МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМ. Р.Е. АЛЕКСЕЕВА»
(НГТУ)

ПРИКАЗ

«____» _____20 г № _____

г. Нижний Новгород

О реализации №152-ФЗ «О персональных данных»

В целях принятия мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», в том числе выполнения требований к защите персональных данных, установленных постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», и постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

ПРИКАЗЫВАЮ:

1. Утвердить Перечень информационных систем персональных данных (Приложение № 1 к настоящему приказу).
2. Утвердить Перечень персональных данных, обрабатываемых в связи с реализацией трудовых отношений, а также в связи с деятельностью организации (Приложение № 2 к настоящему приказу).
3. Утвердить Перечень ответственных лиц за помещения, в которых обрабатываются персональные данные (Приложение №3 к настоящему приказу).
4. Утвердить Порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных (Приложение № 4 к настоящему приказу).
5. Утвердить правила организации режима обеспечения безопасности помещений, в которых размещена информационная система (Приложение № 5 к настоящему приказу).
6. Утвердить примерную форму должностной инструкции ответственного за обеспечение безопасности персональных данных (Приложение № 6 к настоящему приказу).
7. Утвердить правила доступа к персональным данным, обрабатываемым в информационной системе (Приложение № 7 к настоящему приказу).
8. Утвердить таблицы разграничения доступа к персональным данным (Приложение № 8 к настоящему приказу).
9. Утвердить положение по организации и обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных (Приложение № 9 к настоящему приказу).
10. Утвердить форму акта об уничтожении материальных носителей персональных данных (Приложение № 10 к настоящему приказу).
11. Руководителям подразделений и ответственным лицам, указанным в приложении №3 к настоящему приказу, разработать должностные инструкции, ознакомить с должностной инструкцией и настоящим приказом под роспись работников, организующих работу и допущенных к работе с информационными системами, содержащими персональные данные.
12. Директору института переподготовки специалистов Ермилину А.С. спланировать и организовать в 3-4 квартале 2016 года занятие по повышению квалификации с работниками, допущенными к работе с информационными системами, содержащими персональные данные.

13. Контроль за исполнением настоящего приказа возложить на первого проректора Ширяева Михаила Виссарионовича, лицо, ответственное за организацию обработки персональных данных.

Ректор С.М. Дмитриев

Проект вносит:
Начальник УК
А.Ю. Лапшов

Начальник УИ
А.М. Лабаев

СОГЛАСОВАНО:
Первый проректор
М.В.Ширяев
Проректор по учебной работе
Е.Г.Ивашкин
Проректор по научной работе
Н.Ю.Бабанов
Проректор по АХР
А.Г.Князев
Начальник юридической службы
А.В.Маркеева
Главный бухгалтер
Н.Ф. Кузнецова
Начальник ПФУ
С.Ю.Обыденнова
Директор института
В.Г. Баранов
Директор института
М.Г. Михаленко
Директор института
А.Б. Дарьенков
Директор института
С.Н. Митяков
Директор института
А.Е. Хробостов
Директор института
А.Ю. Панов
Директор института
А.М. Грошев
Директор филиала
В.В. Глебов
Директор филиала
В.Ф Кулепов

Приложение № 1
утверждено приказом
от «____» _____ 201_ г. № ____

Перечень информационных систем персональных данных

№ п/п	Наименование информационной системы персональных данных
1	Информационная система персональных данных «Университет» (включает подсистемы «Деканат», «Деканат ДПИ», «Магистратура», «Аспирантура», «Диплом», «Диплом АПИ», «Абитуриент», «Подготовительные курсы», «Олимпиады»)
2	Информационная система персональных данных «Парус» (включает подсистемы «Парус НГТУ», «Парус АПИ», «Парус ДПИ»)
3	Информационная система персональных данных «Единая информационная система АПИ»
4	Информационная система персональных данных «Платежи студентов АПИ»

