Приложение № 1 к приказу

от 03.11.2016 № 117а

ПОЛОЖЕНИЕ
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
ВО ФГУП «НАМИ»

Москва, 2016

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение о защите персональных данных (далее – Положение) регулирует отношения, связанные с обработкой персональных данных, осуществляемой во ФГУП «НАМИ» (далее – Предприятие) с использованием средств автоматизации или без использования таких средств, а также определяет основные требования по организации защиты персональных данных. Действие настоящего Положения не распространяется на отношения, возникающие при обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну на основании Федерального закона Российской Федерации от 21.07.1993 № 5485-1-ФЗ «О государственной тайне».

1.2. Настоящее Положение разработано в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон «О персональных данных»)

1.3. В целях настоящего Положения используются следующие термины, определения и сокращения:

АИС – автоматизированная информационная система;

ИБ – информационная безопасность;

ПДн – персональные данные;

ИСПДн – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

Администратор ИБ – лицо, ответственное за администрирование средств защиты в целях организации безопасности информационных систем персональных данных на Предприятии, назначается приказом генерального директора;

Администратор ИСПДн – лицо, ответственное за организацию разработки, эксплуатацию и сопровождение ИСПДн, назначается приказом генерального директора.

Технологический процесс - процесс, содержащий операции по изменению и (или) определению состояния информационных систем Предприятия. Технологические процессы по обработке персональных данных осуществляются с использованием и без использования средств автоматизации.

Ĥ□ометрические персональные данные - сведения, которые характеризуют физиологические особенности человека, и на основе которых можно установить его личность.

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе, их передачи.

Конфиденциальность персональных данных – требование о нераспространении персональных данных без согласия субъекта или без наличия иного законного основания и обязательно для исполнения оператором (лицом), получившим доступ к персональным данным.

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных, или других лиц, либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

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

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых оператором 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.

Общедоступные персональные данные – доступ к персональным данным неограниченного круга лиц:

а) с согласия субъекта ПДн,

б) если требование соблюдения конфиденциальности не распространяется на данные персональные данные.

Оператор – Предприятие, а также государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации субъекту персональных данных, в том числе, его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация.

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц или на ознакомление с персональными данными неограниченного круга лиц, в том числе, обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Специальная категория персональных данных – данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъекта ПДн.

Субъект персональных данных - физическое лицо.

Трансграничная передача персональных данных - передача персональных данных оператором на территорию иностранного государства, органу власти иностранного государства, физическому или юридическому иностранному лицу.

Уничтожение персональных данных - действия, в результате которых:

а) невозможно восстановить содержание персональных данных в информационной системе персональных данных;

б) уничтожаются материальные носители персональных данных.

1.4. Целью настоящего Положения является выполнение требований Федерального закона «О персональных данных» по обеспечению защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе, защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.5. Обработка персональных данных на Предприятии осуществляется с использованием средств автоматизации, а также без использования средств автоматизации. При этом мероприятия по защите персональных данных являются составной частью технологического процесса.

1.6. Действие настоящего Положения распространяется на все структурные подразделения, филиалы и Представительства Предприятия.

1.7. Приказом генерального директора для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе назначается структурное подразделение, ответственное за обеспечение безопасности персональных данных.

2. ОСНОВНЫЕ ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Принципы обработки персональных данных

Обработка персональных данных на Предприятии осуществляется на основе принципов:

- законности целей и способов обработки персональных данных и добросовестности;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Предприятия, как оператора;

- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;
- обеспечения точности персональных данных, их достаточности, а в необходимых случаях, и актуальности по отношению к целям обработки персональных данных;
- осуществления хранения в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если иной срок не установлен федеральным законом или договором.

