления неправомерных действий с персональными данными Институт в срок, не превышающий трех рабочих дней с даты такого выявления, обязана устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений Институт в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Институт обязана уведомить субъекта персональных данных или его законного

представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, — также указанный орган.

— В случае достижения цели обработки персональных данных Институт обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий 30 рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором с субъектом ПДн и уведомить об этом субъекта персональных данных или его законного представителя.

— В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Институт обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий 30 рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Институтом и субъектом персональных данных. Об уничтожении персональных данных Институт обязан уведомить субъекта персональных данных.

— В случае прекращения трудовых отношений с сотрудником Институт обязан прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий 30 рабочих дней с даты прекращения трудовых отношений. О прекращении трудовых отношениях с сотрудником необходимо уведомить ответственного за обеспечение безопасности персональных данных, ответственного за организацию обработки персональных данных и администратора ИБ.

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

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

8.13.1. Уничтожение носителей, содержащих ПДн, осуществляется в следующем порядке:

— ПДн на бумажных носителях уничтожается путем использования Шредеры (уничтожители документов), установленного в офисе Института.

— ПДн, размещенная в памяти ПЭВМ уничтожается в путем удаления её из памяти ПЭВМ администратором информационной безопасности.

— ПДн, размещенная на флеш-карте, CD-диске, ином носителе информации уничтожается путем удаления файла с носителя, при необходимости путем нарушения работоспособности флеш-карты или CD-диска.

Об уничтожении носителя информации составляется Акт.

8.14. Требования к помещениям, в которых обрабатываются ПДн.

8.14.1. Доступ в помещения, в которых располагаются средства обработки ПДн, должен контролироваться.

8.14.2. Офис, помещения Института, по окончании рабочего дня и отсутствия сотрудников в офисе помещениях, должны запираться, окна должны быть закрыты, должна быть включена сигнализация (при наличии).

8.14.3. Сетевое оборудование, серверы следует располагать в местах, недоступных для посторонних лиц (в специальных помещениях, шкафах, коробах).

8.14.4. Уборка помещений и обслуживание технических средств ИСПДн должна осуществляться под контролем ответственных за данные помещения и технические средства лиц с соблюдением мер, исключающих несанкционированный доступ к ПДн, носителям информации, программным и техническим средствам обработки, передачи и защиты информации ИСПДн.

8.15. Требования к администраторам ИСПДн.

8.15.1. В обязанности администраторов ИСПДн входит управление учетными записями пользователей ИСПДн, поддержание штатной работы ИСПДн, обеспечение резервного копирования данных, а также установка и конфигурирование аппаратного и программного обеспечения ИСПДн, не связанного с обеспечением безопасности ПДн в ИСПДн. Также, в обязанности администраторов ИСПДн входит обеспечение соответствия порядка обработки и обеспечения безопасности ПДн в ИСПДн требованиям по конфиденциальности, целостности и доступности ПДн, предъявляемых к конкретной ИСПДн, и общим требованиям по безопасности ПДн, установленных федеральным законодательством.

8.15.2. В обязанности администраторов ИСПДн также входит установка, конфигурирование и администрирование аппаратных и программных средств защиты информации ИСПДн, учет и хранение машинных носителей ПДн, периодический аудит журналов безопасности и анализ защищенности ИСПДн, а также участие в служебных расследованиях фактов нарушения установленного порядка обработки и обеспечения безопасности ПДн.

8.15.3. В целях обеспечения распределения полномочий, реализации взаимного контроля и недопущения сосредоточения критичных для безопасности ПДн полномочий у одного лица не рекомендуется совмещать роли администратора ИСПДн и администратора ИСПДн в лице одного сотрудника.

8.15.4. Квалификационные требования и детальный перечень прав и обязанностей администраторов ИСПДн закрепляются в соответствующих должностных инструкциях, с которыми сотрудники, назначаемые на данные роли должны быть ознакомлены под роспись.

8.16. Организация внутреннего контроля обработки и обеспечения безопасности ПДн

8.16.1. Организация внутреннего контроля процесса обработки ПДн в Институте осуществляется в целях изучения и оценки фактического состояния защищенности ПДн, своевременного реагирования на нарушения установленного порядка их обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения.

8.16.2. Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности ПДн направлены на решение следующих задач:

— Обеспечение соблюдения сотрудниками Института требований настоящего Положения и нормативно-правовых актов, регулирующих сферу персональных данных.

— Оценка компетентности персонала, задействованного в обработке ПДн.

— Обеспечение работоспособности и эффективности технических средств ИСПДн и средств защиты ПДн, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности ПДн.
— Выявление нарушений установленного порядка обработки ПДн и своевременное предотвращение негативных последствий таких нарушений.
— Принятие корректирующих мер, направленных на устранение выявленных нарушений, как в порядке обработки ПДн, так и в работе технических средств ИСПДн.
— Разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн по результатам контрольных мероприятий.
— Осуществление внутреннего контроля за исполнением рекомендаций и указаний по устранению нарушений.

