НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ ЧАСТНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОЛГОГРАДСКИЙ ГУМАНИТАРНЫЙ ИНСТИТУТ»

| | |
|---|---|
| № _____ / _____ | **Политика** |

Принята Ученым советом НОЧУ ВО «ВгГИ»
Протокол № 1 от «28» августа 2015 г.

УТВЕРЖДАЮ:
Ректор _____ Т.В. Дерюгина
«28» августа 2015 г.

# ПОЛИТИКА
## безопасности персональных данных

2015 г.

## Введение

«Политика безопасности персональных данных» определяет стратегию защиты персональных данных, обрабатываемых в информационной системе персональных данных НОЧУ ВО «Волгоградский гуманитарный институт» (далее – Институт) и формулирует основные принципы и механизмы защиты персональных данных.

Политика является основным руководящим документом Института, определяющим требования, предъявляемые к обеспечению безопасности персональных данных.

Безопасность персональных данных достигается путем исключения 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.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Настоящий документ разработан в соответствии с требованиями Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных», Трудового кодекса РФ от 30.12.2001 № 197-ФЗ (ст.ст. 85-90); Гражданского кодекса РФ; Налогового кодекса РФ, Федерального закона от 29.12.2012 № № 273-ФЗ «Об образовании в Российской Федерации», Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказа 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».

## 1. Общие положения

### 1.1. Цель и область применения политики

Целью Политики является обеспечение безопасности персональных данных, а также реализация положений нормативных правовых актов и иных документов по защите персональных данных.

Основными целями обеспечения безопасности персональных данных являются:

– предотвращение нарушений прав субъекта персональных данных (физического лица) на сохранение конфиденциальности информации, обрабатываемой в информационной системе персональных данных Института;

– предотвращение искажения или несанкционированной модификации информации, содержащей персональные данные, обрабатываемой в информационной системе персональных данных Института;

– предотвращение несанкционированных действий по блокированию информации, содержащей персональные данные.

Требования настоящей Политики обязательны для всех структурных подразделений Института и распространяются на:

– автоматизированные системы Института;

– средства телекоммуникаций;

– информационные ресурсы и носители информации;

– помещения;

– работников Института.

Внутренние документы Организации, затрагивающие вопросы, рассматриваемые в данном документе, должны разрабатываться с учетом положений Политики и не

противоречить им.

**1.2. Период хранения и обработки персональных данных**

Период хранения и обработки персональных данных определяется в соответствии со ст. 21 Закона «О персональных данных». Обработка персональных данных начинается с момента поступления персональных данных в информационную систему персональных данных и прекращается:

- в случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления, Институт устраняет допущенные нарушения. В случае невозможности устранения допущенных нарушений Институт в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, уничтожает персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Институт уведомляет субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, Институт уведомляет также указанный орган;
- в случае достижения цели обработки персональных данных Институт незамедлительно прекращает обработку персональных данных и уничтожает соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, и уведомляет 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, Институт уведомляет также указанный орган;
- в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Институт прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва. Об уничтожении персональных данных Институт уведомляет субъекта персональных данных.
- в случае ликвидации Института, аннулирования и прекращения действия лицензии на право осуществления образовательной деятельности.

## 2. Общие требования по организации защиты персональных данных

2.1. Организационная структура по обеспечению безопасности персональных данных

2.1.1 Общее руководство системой обеспечения безопасности персональных данных осуществляет ректор.

Ректор отвечает за:

- методологическое обеспечение безопасности персональных данных;
- формирование системы технической защиты персональных данных;
- контроль выполнения мер и мероприятий по защите информации.

Ректор обязан:

- организовывать работу и руководить работой группы по формированию и поддержке системы методологического обеспечения безопасности персональных данных;
- организовывать работу и руководить работой группы по формированию и поддержке системы технической защиты персональных данных.

