УТВЕРЖДЕНО

приказом от 03.07.2015г. № П-119/А

# Положение по обеспечению информационной безопасности персональных данных в ФГУ ФНЦ НИИСИ РАН

**2015**

## Содержание

## 1. Общие положения

1.1. Настоящее Положение применительно к процедурам организации защиты персональных данных в ФГУ ФНЦ НИИСИ РАН (далее – Институт) детализирует положения Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – Закона № 152-ФЗ) и Постановления правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Настоящее Положение разработано с учетом нормативных документов, указанных в приложении.

1.2. Целью настоящего Положения являются определение:

– политики Института, как оператора, в отношении обработки персональных данных, осуществляемой в Институте;

– особенностей обработки и обеспечения безопасности персональных данных, а также минимизация ущерба, который может возникнуть вследствие воздействия угроз информационной безопасности, приводящих к нарушению требуемых свойств безопасности персональных данных в Институте.

1.3. На основании настоящего Положения разрабатывается и применяется комплекс организационных, технологических, технических и программных мер, средств и механизмов обеспечения безопасности персональных данных в информационных системах персональных данных Института. Настоящее Положение служит основой для разработки внутренних нормативных документов, описывающих процедуры жизненного цикла системы защиты персональных данных Института.

1.4. Работники Института, осуществляющие обработку персональных данных, должны быть ознакомлены с внутренними нормативными документами Института, устанавливающими правила обработки персональных данных, в соответствии с порядком, изложенным в этих внутренних нормативных документах.

## 2. Список терминов и определений

2.1. **Акт определения требуемого уровня защищенности персональных данных при их обработке в информационной системе персональных данных** – документ, в котором фиксируется результат определения требуемого уровня защищенности персональных данных при их обработке в информационной системе персональных данных Института.

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

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

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

2.5. **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.

2.6. **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.

2.7. **Определения требуемого уровня защищённости персональных данных при их обработке в информационной системе персональных данных –** определение одного из четырёх уровней защищённости персональных данных, в соответствии с критериями, установленными постановлением Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», который требуется обеспечить при обработке персональных данных в информационной системе персональных данных Института**.**

2.8. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

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

2.10. **Система защиты персональных данных** – система правовых, организационных, технических и иных мер по обеспечению доступности, целостности и конфиденциальности персональных данных.

2.11. **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.

## 3. Перечень сокращений

ИБ – информационная безопасность
ИСПДн – информационная система персональных данных.
СКЗИ – средства криптографической защиты информации.

## 4. Общие положения по организации обработки и обеспечению безопасности персональных данных

4.1.Институт, как оператор, осуществляет обработку персональных данных работников Института в рамках требований законодательства Российской Федерации в целях:

- содействия работнику в осуществлении трудовой деятельности, наиболее полного исполнения им своих обязанностей, обязательств и компетенций, определенных должностными обязанностями;
- содействия работнику в обучении, повышении квалификации и должностном росте;
- обеспечения личной безопасности, защиты жизни и здоровья работника;
- учета результатов исполнения работником должностных обязанностей;
- статистических и иных научных целей при условии обязательного обезличивания персональных данных;
- ведения финансово-хозяйственной деятельности учреждения;
- формирования и ведения делопроизводства и документооборота, в том числе и в электронном виде.

4.2. Для всех автоматизированных систем Института, отнесенных к ИСПДн, должен быть определен требуемый уровень защищенности персональных данных при их обработке в ИСПДн. Выбор требований по обеспечению безопасности персональных данных в ИСПДн осуществляется в зависимости от установленного уровня защищенности персональных данных, обрабатываемых в ИСПДн.

4.3. Обработка персональных данных в Институте осуществляется путем сбора, систематизации, накопления, хранения, уточнения, обновления, изменения, передачи (в том числе предоставления, доступа), обезличивания, использования и уничтожения данных (в соответствии со ст. 3 Закона № 152-ФЗ).

4.4. Способ обработки персональных данных: смешанная обработка персональных данных.

4.5. Предоставление персональных данных производится между должностными лицами Института внутри Института, а также между должностными лицами Института и работниками налоговой службы, пенсионного фонда, фонда социального страхования, работниками иных организаций согласно федерального законодательства, законодательства Москвы, нормативно-правовых актов ФАНО и Института, а также в целях исполнения заключенных договоров (соглашений).

