



УТВЕРЖДАЮ
Директор ИГиЛ СО РАН
доктор физико-
математических наук

_____ А.А. Васильев

_____ 10 _____ 2014 г.

**Политика в отношении обработки персональных данных
в институте гидродинамики им. М.А. Лаврентьева СО РАН**

Используемые термины

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. Настоящая Политика в отношении обработки персональных данных (далее – Политика) составлена в соответствии с п. 2 ст. 18.1 Федерального закона РФ «О персональных данных» №152-ФЗ от 27 июля 2006 года и действует в отношении персональных данных, которые институт гидродинамики им. М.А. Лаврентьева СО РАН (далее - ИГиЛ СО РАН) может получить от субъектов персональных данных, являющихся стороной по трудовому договору с ИГиЛ СО РАН, или от субъекта персональных данных, состоящего в гражданско-правовых отношениях с ИГиЛ СО РАН.

1.2. Настоящая Политика разработана на основании Федерального закона РФ «О персональных данных» №152-ФЗ от 27 июля 2006 года, Постановления Правительства Российской Федерации от 15 сентября 2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, Постановления Правительства Российской Федерации от 01 ноября 2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в государственных информационных системах и информационных системах персональных данных», «Положения об организации работы с персональными данными в государственных информационных системах и информационных системах персональных данных ИГиЛ СО РАН», «Положения по организации и проведению работ по обеспечению безопасности персональных данных в государственных информационных системах и информационных системах персональных данных ИГиЛ СО РАН».

1.3. Оператор имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента ее размещения на сайте ИГиЛ СО РАН, если иное не предусмотрено новой редакцией Политики.

1.4. Действующая редакция хранится в месте нахождения Оператора по адресу: Россия, Новосибирская область, г. Новосибирск, проспект Академика Лаврентьева, д. 15.

1.5. Электронная версия Политики – на сайте ИГиЛ СО РАН по адресу: <http://www.hydro.nsc.ru/>

1.6. Обратная связь

Почтовый адрес: 630090, Новосибирск, пр. Лаврентьева, 15

Контактный телефон: (383)333-16-12

Факс: (383)333-16-12

Электронная почта: igil@hydro.nsc.ru

2. Общее описание обработки персональных данных в ИГиЛ СО РАН

2.1. Персональные данные в ИГиЛ СО РАН собираются и обрабатываются в целях осуществления образовательной деятельности (организации и проведения учебной и методической работы), кадрового обеспечения деятельности ИГиЛ СО РАН.

2.2. Обработка персональных данных в ИГиЛ СО РАН осуществляется на законных основаниях в соответствии с целями, определившими их получение;

2.3. Обработка персональных данных граждан осуществляется с письменного согласия субъектов персональных данных, за исключением случаев, предусмотренных федеральными законами, не требующих получения личного согласия субъектов персональных данных;

2.4. Персональные данные субъектов обрабатываются в ИГиЛ СО РАН как в электронном виде (автоматизированная обработка), так и на бумажных носителях (обработка без использования средств автоматизации).

2.5. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за

исключением случаев, предусмотренных частью 2 статьи 10 Федерального закона №152-ФЗ «О персональных данных».

2.6. Обработка персональных данных с использованием средств автоматизации осуществляется в соответствии с законодательством РФ в рамках государственных информационных систем и информационных систем персональных данных ИГиЛ СО РАН, перечень которых утвержден приказом директора ИГиЛ СО РАН.

2.7. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности, путем фиксации их на отдельных носителях. Не допускается фиксация на одном носителе персональных данных, цели обработки которых заведомо несовместимы. Для обработки каждой категории персональных данных должен использоваться отдельный носитель. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна проводиться таким образом, чтобы обеспечивать раздельное хранение персональных данных разных целей обработки.

2.8. Цели обработки персональных данных, содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, определяются в Перечнях персональных данных, обрабатываемых в ИГиЛ СО РАН. 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.

3. Особенности обработки биометрических персональных данных

3.1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ «О персональных данных».

4. Особенности обработки общедоступных персональных данных

4.1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

4.2. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

5. Доступ сотрудников к персональным данным субъектов персональных данных, обрабатываемым в ГИС и ИСПДн

5.1. Сотрудники ИГиЛ СО РАН получают доступ к персональным данным субъектов персональных данных исключительно в объеме, необходимом для выполнения своих должностных обязанностей.

5.2. Перечни лиц, имеющих доступ к обработке персональных данных в ГИС и ИСПДн, утверждаются директором ИГиЛ СО РАН.

5.3. Перечни лиц, имеющих доступ к обработке персональных данных в ГИС и ИСПДн ИГиЛ СО РАН, разрабатываются и пересматриваются по мере необходимости

(прием/увольнение, изменение организационно-штатной структуры, введение новых должностей и т.п.) постоянно действующей экспертной комиссией по информационной безопасности на основании заявок начальников отделов или работников.