2.2. Условия обработки персональных данных

2.2.1. Обработка ПДн осуществляется Предприятием с согласия субъектов ПДн, за исключением следующих случаев, предусмотренных Федеральным законом «О персональных данных», когда согласие субъекта ПДн не требуется:

- обработка персональных данных осуществляется на основании Федерального закона, устанавливающего цель, условия получения персональных данных, круг субъектов, персональные данные которых подлежат обработке, и определяющего полномочия оператора;
- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект ПДн;
- обработка персональных данных осуществляется для статистических целей при условии обязательного обезличивания персональных данных;
- в иных случаях, предусмотренных Федеральным законом «О персональных данных».

2.2.2. Обработка специальных категорий персональных данных не допускается, за исключением случаев, предусмотренных Федеральным законом «О персональных данных».

2.2.3. В случае, если Предприятие на основании договора поручает обработку персональных данных другому лицу, обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке, согласно требованиям Федерального закона «О персональных данных», является существенным условием этого договора.

2.2.4. Если персональные данные были получены Предприятием от третьего лица, а не от субъекта ПДн, за исключением случаев, если персональные данные были предоставлены Предприятию на основании федерального закона или, если персональные данные являются общедоступными, Предприятие до начала обработки таких персональных данных должно уведомить об этом субъекта ПДн.

В уведомлении Предприятия должны быть указаны наименование и адрес Предприятия, цели обработки персональных данных и ее правовое основание, предполагаемые пользователи персональных данных, а также права субъекта ПДн, предусмотренные Федеральным законом «О персональных данных».

2.3. Конфиденциальность персональных данных.

2.3.1. Персональные данные относятся к сведениям конфиденциального характера, и их охрана осуществляется в соответствии с:

- Федеральным законом «О персональных данных»,
- приложением № 2 «Соглашение о конфиденциальности и неразглашении информации» к Коллективному договору на 2016-2019 годы, утвержденного приказом генерального директора от 17 июня 2016 года № 59,
- Положением о коммерческой тайне, утвержденного приказом генерального директора от 01 февраля 2013 года № 9ж,
- и настоящим Положением.

2.3.2. Предприятием и третьими лицами, получающими доступ к персональным данным на основании заключенного договора, должна обеспечиваться конфиденциальность таких данных, за исключением следующих случаев, предусмотренных Федеральным законом «О

персональных данных», когда обеспечение конфиденциальности персональных данных не требуется:

- в случае обезличивания персональных данных;
- в отношении общедоступных персональных данных;
- в иных случаях, предусмотренных федеральным законом.

2.4. Общедоступные источники персональных данных. Обезличивание персональных данных.

2.4.1. В целях информационного обеспечения Предприятием могут создаваться общедоступные источники персональных данных (в том числе, справочники). В общедоступные источники персональных данных, с письменного согласия субъекта ПДн, могут включаться его фамилия, имя, отчество, адрес, абонентский номер и иные персональные данные, предоставленные субъектом ПДн.

2.4.2. Персональные данные могут быть обезличены.

Оценка возможности обезличивания персональных данных и порядок проведения их обезличивания проводится Предприятием с учетом алгоритмов обезличивания персональных данных, на основе анализа национальных и международных стандартов.

2.5. Согласие субъекта персональных данных на обработку своих персональных данных.

2.5.1. Субъект ПДн принимает решение о предоставлении своих персональных данных и дает согласие на их обработку. Согласие на обработку персональных данных может быть отозвано субъектом ПДн.

2.5.2. Обработка персональных данных осуществляется только с письменного согласия субъекта ПДн (Приложение № 1 Сборника типовых документов по организации работы с персональными данными) в следующих случаях:

- обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни;
- обработка сведений, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные);
- трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных;
- в случае смерти субъекта персональных данных согласие на обработку его персональных данных дают в письменной форме наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни;
- в иных случаях, предусмотренных федеральным законом.

2.5.2.1. Письменное согласие субъекта ПДн на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки;
- срок, в течение которого действует согласие, а также порядок его отзыва;
- собственноручную подпись субъекта персональных данных.

Письменное согласие субъекта оформляется в письменной форме в двух экземплярах - один из которых предоставляется субъекту, второй хранится на Предприятии.