8.16.3. Результаты контрольных мероприятий оформляются актами и являются основанием для разработки рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн, по модернизации технических средств ИСПДн и средств защиты ПДн, по обучению и повышению компетентности персонала, задействованного в обработке ПДн.

9. ОСОБЕННОСТИ ОБРАБОТКИ ПДН СОТРУДНИКОВ ИНСТИТУТА

В настоящем разделе установлены дополнительные права и обязанности Института и работников при обработке Пдн работников в Института.

9.1. Персональные данные работника — информация, необходимая Институту в связи с трудовыми отношениями и касающаяся конкретного работника.

9.2. Обработка персональных данных работника 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.

9.3. Институт не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами;

9.4. При принятии решений, затрагивающих интересы работника, Институт не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;

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

9.6. Институт обязуется не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

9.7. Институт обязуется предупредить сотрудников Института, третьих лиц, получающих персональные данные работника (при его согласии), 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 режим секретности (конфиденциальности). Режим конфиденциальности обеспечивается подписанием с лицом соглашения (Приложение к настоящему Положению). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном настоящим Кодексом и иными федеральными законами;

9.8. Доступ к персональным данным работников предоставляется сотрудникам Института, указанным в Приложении к настоящему положению в целях исполнения ими должностных обязанностей по ведению кадрового делопроизводства, выполнения административно-хозяйственных и организационно-распорядительных функций.

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

9.10. Институт обязуется передавать персональные данные работника представителям работников в порядке, установленном настоящим Кодексом и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

9.11. Работник имеет право на определение своих представителей для защиты своих персональных данных.

9.12. Институт обязан осуществлять передачу персональных данных сотрудников в пределах Института в соответствии с настоящим Положением.

10. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НАСТОЯЩЕГО ПОЛОЖЕНИЯ

10.1. Руководство Института несет ответственность за необеспечение конфиденциальности ПДн и несоблюдение прав и свобод субъектов ПДн в отношении их ПДн, в том числе прав на неприкосновенность частной жизни, личную и семейную тайну.

10.2. Работники Института несут персональную ответственность за несоблюдение требований по обработке и обеспечению безопасности ПДн, установленных настоящим Положением, в соответствии с законодательством Российской Федерации.

10.3. Работник Института может быть привлечен к ответственности в случаях:
— умышленного или неосторожного раскрытия ПДн;
— утраты материальных носителей ПДн;
— нарушения требований настоящего Положения и других нормативных документов Института в части вопросов доступа и работы с ПДн.

10.4. В случаях нарушения установленного порядка обработки и обеспечения безопасности ПДн, несанкционированного доступа к ПДн, раскрытия ПДн и нанесения Институту, его работникам, клиентам и контрагентам материального или иного ущерба виновные лица несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Приложение №1

П Е Р Е Ч Е Н Ь

сведений, составляющих персональные данные обрабатываемых в ИСПДн Института

Сведения
фамилия, имя, отчество субъекта ПДн;
дата рождения субъекта ПДн
паспортные данные субъекта ПДн (номер, серия паспорта, кем выдан, адрес регистрации)
сведения о профессиональной квалификации субъекта ПДн
сведения о трудовом стаже субъекта ПДн
иная информация, позволяющая получить сведения о трудовой деятельности субъекта ПДн

Приложение №2

СОГЛАШЕНИЕ № ___

о неразглашении информации, составляющей персональные данные ИСПДн ИСЗФ СО РАН

Я,_____(_____)
ФИО должность работника

добровольно принимаю на себя следующие обязательства:

1. Выполнять установленный в ИСЗФ СО РАН режим конфиденциальности;
2. Не разглашать информацию, составляющую персональные данные, обладателями которой являются ИСЗФ СО РАН и его контрагенты, и без их согласия не использовать эту информацию в личных целях;
3. Передать ИСЗФ СО РАН при прекращении или расторжении трудового договора имеющиеся в пользовании работника материальные носители информации, содержащие информацию, составляющую персональные данные.
4. Письменно информировать непосредственного руководителя ИСЗФ СО РАН о следующих фактах:
   - о попытках получить от меня информацию, составляющую персональные данные;
   - о попытках других работников Института воспользоваться мобильными компьютерами, личными фотоаппаратами, съемными носителями информации на рабочем месте;
   - о любых иных действиях работников Института и иных лиц, представляющих угрозу для соблюдения режима конфиденциальности.
5. Не разглашать и не передавать третьим лицам информацию, составляющую персональные данные после прекращения трудовых отношений с ИСЗФ СО РАН.
6. Выполнять требования нормативных правовых актов и локальных правовых актов, регламентирующих вопросы защиты персональных данных;

Ответственность за разглашение персональных данных

Ответственность за соблюдение режима конфиденциальности ПДн возлагается персонально на каждого работника, допущенного к ПДн.

За разглашение ПДн, и нарушение режима конфиденциальности ПДн работники, имеющие доступ к ИСПДн ИСЗФ СО РАН, а также лица, уволенные из ИСЗФ СО РАН, имевшие доступ к ИСПДн ИСЗФ СО РАН, могут быть привлечены к дисциплинарной ответственности и так же ответственности в соответствии с законодательством Российской Федерации.

_____ _____
(ФИО) (подпись работника)