2.1.2. В целях координации действий по обеспечению безопасности персональных данных в Институте назначается лицо, ответственное за организацию обработки персональных данных и за обеспечение безопасности персональных данных.

Обеспечение безопасности персональных данных, а также разработка и внедрение средств защиты персональных данных основывается на анализе угроз безопасности персональных данных.

Лицо, ответственное за организацию обработки персональных отвечает за проведение мероприятий по обеспечению безопасности персональных данных; эксплуатацию

технических и программных средств защиты персональных данных.

Лицо, ответственное за организацию обработки персональных данных обязано: проводить мониторинг защищённости всех компонентов информационной системы персональных данных; вырабатывать рекомендации по повышению уровня защищённости ресурсов информационной системы персональных данных; контролировать действия лиц, имеющих доступ к персональным данным.

2.1.3. Настройку и поддержку функционирования информационной системы Института осуществляет инженер программного обеспечения.

Инженер программного обеспечения отвечает за безотказное функционирование технических средств информационной системы персональных данных; обеспечение штатного режима функционирования программного обеспечения серверов и рабочих станций информационной системы персональных данных.

Инженер программного обеспечения обязан осуществлять мониторинг состояния ресурсов и компонентов информационной системы персональных данных; осуществлять резервное копирование информации и обеспечивать оперативное восстановление систем при сбоях; своевременно принимать меры по модернизации программного и аппаратного обеспечения; устанавливать, настраивать и поддерживать работоспособность баз данных.

2.1.4. Обработка персональных данных должна осуществляться работниками, имеющими допуск к персональным данным. Данные работники обязаны соблюдать положения настоящей Политики, а также своих должностных инструкций и других документов Института в области защиты персональных данных.

Работники, непосредственно осуществляющие обработку персональных данных, должны быть ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Института в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

2.2. Требования к организационным мерам по обеспечению безопасности персональных данных

2.2.1. Основные положения

Основой организационных мероприятий по обеспечению безопасности персональных данных являются нормативные правовые акты и иные документы по защите персональных данных, в частности Политика. Данные документы определяют стратегию и требования по защите персональных данных. Положения данных документов доводятся до всех работников, ответственных за безопасность персональных данных .

Мероприятия по обеспечению безопасности персональных данных организуются и проводятся в соответствии с требованиями нормативных правовых актов:

– Федерального закона РФ от 27.07.06 № 152-ФЗ «О персональных данных»;

– Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 1 ноября 2012 г. № 1119;

–Положения, утвержденного Постановлением Правительства РФ от 15 сентября 2008 г. «Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

2.3. В случае выявления недостоверных персональных данных субъекта персональных данных, неправомерных действий с ними работников Института при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных осуществляется блокирование персональных данных, относящихся к соответствующему субъекту, с момента такого обращения или получения такого запроса на период проверки.

2.3.1. В случае подтверждения факта недостоверности персональных данных субъекта персональных данных на основании документов, представленных субъектом

персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов производится уточнение персональных данных, соответствующая блокировка снимается.

2.3.2. В случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с момента выявления, лицо, ответственное за безопасность персональных данных или инженер программного обеспечения обязаны устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений в срок, не превышающий трех рабочих дней с момента выявления неправомерности действий с персональными данными, лицо, ответственное за безопасность персональных данных или инженер программного обеспечения обязаны уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных лицо, ответственное за безопасность персональных данных или инженер программного обеспечения обязаны уведомить субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также уведомляется указанный орган.

2.4. Анализ угроз

Обеспечение безопасности персональных данных, а также разработка и внедрение системы защиты персональных данных основывается на анализе угроз безопасности персональных данных.

Лицо, ответственное за организацию обработки персональных данных и инженер программного обеспечения являются ответственными за разработку и поддержку модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных (далее - Частная модель угроз).

Частная модель угроз должна отражать актуальное состояние защищенности информационной системе персональных данных и актуальные угрозы безопасности персональных данных. Разработка Частной модели угроз осуществляется на основании анализа существующих угроз безопасности и возможности их реализации в обследуемой информационной системе персональных данных.