2.5.3. Равнозначным содержащему собственноручную подпись письменному согласию субъекта ПДн на бумажном носителе признается согласие в форме электронного документа, подписанного электронной подписью.

2.5.4. В иных случаях, кроме указанных в п. 2.5.2 настоящего раздела Положения, порядок и форма получения согласия субъекта на обработку его персональных данных определяется Предприятием. Условие о согласии субъекта на обработку его персональных данных может быть включено в текст договоров, заключаемых с субъектами ПДн.

2.6. Трансграничная передача персональных данных

2.6.1. Предприятием может осуществляться трансграничная передача персональных данных субъекта.

До начала осуществления трансграничной передачи персональных данных Предприятие обязано убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных в соответствии с приложением № 1 к настоящему Положению.

2.6.2. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПДн, может осуществляться в случаях:

- наличия согласия в письменной форме субъекта ПДн;
- предусмотренных международными договорами Российской Федерации;
- защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;
- исполнения договора, стороной которого является субъект ПДн;
- защиты жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

3. СУБЪЕКТЫ И КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Субъекты персональных данных.

3.1.1. Предприятие, как оператор персональных данных, осуществляет обработку персональных данных следующих категорий субъектов ПДн:

3.1.1.1. Работники и соискатели. К работникам и соискателям относятся физические лица, вступившие (имеющие намерение вступить) в трудовые отношения с Предприятием;

3.1.1.2. Физические лица – члены органов управления и связанные с Предприятием лица. К данной категории субъектов ПДн относятся:

- руководители и участники;
- члены органов управления Предприятия;
- аффилированные лица, инсайдеры и иные, связанные с Предприятием физические лица.

3.1.1.3. Клиенты (потенциальные клиенты). К категории клиентов (потенциальных клиентов) относятся:

- физические лица, вступившие (имеющие намерение вступить) с Предприятием в договорные отношения (их представители и выгодоприобретатели).
- физические лица – единоличные исполнительные органы и члены коллегиальных органов управления, либо коллегиальных исполнительных органов юридических лиц, вступивших (имеющих намерение вступить) с Предприятием в договорные отношения.

3.1.1.4. Посетители. Под посетителями понимаются физические лица, в отношении которых осуществляются мероприятия по контролю доступа на объекты Предприятия.

3.2. Перечень персональных данных. Категории персональных данных.

3.2.1. Перечень сведений, относящихся к персональным данным, указан в п. 3.1.1 настоящего Положения.

3.2.2. На основании Федерального закона «О персональных данных», нормативных документов Федеральной службы безопасности РФ и Федеральной службы по техническому и экспортному контролю РФ и в соответствии со степенью тяжести последствий потери свойств

безопасности персональных данных для субъекта ПДн устанавливаются следующие категории классификации персональных данных:

категория 1 - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни (специальная категория персональных данных);

категория 2 - персональные данные, характеризующие физиологические и биологические особенности человека, на основании которых можно идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1 (биометрические персональные данные);

категория 3 - персональные данные, позволяющие идентифицировать субъекта ПДн, которые не могут быть отнесены к специальным категориям персональных данных, к биометрическим персональным данным, к общедоступным или обезличенным персональным данным - иные);

категория 4 - общедоступные персональные данные и персональные данные, которые обезличены (общедоступные).

категория 5 – персональные данные работников Предприятия;

категория 6 – персональные данные субъектов, не являющихся работниками Предприятия.

3.3. Права субъекта персональных данных.

3.3.1. Субъект ПДн имеет право на получение сведений о:

- Предприятии,
- месте его нахождения,
- наличии у Предприятия персональных данных, и на ознакомление с ними, за исключением случаев, когда предоставление персональных данных нарушает конституционные права и свободы других лиц.

3.3.2. Субъект ПДн вправе требовать от Предприятия уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

3.3.3. Сведения о наличии персональных данных должны быть предоставлены субъекту персональных данных Предприятием в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

3.3.4. Доступ к персональным данным субъекта предоставляется Предприятием субъекту ПДн или его законному представителю при обращении, либо при получении запроса субъекта ПДн или его законного представителя (Приложение № 6 Сборника типовых документов по организации работы с персональными данными).