Приложение № 2
утверждено приказом
от «____» _____ 201_ г. № ____

Перечень персональных данных, обрабатываемых в связи с реализацией трудовых отношений, а также в связи с деятельностью организации

Наименование информационной системы персональных данных	Цель обработки персональных данных	Перечень персональных данных
1. Информационная система персональных данных «Парус»	Персональные данные сотрудников обрабатываются с целью исполнения трудового договора (контракта), сведения, необходимые для исчисления, удержания и перечисления налогов; сведения по учету в системе обязательного пенсионного страхования и др.	Фамилия, имя, отчество, дата и место рождения, гражданство, ИНН, СНИЛС, Пол, знание иностранного языка, образование, профессия и стаж работы, состояние в браке и состав семьи, номер паспорта, дата и место его выдачи, место жительства и дата регистрации, сведения о воинском учете, другие сведения, предусмотренные унифицированной формой № Т-2, перечень доходов с указанием источника и размера, наличие и размеры налоговых вычетов, дата приема на работу (при приеме на работу в отчетный период), дата увольнения (при увольнении в отчетный период), сумма дохода, на который начислялись страховые взносы, сумма начисленных страховых взносов
2. Информационная система персональных данных «Университет»	Персональные данные сотрудников и несотрудников связанных с образовательной деятельностью НГТУ. Персональные данные студентов и абитуриентов.	Фамилия, имя, отчество, ИНН, дата рождения, гражданство, документ, удостоверяющий личность, его серия и номер, адрес регистрации, сведения об образовании, знание иностранных языков и прочие сведения, предусмотренные федеральным законом N 273-ФЗ от 29.12.2012
3. Информационная система персональных данных «Единая информационная система АПИ»	Персональные данные штатных и внештатных сотрудников, связанных с образовательной деятельностью АПИ. Персональные данные студентов.	Фамилия, имя, отчество, ИНН, дата рождения, гражданство, документ, удостоверяющий личность, его серия и номер, адрес регистрации, сведения об образовании, знание иностранных языков и прочие сведения, предусмотренные федеральным законом N 273-ФЗ от 29.12.2012 Сведения об успеваемости студентов
4. Информационная система персональных данных «Платежи студентов АПИ»	Персональные данные студентов.	Фамилия, имя, отчество, курс, группа, документ, удостоверяющий личность, его серия и номер

Приложение № 4
утверждено приказом
от «____» _____ 201_ г. № ____

Порядок
доступа сотрудников в помещения, в которых ведется обработка персональных данных

1. Доступ сотрудников в помещения, в которых ведется обработка персональных данных, осуществляется с учетом обеспечения безопасности персональных данных.

2. Для помещений, в которых обрабатываются персональные данные (далее – Помещения), обеспечивается режим безопасности, при котором исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

3. Право самостоятельного входа в помещения имеют сотрудники, непосредственно работающие в этих помещениях и лицо, ответственное за организацию обработки персональных данных.

4. Иные лица допускаются в Помещения по согласованию с руководителем или его заместителем по направлению деятельности и в сопровождении лица, работающего в этом Помещении.

5. Помещения по окончании рабочего дня должны закрываться на ключ и сдаваться под охрану.

6. Вскрытие и закрытие (опечатывание) Помещения производится лицами, имеющими право доступа.

7. Уборка Помещения должна производиться в присутствии лица, осуществляющего обработку персональных данных.

8. Перед закрытием Помещения по окончании рабочего дня, лица, имеющие право доступа в помещения, обязаны:

- убрать материальные носители персональных данных в шкафы, закрыть и опечатать шкафы;
- отключить технические средства (кроме постоянно действующей техники) и электроприборы от сети, выключить освещение;
- закрыть окна.

9. Перед открытием Помещения лица, имеющие право доступа в помещения, обязаны:

- провести внешний осмотр с целью установления целостности двери и замка;
- открыть дверь и осмотреть Помещение, проверить наличие и целостность печатей на шкафах, где хранятся материальные носители.