2.5. Порядок уничтожения персональных данных

Ответственным за уничтожение персональных данных является лицо, ответственное за организацию обработки персональных данных.

Лицо, ответственное за организацию обработки персональных данных является председателем комиссии Института по уничтожению персональных данных. Назначение комиссии по уничтожению персональных данных производится приказом ректора института.

При наступлении любого из событий, указанных в разделе 1.2. и повлекших необходимость уничтожения персональных данных, лицо, ответственное за организацию обработки персональных данных обязано:

– уведомить членов комиссии о работах по уничтожению персональных данных; определить (назначить) время, место работы комиссии (время и место уничтожения персональных данных);

– установить перечень, тип, наименование, регистрационные номера и другие данные носителей, на которых находятся персональные данные, подлежащие уничтожению (и/или материальные носители персональных данных);

– определить технологию (приём, способ) уничтожения персональных данных (и/или материальных носителей персональных данных); определить технические (материальные, программные и иные) средства, посредством которых будет произведено уничтожение персональных данных;

– руководя работой членов комиссии, произвести уничтожение персональных данных (и/или материальных носителей персональных данных);

– оформить соответствующий Акт об уничтожении персональных данных (и/или материальных носителей персональных данных) и представить Акт об уничтожении

персональных данных (и/или материальных носителей персональных данных) на утверждение ректору Института;

– в случае необходимости уведомить об уничтожении персональных данных субъекта персональных данных и/или уполномоченный орган.

2.6. Порядок обработки обращений субъектов персональных данных

Ответственным за обработку обращений субъектов персональных данных является лицо, ответственное за организацию обработки персональных данных. При поступлении обращения от субъекта персональных данных лицо, ответственное за организацию обработки персональных данных обязано:

– убедиться, что обращение субъекта персональных данных зарегистрировано согласно процедурам, установленным в Институте;

– действовать в соответствии с Федеральным законом «О персональных данных» № 152-ФЗ;

– уведомить ректора института о поступлении обращения субъекта персональных данных;

– убедиться в отсутствии в обращении требования, нарушающего конституционные права и свободы других лиц;

– подготовить ответ, удовлетворяющий запрос субъекта персональных данных, или мотивированный отказ (в случае если исполнение запроса может повлечь нарушение конституционных прав и свобод других лиц);

– сделать соответствующую запись в «Журнале учета обращений субъектов персональных данных при обработке персональных данных в информационной системе персональных данных Института»;

– направить соответствующий ответ в адрес субъекта персональных данных.

2.7. Порядок действий в случае запросов уполномоченного органа по защите прав субъектов персональных данных или иных надзорных органов, осуществляющих контроль и надзор в области персональных данных

Ответственным за обработку запросов уполномоченного органа по защите прав субъектов персональных данных или иных надзорных органов, осуществляющих контроль и надзор в области персональных данных, является лицо, ответственное за организацию обработки персональных данных.

При поступлении запросов уполномоченного органа по защите прав субъектов персональных данных или иных надзорных органов, осуществляющих контроль и надзор в области персональных данных, лицо, ответственное за организацию обработки персональных данных обязано:

– убедиться, что запрос зарегистрирован согласно процедурам, установленным в Институте;

– действовать в соответствии с Федеральным законом «О персональных данных» № 152-ФЗ;

– уведомить ректора Института о поступлении обращения субъекта персональных данных;

– подготовить ответ в соответствии с запросом уполномоченного органа по защите прав субъектов персональных данных или запросом иных надзорных органов, осуществляющих контроль и надзор в области персональных данных;

– зарегистрировать и направить соответствующий ответ в адрес уполномоченного органа по защите прав субъектов персональных данных или иных надзорных органов, осуществляющих контроль и надзор в области персональных данных.

2.8. Порядок хранения отдельных материальных носителей персональных данных.