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

3.3.5. Субъект ПДн имеет иные права, перечень и порядок реализации которых установлены Федеральным законом «О персональных данных».

4. ОРГАНИЗАЦИОННАЯ СТРУКТУРА УПРАВЛЕНИЯ ПРИ РАБОТЕ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

4.1. В процессе организации работы Предприятия с персональными данными на подразделения Предприятия возлагаются следующие основные задачи и функции:

4.1.1. Управление информационной безопасности:

- организация контроля обеспечения информационной безопасности персональных данных в целях реализации требований раздела 5 настоящего Положения;

- регистрация обращений (запросов) субъектов персональных данных и организация их исполнения;

- организация исполнения запросов федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) (далее - уполномоченный орган по защите прав субъектов ПДн) и надзорных органов, осуществляющих контроль и надзор в области персональных данных;

- сопровождение проверок, проводимых надзорными органами, осуществляющими контроль и надзор в области персональных данных;

- контроль актуальности методологической базы по вопросам защиты персональных данных;

- контроль актуальности перечня (списка) работников Предприятия, осуществляющих обработку персональных данных в ИСПДн, либо имеющих доступ к персональным данным;

- выполнение иных функций в части обеспечения защиты персональных данных.

4.1.2. Управление информационной безопасности совместно с работниками Технической службы:

- организация проведения классификации информационных систем персональных данных и обеспечение безопасности ПДн в указанных информационных системах;

- оценка рисков нарушения безопасности персональных данных.

4.1.3. Управление охраны:

- организация и контроль порядка доступа работников Предприятия и иных лиц в помещения Предприятия, в которых ведется обработка персональных данных.

4.1.4. Управление учета персонала и документооборота:

- ознакомление работников Предприятия, осуществляющих обработку персональных данных в ИСПДн, под роспись со всей совокупностью требований по обработке и обеспечению безопасности ПДн в части, касающейся их должностных обязанностей.

4.2. Подразделения, ответственные за сбор и обработку персональных данных обязаны выполнять требования, предусмотренные Федеральным законом «О персональных данных», иными применимыми нормативно-правовыми актами, настоящим Положением и внутренними документами Предприятия, определяющими принципы обработки и обеспечения безопасности персональных данных в части, касающейся их должностных обязанностей.

5. ОБЩИЕ ТРЕБОВАНИЯ ПО ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ.

5.1. Обязанности Предприятия при сборе персональных данных.

5.1.1. При сборе персональных данных Предприятие обязано предоставить субъекту ПДн по его просьбе информацию, предусмотренную в п. 3.3. настоящего Положения.

5.1.2. Если персональные данные были получены не от субъекта персональных данных, за исключением случаев, если персональные данные были предоставлены Предприятию на основании федерального закона или если персональные данные являются общедоступными, Предприятие до начала обработки таких персональных данных обязано предоставить субъекту ПДн следующую информацию (за исключением случаев, предусмотренных частью 4 статьи 18 Федерального закона «О персональных данных»):

- наименование и адрес Предприятия;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные Федеральным законом «О персональных данных» права субъекта персональных данных;
- источник получения персональных данных.

5.2. Меры по обеспечению безопасности персональных данных при их обработке.

5.2.1. Предприятие при обработке персональных данных обязано:

- принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий;
- соблюдать установленные федеральным законодательством и иными нормативными правовыми актами Российской Федерации, требования к обеспечению безопасности ПДн при их обработке в информационных системах персональных данных.

5.3. Уведомление об обработке персональных данных

5.3.1. В случае необходимости, Предприятие обязано уведомить уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку персональных данных.