10. При обнаружении неисправности двери и запирающих устройств необходимо:

- не вскрывая Помещение, доложить непосредственному руководителю;
- в присутствии лица, ответственного за организацию обработки персональных данных и непосредственного руководителя, вскрыть Помещение и осмотреть его;
- составить акт о выявленных нарушениях и передать его руководителю для организации служебного расследования.

11. Ответственность за соблюдение порядка доступа в Помещения возлагается на ответственных за помещения в которых обрабатываются персональные данные.

12. Сотрудники, должны быть ознакомлены с настоящим «Порядком доступа в помещения, в которых ведется обработка персональных данных».

Приложение № 5
утверждено приказом
от «____» _____ 201_ г. № ____

Правила организации режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения

1. Настоящие правила устанавливают требования к организации режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (далее Помещения).

2. Пропускной режим предусматривает:

- защиту от проникновения посторонних лиц в помещения, которая обеспечивается организацией режима доступа, а также соответствующей инженерно-технической защитой помещений (наличие охранной сигнализации).
- запрет на внос и вынос за пределы помещения материальных носителей персональных данных;
- определение перечня должностных лиц, имеющих право доступа в помещения.

3. Внутриобъектовый режим предусматривает:

- назначение ответственного за помещение;
- помещения, в которых обрабатываются персональные данные с использованием средств автоматизации и без использования таких средств, должны иметь прочные двери, оборудованные механическими замками, а при необходимости, замками с контролем доступа;
- в нерабочее время помещения должны закрываться, а ключи сдаваться охране;
- выдачу ключей от помещений по списку, утвержденному руководителем;
- в случае ухода в рабочее время из помещения сотрудников, необходимо это помещение закрыть на ключ;
- уборка помещения должна производиться в присутствии лица, ответственного за это помещения.
- пребывание в помещениях посторонних лиц, не имеющих права доступа в эти помещения, разрешено только после согласования с руководителем или его заместителем по направлению деятельности и в сопровождении лица, работающего в этом помещении.
- контроль за пребыванием в помещении посторонних лиц, не имеющих права доступа в эти помещения, осуществляет ответственный за это помещение.

4. Защита информационной системы и машинных носителей персональных данных от несанкционированного доступа, повреждения или хищения:

- в период эксплуатации информационных систем персональных данных должны быть предусмотрены меры по исключению случаев несанкционированного доступа при проведении ремонтных, профилактических и других видов работ;
- в случае необходимости проведения ремонтных работ средств вычислительной техники, входящих в состав информационной системы, с привлечением специализированных ремонтных организаций обеспечивается обязательное гарантированное уничтожение (стирание) персональных данных и другой конфиденциальной информации записанной на материальном носителе под контролем лица, ответственного за организацию обработки персональных данных с составлением соответствующего акта (приложение к приказу №10);
- хранение съемных машинных носители персональных данных должно исключать возможность несанкционированного доступа к ним.

5. Сотрудники должны быть ознакомлены с настоящими Правилами.

Приложение № 6
утверждено приказом
от «____» _____ 201_ г. № ____

Примерная форма должностной инструкции
ответственного за обеспечение безопасности персональных данных

1. Общие положения

1.1. Должностная инструкция ответственного за обеспечение безопасности персональных данных (далее – Инструкция) определяет основные обязанности, права и ответственность лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных.

1.2. Лицо, ответственное за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – Ответственный), назначает ректор и оно подотчетно ему.

1.3. Ответственный, в своей работе должен руководствоваться следующими основными законодательными и нормативными правовыми актами Российской Федерации:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);
- Постановление Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Приказ ФСТЭК России от 18 февраля 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»;
- локальные акты Организации.

1.4. Основные понятия и термины, используемые в настоящей Инструкции, применяются в значениях, определенных статьей 3 Федерального закона № 152-ФЗ.

1.5. Ответственный – лицо, выполняющее функции по установке, настройке и сопровождению программных и технических средств, входящих в состав информационной системы персональных данных (далее – ИСПДн), в том числе средств защиты информации.