2.8.1. Основные принципы хранения отдельных материальных носителей персональных данных:

– при фиксации персональных данных на материальных носителях не допускать

фиксацию на одном материальном носителе персональных данных, цели обработки которых различны;

– для каждой категории персональных данных использовать отдельный материальный носитель;

– материальные носители, содержащие персональные данные, обработка которых осуществляется в различных целях, хранить раздельно (в отдельных шкафах (сейфах) или на отдельных полках);

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

2.8.2. Хранение отдельных материальных носителей персональных данных осуществляется на основании соответствующего приказа ректора Института.

В приказе определяются:

– места (номера комнат, шкафы (сейфы)), предназначенные для хранения материальных носителей персональных данных;

– перечень работников (ФИО, должность), ответственных за реализацию принципов и требований по обеспечению безопасности носителей персональных данных;

2.9. Общие требования к доступу в помещения, в которых ведётся обработка персональных данных, и/или размещаются средства обработки персональных данных, и/или хранятся носители персональных данных

Помещения должны размещаться в пределах контролируемой зоны. При этом рекомендуется размещать их на максимальном удалении от границ контролируемой зоны, чтобы ограждающие конструкции (стены, полы, потолки) не являлись смежными с помещениями, расположенными на неохраняемой территории. Целесообразно, чтобы имели шторы (жалюзи).

Эффективность защиты Помещений должна соответствовать требованиям нормативных правовых актов и иных документов по обеспечению безопасности персональных данных.

Достаточность предпринятых мер защиты Помещений, а также необходимость дополнительных мер защиты определяются при проверках Помещений.

2.9.1. Организационно-режимные требования к помещениям, в которых ведётся обработка персональных данных, и/или размещаются средства обработки персональных данных, и/или хранятся носители персональных данных

2.9.1.1. Для Помещений, в которых ведётся обработка персональных данных, необходимо выполнять следующие требования:

– выдача ключей от Помещений должна производиться лицам, работающим в нем или ответственным за это помещение;

– уборка этих Помещений должна производиться в присутствии лиц, ответственных за эти помещения;

– в случае ухода из этих Помещений в рабочее время необходимо их закрывать на ключ.

2.9.1.2. Для Помещений, в которых размещаются средства обработки персональных данных и/или хранятся носители персональных данных, необходимо выполнять следующие требования:

– помещения должны быть оборудованы охранной и противопожарной сигнализацией, камерами видеонаблюдения;

– помещения кабинетов должны быть оборудованы шкафами для хранения информации на бумажных носителях;

– ремонт Помещения должен проводиться под наблюдением специально назначенного лица.

2.9.1.3. В случае обнаружения факта несанкционированного проникновения в Помещения должно производиться расследование.

## 3. Пресечение (устранение) нарушений установленных норм и требований по обеспечению безопасности персональных данных

Своевременное и оперативное пресечение (устранение) нарушений норм и требований по обеспечению безопасности персональных данных является важнейшим требованием сохранения конфиденциальности персональных данных.

Невыполнение предписанных мер по обеспечению безопасности персональных данных считается предпосылкой к нарушению конфиденциальности персональных данных (далее – предпосылка).

По каждой предпосылке немедленно докладывается лицу, ответственному за организацию обработки персональных данных или непосредственно ректору Института; для выяснения обстоятельств и причин невыполнения установленных требований проводится расследование.

Для проведения расследования по приказу ректора Института назначается комиссия из компетентных лиц. Комиссия обязана установить, имелось ли нарушение конфиденциальности персональных данных. После окончания расследования принимаются меры по устранению нарушений.

Работники, организующие и осуществляющие обработку и/или защиту персональных данных, обязаны строго соблюдать требования по защите персональных данных и несут ответственность за нарушения, приводящие к нарушению конфиденциальности персональных данных.