5.3.2. Уведомление, предусмотренное п. 5.3.1 настоящего Положения, должно быть направлено в письменной форме и подписано уполномоченным лицом Предприятия или направлено в электронной форме и подписано электронной подписью в соответствии с законодательством Российской Федерации. Уведомление должно содержать следующие сведения:

- наименование (фамилия, имя, отчество), адрес Предприятия;
- цель обработки персональных данных;
- категории персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- правовое основание обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;
- описание мер, которые Предприятие обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке;
- наименование Предприятия и номера его контактных телефонов, почтовые адреса и адреса электронной почты;
- дата начала обработки персональных данных;
- срок или условие прекращения обработки персональных данных;
- сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
- сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации;
- сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

5.4. Обработка персональных данных

5.4.1. Для организации обработки персональных данных Предприятием определяются:

- цели обработки персональных данных;
- сроки обработки, в том числе сроки хранения персональных данных;
- необходимость получения согласия субъектов персональных данных.
- перечень информационных систем персональных данных;
- объем и содержание обрабатываемых персональных данных.

5.4.2. Перечень персональных данных, цели и сроки обработки персональных данных, а также необходимость получения согласия субъектов персональных данных применительно для каждой из категорий субъектов персональных данных.

5.4.3. Порядок отнесения информационных систем Предприятия к ИСПДн, перечень ИСПДн, а также информационные технологические процессы, в рамках которых обрабатываются персональные данные в ИСПДн, определяются разделом 6 настоящего Положения.

5.4.4. При обработке персональных данных на бумажных носителях, в частности, при использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться требования, установленные «Положением об особенностях обработки персональных данных,

осуществляемой без использования средств автоматизации», утвержденным Постановлением Правительства РФ от 15 сентября 2008 г. № 687.

5.5. Доступ работников Предприятия к персональным данным

5.5.1. Приказом генерального директора Предприятия утверждается перечень (список) работников, осуществляющих обработку персональных данных в ИСПДн либо имеющих доступ к персональным данным.

Допускается ведение указанного перечня (списка) в электронном виде при условии предоставления работникам прав доступа в ИСПДн только на основании распорядительного документа. При этом в случае необходимости (в т.ч. при проведении проверок) перечень (список) распечатывается на бумажном носителе в виде базы пользователей определенной ИСПДн.

5.5.2. Доступ работников Предприятия к персональным данным и обработка персональных данных работниками Предприятия должны осуществляться только для выполнения их должностных обязанностей.

5.5.3. Работники Предприятия, осуществляющие обработку персональных данных в ИСПДн, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также должны быть ознакомлены под роспись со всей совокупностью требований по обработке и обеспечению безопасности персональных данных в части, касающейся их должностных обязанностей.

6. ОБЩИЕ ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ (ХРАНЕНИИ) ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Общие положения по обеспечению информационной безопасности при обработке (хранении) ПДн

6.1.1. Для разработки и осуществления мероприятий по обеспечению информационной безопасности персональных данных при их обработке в информационных системах Предприятия приказом генерального директора назначаются:

- структурное подразделение, ответственное за обеспечение безопасности персональных данных;
- администратор ИБ;
- администратор ИСПДн;
- ответственный за организацию обработки персональных данных.

Структурное подразделение, ответственное за обеспечение безопасности персональных данных (администратор ИБ), осуществляет выбор и реализацию методов и способов защиты информации. Для выбора и реализации методов и способов защиты информации в информационной системе по решению генерального директора может привлекаться организация, имеющая оформленную в установленном порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации.

6.1.2. В целях обеспечения информационной безопасности при обработке (хранении) ПДн Предприятие:

6.1.2.1. Проводит классификацию информационных систем персональных данных, устанавливает критерии классификации и порядок проведения классификации информационных систем персональных данных Предприятия.

6.1.2.2. Определяет меры по обеспечению безопасности персональных данных при автоматизированной обработке и утверждает модели угроз для каждой ИСПДн;

6.1.2.3. Определяет меры по обеспечению безопасности персональных данных при их обработке без использования средств автоматизации.

6.1.2.4. Устанавливает порядок доступа работников и иных лиц в помещения Предприятия, в которых ведется обработка персональных данных, в целях предотвращения несанкционированного доступа к персональным данным.