1.6. Ответственный получает указания непосредственно от руководителей отделов, в которых обрабатываются персональные данные.

2. Обязанности:

2.1 знать и выполнять требования, действующих нормативных правовых актов, Российской Федерации, а также локальных актов, регламентирующих деятельность по защите персональных данных;

2.2 знать требования к защите ПДн, организационные и технические меры по обеспечению безопасности ПДн при их обработке в ИСПДн;

2.3 устанавливать, настраивать и сопровождать средства защиты информации (далее – СЗИ) ИСПДн;

2.4 управлять СЗИ ИСПДн и поддерживать их функционирование;

2.5 резервировать СЗИ ИСПДн или осуществлять контроль за их резервированием, восстанавливать СЗИ ИСПДн;

2.6 участвовать в приемке новых СЗИ ИСПДн;

2.7 назначать права доступа пользователей к объектам доступа (программам, файлам, каталогам, портам и устройствам ввода-вывода) согласно надлежащим образом оформленным разрешениям;

2.8 генерировать ключи, личные идентификаторы для пользователей ИСПДн;

2.9 формировать и управлять списком необходимых реквизитов и значениями атрибутов объектов и субъектов доступа;

2.10 контролировать целостность эксплуатируемого в ИСПДн программного обеспечения, в том числе самих СЗИ, их параметров и режимов с целью недопущения и выявления несанкционированных модификаций;

2.11 контролировать физическую сохранность оборудования ИСПДн, СЗИ ИСПДн, эксплуатационной и технической документации СЗИ ИСПДн, носителей персональных данных, носителей программных СЗИ ИСПДн;

2.12 не допускать установку, использование, хранение и распространение в ИСПДн программных средств, не связанных с выполнением пользователями ИСПДн трудовых (служебных) обязанностей;

2.13 осуществлять текущий, после сбоев, и периодический (не реже 3 раз в год) контроль работоспособности СЗИ ИСПДн;

2.14 контролировать работу пользователей в сетях общего пользования и (или) международного информационного обмена;

2.15 выявлять подозрительные действия пользователей и попытки несанкционированного доступа к информации, обрабатываемой в ИСПДн, путем анализа системных журналов безопасности в ИСПДн. В случае обнаружения или выявления таких попыток, немедленно докладывать ответственному за организацию обработки персональных данных;

2.16 консультировать пользователей ИСПДн в части правил работы с СЗИ, вопросов защиты информации в ИСПДн;

2.17 осуществлять ведение журналов:

– Журнал учета машинных носителей персональных данных;
– Журнал учета СЗИ;

– Журнал учета СКЗИ.

2.18 предоставлять ответственному за организацию обработки персональных данных отчет о состоянии защиты ИСПДн, своевременно докладывать о внештатных ситуациях, выявленных нарушениях требований по защите персональных данных;

2.19 в случае отказа технических средств или программного обеспечения ИСПДн, в том числе средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу.

2.20 принимать меры по реагированию, в случае возникновения внештатных и аварийных ситуаций, с целью ликвидации их последствий.

3. Права:

3.1 требовать от пользователей ИСПДн выполнения законодательных, нормативных правовых актов Российской Федерации, а также локальных актов Организации в части обработки и защиты персональных данных;

3.2 приостанавливать обработку персональных данных в ИСПДн в случаях угрозы их безопасности при нарушении установленной технологии обработки данных и нарушения работы СЗИ ИСПДн;

3.3 вносить предложения по изменению содержания локальных актов Организации с целью соответствия реальным условиям или в случае изменения законодательных и нормативных правовых актов;

3.4 докладывать непосредственному руководителю о нарушениях или невыполнении пользователями требований по защите (обеспечению безопасности) информации.

4. Ответственность

Лицо, ответственное за обеспечение безопасности персональных данных, несет ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

Приложение № 7
утверждено приказом
от «____» _____ 201_ г. № ____

ПРАВИЛА
доступа к персональным данным, обрабатываемым в информационной системе

1. Общие положения

1.1. Настоящие правила определяют порядок доступа к персональным данным, обрабатываемым в информационной системе персональных данных лиц, имеющих доступ к этим персональным данным.