5.4. Должностному лицу ИГиЛ СО РАН, должность которого не включена в Перечень подразделений и работников, допущенных к работе с персональными данными, обрабатываемыми в ИГиЛ СО РАН, но которому необходим разовый или временный доступ к персональным данным субъектов персональных данных в связи с исполнением должностных обязанностей, приказом директора ИГиЛ СО РАН может быть предоставлен такой доступ на основании письменного мотивированного запроса непосредственного руководителя работника.

5.5. Должностное лицо ИГиЛ СО РАН получает доступ к обработке персональных данных субъектов персональных данных после:

- ознакомления и изучения требований внутренних нормативных документов ИГиЛ СО РАН по защите персональных данных в части, его касающейся;
- прохождения инструктажа о соблюдении правил обработки персональных данных, обрабатываемых в ИГиЛ СО РАН;
- ознакомления с видами ответственности за нарушение (невыполнение) норм законодательства РФ в сфере обработки персональных данных.

6. Доступ субъектов персональных данных к персональным данным, обрабатываемым в ГИС и ИСПДн ИГиЛ СО РАН

6.1. Субъект персональных данных имеет право на получение сведений о наличии обработки в ИГиЛ СО РАН его персональных данных, сроках обработки, в том числе сроках хранения, на ознакомление с такими персональными данными, а также имеет право требовать уточнения, блокирования или уничтожения неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для заявленной цели обработки персональных данных.

6.2. Право на получение информации, касающейся обработки персональных данных, закрепляется за субъектом персональных данных с момента заключения договора (контракта) с ИГиЛ СО РАН лично им или лицом, которому субъект персональных данных дал письменное согласие на передачу своих персональных данных третьему лицу, и действует на протяжении всего срока обработки персональных данных (включая хранение), предусмотренного действующим законодательством Российской Федерации.

6.3. Сведения должны быть предоставлены субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его представителя 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, установленных законодательством.

6.4. Запрос на предоставление сведений 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 ИГиЛ СО РАН (номер контракта, договора, соглашения, дата заключения контракта, договора, соглашения, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных ИГиЛ СО РАН, подпись субъекта персональных данных или его представителя.

6.5. Письменный запрос субъекта должен быть удостоверен следующими документами:

- общегражданским паспортом – в случае непосредственного обращения субъекта персональных данных с запросом в ИГиЛ СО РАН;

- электронной цифровой подписью – в случае направления в ИГиЛ СО РАН электронного запроса;
- нотариально заверенной подписью – в случае направления в ИГиЛ СО РАН почтового запроса;
- документом, подтверждающим полномочия законного представителя субъекта персональных данных, – в случае направления в ИГиЛ СО РАН запроса от законного представителя субъекта персональных данных. При этом непосредственно запрос должен быть удостоверен одним из вышеприведенных способов.

6.6. Все поступившие письменные и электронные запросы субъектов персональных данных (или их законных представителей) регистрируются ответственным работником в Журнале регистрации запросов субъектов персональных данных на предоставление доступа к своим персональным данным.

6.7. Ответ в письменной форме на запрос субъекта должен быть сформирован компетентным работником, подписан директором ИГиЛ СО РАН или руководителем подразделения (отдела), передан лично или отправлен в адрес субъекта через отделение почтовой связи заказным письмом с уведомлением о вручении или курьером (непосредственно в руки адресату под роспись) в течение тридцати дней с даты поступления в ИГиЛ СО РАН запроса от субъекта персональных данных.

6.8. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя, Оператор должен дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона №152-ФЗ «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

6.9. 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.

6.10. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами.

6.11. 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 запроса.

7. Передача персональных данных и доступ третьих лиц к персональным данным, обрабатываемым в ГИС и ИСПДн ИГиЛ СО РАН

7.1. Трансграничная передача персональных данных на территории иностранных государств запрещается.

7.2. Передача информации третьей стороне возможна только при письменном согласии субъектов персональных данных или без такового, если такая передача предусмотрена действующими законодательными актами.

7.3. Не допускается отвечать на вопросы сторонних организаций, если ответ связан с передачей персональных данных по открытым каналам передачи данных (телефон, факс и т.д.).

7.4. Персональные данные, обрабатываемые в связи с реализацией служебных отношений, а также персональные данные, обрабатываемые в связи с предоставлением государственных услуг и исполнением государственных функций (внешний доступ), могут представляться в следующие государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- контрольно-надзорные органы;
- органы статистики;
- страховые агентства;
- военные комиссариаты;
- органы социального и медицинского страхования;
- пенсионные фонды.

8. Обеспечение безопасности персональных данных

8.1. Во всех случаях отказ субъекта персональных данных от своих прав на сохранение и защиту персональных данных недействителен.

8.2. Защита персональных данных от неправомерного их использования или утраты обеспечивается ИГиЛ СО РАН за счет средств федерального бюджета в порядке, установленном федеральным законом.

