Федеральное государственное
бюджетное образовательное
учреждение высшего
профессионального образования
«Майкопский государственный
технологический университет»

УТВЕРЖДАЮ
Ректор
_____ С.К. Куижева
«31» 12 2013 г.

ПОЛОЖЕНИЕ
О РАБОТЕ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ В ФГБОУ ВПО «МГТУ»

1. Общие положения

1.1. Положение о работе с персональными данными (далее — Положение) определяет условия и порядок обработки персональных данных, которые осуществляет ФГБОУ ВПО "МГТУ" (далее — Оператор).

1.2. Положение разработано во исполнение Политики в отношении работы с персональными данными (далее — Политика) и в соответствии с п. 2 ч. 1 ст. 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее — ФЗ «О персональных данных»), а также следующими нормативными правовыми актами:

— часть вторая Гражданского Кодекса Российской Федерации от 26 января 1996 г. № 14-ФЗ (далее — часть вторая ГК РФ);

— Трудовой Кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ (далее –ТК РФ);

— часть первая Налогового Кодекса Российской Федерации от 31 июля 1998 г. № 146-ФЗ (далее — часть первая НК РФ);

— Федеральный закон «О бухгалтерском учёте» от 6 декабря 2011 г. № 402-ФЗ (далее — ФЗ «О бухгалтерском учёте»);

— постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

— постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2. Организация обработки персональных данных

2.1. В целях обеспечения выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, Оператором назначается ответственный за организацию обработки персональных данных (далее — Ответственный).

2.2. Ответственный обязан:

— обеспечивать утверждение, приведение в действие, а также обновление в случае необходимости Политики, Положения и иных локальных актов по вопросам обработки персональных данных;

— обеспечить неограниченный доступ к Политике, копия которой размещается по адресу нахождения Оператора;

— проводить оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы Оператора;

— ежегодно проводить оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения ФЗ «О персональных данных»;

— ежегодно осуществлять внутренний контроль за соблюдением Оператором и его работниками законодательства о персональных данных, Политики, Положения и иных локальных актов по вопросам обработки персональных данных, в том числе требований к защите персональных данных (далее — Нормативные акты);

— доводить до работников под подпись положения Нормативных актов при

заключении трудового договора, а также по собственной инициативе;

— осуществлять допуск работников к персональным данным, обрабатываемым в информационной системе Оператора, а также к их материальным носителям только для выполнения трудовых обязанностей;

— организовывать и контролировать приём и обработку обращений и запросов субъектов персональных данных, обеспечивать осуществление их прав;

— обеспечивать взаимодействие с уполномоченным органом по защите прав субъектов персональных данных (далее — Роскомнадзор).

3. Обеспечение безопасности персональных данных

3.1. Работники, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять их без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3.2. В целях защиты персональных данных от неправомерных действий (в частности, неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения) Оператором применяется комплекс правовых, организационных и технических мер по обеспечению безопасности персональных данных, составляющий систему защиты персональных данных.

3.3. Применение комплекса мер по обеспечению безопасности персональных данных обеспечивает установленный уровень защищенности персональных данных при их обработке в информационной системе Оператора.

3.4. В целях обеспечения выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, Оператором назначается ответственный за обеспечение безопасности персональных данных в информационной системе.

3.5. Ответственный за обеспечение безопасности персональных данных в информационной системе обязан:

— ежегодно выполнять определение угроз безопасности персональных данных при их обработке в информационной системе Оператора;

— обеспечивать реализацию организационных и технических мер по обеспечению безопасности персональных данных и применение средств защиты информации, необходимых для достижения установленного уровня защищенности персональных данных при обработке в информационной системе Оператора;

— устанавливать правила доступа к персональным данным, обрабатываемым в информационной системе Оператора, а также обеспечивать регистрацию и учёт всех действий с ними;

— организовывать обнаружение фактов несанкционированного доступа к персональным данным и принятие мер по реагированию, включая восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

— ежегодно осуществлять внутренний контроль за обеспечением установленного уровня защищённости персональных данных при обработке в информационной системе Оператора.

4. Осуществление прав субъектов персональных данных

4.1. При обращении субъекта персональных данных или при получении его запроса (далее — Обращение) Ответственный обеспечивает предоставление субъекту персональных данных информации о наличии относящихся к нему персональных данных, а также возможности ознакомления с этими персональными данными в течение 30 дней с даты Обращения.

4.2. При наличии законных оснований для отказа в предоставлении субъекту персональных данных информации о наличии относящихся к нему персональных данных, а также возможности ознакомления с этими персональными данными Ответственный обеспечивает направление субъекту персональных данных мотивированного ответа в письменной форме, содержащего ссылку на положение ч. 8 ст. 14 ФЗ «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в течение 30 дней с даты Обращения.

4.3. При предоставлении субъектом персональных данных сведений, подтверждающих, что его персональные данные, обрабатываемые Оператором, являются неполными, неточными или неактуальными, Ответственный обеспечивает внесение необходимых изменений в персональные данные в течение 7 рабочих дней с даты Обращения.

4.4. При предоставлении субъектом персональных данных сведений, подтверждающих, что его персональные данные, обрабатываемые Оператором, являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Ответственный обеспечивает уничтожение таких персональных данные в течение 7 рабочих дней с даты Обращения.

4.5. Ответственный обеспечивает уведомление субъекта персональных данных о внесенных в его персональные данные изменениях и предпринятых мерах, а также принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

4.6. В случае отзыва субъектом персональных данных согласия на их обработку она может быть продолжена при наличии оснований, указанных в п. 2—11 ч. 1 ст. 6, ч. 2 ст. 10 и ч. 2 ст. 11 ФЗ «О персональных данных».

5. Взаимодействие с Роскомнадзором

5.1. По запросу Роскомнадзора Ответственный организует предоставление локальных актов в отношении обработки персональных данных и документов, подтверждающих принятие мер по выполнению требований ФЗ «О персональных данных», в течение 30 дней с даты получения запроса.

5.2. По требованию Роскомнадзора Ответственный организует уточнение, блокирование или уничтожение недостоверных, или полученных незаконным путем персональных данных в течение 30 дней с даты получения требования.

5.3. В случаях, предусмотренных ст. 22 ФЗ «О персональных данных», Ответственный направляет в Роскомнадзор уведомление о намерении осуществлять обработку персональных данных.

5.4. В случае необходимости Ответственный направляет в Роскомнадзор обращения по вопросам обработки персональных данных, осуществляемой Оператором.

6. Ответственность за нарушение порядка обработки и обеспечения безопасности персональных данных

6.1. В случае нарушения работником положений законодательства в области персональных данных он может быть привлечён к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в порядке, установленном ТК РФ и иными федеральными законами, в соответствии с ч. 1 ст. 24 ФЗ «О персональных данных» и ст. 90 ТК РФ.

6.2. В случае разглашения работником персональных данных, ставших ему известными в связи с исполнением его трудовых обязанностей, трудовой договор с ним может быть расторгнут в соответствии с пп. «в» п. 6 ст. 81 ТК РФ.

Приложения:

1. Порядок работы с персональными данными без использования средств автоматизации в ФГБОУ ВПО «МГТУ».

– Перечень форм, содержащих персональные данные (Приложение № 1);

– Согласие на обработку персональных данных работника (Приложение № 2);

– Обязательство о неразглашении информации, содержащих персональные данные (Приложение № 3);

– Разъяснение юридических последствий отказа предоставить персональные данные (Приложение № 4).

2. Порядок доступа в помещения, в которых ведётся обработка персональных данных в ФГБОУ ВПО «МГТУ».

3. Инструкция по учёту и хранению съёмных носителей персональных данных в ФГБОУ ВПО «МГТУ».

– Журнал учёта съёмных носителей персональных данных в ФГБОУ ВПО «МГТУ» (Приложение).

4. Инструкция по антивирусной защите в информационных системах персональных данных ФГБОУ ВПО «МГТУ».

5. Инструкция по проведению инструктажа лиц, допущенных к работе с информационной системой персональных данных ФГБОУ ВПО «МГТУ».

– Перечень законодательных актов Российской Федерации о персональных данных, документов, определяющих требования к защите персональных данных, внутренних локальных актов, определяющих политику организации в отношении обработки персональных данных, с которыми необходимо ознакомить нового сотрудника при проведении первичного инструктажа (Приложение № 1);

– Журнал учёта прохождения первичного инструктажа работниками, допущенными к работе с ПДн в ИСПДн (Приложение № 2).

