



САНКТ-ПЕТЕРБУРГСКОЕ ОТДЕЛЕНИЕ
РОССИЙСКОЙ АКАДЕМИИ НАУК

ПОЛОЖЕНИЕ
О РАБОТЕ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ
В ФЕДЕРАЛЬНОМ ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ
УЧРЕЖДЕНИИ «САНКТ-ПЕТЕРБУРГСКОЕ ОТДЕЛЕНИЕ
РОССИЙСКОЙ АКАДЕМИИ НАУК»

1. Общие положения

1.1. Настоящее Положение о работе с персональными данными в федеральном государственном бюджетном учреждении «Санкт-Петербургское отделение Российской академии наук» (далее – положение) разработано в соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», а также иными нормативными правовыми актами Российской Федерации в области обработки и защиты персональных данных.

1.2. Настоящее Положение определяет порядок работы (сбора, обработки, использования, хранения и т.д.) с персональными данными и действует в отношении всех персональных данных, которые СПБО РАН получает или может получить от субъекта персональных данных.

1.4. Положение и изменения к нему утверждаются приказом СПБО РАН за подписью председателя СПБО РАН, или иного уполномоченного лица.

1.5. Члены СПБО РАН, кандидаты в члены СПБО РАН, работники СПБО РАН и физические лица, являющиеся соискателями на замещение вакантных должностей в СПБО РАН (далее - субъекты), должны быть ознакомлены оператором персональных данных (далее - оператор) под расписку с документами СПБО РАН, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

2. Понятие и состав персональных данных

2.1. Персональными данными является любая информация, прямо или косвенно относящаяся к субъекту персональных данных - определенному или определяемому физическому лицу.

2.2. Состав персональных данных физического лица:

- личный листок по учету кадров;
- автобиография;
- образование, специальность, квалификация;
- сведения о трудовом и общем стаже;
- сведения о предыдущем месте работы;
- семейное положение, наличие детей, родственные связи;
- паспортные данные;
- адрес места жительства;
- домашний телефон;
- сведения о воинском учете;
- наличие судимостей;
- фотографии;
- личные дела и трудовые книжки работников;
- занимаемая должность;
- содержание трудового договора;
- сведения о заработной плате работника;
- сведения о социальных льготах;
- содержание декларации, подаваемой в налоговую инспекцию;

подлинники и копии приказов и/или распоряжений СПБО РАН по личному составу;

основания к приказам и/или распоряжениям СПБО РАН по личному составу;

дела, содержащие материалы по повышению квалификации и переподготовке работников, их аттестации, служебным расследованиям;

результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;

рекомендации, характеристики, резюме;

принадлежность лица к конкретной нации, этнической группе, расе;

привычки и увлечения, в том числе вредные (алкоголь, наркотики и др.);

религиозные и политические убеждения (принадлежность к религиозной конфессии, членство в политической партии, участие в общественных объединениях, в том числе в профсоюзе, и др.);

финансовое положение (доходы, долги, владение недвижимым имуществом, денежные вклады и др.);

деловые и иные личные качества, которые носят оценочный характер;

комплекты документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении;

комплект материалов по анкетированию, тестированию, проведению собеседований с кандидатом на должность;

дела, содержащие материалы аттестаций работников;

дела, содержащие материалы внутренних расследований;

справочно-информационный банк данных по персоналу (картотеки, журналы);

подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству СПБО РАН, руководителям структурных подразделений СПБО РАН;

копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения.

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

2.3. Данные документы являются конфиденциальными. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении срока хранения, если иное не определено законом.

3. Получение и обработка персональных данных

3.1. Источником информации обо всех персональных данных являются члены СПБО РАН, кандидаты в члены СПБО РАН, работники СПБО РАН, физические лица, являющиеся соискателями на замещение вакантных должностей в СПБО РАН. Если персональные данные возможно получить только у третьей стороны, то субъект персональных данных должен быть заранее в письменной форме уведомлен об этом и от него должно быть

получено письменное согласие. Оператор обязан сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

Сбор персональных данных осуществляется в пределах установленного объема, необходимого для каждой категории субъектов персональных данных, с которыми взаимодействует СПБО РАН, и не может превышать объем, предусмотренный Трудовым кодексом Российской Федерации, иными законодательными актами.