4.6. Обработка персональных данных разрешена на срок действия трудовых отношений работника с Институтом. Обработка персональных данных работника, не включенных в общедоступные источники, прекращается по истечении двух лет после окончания трудового договора с Институтом. В дальнейшем бумажные носители персональных данных работника находятся на архивном хранении (постоянно или 75 лет), а персональные данные на электронных носителях удаляются из информационной системы.

## 5. Обработка персональных данных без использования средств автоматизации

5.1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных Материальных носителях, в специальных разделах или на полях форм (бланков).

5.2. При обработке персональных данных работниками Института без использования средств автоматизации не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых несовместимы.

5.3. В отношении каждой категории персональных данных, обрабатываемых в Институте без использования средств автоматизации:

– должны быть определены места хранения персональных данных (материальных носителей) и установлен перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;

– обеспечено раздельное хранение персональных данных (материальных носителей) обработка которых осуществляется в различных целях (например, документация кадрового и бухгалтерского учета);

– места хранения материальных носителей должны обеспечивать сохранность персональных данных и исключать несанкционированный к ним доступ.

5.4. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

5.5. При разработке и использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

– типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес Института, поля для указания фамилии, имени, отчества и адреса субъекта персональных данных, данные которого будут обрабатываться, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональных данных, которые будут совершаться в процессе их обработки, общее описание используемых способов обработки персональных данных;

– типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

– типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, не имея возможности доступа к персональным данным иных лиц, содержащихся в указанной типовой форме;

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

5.6. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, организуется принятие мер по обеспечению раздельной обработки персональных данных, в частности:

– при необходимости использования или распространения определенных персональных данных отдельно от других, находящихся на том же материальном носителе, осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

– при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

5.7. 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).

5.8. Правила, предусмотренные п. 5.6, 5.7 настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

5.9. 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, то путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

## 6. Принципы построения системы обеспечения безопасности персональных данных ИСПДн Института

6.1. Объектами защиты являются персональные данные, обрабатываемые в ИСПДн.

6.2. Система защиты персональных данных в Институте строится на базе действующих законов, стандартов и нормативно-методических документов по защите персональные данных и учитывает лучшие мировые практики.

6.3. Системный подход обеспечивает принятие во внимание всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблем обеспечения информационной безопасности Института.

6.4. Система обеспечения безопасности персональных данных Института строится на основе единой технической политики, с учетом возможностей информационных технологий, реализованных в информационной системе и имеющихся систем и средств защиты в соответствии с типовой моделью угроз персональных данных. При создании системы защиты персональных данных могут применяться сертифицированные системы и средства защиты информации, используемые для обеспечения безопасности конфиденциальной информации и персональных данных.

6.5. Непрерывность защиты персональных данных подразумевает обеспечение безопасности персональных данных на всех технологических этапах обработки и для всех режимов функционирования, включая ремонтные и регламентные работы.

6.6. Меры по обеспечению безопасности персональных данных должны носить упреждающий характер, обеспечивая своевременность защиты. Системы защиты персональных данных разрабатываются при создании ИСПДн, что позволяет учитывать требования по безопасности персональных данных при проектировании и модернизации ИСПДн.

6.7. Совершенствование мер защиты обеспечивается анализом результатов функционирования ИСПДн и системы обеспечения безопасности персональных данных Института с учетом выявления новых способов и средств реализации угроз безопасности персональных данных, отечественного и зарубежного положительного опыта защиты информации.

6.8. Стоимость реализации мер защиты соизмеряется с рисками связанными с обработкой и характером персональных данных с учетом достаточности и адекватности применяемых защитных мер.

6.9. Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики и производительность ИСПДн Института.

6.10. Персональная ответственность за обеспечение безопасности персональных данных возлагается на каждого работника Института в пределах его полномочий. Роли и обязанности сотрудников определяются во внутренних нормативных документах Института, что обеспечивает в случае необходимости выявление лиц виновных в нарушениях безопасности персональных данных.

6.11. Система обеспечения безопасности персональных данных должна учитывать, что в процессе функционирования ИСПДн могут меняться ее характеристики, а также объем и категории обрабатываемых персональных данных Института.

6.12. Реализация мер по обеспечению безопасности персональных данных и эксплуатация системы защиты персональных данных осуществляется профессионально подготовленными специалистами.