6. Инструкция по рассмотрению обращений субъектов персональных данных и их законных представителей в ФГБОУ ВПО «МГТУ».

– Сводная таблица действий Оператора в ответ на обращение субъектов персональных данных, их представителей и запросы Уполномоченного органа по защите прав субъектов персональных данных (Приложение № 1);

– Журнал учёта обращений субъектов персональных данных и их законных представителей в ФГБОУ ВПО «МГТУ». (Приложение № 2);

– Форма запроса субъекта персональных данных о наличии и ознакомлении с персональными данными (Приложение № 3);

– Форма запроса субъекта персональных данных на уточнение персональных данных (Приложение № 4);

– Форма запроса субъекта персональных данных с отзывом согласия на обработку персональных данных (Приложение № 5);

– Форма запроса субъекта персональных данных на блокирование персональных данных (Приложение № 6);

– Форма запроса субъекта персональных данных с отзывом согласия на обработку персональных данных (Приложение № 7);

– Форма уведомления субъекта об устранении неправомерных действий с его персональными данными (Приложение № 8);

– Форма уведомления субъекта об отказе внесения изменений в персональные данные субъекта (Приложение № 9);

– Форма уведомления органа по защите прав субъектов персональных данных (Приложение № 10).

7. Инструкция по порядку уничтожения и обезличивания персональных данных в ИСПДн ФГБОУ ВПО «МГТУ».

– Акт об уничтожении персональных данных.

8. Инструкция по проведению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ФГБОУ ВПО «МГТУ».

– Акт о контроле соответствия обработки персональных данных (Приложение № 1);

– План проведения периодического внутреннего контроля условий обработки персональных данных в ИСПДн ФГБОУ ВПО «МГТУ» (Приложение № 2).

9. Инструкция по организации резервирования и восстановления программного обеспечения, баз персональных данных информационной системы персональных данных ФГБОУ ВПО «МГТУ».

10. Инструкция по учёту лиц, допущенных к работе с персональными данными в информационных системах персональных данных ФГБОУ ВПО «МГТУ».

11. Инструкция пользователя информационной системы персональных данных ФГБОУ ВПО «МГТУ».

12. Инструкция пользователя информационной системы персональных данных при возникновении нештатных ситуаций.

– Источники угроз безопасности персональных данных.

Проректор по информатизации,
безопасности, развитию и
телекоммуникациям В.Ю. Чундышко

Приложение № 1
к Положению о работе с
персональными данными в
ФГБОУ ВПО «МГТУ»

ПОРЯДОК РАБОТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ В ФГБОУ ВПО «МГТУ»

1. Общие положения

1.1. Порядок работы с персональными данными без использования средств автоматизации (далее — Порядок) определяет особенности и порядок работы с персональными данными при их обработке без использования средств автоматизации в ФГБОУ ВПО "МГТУ" (далее — Оператор).

1.2. Порядок разработан во исполнение Политики в отношении работы с персональными данными и в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации».

1.3. Все работники Оператора, непосредственно осуществляющие обработку персональных данных без использования средств автоматизации, должны быть ознакомлены с настоящим Положением под подпись.

2. Особенности и порядок обработки

2.1. Оператор обеспечивает раздельное хранение персональных данных, обрабатываемых без использования средств автоматизации с разными целями.

2.2. Для обработки каждой категории персональных данных используется отдельный материальный носитель.

2.3. При необходимости уничтожение или обезличивание части персональных данных, производится способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на том же материальном носителе (удаление, вымарывание).

2.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), соблюдаются условия:

— типовая форма или связанные с ней документы содержат сведения о цели обработки персональных данных, наименование и адрес Оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

— типовая форма предусматривает поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных,

при необходимости получения такого согласия;

— типовая форма составлена таким образом, что каждый из субъектов персональных данных, содержащихся в документе, имеет возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

— типовая форма исключает объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

Перечень типовых форм, использующихся Оператором, приведён в Приложении к настоящему Порядку.

2.5. Работники Оператора, осуществляющие обработку персональных данных без использования средств автоматизации, информируются о факте такой обработки, об особенностях и правилах.

2.6. Оператор принимает организационные и физические меры, обеспечивающие сохранность материальных носителей персональных данных и исключающие возможность несанкционированного доступа к ним.

2.7. Документы и внешние электронные носители информации, содержащие персональные данные, могут храниться в служебных помещениях Оператора в запираемых шкафах (в сейфах, если таковые имеются в подразделении).

2.8. Перечень лиц, имеющих доступ к персональным данным, обрабатываемым без использования средств автоматизации, в помещения и к местам хранения носителей, ограничен работниками, работающими в указанных помещениях на постоянной основе. Исключена возможность доступа в помещения, где обрабатываются персональные данные без использования средств автоматизации, посторонних лиц без сопровождения допущенного работника.

2.9. Работа с материальными носителями, содержащими персональные данные, организовывается следующим образом. Материальные носители могут находиться на рабочем месте работника в течение времени, необходимого для обработки персональных данных, но не более одного рабочего дня. При этом должна быть исключена возможность просмотра персональных данных посторонними лицами. В конце рабочего дня все материальные носители, содержащие персональные данные, должны быть убраны в запираемые шкафы (в сейфы, если таковые имеются в подразделении). Черновики и редакции документов, испорченные бланки, листы со служебными записями в конце рабочего дня уничтожаются.

3. Ответственность

3.1. Все работники Оператора, допущенные к обработке персональных данных без использования средств автоматизации, несут административную, материальную, уголовную ответственность в соответствии с действующим законодательством за обеспечение сохранности и соблюдение правил работы с персональными данными.

3.2. Ответственность за доведение требований настоящего Положения до работников Оператора несёт ответственный за организацию обработки персональных данных.

Приложение № 1
к Порядку обработки персональных
данных без использования автоматизации
в ФГБОУ ВПО «МГТУ»

Перечень форм, содержащих персональные данные

Наименование формы	Хранить	Основание
Т-1 "Приказ (распоряжение) о приеме работника на работу"	75 лет	Постановление Госкомстата РФ от 5 января 2004 г. № 1
Т-2 "Личная карточка работника"	75 лет	Постановление Госкомстата РФ от 5 января 2004 г. № 1
Т-5 "Приказ (распоряжение) о переводе работника на другую работу"	75 лет	Постановление Госкомстата РФ от 5 января 2004 г. № 1
Т-6 "Приказ (распоряжение) о предоставлении отпуска работнику"	5 лет	Постановление Госкомстата РФ от 5 января 2004 г. № 1
Т-8 "Приказ (распоряжение) о прекращении (расторжении) трудового договора с работником (увольнении)"	75 лет	Постановление Госкомстата РФ от 5 января 2004 г. № 1
Т-9 "Приказ (распоряжение) о направлении работника в командировку"	10 лет	Постановление Госкомстата РФ от 5 января 2004 г. № 1
Т-54 "Лицевой счет"	10 лет	Постановление Госкомстата РФ от 5 января 2004 г. № 1
Т-60 "Записка-расчет о предоставлении отпуска работнику"	5 лет	Постановление Госкомстата РФ от 5 января 2004 г. № 1
Т-61 "Записка-расчет при прекращении (расторжении) трудового договора с работником (увольнении)"	5 лет	Постановление Госкомстата РФ от 5 января 2004 г. № 1
Трудовой договор с работником	75 лет	Трудовой кодекс РФ

Приложение № 2
к Порядку работы с
персональными данными в
ФГБОУ ВПО «МГТУ»

Согласие на обработку и передачу определенному Положением о работе с персональными данными федерального государственного образовательного учреждения высшего профессионального образования «Майкопский государственный технологический университет»» кругу лиц персональных данных.

Обработка персональных данных федеральным государственным бюджетным образовательным учреждением высшего профессионального образования «Майкопский государственный технологический университет», (далее – Университет) осуществляется с целью содействия субъектам персональных данных в осуществлении учебной, научной, трудовой деятельности, обеспечения личной безопасности, а так же наиболее полного исполнения университетом своих обязательств и компетенций. Обработка персональных данных может осуществляться способами, предусмотренными законодательством Российской Федерации.

Перечень персональных данных для обработки, должностных лиц, имеющих доступ к ним, перечень действий с персональными данными определяется Положением о работе с персональными данными ФГБОУ ВПО «МГТУ».

Персональные данные разрешено обрабатывать до момента отзыва настоящего согласия на обработку персональных данных.

Мне известно, что моё согласие на обработку моих персональных данных, может быть отозвано путем подачи мной письменного заявления.

