МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Челябинский государственный педагогический университет»
(ФГБОУ ВПО «ЧГПУ»)

Челябинск

Утверждено Приказом
Ректора ФГБОУ ВПО «ЧГПУ»
№ 870 от 30.12 20 13 г.

ИНСТРУКЦИЯ ПО ПРОВЕДЕНИЮ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИХ ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ

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 «ЧГПУ» (далее – Оператор) в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», 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 либо комиссия по персональным данным, назначенная Оператором.

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

2.4. Ответственный за организацию обработки персональных данных 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 (Приложение 1).

2.6. При выявлении нарушений в ходе проверки. Ответственный за организацию обработки персональных данных либо Председатель комиссии делает запись в Акте контроля соответствия обработки персональных данных о мероприятиях по устранению нарушений и сроках исполнения. Руководитель Оператора ставится в известность о выявленных нарушениях и мерах, которые необходимо принять для их устранения. Ответственным за организацию обработки либо Председателем комиссии.

2.7. В ходе внутренней проверки контролирующие проводят:

– контроль соответствия обработки персональных данных требованиям законодательства, нормативным актам 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 ее 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 учету и хранению съемных носителей персональных данных. Положения о порядке доступа в помещения и других локальных актов, регламентирующих обработку персональных данных Оператора;

– проверку «Журнала учета съемных носителей персональных данных»

3. ОТВЕТСТВЕННОСТЬ

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

3.2. 3.За соблюдение Инструкции возлагается на всех работников Оператора, на которых распространяется Инструкция.

– отказы и сбои технических средств ИСПДн, приводящие к ее модификации, блокированию, уничтожению или несанкционированному копированию, а также нарушению правил эксплуатации ЭВМ и сетевого оборудования.

3.3. Целью защиты информации является:

– предотвращение утечки, хищения, утраты, подделки информации, а также неправомерных действий по уничтожению, модификации, искажению, несанкционированному копированию, блокированию информации, предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы обеспечения правового режима документированной информации как объекта собственности;

– защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в ИСПДн ФГБОУ ВПО «ЧГПУ»;

– сохранение конфиденциальности информации в соответствии с законодательством Российской Федерации;

– обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

3.4. Ответственность за соблюдение требований по защите информации ограниченного доступа и надлежащего порядка проводимых работ возлагается на пользователей ИСПДн, администратора безопасности ИСПДн и ответственного за обеспечение безопасности персональных данных ФГБОУ ВПО «ЧГПУ».

3.5. Администратор безопасности ИСПДн обязан вести «Журнал учета паролей пользователей ИСПДн».

3.6. Субъекты доступа, получающие доступ к базам данных и другим информационным ресурсам, должны изучить «Инструкцию пользователя информационных систем персональных данных» и оставить письменное подтверждение (подпись) о неразглашении ими информации, к которой они имеют доступ, паролей, а также в том, что за нарушение правил информационной безопасности и данной инструкции они несут персональную ответственность в соответствии с законодательством Российской Федерации.

4. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

4.1. **Информация** – сведения (сообщения, данные) независимо от формы их представления.

4.2. **Носитель информации** – любой материальный объект или среда, используемый для хранения или передачи информации.

4.3. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

4.4. **Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

4.5. **Доступ к информации** – возможность получения информации и ее использования.

4.6. **Несанкционированный доступ (НСД)** – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных

базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путем изменения (повышения, фальсификации) своих прав доступа.

4.7. **Автоматизированное рабочее место (АРМ)** – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

5. РАЗГРАНИЧЕНИЕ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К ИНФОРМАЦИОННЫМ РЕСУРСАМ И СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ

5.1. Защита от несанкционированного доступа осуществляется:

– идентификацией и проверкой подлинности пользователей ИСПДн при доступе к информационным ресурсам ФГБОУ ВПО «ЧГПУ»;

– разграничением доступа к обрабатываемым базам данных. Пользователь ИСПДн имеет доступ только к тем информационным ресурсам, которые разрешены для него согласно Матрице доступа. Для осуществления доступа к информационным ресурсам, администратор безопасности ИСПДн назначает конкретному пользователю ИСПДн идентифицирующее имя пользователя, кодирует аппаратный идентификатор (при его наличии) и предоставляет возможность задать пароль;

– администратор безопасности ИСПДн должен осуществлять мероприятия по обеспечению защиты информационных ресурсов ФГБОУ ВПО «ЧГПУ» от несанкционированного доступа и непреднамеренных изменений и разрушений, а также иметь в наличии средства восстановления, резервные копии, предусматривающие процедуру восстановления свойств информационных ресурсов после сбоев и отказов оборудования.

6. ОБЕСПЕЧЕНИЕ СОХРАННОСТИ ИНФОРМАЦИИ

6.1. Для обеспечения сохранности электронных информационных ресурсов ФГБОУ ВПО «ЧГПУ» необходимо соблюдать следующие требования:

– администратор безопасности ИСПДн должен иметь не менее двух резервных копий программного обеспечения для работы с информационными ресурсами, хранимых в разных помещениях, а также методику восстановления данных;

– резервное копирование информационных ресурсов ФГБОУ ВПО «ЧГПУ» должно производиться в соответствии с документацией на используемое программное обеспечение;

– в случае сбоя или порчи восстановление информационных ресурсов из резервных копий производится в соответствии с документацией на используемое программное обеспечение с составлением акта;

– для копирования информации должны использоваться только проверенные на наличие компьютерных вирусов и других вредоносных программ носители информации.

6.2. Субъектам доступа запрещается:

– установка и использование при работе с электронно-вычислительными машинами вредоносных программ, ведущих к блокированию работы системы;

– самовольное изменение сетевых адресов;

– самовольное вскрытие блоков электронно-вычислительных машин, модернизация или модификация электронно-вычислительных машин и программного обеспечения;

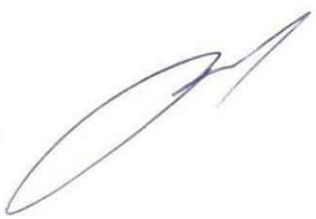
– самовольное вскрытие блоков электронно-вычислительных машин, модернизация или модификация электронно-вычислительных машин и программного обеспечения;

– несанкционированная передача компьютеров с прописанными сетевыми настройками. Передача компьютеров производится только администратором безопасности ИСПДн с предварительно удаленными сетевыми настройками.

6.3. Сведения, содержащиеся в электронных документах, и базы данных ФГБОУ ВПО «ЧГПУ» должны использоваться только в служебных целях в рамках полномочий работника, работающего с соответствующими материалами.

СОГЛАСОВАНО:

Начальник Управления
правовой, финансово-экономической работы
и перспективного развития
«28» 12 2015 г.



А.Г. Базаев

Приложение 1

Акт контроля 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 «ЧГПУ» (далее - Оператор) проведен контроль соответствия обработки персональных данных следующим актам:

– Федеральному закону от 27 июля 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:

1.
2.
3.

Меры по устранению нарушений:

1.
2.
3.

Срок устранения нарушений: ____.

Ответственный за организацию
обработки персональных данных

_____	_____	_____
(дата)	(подпись)	(инициалы, фамилия)