8.3. В целях организации и проведения работ по обеспечению безопасности персональных данных в ИГиЛ СО РАН приказом директора назначаются:

- постоянно действующая экспертная комиссия по обеспечению информационной безопасности;
- уполномоченное лицо, ответственное за организацию работ и обеспечение безопасности персональных данных;
- администраторы информационной безопасности, ответственные за обслуживание средств защиты информации, применяемых в ИГиЛ СО РАН для обеспечения безопасности персональных данных, а также за организацию и проведение инструктажа работников по основам информационной безопасности при работе с персональными данными;
- лица, ответственные за эксплуатацию государственных информационных систем и информационных систем персональных данных;
- В случае использования криптографических средств защиты назначается ответственный пользователь криптосредств, на которого возлагается обеспечение функционирования и безопасности криптосредств.

8.4. Указанные лица ответственны за проведение следующих мероприятий по обеспечению безопасности персональных данных:

- планирование работ по обеспечению безопасности персональных данных в ИГиЛ СО РАН;
- осуществление внутреннего контроля за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доведение до сведения работников оператора положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

- организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов.
- разработка и при необходимости последующее внесение изменений в Перечень персональных данных, обрабатываемых в ГИС и ИСПДн ИГиЛ СО РАН;
- определение круга должностных лиц, допущенных к обработке персональных данных;
- определение технологического процесса обработки персональных данных, структуры и топологии сети, состава программного обеспечения и технических средств, с помощью которых производится обработка персональных данных;
- создание системы защиты ГИС и ИСПДн, привлечение к данным работам сторонних организаций, имеющих лицензии на деятельность в области обеспечения безопасности, участие в определении обязательных требований к СЗПДн, порядка и условий ее эксплуатации;
- обслуживание технических и (или) криптографических средств защиты информации, установленных в государственных информационных системах и информационных системах персональных данных ИГиЛ СО РАН;
- внедрение организационных мер и разработка соответствующих регламентов и положений;
- инструктаж и обучение лиц, которые будут использовать средства защиты информации;
- контроль выполнения работ по обеспечению безопасности персональных данных и контроль за соблюдением пользователями регламентов и инструкций, касающихся обработки и обеспечения безопасности персональных данных в ИГиЛ СО РАН.
- проведение разбирательств и составление заключений по фактам несоблюдения условий обработки защищаемой информации.

8.5. Для обеспечения безопасности персональных данных в ИГиЛ СО РАН применяются следующие меры безопасности:

- организационные меры безопасности:
 - определение и закрепление порядка обработки и защиты персональных данных в ГИС и ИСПДн (описание технологического процесса обработки, разработка регламентов лиц, ответственных за различные аспекты безопасности, и инструкций пользователя, парольной и антивирусной защиты)
 - инструктаж работников по правилам обеспечения безопасности обрабатываемых персональных данных. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных;
 - учет и хранение носителей информации и порядок их обращения, исключающие хищение, подмену и уничтожение (определение мест хранения носителей);
 - мониторинг и реагирование на инциденты информационной безопасности, связанные с персональными данными, включая проведение внутренних проверок, разбирательств и составление заключений;
 - постоянный контроль за соблюдением требований по обеспечению безопасности персональных данных (реализуется путем проведения внутренних проверок состояния информационной безопасности);
- меры физической безопасности:

- ограничение и контроль доступа пользователей в помещения, где размещаются технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации.
 - закрепление приказом директора ИГиЛ СО РАН границ контролируемой зоны; утверждение перечня помещений, в которых осуществляется обработка персональных данных, и списка лиц, допущенных в эти помещения; определение порядка доступа лиц, не указанных в списках доступа, в том числе обеспечивающих техническое и бытовое обслуживание (уборку, ремонт оборудования и технических средств);
 - размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории в порядке, исключающем несанкционированный просмотр информации;
 - организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;
- технические меры безопасности:
- использование средств охранной и пожарной сигнализации, средств видеонаблюдения.
 - разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
 - регистрация действий пользователей, доступа к персональным данным с помощью электронного журнала сообщений;
 - резервирование технических средств, программного обеспечения, дублирование массивов и носителей информации;
 - использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.
 - использование антивирусных средств защиты, предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок;
 - использование средств криптографической защиты при передаче персональных данных по открытым каналам связи;

9. Ответственность за нарушение норм, регулирующих обработку персональных данных

9.1. ИГиЛ СО РАН, в соответствии со своими полномочиями владеющее информацией о гражданах, получающее и использующее ее, несет ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

9.2. Руководитель, утверждающий список лиц, имеющих доступ к обработке персональных данных, несет персональную ответственность за данное разрешение.

9.3. Должностные лица, имеющие доступ к обработке персональных данных, несут личную ответственность за сохранность и конфиденциальность находящихся в их распоряжении документов и носителей информации.

9.4. За неисполнение или ненадлежащее исполнение работником (по его вине) возложенных на него обязанностей по соблюдению установленного порядка работы с

персональными данными работодатель вправе применять предусмотренные Трудовым кодексом Российской Федерации дисциплинарные взыскания.

9.5. Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, могут привлекаться к дисциплинарной, административной, гражданско-правовой или уголовной ответственности в соответствии с действующим законодательством Российской Федерации.