3.2. Субъект обязан:

3.2.1. передавать оператору или его представителю комплект достоверных документированных персональных данных, перечень которых установлен Трудовым кодексом Российской Федерации, уставом СПБО РАН;

3.2.2. при изменении персональных данных субъект письменно уведомляет оператора о таких изменениях в разумный срок, не превышающий 14 дней.

3.3. Оператор не имеет права получать и обрабатывать персональные данные субъекта о его расовой, национальной принадлежности, политических взглядах, религиозных и философских убеждениях, состоянии здоровья (за исключением тех сведений, которые относятся к вопросу о возможности выполнения субъектом трудовой функции), интимной жизни, за исключением случаев, предусмотренных Трудовым кодексом Российской Федерации и другими федеральными законами.

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

3.5. Обработка персональных данных субъекта - 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 субъекта.

3.6. Обработка персональных данных субъекта оператором возможна только с их согласия. Исключения составляют случаи, предусмотренные законодательством Российской Федерации (в частности, согласие не требуется при наличии оснований, перечисленных в пунктах 2-11 части 1 статьи 6, пунктах 2-10 части 2 статьи 10, части 2 статьи 11 Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных»).

3.7. Письменное согласие субъекта на обработку своих персональных данных должно включать в себя, в частности, сведения, указанные в пунктах 1-9 части 4 статьи 9 Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных».

Согласие на обработку персональных данных может быть отозвано субъектом. В случае отзыва субъектом согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта при наличии оснований, указанных в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных».

3.8. Работники СПБО РАН и другие субъекты персональных данных представляют в Отдел кадров и делопроизводства СПБО РАН достоверные сведения о себе. Отдел кадров и делопроизводства СПБО РАН проверяет достоверность сведений, сверяя представленные данные, с имеющимися документами.

3.9. В соответствии со статьей 86 Трудового кодекса Российской Федерации в целях обеспечения прав и свобод человека и гражданина оператор и его представители при обработке персональных данных должны соблюдать следующие общие требования:

3.9.1. при определении объема и содержания обрабатываемых персональных данных субъекта оператор должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами;

3.9.2. при принятии решений, затрагивающих интересы субъекта, оператор не имеет права основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.10. При поступлении на работу субъект заполняет личный листок по учету кадров и автобиографию:

3.10.1. личный листок по учету кадров представляет собой перечень вопросов о персональных данных субъекта;

3.10.2. личный листок по учету кадров заполняется субъектом самостоятельно в строгом соответствии с записями, которые содержатся в его личных документах;

3.10.3. автобиография - документ, содержащий описание в хронологической последовательности основных этапов жизни и деятельности принимаемого субъекта;

3.10.4. автобиография составляется в произвольной форме, без помарок и исправлений;

3.10.5. личный листок по учету кадров и автобиография субъекта должны храниться в личном деле. В личном деле также хранятся иные документы персонального учета, относящиеся к персональным данным субъекта;

3.10.6. личное дело оформляется после издания приказа о приеме на работу;

3.10.7. все документы личного дела подшиваются в обложку установленного образца. На ней указываются фамилия, имя, отчество работника, номер личного дела;

3.10.8. к каждому личному делу прилагаются две фотографии работника размером 3 x 4 см;

3.10.9. все документы, поступающие в личное дело, располагаются в хронологическом порядке. Листы документов, подшитых в личное дело, нумеруются;

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

3.11. По мере необходимости оператор может потребовать у субъекта дополнительные сведения. Субъект представляет требуемые сведения и в случае необходимости предъявляет документы, подтверждающие достоверность этих сведений.

3.12. Оператор может производить блокирование персональных данных.

3.12.1. Под блокированием персональных данных понимается временное прекращение оператором операций по их обработке по требованию субъекта при выявлении им недостоверности обрабатываемых сведений или неправомерных, по мнению субъекта, действий в отношении его данных.

3.12.2. Блокирование персональных данных осуществляется на основании письменного заявления от субъекта.