Нарушения норм и требований по обеспечению безопасности персональных данных делятся на три категории:

**нарушение первой категории:**

невыполнение норм и требований по обеспечению безопасности персональных данных, в результате которого произошло нарушение конфиденциальности персональных данных;

По всем случаям нарушений первой категории немедленно докладывается лицу, ответственному за организацию обработки персональных данных или непосредственно ректору Института.

**нарушение второй категории:**

невыполнение норм и требований по обеспечению безопасности персональных данных, в результате которого имелась или имеется реальная возможность нарушения конфиденциальности персональных данных;

**нарушение третьей категории:**

невыполнение других требований по обеспечению безопасности персональных данных, не приводящих к нарушениям первой и второй категорий.

О нарушениях второй и третьей категорий докладывается лицу, ответственному за организацию обработки персональных данных. По указанию данного лица немедленно организуется пресечение нарушения, выявляется причина допущенного нарушения, оценивается степень возможного ущерба и принимаются меры к его устранению.

## 4. Регулирование деятельности по обеспечению безопасности персональных данных

Регулирование деятельности по обеспечению безопасности персональных данных осуществляется посредством разработки и ввода в действие следующих документов:

1. Приказ о перечне лиц, имеющих необходимый доступ к персональным данным, обрабатываемым в информационной системе персональных данных;
2. Приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;
3. Перечень персональных данных, обрабатываемых в информационных системах персональных данных;
4. Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных;

5. Политика безопасности персональных данных;

6. Журнал ознакомления работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Института в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

7. Журнал учета машинных носителей персональных данных в информационной системе персональных данных.

8. Границы контролируемой зоны информационной системы персональных данных.

9. Требования к обработке в информационной системе персональных определяются в соответствии с Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

10. Журнал учета обращений субъектов персональных данных при обработке персональных данных в информационной системе персональных данных.

11. Соглашение о неразглашении персональных данных;

12. Типовой раздел по конфиденциальности в трудовом, гражданско-правовом договоре;

13. Согласие на обработку персональных данных;

14. Инструкции пользователя информационной системы персональных данных и лица, обрабатывающего персональные данные без использования информационных систем;

15. Иное.

## 5. Осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных законодательству РФ

5.1. Внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному закону от 27 июля 2006г. № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, Положению о персональных данных, иным локальным нормативным актам о персональных данных осуществляется лицом, ответственным за организацию обработки персональных данных и за обеспечение безопасности персональных данных.

5.2. Внутренний контроль включает в себя:

- мониторинг состояния технических и программных средств, входящих в состав системы защиты персональных данных;

- контроль соблюдения требований по обеспечению безопасности персональных данных (требований законодательства в области защиты персональных данных, требований локальных актов Института, сформулированных на основе анализа рисков нарушения безопасности персональных данных, договорных требований).

5.3. Перечень мероприятий по проведению внутреннего контроля соответствия обработки персональных данных требованиям законодательства устанавливается приказом ректора Института.

## 6. Техническая защита персональных данных

6.1. Общие положения

Для защиты персональных данных, обрабатываемых в Институте, внедрена система защиты персональных данных – комплексная система, позволяющая обеспечить конфиденциальность (целостность, доступность и др.) персональных данных, хранящихся и обрабатываемых в Организации.

Внедрение или модернизация системы защиты персональных данных представляет собой поэтапный процесс, учитывающий особенности имеющейся информационной системы персональных данных и включает в себя следующие этапы:

– предпроектное обследование информационной системы персональных данных;
– определение требований к системе защиты персональных данных;
– проектирование системы защиты персональных данных;
– создание системы защиты персональных данных.

Обоснование комплекса мероприятий по обеспечению безопасности персональных данных в информационной системе персональных данных Института производится с учетом результатов оценки опасности угроз, проведенных Институтом, и определения класса информационной системы персональных данных.