1.2. Настоящие правила разработаны в соответствии с Федеральным законом от 27.07.200 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11. 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.3. Основные понятия и термины, используемые в настоящих правилах, применяются в значениях, определенных статьей 3 Федерального закона № 152-ФЗ.

1.4. Утверждается Перечень персональных данных, обрабатываемых в информационной системе, а также перечень информационных систем.

1.5. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы.

1.6. Управление системой защиты осуществляет ответственный за обеспечение безопасности персональных данных (администратор сети).

2. Организация доступа к персональным данным

2.1. Перечень лиц, доступ которых к персональным данным, обрабатываемым в информационных системах и на материальных (бумажных) носителях, необходим для выполнения ими служебных (трудовых) обязанностей (далее – лица, допущенные к персональным данным) утверждается ректором или лицом, ответственным за обработку персональных данных.

2.2. На основании и в соответствии с утвержденным Перечнем лиц, допущенных к персональным данным, ответственный за обеспечение безопасности разрабатывает Таблицу разграничения доступа к персональным данным, форма которой приведена в Приложении № 1 к настоящим правилам.

2.3. Таблица (матрица) разграничения доступа составляется как на электронном, так и на бумажном носителях.

2.4. Ответственный за обеспечение безопасности персональных данных на основании таблицы доступа предоставляет пользователям доступ к персональным данным, проверяет на его автоматизированном рабочем месте (далее - АРМ) заданные возможности доступа и выдает под расписку персональный идентификатор.

3. Обязанности лиц, допущенных к персональным данным:

- не сообщать конфиденциальную информацию лицам, не имеющим права доступа к ней;
- обеспечивать сохранность материалов с персональными данными;
- не делать неучтенных копий на бумажных и электронных носителях;
- не оставлять включенными АРМ с предоставленными правами доступа после окончания работы (в перерывах) не оставлять материалы с конфиденциальной информацией на рабочих столах. Покидая рабочее место, пользователь обязан убрать документы и электронные носители с конфиденциальной информацией в закрываемые на замок шкафы (сейфы);
- при работе с документами, содержащими персональные данные, исключить возможность ознакомления, просмотра этих документов лицами, не допущенными к работе с ними;
- не выносить документы и иные материалы с персональными данными из служебных помещений, предназначенных для работы с ними;
- не вносить изменения в настройку средств защиты информации;
- немедленно сообщать непосредственному руководителю об утрате, утечке или искажении персональных данных, об обнаружении неучтенных материалов с указанной информацией;
- не допускать действий, способных повлечь утечку персональных данных;
- предъявлять для проверки лицам, наделенным необходимыми полномочиями в соответствии с законодательством Российской Федерации, числящиеся и имеющиеся в наличии документы, касающиеся персональных данных только по согласованию с руководителем Оператора.

4. Порядок доступа должностных лиц органов государственной власти, должностных лиц Оператора и субъектов персональных данных к персональным данным

4.1. Право доступа к персональным данным имеют должностные лица органов государственной власти, иных государственных органов, органов местного самоуправления, которым доступ к такой информации предусмотрен Федеральными законами.

4.2. Право доступа к персональным данным имеют должностные лица Оператора, которым доступ к такой информации предусмотрен Федеральными законами и (или) локальными актами Оператора.

4.3. Доступ к персональным данным субъектов персональных данных осуществляется на основании направленного оператору запроса.

4.4. Порядок учета (регистрации), рассмотрения запросов осуществляется в соответствии с утвержденными Оператором Правилами рассмотрения запросов субъектов персональных данных или их представителей.

4.5. При работе с документами, связанными с предоставлением персональных данных, должен обеспечиваться режим ограниченного доступа к соответствующим документам.

5. Лица, допущенные к персональным данным, должны ознакомиться с настоящими Правилами под роспись.