6.1.4. Для обеспечения безопасности персональных данных в ИСПдн Предприятием могут применяться шифровальные (криптографические) средств защиты информации,

использование которых осуществляется в соответствии с лицензиями Федеральной службы безопасности России, полученными Предприятием в установленном порядке.

6.2. Классификация ИСПДн.

6.2.1. Общие положения.

6.2.1.1. Предприятием определяется и утверждается перечень информационных систем ПДн, целью работы которых является обработка персональных данных.

Классификация ИСПДн проводится в соответствии с порядком проведения классификации информационных систем персональных данных, утвержденным приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» 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».

6.3. Меры по обеспечению безопасности персональных данных при автоматизированной обработке

6.3.1. Безопасность ПДн при их обработке в информационных системах Предприятия обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, средства защиты от утечки информации по техническим каналам, от программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

6.3.2. В соответствии с Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» Предприятием формируются требования по обеспечению безопасности ПДн при их обработке в соответствующей ИСПДн.

6.4. Меры по обеспечению безопасности персональных данных при их обработке без использования средств автоматизации.

6.4.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

6.4.2. Персональные данные (материальные носители), обработка которых осуществляется в различных целях, подлежат раздельному хранению.

6.4.3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

6.4.4. При определении информационных технологических процессов, в рамках которых обрабатываются персональные данные в ИСПДн:

- исключается фиксация на одном материальном носителе и персональных данных, и иных видов информационных активов, а также персональных данных, цели обработки которых заведомо несовместимы;

- при обработке различных категорий персональных данных для каждой категории персональных данных рекомендуется использовать отдельный материальный носитель.

6.4.5. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе работники Предприятия или лица, осуществляющие такую обработку по договору с Предприятием), должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

7. ОБЩИЕ ТРЕБОВАНИЯ К ХРАНЕНИЮ ПЕРСОНАЛЬНЫХ ДАННЫХ. УТОЧНЕНИЕ. БЛОКИРОВАНИЕ И УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Порядок хранения носителей персональных данных.

7.1.1. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

7.1.2. Сроки обработки (хранения) персональных данных, содержащихся в ИСПДн и на материальных носителях, определяются Предприятием исходя из сроков действия договора с субъектом ПДн и исковой давности с учетом требований Росархива, иных требований законодательства и устанавливаются отдельным внутренним документом Предприятия.

7.1.3. В целях организации хранения материальных носителей персональных данных Предприятием определяются:

- места хранения материальных носителей персональных данных;
- требования по обеспечению безопасности персональных данных при хранении их носителей;
- порядок контроля выполнения требований по обеспечению безопасности персональных данных при хранении материальных носителей персональных данных.

Порядок хранения материальных носителей персональных данных определяется Положением по обеспечению информационной безопасности технологических процессов при обработке персональных данных на Предприятии.

7.1.4. Носители информации на магнитной (магнитно-оптической), оптической и бумажной основе должны учитываться, храниться и уничтожаться в подразделениях Предприятия в установленном порядке.

7.2. Уточнение и блокирование персональных данных

7.2.1. В случае выявления недостоверных персональных данных или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных Предприятие обязано осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки.

7.2.2. В случае подтверждения факта недостоверности персональных данных Предприятие на основании документов, представленных субъектом персональных данных или его законным представителем, либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязано уточнить персональные данные и снять их блокирование.

7.2.3. В случае выявления неправомерных действий с персональными данными допущенные нарушения должны быть устранены в срок, не превышающий 3 (Трех) рабочих дней с даты такого выявления. В случае невозможности устранения допущенных нарушений в срок, не превышающий 3 (Трех) рабочих дней с даты выявления неправомерности действий с персональными данными, такие персональные данные должны быть уничтожены.

Об устранении допущенных нарушений или об уничтожении персональных данных уведомляется субъект персональных данных (или его законный представитель) (Приложение № 13, Сборника типовых документов по организации работы с персональными данными), а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, - также в указанный орган.