Моё согласие на обработку персональных данных действует в течение срока трудовых отношений (обучения), а также после их прекращения по истечении 75-летнего срока хранения, если иное не определено законом.

Обязуюсь незамедлительно уведомить управление кадров о любых изменениях в персональных данных.

Согласие на обработку персональных данных

_____ _____

(подпись) (ФИО)

Приложение № 3
к Порядку обработки персональных
данных без использования автоматизации
в ФГБОУ ВПО «МГТУ»

Обязательство о неразглашении информации, содержащей персональные данные

Я _____
паспорт серия_____, № _____, выдан _____
_____
предупрежден (-а) о том, что на период исполнения мной должностных обязанностей по Трудовому договору №_____ от _____, заключенному между мной и ФГБОУ ВПО «МГТУ» (далее - оператор), мне может быть предоставлен доступ к персональным данным работников, обучающихся, поступающих в ФГБОУ ВПО «МГТУ» иных лиц, перечень которых утвержден приказом ректора «Об утверждении перечня обрабатываемых персональных данных». Я также понимаю, что во время исполнения своих обязанностей я занимаюсь сбором, обработкой и хранением персональных данных.

Я подтверждаю, что не имею права разглашать персональные данные.

Я обязуюсь при работе с персональными данными соблюдать все требования, описанные в Положении о персональных данных ФГБОУ ВПО «МГТУ», в том числе:

— не использовать и/или не передавать (в любом виде) работникам оператора и третьим лицам, не имеющим на это право, информацию, содержащую указанные персональные данные, которая мне доверена (или будет доверена) или станет известной в связи с исполнением должностных обязанностей;

— в случае попытки третьих лиц или работников оператора, не имеющих на это право, получить от меня информацию, содержащую персональные данные, немедленно сообщать об этом факте своему непосредственному или (в случае отсутствия непосредственного) вышестоящему руководителю;

— не использовать информацию, содержащую персональные данные, с целью получения выгоды;

— в течение 1 (одного) года после прекращения моих прав на допуск к информации, содержащей персональные данные (из-за перехода на должность, не предусматривающую доступ к персональным данным, или прекращения действия Трудового договора), не разглашать и не передавать третьим лицам и неуполномоченным на это работникам оператора известную мне информацию, содержащую персональные данные.

Я понимаю, что разглашение такого рода информации и может нанести ущерб субъектам персональных данных, как прямой, так и косвенный.

Я предупрежден о том, что в случае нарушения мной данного Обязательства, в том числе разглашения мной сведений, содержащих персональные данные, или их утраты, я несу ответственность, предусмотренную действующим законодательством Российской Федерации, в том числе статьей 90 Трудового кодекса Российской Федерации.

С Положением о персональных данных ФГБОУ ВПО «МГТУ» ознакомлен(а).

«____» _____ _____ _____ /_____/
дата подпись расшифровка подписи

Приложение № 4
к Порядку обработки персональных
данных без использования автоматизации
в ФГБОУ ВПО «МГТУ»

Разъяснение юридических последствий отказа предоставить персональные данные

Мне,_____ ,

в соответствии с ч. 2 ст. 18 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» разъяснены юридические последствия моего отказа предоставить свои персональные данные в ФГБОУ ВО "МГТУ".

Я предупрежден(а), что без предоставления моих персональных данных в ФГБОУ ВО "МГТУ", обязательных для заключения трудового договора согласно ст. 57 и 65 Трудового кодекса Российской Федерации, трудовой договор не может быть заключен.

Мне известно, что на основании п. 11 ч. 1 ст. 77 Трудового кодекса Российской Федерации трудовой договор прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность продолжения работы.

___.___._____ _____ _____

Приложение № 2
к Положению о работе с
персональными данными в
ФГБОУ ВПО «МГТУ»

ПОРЯДОК ДОСТУПА В ПОМЕЩЕНИЯ, В КОТОРЫХ ВЕДЁТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В ФГБОУ ВПО «МГТУ»

1. Порядок доступа работников в помещения, в которых ведёт обработку персональных данных ФГБОУ ВПО "МГТУ" (далее — Оператор), устанавливается в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

2. Порядок доступа в помещения распространяется на всех работников Оператора.

3. В помещениях, в которых хранятся и обрабатываются персональные данные, должна быть исключена возможность бесконтрольного проникновения посторонних лиц и несанкционированного доступа к персональным данным.

4. В контролируемые помещения допускаются только работники, уполномоченные на обработку персональных данных в соответствии с «Приказом о допуске к обработке персональных данных». Иные лица допускаются только в присутствии допущенных работников Оператора.

5. Входные двери помещений оборудуются замками, гарантирующими надёжное закрытие в нерабочее время и при выходе из помещения в рабочее время. В случае утери ключей, замок заменяется.

6. Уборка в помещениях, где хранятся и обрабатываются персональные данные, производится только в присутствии допущенного работника.

7. При обнаружении повреждений замков или других признаков, указывающих на возможное проникновение посторонних лиц в помещения, в которых ведется обработка персональных данных, составляется акт и о случившемся немедленно ставится в известность ответственный за обработку персональных данных.

Контроль за соблюдением порядка доступа в помещение, в котором ведется обработка персональных данных, проводится лицом, ответственным за организацию обработки персональных данных.

Приложение № 3
к Положению о работе с
персональными данными в
ФГБОУ ВПО «МГТУ»

Инструкция
по учёту и хранению съёмных носителей
персональных данных в ФГБОУ ВПО «МГТУ»

1. Общие положения

1.1. Настоящая «Инструкция по учёту и хранению съёмных носителей персональных данных» (далее — Инструкция) определяет порядок работы со съёмными носителями персональных данных в ФГБОУ ВПО "МГТУ" (далее — Оператор) в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», иными нормативными правовыми актами РФ в области защиты персональных данных.

1.2. С Инструкцией знакомятся под подпись и выполняют её все лица, допущенные к обработке персональных данных «Приказом о допуске к обработке персональных данных».

2. Определения

2.1. Съёмный носитель персональных данных — носитель информации, используемый для хранения и передачи персональных данных в электронной форме.

2.2. Пользователь — работник Оператора или сотрудник по договору гражданско-правового характера, допущенный к обработке персональных данных «Приказом о допуске к обработке персональных данных».

3. Порядок работы со съёмными носителями

3.1. Ответственный за обеспечение безопасности персональных данных, либо уполномоченный им работник, выдаёт съёмные носители пользователям только в случаях производственной необходимости.

3.2. Все съёмные носители персональных данных учитываются и выдаются пользователям под подпись.

3.3. Пользователям, получившим съёмные носители персональных данных под подпись, запрещается передавать их третьим лицам.

3.4. Ответственный за обеспечение безопасности персональных данных, либо уполномоченный им работник, изымает съёмные носители персональных данных при увольнении пользователя.

3.5. Все съёмные носители персональных данных хранятся в запираемых шкафах или сейфах (металлических шкафах) с кодовыми или внутренними замками (с не менее чем двумя дубликатами ключей).

3.6. Допускается хранение съёмных носителей персональных данных вне запираемых шкафов или сейфов (металлических шкафов) при условиях уничтожения персональных данных в соответствии с Инструкцией по порядку уничтожения и обезличивания персональных данных, либо если на съёмном носителе персональных данных хранятся только персональные данные в зашифрованном или обезличенном виде.

3.7. Право на перемещение съёмных носителей информации за пределы территории, на которой осуществляется обработка, имеют только те лица, которым это необходимо для выполнения своих должностных обязанностей.

3.8. Использование неучтённых съёмных носителей для обработки персональных данных фиксируется как несанкционированное, а ответственный за обеспечение безопасности персональных данных инициирует служебную проверку. По факту выясненных обстоятельств составляется Акт проведения расследования инцидента.

3.9. Пользователи, в случаях утраты или кражи съёмных носителей персональных данных, сообщают об этом ответственному за обеспечение безопасности персональных данных.

3.10. Съёмные носители персональных данных, пришедшие в негодность, или отслужившие в установленный срок, подлежат уничтожению в соответствии с Инструкцией по порядку уничтожения и обезличивания персональных данных. По результатам уничтожения составляется Акт уничтожения персональных данных.

4. Порядок организации учёта съёмных носителей

4.1. На каждом съёмном носителе персональных данных размещается этикетка с уникальным учётным номером.