Защита персональных данных обеспечивается на всех технологических этапах передачи, обработки и хранения персональных данных и при всех режимах работы информационной системы персональных данных. При этом реализованные в системе меры (механизмы) защиты от несанкционированного доступа не должны ухудшать основные функциональные характеристики информационной системы персональных данных.

Меры технической защиты:

- защита паролем компьютеров с персональными данными;
- использование системы паролей при работе в сети (на портале);

6.2. Требования к уровням системы защиты персональных данных

Физический уровень защиты должен обеспечивать невозможность доступа, изменения, уничтожения материальных носителей персональных данных лицами, не уполномоченными на такие действия. Физический уровень защиты обеспечивается средствами: ограничения доступа третьих лиц в помещения, где ведется обработка персональных данных, ограничение доступа к компьютерной технике с помощью которой ведется автоматизированная обработка персональных данных для категорий работников, не имеющих права доступа к персональным данным; защита от несанкционированного физического доступа к информации (хранение персональных данных в закрытых шкафах, ящиках, сейфах); контроль за действиями лиц, обрабатывающими персональные данные; территориальное разделение деятельности лиц, имеющих различные полномочия в области обработки персональных данных; и иное.

Информационный уровень защиты должен обеспечивать невозможность доступа, изменения, уничтожения персональных данных, обрабатываемых в информационной системе персональных данных, лицами, не уполномоченными на такие действия. Информационный уровень защиты обеспечивается путем: разграничения доступа к данным; использования аппаратных ключей; использования защиты паролем компьютеров с персональными данными; использования системы паролей при работе в сети (на портале); использования средств антивирусной защиты; использования средств межсетевого экранирования; ведения журнала входов/выходов в систему; ведения журнала событий; и иное.

Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Для функционирующих информационных систем персональных данных доработка (модернизация) системы защиты персональных данных должна проводиться в случае, если:

– изменился состав или структура самой информационной системы персональных данных или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки персональных данных, топологии информационной системы персональных данных);

– изменился состав угроз безопасности персональных данных, обрабатываемых в информационной системе персональных данных;

– изменился класс информационной системы персональных данных.

## 7. Требования к квалификации работников, осуществляющих обработку персональных данных

Работники, осуществляющие обработку персональных данных и ответственные за обеспечение её безопасности, должны иметь квалификацию, достаточную для поддержания требуемого режима безопасности персональных данных.

В этих целях вводится система обеспечения требуемого уровня квалификации. Для всех лиц, обрабатывающих персональные данные, проводятся инструктажи по обеспечению безопасности персональных данных.

Обязанность по реализации системы обеспечения требуемого уровня квалификации возлагается на лицо, ответственное за организацию обработки персональных данных, которое обязано организовывать инструктирование и обучение работников; и вести персональный учёт работников, прошедших инструктирование и обучение.

## 8. Ответственность

Работники Института, разгласившие персональные данные субъектов персональных данных, а также работники, по вине которых произошло нарушение конфиденциальности персональных данных, и работники, создавшие предпосылки к нарушению конфиденциальности персональных данных, несут ответственность, предусмотренную действующим законодательством Российской Федерации, внутренними документами Института и условиями трудового договора.

## 9. Заключительные положения

Развитие системы информационной безопасности и совершенствование методов и средств защиты является непрерывным процессом, в связи с чем возникает необходимость пересмотра положений настоящей Политики.

Внесение изменений в Политику может быть вызвано изменениями в информационной системе персональных данных, системе защиты персональных данных, изменениями нормативных правовых актов и иных документов.

Внесению изменений в Политику предшествуют:

– обследование и анализ изменений в информационной системе персональных данных, системе защиты персональных данных;

– анализ изменений нормативных правовых актов и иных документов.

По завершении вышеназванных процедур анализа и обследования в Политику обеспечения безопасности персональных данных вносятся изменения (дополнения, исключения, новые редакции).

Контроль исполнения требований настоящей Политики осуществляется лицом, ответственным за организацию обработки персональных данных Организации.

Ответственность должностных лиц Института, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами Института.