7.3. Прекращение обработки и уничтожение персональных данных.

7.2.1. Предприятие обязано прекратить обработку персональных данных и уничтожить собранные персональные данные, если иное не установлено законодательством РФ, в следующих случаях и в сроки, установленные законодательством РФ:

- по достижении целей обработки или при утрате необходимости в их достижении;
- по требованию субъекта персональных данных или уполномоченного органа по защите прав субъектов персональных данных - если персональные данные являются неполными,

устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

- при отзыве субъектом персональных данных согласия на обработку своих персональных данных, если такое согласие требуется в соответствии с законодательством РФ;
- при невозможности устранения допущенных нарушений при обработке персональных данных.

Носители ПДн также подлежат уничтожению в случаях выхода из строя, повреждения носителя ПДн, в результате которого невозможно осуществлять корректную обработку ПДн с использованием данного носителя ПДн.

7.2.2. При достижении цели обработки персональных данных Предприятие обязано уничтожить соответствующие персональные данные в срок, не превышающий 3 (Трех) рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомить об этом 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.

7.2.3. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Предприятие обязано уничтожить персональные данные в срок, не превышающий 3 (Трех) рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Предприятием и субъектом персональных данных. Об уничтожении персональных данных Предприятие обязано уведомить субъекта персональных данных.

7.2.4. Порядок уничтожения персональных данных (в том числе и материальных носителей персональных данных) определяется Положением по обеспечению информационной безопасности технологических процессов при обработке персональных данных на Предприятии.

8. ПОРЯДОК ОБРАБОТКИ ОБРАЩЕНИЙ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ И ЗАПРОСОВ НАДЗОРНЫХ ОРГАНОВ, ОСУЩЕСТВЛЯЮЩИХ КОНТРОЛЬ И НАДЗОР В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Обязанности Предприятия при обращении, либо при получении запроса субъекта персональных данных или его законного представителя.

8.1.1. Предприятие обязано в порядке, предусмотренном в разделе 2 настоящего Положения, сообщить субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных (Приложение № 12 Сборника типовых документов по организации работы с персональными данными), а также предоставить возможность ознакомления с ними при обращении субъекта персональных данных или его законного представителя либо в течение 10 (Десяти) рабочих дней с даты получения запроса субъекта персональных данных или его законного представителя.

8.1.2. В случае отказа в предоставлении субъекту персональных данных или его законному представителю при обращении, либо при получении запроса субъекта персональных данных или его законного представителя информации о наличии персональных данных о соответствующем субъекте персональных данных, а также таких персональных данных Предприятие обязано дать в письменной форме мотивированный ответ (Приложение № 16 Сборника типовых документов по организации работы с персональными данными), в срок, не превышающий 7 (Семи) рабочих дней со дня обращения субъекта персональных данных или его законного представителя либо с даты получения запроса субъекта персональных данных или его законного представителя.

8.1.3. Предприятие обязано безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом персональных данных или его законным представителем сведений,

подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет Предприятие, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах Предприятие обязано уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы (Приложение № 14 Сборника типовых документов по организации работы с персональными данными).

8.2. Обязанности Предприятия при получении запросов государственных органов, осуществляющих контроль и надзор в области персональных данных.

8.2.1. При получении запроса уполномоченного органа по защите прав субъектов персональных данных Предприятие обязано сообщить указанную в запросе информацию, необходимую для осуществления деятельности указанного органа, в течение 7 (Семи) рабочих дней с даты получения такого запроса.

8.2.2. Порядок взаимодействия Предприятия с иными государственными органами, осуществляющими контроль и надзор в области персональных данных, определяется законодательными и нормативными актами, регулирующими деятельность соответствующего надзорного органа.

9. КОНТРОЛЬ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Оценка (самооценка) соответствия Предприятия требованиям Федерального закона «О персональных данных» может проводиться Предприятием самостоятельно или с привлечением сторонней организации (внешний аудит).