4.2. Ответственный за обеспечение безопасности персональных данных, либо уполномоченный им работник, при выдаче, приёме, уничтожении съёмных носителей персональных данных вносит в Журнал учета съёмных носителей персональных данных (Приложение):

— учётный номер, размещённый на этикетке на съёмном носителе персональных данных;

— тип съёмного носителя (USB-накопитель, внешний жёсткий диск, CD/DVD диск);

— серийный или инвентарный номер съёмного носителя;

— место хранения (номер запираемого шкафа или сейфа, номер помещения);

— дату и номер Акта уничтожения персональных данных в случае уничтожения съёмного носителя;

— подпись.

4.3. Пользователи при получении либо сдаче съёмных носителей персональных данных заносят в Журнал учёта съёмных носителей персональных данных свои фамилию, имя, отчество, ставят дату и подпись.

5. Ответственность

5.1. Все работники Оператора, допущенные в установленном порядке к работе с

персональными данными, несут административную, материальную, уголовную ответственность в соответствии с действующим законодательством за обеспечение сохранности и соблюдению правил работы с персональными данными.

5.2. Ответственность за доведение требований настоящей Инструкции до работников Оператора несёт ответственный за организацию обработки персональных данных.

Ответственность за обеспечение мероприятий по реализации требований настоящей Инструкции, в том числе учёт, выдачу, уничтожение съёмных носителей персональных данных несёт ответственный за обеспечение безопасности персональных данных.

Приложение
к Инструкции по учёту и хранению
съёмных носителей персональных данных

ЖУРНАЛ УЧЁТА

съёмных носителей персональных данных

Начато:

Окончено:

Срок хранения:

№ п/п	Учётный номер	Тип носителя	Номер (серийный / инвентарный)	Место хранения	Расписка в получении		Дата и номер акта уничтожения	Подпись ответственного лица	Примечание
					ФИО, дата получения, подпись	ФИО, дата сдачи, подпись			
1	2	3	4	5	6	7	8	9	10

Приложение № 4
к Положению о работе с
персональными данными в
ФГБОУ ВПО «МГТУ»

Инструкция по антивирусной защите в информационных системах персональных данных ФГБОУ ВПО «МГТУ».

1. Настоящая инструкция разработана с целью защиты персональных данных от несанкционированного, в том числе случайного, доступа, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

2. Пользователи ИСПДн при работе со съемными носителями обязаны перед началом работы осуществить их проверку на предмет наличия компьютерных вирусов.

3. Ответственный за обеспечение безопасности персональных данных настраивает антивирусное средство на автоматическое обновление и ведет за ним контроль.

4. Ответственный за обеспечение безопасности персональных данных проводит периодическое тестирование всех элементов ИСПДн и установленного программного обеспечения на предмет наличия компьютерных вирусов.

5. Использование для обработки и хранения персональных данных неучтенных носителей запрещается.

6. При обнаружении компьютерного вируса пользователи ИСПДн обязаны немедленно поставить в известность ответственного за обеспечение безопасности персональных данных и прекратить какие-либо действия в соответствующей ИСПДн.

7. Ответственный за обеспечение безопасности персональных данных при обнаружении компьютерного вируса принимает меры для «лечения» зараженного файла и удаления вируса и после этого вновь проводит антивирусный контроль.

8. В случае обнаружения на учтенном в Журнале учёта съёмных носителей персональных данных носителе вируса, не поддающегося лечению, ответственный за обеспечение безопасности персональных данных обязан:

— запретить использование носителя;

— поставить в известность ответственного за организацию обработки персональных данных;

— запретить работу в ИСПДн;

— в возможно короткие сроки обновить пакет антивирусных программ — провести антивирусное сканирование ИСПДн.

Ответственность за поддержание установленного в настоящей инструкции порядка проведения антивирусного контроля возлагается на ответственного за обеспечение безопасности персональных данных.

Приложение № 5
к Положению о работе с
персональными данными в
ФГБОУ ВПО «МГТУ»

Инструкция
по проведению инструктажа лиц, допущенных к работе с информационной системой персональных данных ФГБОУ ВПО «МГТУ»

1. Настоящая инструкция разработана с целью обеспечения безопасности персональных данных, обрабатываемых в информационных системах персональных данных ФГБОУ ВПО "МГТУ" (далее - ИСПДн).

2. При поступлении на работу сотрудника, которому для выполнения своих трудовых обязанностей необходим доступ к ИСПДн (далее - новый сотрудник), ответственный за организацию обработки персональных данных:

а) в соответствии с п.6 ч.1 ст.18.1 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» проводит ознакомление нового сотрудника с положениями законодательства Российской Федерации о персональных данных и локальными актами организации в отношении обработки персональных данных, перечисленными в Приложении к данной инструкции;

б) знакомит нового сотрудника с ответственностью за неисполнение требований по обеспечению безопасности персональных данных в ИСПДн, предусмотренной действующим законодательством Российской Федерации;

в) отмечает в Журнале учета прохождения первичного инструктажа данные о проведении инструктажа.

Новый сотрудник может приступить к исполнению своих непосредственных трудовых обязанностей, связанных с обработкой персональных данных, только после успешного прохождения первичного инструктажа.

Приложение
к Инструкции по проведению инструктажа
лиц, допущенных к работе с информационными
системами персональных данных

Перечень законодательных актов Российской Федерации о персональных данных, документов, определяющих требования к защите персональных данных, внутренних локальных актов, определяющих политику организации в отношении обработки персональных данных, с которыми необходимо ознакомить нового сотрудника при проведении первичного инструктажа

Законодательные акты Российской Федерации о персональных данных:

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 21.07.2014).
2. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
3. Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (для сотрудников, обрабатывающих персональные данные в том числе без использования средств автоматизации).

Внутренние локальные акты ФГБОУ ВО "МГТУ":

- Приказ о допуске к обработке персональных данных.
- Политика в отношении обработки персональных данных.
- Положение об обработке персональных данных.
- Положение о порядке доступа в помещения, в которых ведётся обработка персональных данных.
- Положение об обработке персональных данных без использования средств автоматизации.
- Инструкция по учёту и хранению съёмных носителей персональных данных.
- Инструкция по организации резервного копирования и восстановления в ИСПДн.
- Инструкция по учёту лиц, допущенных к обработке.
- Инструкция по антивирусной защите.
- Инструкция по проведению инструктажа лиц, допущенных к работе с ПДн.
- Инструкция по проведению внутреннего контроля.
- Инструкция по порядку уничтожения и обезличивания персональных данных.
- Инструкция пользователя ИСПДн.

- Инструкция пользователя при возникновении нештатной ситуации.
- План проведения внутреннего контроля.
- Приказ об утверждении перечня помещений, в которых ведется обработка.

Приложение
к Инструкции по проведению инструктажа лиц,
допущенных к работе с информационной системой
персональных данных ФГБОУ ВПО «МГТУ».

ЖУРНАЛ УЧЁТА

прохождения первичного инструктажа работниками, допущенными к работе с персональными данными в информационной системе персональных данных

Начато:

Окончено:

Срок хранения:

№ п/п	ФИО работника	Дата прохождения инструктажа	Подпись работника	ФИО должностного лица, проводившего инструктаж	Подпись должностного лица
1	2	3	4	5	6

Приложение № 6
к Положению о работе с
персональными данными в
ФГБОУ ВПО «МГТУ»

Инструкция
по рассмотрению обращений субъектов персональных данных и их законных представителей в ФГБОУ ВПО "МГТУ"

1. Общие положения

1.1. Настоящая «Инструкция по рассмотрению обращений субъектов персональных данных и их представителей» (далее — Инструкция) определяет порядок обработки поступающих в ФГБОУ ВПО "МГТУ" обращений субъектов персональных данных (далее — Оператор) в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее — ФЗ «О персональных данных»), Постановления Правительства от 21 марта 2012 г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и иными нормативными правовыми актами РФ в области защиты персональных данных.

1.2. С Инструкцией знакомится под подпись ответственный за организацию обработки персональных данных.

2. Права субъектов персональных данных

2.1. В соответствии с ч. 7 ст. 14 ФЗ «О персональных данных» субъект персональных данных имеет право на получение информации в доступной форме, касающейся обработки его персональных данных, в том числе содержащей:

— подтверждение факта обработки персональных данных Оператором;

— правовые основания и цели обработки персональных данных;

— способы обработки персональных данных, применяемые Оператором;

— сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен доступ на основании договора или федерального закона;

— перечень обрабатываемых персональных данных субъекта и источник их получения;

— сроки обработки персональных данных и сроки их хранения;

— порядок осуществления субъектом персональных данных прав,

предусмотренных ФЗ «О персональных данных»;

— сведения о наличии трансграничной передачи;

— наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу.