6. Лица, виновные в нарушении требований настоящих Правил и иных документов, регламентирующих вопросы защиты персональных данных, несут ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение № 9
утверждено приказом
от «____» _____ 201_ г. № ____

Положение по организации и обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных

1. Данное Положение регулирует отдельные вопросы обработки персональных данных субъектов в ФЕДЕРАЛЬНОМ ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМ. Р.Е. АЛЕКСЕЕВА» (НГТУ)**,** в целях обеспечения их защиты от несанкционированного доступа, неправомерного использования или утраты.
2. Настоящее Положение разработано на основании Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона «Об информации, информационных технологиях и защите информации», Федерального закона «О персональных данных», Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правыми актами, операторами, являющимися государственными или муниципальными органами».
3. Настоящее Положение является обязательным для исполнения всеми сотрудниками Организации.
4. Право доступа к персональным данным, в том числе к персональным данным сотрудников, имеют:
- руководитель Организации;
- руководители структурных подразделений Организации (доступ к персональным данным только сотрудников своего подразделения);
- сотрудники Организации в соответствии с должностными регламентами и должностными инструкциями.
5. Утвердить «Обязательство о неразглашении информации содержащей персональные данные» (Приложение).
6. Обработка персональных данных осуществляется после получения согласия субъекта персональных данных, составленного по форме согласно приложению № 1 к настоящему Положению, за исключением случаев, предусмотренных Федеральным законом «О персональных данных», при условии осуществления мер по защите персональных данных.
7. Контроль за исполнением настоящего приказа возложить на заместителя руководителя Организации.

Приложение

Обязательство о неразглашении информации содержащей персональные данные.

Я, _____, паспорт серии _____, номер_____, выданный _____ « ___ » _____ _____ года в период трудовых отношений с НГТУ и в течение _____ лет после их прекращения в соответствии с Положением об обработке и защите персональных данных в НГТУ обязуюсь:

1) не разглашать и не передавать третьим лицам сведения, содержащие персональные данные, которые мне будут доверены или станут известны по работе, кроме случаев, предусмотренных законодательством Российской Федерации и с разрешения ответственного за обработку данных в организации;
2) выполнять требования приказов, положения и инструкций по обработке персональных данных в части меня касающейся;
3) в случае попытки посторонних лиц получить от меня сведения, содержащие персональные данные, а также в случае утери носителей информации, содержащих такие сведения, немедленно сообщить об этом лицу, ответственному за обработку персональных данных;
4) не производить преднамеренных действий, нарушающих достоверность, целостность или конфиденциальность персональных данных, хранимых и обрабатываемых в НГТУ.

До моего сведения также доведены с разъяснениями соответствующие положения по обеспечению сохранности персональных данных при автоматизированной обработке информации, а также при обработке информации без использования средств автоматизации.

Мне известно, что нарушение этого обязательства может повлечь ответственность, предусмотренную трудовым, административным и уголовным законодательством Российской Федерации.

« ___ » _____ 20___ г. _____

(подпись)

Приложение № 10
утверждено приказом
от «____» _____ 201_ г. № ____

_____ _____
(место составления) (дата составления)

АКТ № _____

об уничтожении материальных носителей персональных данных

_____
(наименование подразделения)

Комиссия в составе:
Председатель – _____
Члены комиссии:
_____
_____

провела отбор материальных носителей персональных данных, не подлежащих дальнейшему хранению, и составила настоящий акт о том, что перечисленные в нем материальные носители персональных данных подлежат гарантированному уничтожению.

№ п/п	Дата	Тип и наименование	Регистрационный номер	Производимая операция (стирание, уничтожение и т.п.)	Примечание

Регистрационные данные носителей перед их уничтожением сверили с записями в акте.
На указанных носителях персональные данные уничтожены путем
_____
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители персональных данных уничтожены путем
_____.
(разрезания, сжигания, механического уничтожения и т.п.)

Председатель комиссии: _____ /_____/
Члены комиссии: _____ /_____/