6.13. Знание своих партнеров и работников позволяет минимизировать вероятность реализации угроз безопасности Персональных данных, связанных с человеческим фактором.

6.14. Подразделениями, ответственными за обеспечение информационной безопасности, проводится постоянный мониторинг использования систем обработки и защиты персональных данных с целью своевременного выявления и пресечения попыток нарушения установленных правил обеспечения безопасности персональных данных Института.

## 7. Требования к подсистемам обеспечения безопасности персональных данных

7.1. Управления доступом:

7.1.1. Идентификации и аутентификации. Каждый пользователь для получения соответствующих прав доступа при подключении к ИСПДн проходит процедуру идентификации, при этом используются уникальные признаки и имена. Подлинность личности пользователя проверяется посредством пароля (аутентификации).

7.1.2. Физической защиты. Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующего режима охраны, в том числе с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации или несанкционированного копирования, модификации, блокирования, уничтожения персональных данных.

7.2. Регистрации и учета:

7.2.1 Регистрация входа в ИСПДн (выхода из ИСПДн) является обязательной. Должны быть установлены процедуры применения мониторинга действий с персональными данными, результаты регистраций событий должны регулярно анализироваться.

7.2.1 В Институте должен быть определен и документально зафиксирован порядок постановки на учет и снятия с учета машинных носителей персональных данных. Снятие с учета машинных носителей производится по акту путем стирания с

них информации средствами гарантированного стирания или по акту путем их уничтожения.

7.3. Антивирусной защиты. Все информационные ресурсы, принадлежащие ИСПДн Института, должны быть защищены от воздействия вредоносного кода лицензионным антивирусным программным обеспечением.

7.4. Обеспечения целостности. Сохранность и целостность программных средств ИСПДн и персональных данных является обязательной и обеспечивается, в том числе, за счет создания резервных копий. Резервному копированию подлежат все программные средства, архивы, журналы, информационные ресурсы (данные), используемые и создаваемые в процессе эксплуатации ИСПДн. Средства восстановления функций обеспечения безопасности персональных данных в ИСПДн должны предусматривать ведение не менее двух независимых копий программных средств.

7.5. Межсетевого взаимодействия. Подключение ИСПДн к ИСПДн другого уровня защищенности или сети Интернет должно осуществляться с использованием средств межсетевого экранирования, которые реализуются программными или программно-аппаратными межсетевыми экранами, обеспечивающими: скрытие внутренней сетевой структуры ИСПДн, фильтрацию входящего и исходящего трафика ИСПДн, блокирование любого не разрешенного явно трафика.

7.6. Криптографической защиты. В случае осуществления передачи персональных данных по телекоммуникационным каналам и линиям связи между подразделениями Института и внешними организациями должна использоваться сертифицированная криптографическая защита. СКЗИ, применяемые для защиты персональных данных, должны иметь класс не ниже КС2. Работы по обеспечению с помощью СКЗИ безопасности информации проводятся в соответствии с действующими в настоящее время нормативными документами, регламентирующими вопросы эксплуатации СКЗИ, технической документацией на СКЗИ и лицензионными требованиями ФСБ России.

## 8. Контроль за соблюдением требований настоящего Положения

8.1. Контроль за обеспечением безопасности персональных данных и соблюдением требований настоящего Положения осуществляют подразделения ответственные за обеспечение информационной безопасности.

8.2. Контроль осуществляется путем проведения мониторинга ИБ и менеджмента инцидентов ИБ, по результатам оценки состояния ИБ, а также в рамках иных контрольных мероприятий.

## 9. Ответственность за несоблюдение положений настоящего Положения

Ответственность работников Института за несоблюдение требований настоящего Положения, повлекшее за собой разглашение, утрату или нарушение целостности персональных данных, определяется законодательством Российской Федерации, внутренними нормативными документами, а также трудовыми договорами и должностными инструкциями работников Института.

**Приложение**

к «Положению по обеспечению
информационной безопасности
персональных данных в
ФГУ ФНЦ НИИСИ РАН»

**Перечень нормативных документов, использованных при разработке настоящего Положения**

1. Федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных».

2. Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3. Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

4. «Перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», утвержден приказом Минкультуры России от 25.08.2010 г. № 558.

5. Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

6. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».