3.13. уничтожение персональных данных:

3.13.1. под уничтожением персональных данных понимаются действия, в результате которых становится невозможным восстановить содержание персональных данных и/или уничтожаются материальные носители персональных данных;

3.13.2. субъект вправе в письменной форме требовать уничтожения своих персональных данных в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

3.13.3. в случае отсутствия возможности уничтожения персональных данных оператор осуществляет блокирование таких персональных данных;

3.13.4. уничтожение персональных данных осуществляется путем стирания информации с использованием сертифицированного программного обеспечения с гарантированным уничтожением (в соответствии с заданными характеристиками для установленного программного обеспечения с гарантированным уничтожением).

4. Хранение персональных данных

4.1. В целях обеспечения сохранности и конфиденциальности персональных данных все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться только работниками Отдела кадров и делопроизводства СПБО РАН, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях.

4.2. Вся информация, которая относится к персональным данным члена СПБО РАН, работника СПБО РАН, хранится в личном деле. Ведение личных дел возложено на Отдел кадров и делопроизводства СПБО РАН.

4.3. Личные дела и личные карточки хранятся в бумажном виде в папках, прошитые и пронумерованные по страницам. Личные дела и личные карточки хранятся в специальных металлических шкафах, обеспечивающих защиту от несанкционированного доступа.

4.4. Персональные данные членов СПбО РАН и работников СПбО РАН могут также храниться в электронном виде в локальной компьютерной сети. Доступ к электронным базам данных, содержащим персональные данные членов СПбО РАН и работников СПбО РАН, обеспечивается системой паролей: на уровне локальной компьютерной сети и на уровне баз данных. Пароли устанавливаются уполномоченными работниками Отдела кадров и делопроизводства СПбО РАН и сообщаются индивидуально работникам СПбО РАН, имеющим доступ к персональным данным работников СПбО РАН.

4.5. Доступ к персональным данным членов СПбО РАН и работников СПбО РАН имеют:

4.5.1. в СПбО РАН:

Председатель СПбО РАН,

главный ученый секретарь СПбО РАН,

члены президиума СПбО РАН,

заместители председателя СПбО РАН,

начальник Финансово-экономического управления СПбО РАН - главный бухгалтер СПбО РАН - к тем данным, которые необходимы для выполнения конкретных функций,

работники Финансово-экономического управления СПбО РАН - к тем данным, которые необходимы для выполнения конкретных функций,

работники Отдела кадров и делопроизводства СПбО РАН - к тем данным, которые необходимы для выполнения конкретных функций,

работники Юридического отдела СПбО РАН - к тем данным, которые необходимы для выполнения конкретных функций,

работники Управления научно-методической деятельностью СПбО РАН - к тем данным, которые необходимы для выполнения конкретных функций,

работники Управления научно-организационной деятельностью СПбО РАН - к тем данным, которые необходимы для выполнения конкретных функций,

работники Отдела информационной политики и пресс-службы СПбО РАН - к тем данным, которые необходимы для выполнения конкретных функций,

работники Управления имуществом СПбО РАН - к тем данным, которые необходимы для выполнения конкретных функций,

работники Административно-хозяйственного управления СПбО РАН - к тем данным, которые необходимы для выполнения конкретных функций,

работники Отдела информационных технологий СПбО РАН - к тем данным, которые необходимы для выполнения конкретных функций,

работники Отдела международного сотрудничества СПбО РАН - к тем данным, которые необходимы для выполнения конкретных функций,

начальники управлений и самостоятельных отделов СПбО РАН, являющиеся непосредственными руководителями работника СПбО РАН.

При переводе из одного структурного подразделения СПБО РАН в другое доступ к персональным данным работника СПБО РАН может иметь руководитель нового структурного подразделения по согласованию с руководством СПБО РАН.

Доступ иных работников СПБО РАН управлений и самостоятельных отделов СПБО РАН к персональным данным осуществляется на основании письменного разрешения председателя СПБО РАН или уполномоченного им лица.

4.5.2. Вне СПБО РАН (внешний доступ. Персональные данные вне СПБО РАН могут представляться в государственные и негосударственные функциональные структуры):

налоговые инспекции, правоохранительные органы,
органы статистики,
органы социального страхования,
пенсионные фонды.

4.6. Сведения о членах СПБО РАН или работниках СПБО РАН (в том числе уволенных) могут быть предоставлены другой организации только с письменного запроса на бланке организации с приложением копии заявления субъекта.