2.2. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в случае, если:

— обработка персональных данных, в том числе полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

— обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством РФ случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

— доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

— в иных случаях, предусмотренных ч. 8 ст. 14 ФЗ «О персональных данных».

2.3. Субъект персональных данных вправе требовать от Оператора уточнения своих персональных данных, блокирования или их уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

2.4. Субъект персональных данных вправе принимать предусмотренные законом меры по защите своих прав.

2.5. Если сведения, указанные в пункте 2.1 Инструкции, были предоставлены субъекту персональных данных, то повторно субъект может обратиться не ранее чем через тридцать дней после первоначального обращения. Если предоставленные сведения были неполными, то субъект может обратиться повторно до истечения тридцати дней. Обращение должно содержать обоснование направления повторного обращения.

3. Порядок работы с обращениями субъектов персональных данных

3.1. Оператор отвечает на обращения субъектов персональных данных или их законных представителей в сроки, установленные ФЗ «О персональных данных» (Приложение № 1).

3.2. При поступлении обращения субъекта или его законного представителя, ответственный за организацию обработки персональных данных регистрирует обращение в «Журнале учёта обращений субъектов персональных данных и их законных представителей» (Приложение № 2).

3.4. При поступлении обращения субъекта или его законного представителя,

Оператор предоставляет информацию о персональных данных субъекта в течение тридцати дней (Приложение № 3- № 7).

3.5. В случае отзыва субъектом персональных данных согласия на их обработку, она может быть продолжена при наличии оснований, указанных в п. 2—11 ч. 1 ст. 6, ч. 2 ст. 10 и ч. 2 ст. 11 ФЗ «О персональных данных».

3.6. В случае отказа в предоставлении информации субъекту персональных данных или его законному представителю, Оператор даёт в письменной форме мотивированный ответ в течение тридцати дней со дня обращения либо с даты получения обращения.

3.7. При предоставлении субъектом или его законным представителем сведений, подтверждающих, что персональные данные субъекта являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, Оператор вносит в них необходимые изменения, уничтожает или блокирует. О внесенных изменениях и предпринятых мерах Оператор уведомляет субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные субъекта были переданы (Приложение № 8).

3.8. При отсутствии сведений, подтверждающих, что персональные данные субъекта являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, Оператор отказывается вносить изменения и даёт ответ субъекту персональных данных (Приложение № 9).

3.9. Оператор сообщает в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение тридцати дней с даты получения такого запроса (Приложение № 10).

4. Ответственность

– 4.1. Ответственный за организацию обработки персональных данных несёт ответственность в соответствии с действующим законодательством за организацию приёма и обработки обращений субъектов персональных данных и их законных представителей.

Приложение № 1
к Инструкции по рассмотрению
обращений субъектов
персональных данных и их знакомых
представителей

Сводная таблица действий Оператора в ответ на обращения субъектов персональных данных, их представителей и запросы Уполномоченного органа по защите прав субъектов персональных данных

Обращение, запрос	Действия	Срок	Ответ
Обращение субъекта персональных данных или его представителя			
Наличие персональных данных	Подтверждение обработки персональных данных	30 дней (согласно ч. 1 ст. 20 152-ФЗ)	Подтверждение обработки персональных данных
	Отказ от подтверждения обработки персональных данных	30 дней (согласно ч. 2 ст. 20 152-ФЗ)	Уведомление об отказе подтверждения обработки персональных данных

Ознакомление с персональными данными	Предоставление информации по персональным данным	30 дней (согласно ч. 1 ст. 20 152-ФЗ)	Подтверждение обработки персональных данных, правовые основания и цели такой обработки
			Способы обработки персональных данных
			Сведения о лицах, которые имеют доступ к персональным данным
			Перечень обрабатываемых персональных данных и источник их получения
			Сроки обработки персональных данных, в том числе сроки их хранения
			Информация об осуществленной или о предполагаемой трансграничной передаче
	Отказ от предоставления информации по персональным данным	30 дней (согласно ч. 2 ст. 20 152-ФЗ)	Уведомление об отказе предоставления информации по персональным данным

Уточнение персональных данных	Изменение персональных данных	7 рабочих дней со дня предоставления уточняющих сведений (согласно ч. 3 ст. 20 152-ФЗ)	Уведомление о внесенных изменениях
	Отказ от изменения персональных данных	30 дней	Уведомление об отказе изменений персональных данных
Уничтожение персональных данных	Уничтожение персональных данных	7 рабочих дней со дня предоставления сведений о незаконном получении персональных данных или отсутствии необходимости персональных данных для заявленной цели обработки (согласно ч. 3 ст. 20 152-ФЗ)	Уведомление об уничтожении
	Отказ от уничтожения персональных данных	30 дней	Уведомление об отказе уничтожения персональных данных
Отзыв согласия на обработку персональных данных	Прекращение обработки и уничтожение персональных данных	30 дней (согласно ч. 5 ст. 21 152-ФЗ)	Уведомление о прекращении обработки и уничтожении персональных данных
	Отказ от прекращения обработки и уничтожения персональных данных	30 дней	Уведомление об отказе прекращения обработки и уничтожения персональных данных

Недостоверность персональных данных субъекта	Блокировка персональных данных	С момента обращения субъекта персональных данных о недостоверности его персональных данных или с момента получения запроса на период проверки (согласно ч. 1 ст. 21 152-ФЗ)	Уведомление о внесенных изменениях
	Изменение персональных данных	7 рабочих дней со дня предоставления уточненных сведений (согласно ч. 2 ст. 21 152-ФЗ)	
	Снятие блокировки персональных данных		Уведомление об отказе изменения персональных данных
	Отказ изменения персональных данных	30 дней	
Неправомерность действий с персональными данными субъекта	Прекращение неправомерной обработки персональных данных	3 рабочих дня (согласно ч. 3 ст. 21 152-ФЗ)	Уведомление об устранении нарушений
	Уничтожение персональных данных в случае невозможности обеспечения правомерности обработки	10 рабочих дней (согласно ч. 3 ст. 21 152-ФЗ)	Уведомление об уничтожении персональных данных
Достижение цели обработки персональных данных субъекта	Прекращение обработки персональных данных	30 дней (согласно ч. 4 ст. 21 152-ФЗ)	Уведомление об уничтожении персональных данных
	Уничтожение персональных данных		

Информация для осуществления деятельности уполномоченного органа	Предоставление затребованной информации по персональным данным	30 дней (согласно ч. 4 ст. 20 152-ФЗ)	Предоставление затребованной информации по персональным данным
Недостоверность персональных данных субъекта	Блокировка персональных данных	С момента обращения Уполномоченного органа о недостоверности или с момента получения запроса на период проверки (согласно ч. 1 ст. 21 152-ФЗ)	Уведомление о внесённых изменениях
	Изменение персональных данных	7 рабочих дней со дня предоставления уточнённых сведений (согласно ч. 2 ст. 21 152-ФЗ)	
	Снятие блокировки персональных данных		
	Отказ от изменения персональных данных	30 дней	Уведомление об отказе изменения персональных данных
Неправомерность действий с персональными данными субъекта	Прекращение неправомерной обработки персональных данных	3 рабочих дня (согласно ч. 3 ст. 21 152-ФЗ)	Уведомление об устранении нарушений
	Уничтожение персональных данных в случае невозможности обеспечения правомерности обработки	10 рабочих дней (согласно ч. 3 ст. 21 152-ФЗ)	Уведомление об уничтожении персональных данных

Достижение целей обработки персональных данных субъекта	Блокировка персональных данных	30 дней (согласно ч. 4 ст. 21 152-ФЗ	Уведомление об уничтожении персональных данных
	Уничтожение персональных данных		

Приложение № 2
к Инструкции по рассмотрению обращений субъектов
персональных данных и их законных представителей

ЖУРНАЛ УЧЁТА

обращений субъектов персональных данных и

их законных представителей в ФГБОУ ВПО «МГТУ»

Начато:

Окончено:

Срок хранения:

№ п/п	Дата	Номер, реквизиты входящего документа	ФИО запрашивающего лица	Цель обращения	Действия по результатам обращения	Подпись ответственного лица	Примечание
1	2	3	4	5	6	7	8

Приложение № 3
к Инструкции по рассмотрению обращений субъектов
персональных данных и их законных представителей

Форма запроса субъекта персональных данных о наличии и ознакомлении с персональными данными

Кому: ФГБОУ ВПО "МГТУ"
От_____
ФИО субъекта
_____
вид документа
_____
номер документа
_____
дата выдачи и кем выдан документ

Запрос

В соответствии со ст. 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О данных» я имею право получить от вас информацию, касающуюся обработки моих персональных данных.