Указанная оценка (самооценка) должна проводиться Предприятием не реже одного раза в три года.

9.1.1. В целях проведения самооценки приказом генерального директора создается постоянно действующая комиссия. В состав данной комиссии входят представители юридического подразделения, подразделений общей и информационной безопасности, подразделений автоматизации, а также представители других структурных подразделений, имеющих непосредственное отношение к сфере действия Федерального закона «О персональных данных».

9.2. Организация контроля эффективности принимаемых Предприятием мер защиты персональных данных в информационных системах Предприятия реализуется путем внутренних проверок состояния защиты персональных данных. По окончании внутренней проверки производится экспертная оценка эффективности защиты персональных данных. План проведения внутренних проверок составляется в соответствии с Положением по обеспечению информационной безопасности технологических процессов при обработке персональных данных на Предприятии.

9.3. Текущий контроль за обеспечением информационной безопасности Предприятия, включая защиту персональных данных, осуществляется Управлением информационной безопасности.

10. ЗАКЛЮЧЕНИЕ

10.1. Изменения и дополнения в настоящее Положение вносятся на основании Приказа генерального директора.

10.2. Если в результате изменения законодательства или нормативных актов Российской Федерации отдельные статьи настоящего Положения вступают в противоречие с ними, эти статьи утрачивают силу и до момента внесения соответствующих изменений настоящее Положение применяется с учетом норм действующего законодательства Российской Федерации.

Приложение 1

ПЕРЕЧЕНЬ

иностранных государств, которые обеспечивают адекватную защиту прав субъектов персональных данных[1]

Государства - члены Совета Европы	Дата подписания	Дата ратификации	Дата вступления в силу
Австрия	28.01.1981	30.03.1988	01.07.1988
Албания	09.06.2004	14.02.2005	01.06.2005
Андорра	31.05,2007	06.05.2008	01.09.2008
Бельгия	07.05.1982	28.05.1993	01.09.1993
Болгария	02.06.1998	18.09.2002	01.01.2003
Босния и Герцеговина	02.03.2004	31.03.2006	01.07.2006
Бывшая Югославская Республика Македония	24.03.2006	24.03.2006	01.07.2006
Великобритания	14.05.1981	26.08.1987	01.12.1987
Венгрия	13.05.1993	08.10.1997	01.02.1998
Германия	28.01.1981	19.06.1985	01.10.1985
Греция	17.02.1983	11.08.1995	01.12.1995
Грузия	21.11.2001	14.12.2005	01.04.2006
Дания	28.01.1981	23.10.1989	01.02.1990
Ирландия	18.12.1986	25.04.1990	01.08.1990
Исландия	27.09.1982	25.03.1991	01.07.1991
Испания	28.01.1982	31.01.1984	01.10.1985
Италия	02.02.1983	29.03.1997	01.07.1997
Кипр	25.07.1986	21.02.2002	01.06.2002
Латвия	31.10.2000	30.05.2001	01.09.2001
Литва	11.02.2000	01.06.2001	01.10.2001
Лихтенштейн	02.03.2004	11.05.2004	01.09.2004
Люксембург	28.01.1981	10.02.1988	01.06.1988
Мальта	15.01.2003	28.02.2003	01.06.2003
Молдова	04.05.1998	28.02.2008	01.06.2008
Монако	01.10.2008	24.12.2008	01.04.2008
Нидерланды	21.01.1988	24.08.1993	01.12.1993
Норвегия	13.03.1981	20.02.1984	01.10.1985
Польша	21.04.1999	23.05.2002	01.09.2002

[1] Настоящий Перечень на основе перечня иностранных государств, подписавших и ратифицировавших КОНВЕНЦИЮ О ЗАЩИТЕ ФИЗИЧЕСКИХ ЛИЦ В ОТНОШЕНИИ АВТОМАТИЗИРОВАННОЙ ОБРАБОТКИ ДАННЫХ ЛИЧНОГО ХАРАКТЕРА (ETS №108),