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

4.8. Копировать и делать выписки из персональных данных субъекта разрешается исключительно в служебных целях.

5. Передача и распространение персональных данных

5.1. Оператор не вправе предоставлять персональные данные субъекта третьей стороне и распространять их без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных федеральным законом.

5.2. При передаче оператором персональных данных субъекта субъект должен дать на это согласие в письменной или электронной форме. Если субъект оформил согласие на передачу персональных данных в электронной форме, то он подписывает согласие усиленной электронной цифровой подписью.

5.3. При передаче персональных данных субъекта оператор должен соблюдать следующие требования:

5.3.1. не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных **Трудовым кодексом** Российской Федерации или иными федеральными законами;

5.3.2. передавать персональные данные субъекта в порядке, установленном **Трудовым кодексом** Российской Федерации и иными федеральными законами, и ограничивать эту информацию только теми

персональными данными, которые необходимы для выполнения указанными представителями их функции;

5.3.3. разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции;

5.3.4. предупреждать лиц, получивших персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждение того, что это правило соблюдено. Лица, получившие персональные данные субъекта, обязаны соблюдать режим секретности (конфиденциальности). Данное правило не распространяется на обмен персональными данными субъектов в порядке, установленном **Трудовым кодексом** Российской Федерации и иными федеральными законами;

5.3.5. осуществлять передачу персональных данных субъектов в пределах СПБО РАН в соответствии с настоящим Положением, с которым работники СПБО РАН должны быть ознакомлены под подпись;

5.3.6. давать ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий в письменной форме на бланке СПБО РАН и в том объеме, который позволяет не разглашать излишний объем персональных сведений о членах СПБО РАН и работниках СПБО РАН.

5.4. Оператор не вправе распространять персональные данные субъектов третьим лицам без согласия субъекта на их передачу.

5.5. Согласие на обработку персональных данных, разрешенных субъектом для распространения, оформляется отдельно от иных согласий субъекта на обработку его персональных данных.

5.6. Оператор обязан обеспечить субъекту возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на их распространение.

5.7. В случае, если из предоставленного субъектом согласия на распространение персональных данных не следует, что субъект согласился с их распространением, такие персональные данные обрабатываются оператором без права распространения.

5.8. В случае, если из предоставленного субъектом согласия на передачу персональных данных не следует, что субъект не установил запреты и условия на обработку персональных данных или не указал категории и перечень персональных данных, для обработки которых субъект устанавливает условия и запреты, оператор обрабатывает их без возможности передачи (распространения, предоставления, доступа) неограниченному кругу лиц.

5.9. Согласие субъекта на распространение персональных данных может быть предоставлено оператору:

непосредственно;

с использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных.

5.10. В согласии на распространение персональных данных субъект вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц. Отказ оператора в установлении субъектом данных запретов и условий не допускается.

5.11. Оператор обязан в срок не позднее трех рабочих дней с момента получения согласия субъекта на распространение персональных данных опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных субъекта для распространения.

5.12. Передача (распространение, предоставление, доступ) персональных данных, разрешенных субъектом для распространения, должна быть прекращена в любое время по его требованию. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта, а также перечень персональных данных, обработка которых подлежит прекращению.

5.13. Действие согласия субъекта на распространение персональных данных, прекращается с момента поступления оператору требования, указанного в **пункте 5.12** настоящего Положения.

5.14. Субъект вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных для распространения, к любому лицу, обрабатывающему его персональные данные, в случае несоблюдения положений **Федерального закона** от 27 июля 2006 г. N 152-ФЗ «О защите персональных данных» или обратиться с таким требованием в суд.

5.15. Передача информации, содержащей сведения о персональных данных членов СПБО РАН и работников СПБО РАН, по телефону, факсу, электронной почте без письменного согласия запрещается.

6. Система защиты персональных данных

6.1. Меры по обеспечению безопасности персональных данных при их обработке:

6.1.1. Оператор при обработке персональных данных 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.

6.1.2. Обеспечение безопасности персональных данных достигается, в частности:

определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных

системах персональных данных, необходимых для выполнения требований к защите персональных данных;

применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

учетом машинных носителей персональных данных;

обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

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

контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

6.1.3. Для целей настоящего Положения под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационной системе персональных данных.