Прошу вас предоставить мне следующие сведения:

1. Подтверждение факта обработки моих персональных данных;
2. Правовые основания и цели обработки персональных данных;
3. Применяемые способы обработки персональных данных;
4. Какие лица имеют доступ или могут получить доступ к персональным данным;
5. Перечень обрабатываемых персональных данных и источник их получения;
6. Срок хранения персональных данных;
7. Осуществлялась ли трансграничная передача персональных данных, а, если нет, то предполагается ли такая передача.

Ответ на настоящий запрос прошу направить в письменной форме по адресу: _____

в установленные законом сроки.

___.___._____ _____ _____

Приложение № 4
к Инструкции по рассмотрению обращений субъектов
персональных данных и их законных представителей

Форма запроса субъекта персональных данных на уточнение персональных данных

Кому: ФГБОУ ВПО "МГТУ"
От_____
ФИО субъекта
_____
вид документа
_____
номер документа
_____
дата выдачи и кем выдан документ

Запрос

В соответствии с ч. 1 ст. 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О данных» прошу уточнить, обрабатываемые вами, мои персональные данные в соответствии со сведениями:

_____;
(указать уточнённые персональные данные)

и в связи с тем, что _____.
(указать причину уточнения персональных данных)

Ответ на настоящий запрос прошу направить в письменной форме по адресу:

_____в установленные законом сроки.

___.___._____ _____ _____

Приложение № 5
к Инструкции по рассмотрению обращений субъектов
персональных данных и их законных представителей

Форма запроса субъекта персональных данных с отзывом согласия на обработку с персональных данных

Кому: ФГБОУ ВПО "МГТУ"
От_____
ФИО субъекта

_____
вид документа

_____
номер документа

_____
дата выдачи и кем выдан документ

Запрос

В соответствии со ст. 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О данных» прошу уничтожить мои персональные данные:

_____
(указать уничтожаемые персональные данные)

в связи с тем, что_____.
(указать причину уничтожения персональных данных)

Ответ на настоящий запрос прошу направить в письменной форме по адресу:

_____

в установленные законом сроки.

___.___._____ _____ _____

Приложение № 6
к Инструкции по рассмотрению обращений субъектов
персональных данных и их законных представителей

Форма запроса субъекта персональных данных на блокирование персональных данных

Кому: ФГБОУ ВПО "МГТУ"
От_____
ФИО субъекта
_____
вид документа
_____
номер документа
_____
дата выдачи и кем выдан документ

Запрос

В соответствии с ч. 1 ст. 14 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» прошу заблокировать следующие мои персональные данные:

_____;
(указать блокируемые персональные данные)

на срок: _____;
(указать срок блокирования)

в связи с тем, что_____.
(указать причину блокирования персональных данных)

Ответ на настоящий запрос прошу направить в письменной форме по адресу:
_____

в установленные законом сроки.

____.____._____ _____ _____

Приложение № 7
к Инструкции по рассмотрению обращений субъектов
персональных данных и их законных представителей

Форма запроса субъекта персональных данных с отзывом согласия на обработку персональных данных

Кому: ФГБОУ ВПО "МГТУ"
От_____
ФИО субъекта
_____
вид документа
_____
номер документа
_____
дата выдачи и кем выдан документ

Запрос

В соответствии с ч. 5 ст. 21 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» прошу вас прекратить обработку моих персональных данных:
_____.
(указать перечень персональных данных)

Ответ на настоящий запрос прошу направить в письменной форме по адресу: _____в установленные законом сроки.

___.___._____ _____ _____

Приложение № 8
к Инструкции по рассмотрению обращений субъектов
персональных данных и их законных представителей

Форма уведомления субъекта об устранении неправомерных действий с его персональными данными

Субъекту персональных данных:

_____
ФИО
От ФГБОУ ВПО "МГТУ"

Уведомление

Сообщаю вам о том, что допущенные нарушения при обработке персональных данных, а именно

_____

_____, устранены.
(указать допущенные нарушения)

Ректор С.К. Куижева

Приложение № 9
к Инструкции по рассмотрению обращений субъектов
персональных данных и их законных представителей

Форма уведомления субъекта об отказе внесения изменений в персональные данные субъекта

Субъекту персональных данных:

_____
ФИО

От ФГБОУ ВПО "МГТУ"

Уведомление

Сообщаю вам о том, что мы не можем внести изменения в Ваши персональные данные, так как вами не было предоставлено необходимых документов, подтверждающих запрашиваемые вами изменения.

Ректор С.К. Куижева

Приложение № 10
к Инструкции по рассмотрению обращений субъектов
персональных данных и их законных представителей

Форма уведомления органа по защите прав субъектов персональных данных

Руководителю _____
От ФГБОУ ВПО "МГТУ"

Уведомление

Сообщаю вам о том, что персональные данные субъекта

_____

(ФИО)

обрабатываются в ФГБОУ ВПО "МГТУ" с целью

_____

на основании_____;

и составляют: _____.

(перечень персональных данных)

Ректор С.К. Куижева

Приложение № 7
к Положению о работе с
персональными данными в
ФГБОУ ВПО «МГТУ»

Инструкция
по порядку уничтожения и обезличивания персональных данных в ИСПДн ФГБОУ ВПО "МГТУ"

1. Общие положения

1.1. Настоящая инструкция определяет порядок уничтожения и обезличивания информации, содержащей персональные данные, при достижении целей обработки или при наступлении иных законных оснований в ФГБОУ ВПО "МГТУ" (далее — Оператор).

1.2. Инструкция разработана в соответствии с ч. 7 ст. 5, ч. 4 ст. 21 и п. 9 ч. 1 ст. 6 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее — ФЗ «О персональных данных»), «Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ», утверждёнными приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. № 996 и иными нормативными правовыми актами РФ в области защиты персональных данных.

2. Условия и порядок уничтожения информации, содержащей персональные данные

2.1. Оператор уничтожает информацию, содержащую персональные данные:

— по достижении целей обработки или в случае утраты необходимости в достижении этих целей;

— по достижении окончания срока хранения;

— при наступлении иных законных оснований.

2.2. Уничтожение информации, содержащей персональные данные, производится в случае достижения цели обработки в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных.

2.3. Уничтожение информации, содержащей персональные данные, производится в случае выявления неправомерной обработки в срок, не превышающий десяти дней с момента выявления неправомерной обработки персональных данных.

2.4. Ответственными за уничтожение информации, содержащей персональные данные, назначаются ответственный за организацию обработки персональных данных и ответственный за обеспечение безопасности персональных данных в информационной системе Оператора. Ответственные лица подписывают соответствующий «Акт об уничтожении персональных данных» (Приложение).

2.5. К персональным данным, хранимым в электронном виде, относятся файлы, папки, электронные архивы на жестком диске компьютера и съёмных машинных носителях (компакт-дисках CD-R/RW или DVD-R/RW, дискетах 3,5, флеш-носителях).

2.6. Съёмные машинные носители по истечению сроков обработки и хранения на них

персональных данных подлежат уничтожению с целью невозможности восстановления и дальнейшего использования. Это достигается путем деформирования, нарушения единой целостности носителя или его сжигания.

2.7. В случае допустимости повторного использования съёмного машинного носителя применяется программное удаление («затирание») содержимого путём его форматирования с последующей записью новой информации на данный носитель.

2.8. Подлежащие уничтожению файлы с персональными данными, расположенные на жестком диске информационной системы персональных данных, удаляются средствами операционной системы компьютера с последующим «очищением корзины».

2.9. Черновики документов, испорченные листы, варианты и неподписанные проекты документов уничтожаются путём их сожжения или измельчения, или другим путем, исключающим восстановление текста документов.

3. Условия и порядок обезличивания информации, содержащей персональные данные

3.1. Оператор может обезличивать персональные данные в статистических или иных исследовательских целях, по достижении целей обработки персональных данных или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

— замена части данных идентификаторами;

— обобщение, изменение или удаление части данных;

— деление данных на части и обработка в разных информационных системах;

— перемешивание данных;

— другие способы.

3.3. В случае достижения целей обработки персональных данных или в случае утраты необходимости в достижении этих целей способом обезличивания является уменьшение перечня обрабатываемых данных.

3.4. Ответственный за организацию обработки персональных данных назначается ответственным за проведение мероприятий по обезличиванию персональных данных.

3.5. Решение о необходимости обезличивания персональных данных и способе обезличивания принимает ответственный за организацию обработки персональных данных.

3.6. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

3.7. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

3.8. При использовании процедуры обезличивания не допускается совместное хранение персональных данных и обезличенных данных.

3.9. В процессе обработки обезличенных данных, при необходимости, может производиться деобезличивание. После обработки персональные данные, полученные в результате такого деобезличивания, уничтожаются.

3.10. Обработка персональных данных до осуществления процедур обезличивания и

после выполнения операций деобезличивания должна осуществляться в соответствии с законодательством Российской Федерации с применением мер по обеспечению безопасности персональных данных.

4. Ответственность

4.1. Ответственность за осуществление контроля выполнения требований настоящей инструкции несет ответственный за организацию обработки персональных данных Оператора.

4.2. Ответственность за выполнение настоящей инструкции возлагается на ответственного за организацию обработки персональных данных, ответственного за обеспечение безопасности персональных данных и всех работников Оператора, допущенных к обработке обезличенных персональных данных, в соответствии с действующим законодательством.

Приложение
к Инструкции по порядку уничтожения и обезличивания персональных данных

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Майкопский государственный технологический университет»

УТВЕРЖДАЮ
Ректор
_____ С.К. Куижева

«___» _____20____ г.

Структурное подразделение

АКТ

_____ №_____

Об уничтожении персональных данных

Ответственным за организацию обработки персональных данных проведены следующие мероприятия по уничтожению информации, содержащей персональные данные, в информационной системе персональных данных ФГБОУ ВО "МГТУ":

1. Определение носителей персональных данных, цели обработки которых достигнуты или необходимость достижения целей обработки утрачена, либо достигнуто окончание срока хранения.
2. Уничтожение указанных в п. 1 носителей в соответствии с Таблицей № 1:

№ п/п	Название, дата, рег. № носителя	Тип носителя	Метод гарантированного уничтожения информации
1	2	3	4

Ответственный за организацию обработки персональных данных за организацию _____

Приложение № 8
к Положению о работе с
персональными данными в
ФГБОУ ВПО «МГТУ»

Инструкция
по проведению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ФГБОУ ВПО "МГТУ"

1. Общие положения

1.1. Настоящая «Инструкция по проведению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных» (далее — Инструкция) определяет порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ФГБОУ ВПО "МГТУ" (далее — Оператор) в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», иными нормативными правовыми актами РФ в области защиты персональных данных.

1.2. Инструкцию обязаны выполнять все работники Оператора, допущенные к обработке персональных данных «Приказом о допуске к обработке персональных данных».

2. Порядок проведения внутреннего контроля

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям Оператор организует проведение периодических проверок условий обработки персональных данных.

2.2. Внутренний контроль проводит ответственный за организацию обработки персональных данных (далее — Ответственный) либо комиссия по персональным данным, назначенная Оператором.

2.3. Внутренний контроль осуществляется не реже 1 раза в год. При необходимости контроль может проводиться чаще в соответствии с поручением Оператора.

2.4. Ответственный либо комиссия проводит внутренний контроль непосредственно на месте обработки персональных данных, опрашивает работников, осуществляющих обработку персональных данных, осматривает рабочие места. Все работники обязаны по запросу контролирующих предъявить все материалы и документы, числящиеся за ними, дать устные или письменные объяснения по существу заданных вопросов.

2.5. По результатам проверки составляется Акт контроля соответствия обработки персональных данных по форме, приведённой в Приложении 1.

2.6. При выявлении нарушений в ходе проверки Ответственным либо

Председателем комиссии:

2.6.1. делается запись в Акте контроля соответствия обработки персональных данных о мероприятиях по устранению нарушений и сроках их исполнения;

2.6.2. информация о нарушениях и о мерах для их устранения доводится до сведения руководителя организации.

2.7. В ходе внутренней проверки контролирующие проводят:

— контроль соответствия обработки персональных данных требованиям законодательства, нормативных актов по вопросам обработки персональных данных;

— контроль выполнения организационных и технических мер по обеспечению безопасности персональных данных при их обработке;

— проверку параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;

— анализ изменения угроз безопасности персональных данных в информационной системе Оператора, возникающих в ходе её эксплуатации;

— контроль наличия или отсутствия фактов несанкционированного доступа к персональным данным;

— контроль соблюдения работниками, допущенными к обработке персональных данных, «Положения об обработке персональных данных», «Инструкции по порядку уничтожения и обезличивания персональных данных», «Инструкции по учёту и хранению съёмных носителей персональных данных», «Положения о порядке доступа в помещения» и других локальных актов, регламентирующих обработку персональных данных Оператора;

— проверку «Журнала учёта съёмных носителей персональных данных»

3. Ответственность

3.1. За организацию проведения внутреннего контроля соответствия обработки персональных данных требованиям законодательства отвечает Ответственный либо Председатель комиссии.

3.2. Ответственность за соблюдение Инструкции возлагается на всех работников Оператора, на которых распространяется Инструкция.

Приложение № 1
к Инструкции по проведению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Майкопский государственный технологический университет»

УТВЕРЖДАЮ
Ректор
_____ С.К. Куижева

«___» _____20____ г.

АКТ
О контроле соответствия обработки персональных данных

В соответствии с п. 4 ч. 1 ст. 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» в ФГБОУ ВПО "МГТУ" (далее — Оператор) проведен контроль соответствия обработки персональных данных следующим актам:

— Федеральному закону от 27июля 2006 г. № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, в том числе «Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утверждённому постановлением Правительства от 15 сентября 2008 г. № 687, и «Требованиям к защите персональных данных при их обработке в информационных системах персональных данных», утверждённым постановлением Правительства от 1 ноября 2012 г. № 1119;

— Политике в отношении обработки персональных данных;

— Положению об обработке персональных данных;

— иным локальным актам.

В результате проведения контроля

Выявлены нарушения:

Меры по устранению нарушений:

Срок устранения нарушений:

Ответственный за организацию обработки персональных данных _____

Приложение № 2
к Инструкции по проведению внутреннего контроля
соответствия обработки персональных данных
требованиям к защите персональных данных

План проведения периодического внутреннего контроля условий обработки персональных данных в ИСПДн ФГБОУ ВПО "МГТУ"

Общие положения

1. Периодический внутренний контроль соответствия обработки и защиты персональных данных установленным требованиям (далее - внутренний контроль) в информационных системах персональных данных ФГБОУ ВПО "МГТУ" (далее - ИСПДн) проводится в целях выполнения требований п. 4 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

2. Внутренний контроль:

— осуществляется в соответствии с Инструкцией по проведению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;

— проводится комиссией, назначенной приказом «О создании комиссии», а при отсутствии таковой - Ответственным за организацию обработки персональных данных.

3. План проведения внутреннего контроля содержит следующую информацию:

— название мероприятия;

— период проведения контроля.

4. По результатам проведения внутреннего контроля оформляется Акт контроля соответствия обработки персональных данных.

Ректор ФГБОУ ВПО "МГТУ" определяет сроки внутреннего контроля, но не реже 1 раза в 3 года.

План проведения внутреннего контроля

№	Мероприятие	Дата
1.	Проверка полноты, качества и актуальности разработанных внутренних распорядительных и нормативно-методических документов, регламентирующих обработку и обеспечение безопасности ПДн	
2.	Контроль выполнения требований по режиму доступа в здание, помещения и на автоматизированные рабочие места, где ведется обработка ПДн	
3.	Проверка порядка использования технических средств защиты ПДн	
4.	Проверка выполнения требований действующих нормативных документов по защите персональных данных	
5.	Проверка и выявления изменений в режиме обработки ПДн	
6.	Анализ и пересмотр имеющихся угроз безопасности ПДн, выявление новых угроз	
7.	Проверка актуальности сведений в Реестре операторов персональных данных Роскомнадзора (если организация включена в Реестр)	
8.	Подведение итогов	
9.	Устранение недостатков	
10.	Составление акта внутреннего контроля	
11.	Доклад руководителю ФГБОУ ВПО "МГТУ"	

Приложение № 9
к Положению о работе с
персональными данными в
ФГБОУ ВПО «МГТУ»

Инструкция
по организации резервирования
и восстановления программного обеспечения,
баз персональных данных информационной системы
персональных данных ФГБОУ ВПО "МГТУ"

1. Настоящая инструкция разработана с целью обеспечения возможности незамедлительного восстановления персональных данных в информационной системе персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационной системы персональных данных ФГБОУ ВПО "МГТУ".

2. Резервированию подлежат базы данных и файлы, содержащие персональные данные.