6.2. Защищаемые сведения о субъекте персональных данных:

К защищаемым сведениям о субъекте персональных данных относятся данные, позволяющие идентифицировать субъект персональных данных и/или получить о нем дополнительные сведения, предусмотренные законодательством и настоящим Положением.

6.3. Защищаемые объекты персональных данных:

6.3.1. К защищаемым объектам персональных данных относятся:

объекты информатизации и технические средства автоматизированной обработки информации, содержащей персональные данные;

информационные ресурсы (базы данных, файлы и др.), содержащие информацию об информационно-телекоммуникационных системах, в которых циркулируют персональные данные, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;

каналы связи, которые используются для передачи персональных данных в виде информативных электрических сигналов и физических полей;

отчуждаемые носители информации на магнитной, магнитно-оптической и иной основе, применяемые для обработки персональных данных.

6.3.2. Технологическая информация об информационных системах и элементах системы защиты персональных данных, подлежащая защите, включает:

сведения о системе управления доступом на объекты информатизации, на которых осуществляется обработка персональных данных;

управляющую информацию (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);

технологическую информацию средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);

характеристики каналов связи, которые используются для передачи персональных данных в виде информативных электрических сигналов и физических полей;

информацию о средствах защиты персональных данных, их составе и структуре, принципах и технических решениях защиты;

служебные данные (метаданные), появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия в результате обработки персональных данных.

6.4. Требования к системе защиты персональных данных:

Система защиты персональных данных должна соответствовать требованиям **постановления** Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

6.4.1. Система защиты персональных данных должна обеспечивать:

своевременное обнаружение и предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

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

возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

постоянный контроль за обеспечением уровня защищенности персональных данных.

6.4.2. Средства защиты информации, применяемые в информационных системах персональных данных, должны в установленном порядке проходить процедуру оценки соответствия.

6.5. Методы и способы защиты информации в информационных системах персональных данных:

6.5.1. Методы и способы защиты информации в информационных системах персональных данных оператора должны соответствовать требованиям:

приказа Федеральной службы по техническому и экспортному контролю Российской Федерации (ФСТЭК России) от 18 февраля 2013 г. N 21 «Об утверждении Составы и содержания организационных и

технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

приказа ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (в случае определения оператором необходимости использования средств криптографической защиты информации для обеспечения безопасности персональных данных).

6.5.2. Основными методами и способами защиты информации в информационных системах персональных данных являются методы и способы защиты информации от несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий (далее - методы и способы защиты информации от НСД).

6.5.3. Выбранные и реализованные методы и способы защиты информации на сайте должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных при их обработке.

6.6. Меры защиты информации, составляющей персональные данные:

6.6.1. Меры по охране баз данных, содержащих персональные данные, принимаемые оператором, должны включать в себя:

определение перечня информации, составляющей персональные данные;
ограничение доступа к информации, содержащей персональные данные, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка.

6.6.2. Меры по охране конфиденциальности информации признаются разумно достаточными, если:

исключается доступ к персональным данным любых третьих лиц без согласия оператора;

обеспечивается возможность использования информации, содержащей персональные данные, без нарушения законодательства о персональных данных;

при работе устанавливается такой порядок действий оператора, при котором обеспечивается сохранность сведений, содержащих персональные данные субъекта.

6.6.3. Персональные данные не могут быть использованы в целях, противоречащих требованиям Федерального закона, защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

7. Гарантии конфиденциальности персональных данных

7.1. Информация, относящаяся к персональным данным субъекта, является конфиденциальной информацией и охраняется законом.

7.2. Члены СПБО РАН и работники СПБО РАН вправе требовать полную информацию о своих персональных данных, об их обработке, использовании и хранении.

7.3. В случае разглашения персональных данных субъекта без его согласия он вправе требовать от работодателя разъяснений.

Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном **Трудовым кодексом** Российской Федерации и иными федеральными законами, а также привлекаются к административной, гражданско-правовой или уголовной ответственности в порядке, установленном федеральными законами.

Моральный вред, причиненный субъекту вследствие нарушения его прав, нарушения правил обработки персональных данных, а также несоблюдения требований к защите персональных данных, установленных **Федеральным законом** от 27 июля 2006 г. N 152-ФЗ, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом убытков.