3. Резервирование выполняется штатным средством архивирования системы и данных «ntbackup» и производится на локальный дисковый массив. Процедура резервного копирования производится каждый день.

4. Ответственным за процедуру резервирования и восстановления назначается ответственный за организацию обработки персональных данных.

5. Восстановление файлов производится путем разархивирования файлов базы данных в исходный каталог.

Приложение № 10
к Положению о работе с
персональными данными в
ФГБОУ ВПО «МГТУ»

Инструкция
по учету лиц, допущенных к работе с персональными данными в информационных системах персональных данных ФГБОУ ВПО "МГТУ"

1. Настоящая инструкция определяет порядок учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных ФГБОУ ВПО "МГТУ" (далее - ИСПДн).

2. Порядок допуска работника к работе с персональными данными:

— утверждение приказом о допуске к обработке персональных данных перечня должностей работников, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей (далее - Перечень);

— прохождение первичного инструктажа, включающего ознакомление со всеми нормативными документами, регламентирующими работу с персональными данными, согласно Инструкции по проведению инструктажа лиц, допущенных к работе с персональными данными с внесением соответствующей информации в Журнал учёта прохождения первичного инструктажа сотрудниками, допущенными к работе с персональными данными в ИСПДН;

— внесение записи в Журнал учёта прав доступа к ИСПДн.

3. Допуск работника к персональным данным прекращается:

— в случае обнаружения нарушений порядка обработки персональных данных до выяснения и устранения причин нарушений;

— в случае увольнения сотрудника с момента подписания приказа об увольнении;

— при изменении его служебных обязанностей с момента утверждения нового Перечня.

Приложение № 11
к Положению о работе с
персональными данными в
ФГБОУ ВПО «МГТУ»

Инструкция пользователя информационной системы персональных данных ФГБОУ ВПО "МГТУ"

1. Пользователем информационной системы персональных данных ФГБОУ ВПО "МГТУ" (далее - Пользователь) является любой работник ФГБОУ ВПО "МГТУ", осуществляющий обработку персональных данных в информационной системе персональных данных ФГБОУ ВПО "МГТУ" (далее - ИСПДн).

Согласно ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных» обработка ПДн - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (далее - ПДн).

2. Пользователь в своей работе руководствуется настоящей Инструкцией, Положением об обеспечении безопасности ПДн, руководящими и нормативными документами ФСТЭК и ФСБ России и внутренними нормативными актами ФГБОУ ВО "МГТУ", с которыми он был ознакомлен при прохождении первичного инструктажа.

3. Пользователь несет персональную ответственность за свои действия.

4. Пользователь обязан:

— знать и выполнять требования Положения об обработке данных, Политики в отношении обработки данных, других локальных актов оператора в отношении персональных данных;

— знать и выполнять установленные требования по режиму обработки ПДн, учету, хранению и использованию носителей ПДн, обеспечению безопасности ПДн;

— соблюдать требования парольной политики;

— блокировать АРМ в случае отсутствия на рабочем месте;

— оповещать ответственного за обеспечение безопасности ПДн о фактах нарушения информационной безопасности и возникновения нештатных ситуаций;

— при возникновении нештатных и аварийных ситуаций действовать согласно Инструкции пользователя при возникновении нештатных ситуаций с целью ликвидации их последствий и возможного ущерба.

5. Пользователю запрещается:

— разглашать обрабатываемые ПДн;

— производить несанкционированное копирование ПДн на учтенные носители;

— производить копирование ПДн на неучтенные носители;

— оставлять незаблокированным АРМ при отсутствии на рабочем месте;

— сообщать и передавать третьим лицам личные пароли и атрибуты доступа к ресурсам ИСПДн.

6. За нарушение информационной безопасности Пользователь несет ответственность согласно действующему законодательству Российской Федерации.

Приложение № 12
к Положению о работе с
персональными данными в
ФГБОУ ВПО «МГТУ»

Инструкция пользователя информационной системы персональных данных при возникновении нештатных ситуаций

1. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием информационных систем персональных данных ФГБОУ ВПО "МГТУ" (далее - ИСПДн), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

2. Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания работоспособности в случае реализации рассматриваемых угроз.

3. Задачами данной Инструкции являются:

— определение мер защиты от прерывания работоспособности;

— определение действий по восстановлению в случае прерывания работоспособности.

4. Действие настоящей Инструкции распространяется на всех пользователей ИСПДн, имеющих доступ к ресурсам ИСПДн, а также на основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

— системы жизнеобеспечения;

— системы обеспечения отказоустойчивости;

— системы резервного копирования и хранения данных;

— системы контроля физического доступа.

5. Под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в Приложении.

6. При реагировании на инцидент важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

— Уровень 1. Незначительный инцидент - локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты;

— Уровень 2. Авария - любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты;

— Уровень 3. Катастрофа - любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, к уничтожению, блокированию, неправомерной модификации или компрометации защищаемых

персональных данных, а также к угрозе жизни пользователей ИСПДн.

7. При возникновении нештатной ситуации любого уровня пользователь обязан оповестить ответственного за организацию обработки персональных данных, сообщив характер аварийной ситуации, масштаб ситуации по предварительной субъективной оценке.

8. Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за организацию обработки персональных данных в Журнале регистрации фактов нарушения и восстановления работоспособности оборудования или ИСПДн. В кратчайшие сроки, не превышающие одного рабочего дня, должны быть предприняты меры по восстановлению работоспособности ИСПДн.

9. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные (программно-аппаратные) и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

— системы жизнеобеспечения;

— системы обеспечения отказоустойчивости;

— системы резервного копирования и хранения данных;

— системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

— пожарные сигнализации и системы пожаротушения;

— системы вентиляции и кондиционирования;

— системы резервного питания.

Все критичные помещения, в которых размещаются элементы ИСПДн и средства защиты, должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Порядок предотвращения потерь информации и организации восстановления ИСПДн описан в Инструкции по организации резервирования и восстановления программного обеспечения, баз персональных данных ИСПДн.

10. Ответственный за организацию обработки персональных данных:

— ознакомляет всех сотрудников, находящихся в его зоне ответственности, с данной инструкцией в срок, не превышающий 3х рабочих дней с момента выхода нового сотрудника на работу;

— обучает пользователей, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций.

Пользователи ИСПДн должны получить базовые знания в следующих областях:

— оказание первой медицинской помощи;

— пожаротушение;

— эвакуация людей;

— защита материальных и информационных ресурсов;

— методы оперативной связи со службами спасения и руководителями структурных подразделений;

— выключение оборудования, электричества, водоснабжения, газоснабжения;

— по окончанию ознакомления сотрудников получает их роспись в Журнале учета прохождения первичного инструктажа.

11. Навыки и знания пользователей ИСПДн по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение пользователей ИСПДн порядку действий при возникновении аварийной ситуации. Ответственность за организацию обучения пользователей ИСПДн несет ответственный за организацию обработки персональных данных. Ректор ФГБОУ ВПО "МГТУ" согласует сроки и порядок их обучения.

Приложение
к Инструкции пользователя ИСПДн
при возникновении нештатной ситуации

Источники угроз безопасности персональных данных

Технологические угрозы:

— Пожар в здании;

— Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения);

— Взрыв (бытового газа, взрывчатых веществ или приборов, работающих под давлением);

— Химический выброс в атмосферу.

Внешние угрозы:

— Массовые беспорядки;

— Сбои общественного транспорта;

— Эпидемия;

— Массовое отравление персонала;

— Теракт.

Стихийные бедствия:

— Удар молнии;

— Сильный снегопад;

— Сильные морозы;

— Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания;

— Затопление водой в период паводка;

— Наводнение, вызванное проливным дождем;

— Торнадо;

— Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод).

ИТ-угрозы:

— Сбой системы кондиционирования в серверном помещении;

— Выход из строя файлового сервера;

— Частичная потеря информации на сервере без потери его работоспособности;

— Выход из строя локальной сети;

— Выход из строя рабочей станции;

— Частичная потеря информации на рабочей станции без потери её работоспособности. Угроза, связанная с человеческим фактором:

— Ошибка персонала, имеющего доступ к элементам ИСПДн;

— Нарушение конфиденциальности, целостности и доступности конфиденциальной информации, а также несанкционированные действия, заблокированные средствами защиты и зафиксированные средствами регистрации.

Угрозы, связанные с внешними поставщиками:

— Отключение электроэнергии;

— Сбой в работе интернет-провайдера;

— Физический разрыв внешних каналов связи.