



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»
№ 810 от 30.12 2015 г.

**ИНСТРУКЦИЯ
ПО РАЗГРАНИЧЕНИЮ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ
К СРЕДСТВАМ ЗАЩИТЫ И ИНФОРМАЦИОННЫМ РЕСУРСАМ**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная инструкция определяет порядок организации работ по разграничению доступа пользователей к средствам защиты и информационным ресурсам, обрабатываемым в информационных системах персональных данных (далее – ИСПДн) ФГБОУ ВПО «ЧГПУ».

1.2. Основными видами угроз безопасности информационных систем являются:

- противоправные действия третьих лиц;
- ошибочные действия пользователей ИСПДн;
- отказы и сбои технических средств ИСПДн, приводящие к ее модификации, блокированию, уничтожению или несанкционированному копированию, а также нарушению правил эксплуатации ЭВМ и сетевого оборудования.

1.3. 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, имеющих 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.

1.4. 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».

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

1.6. 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.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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

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

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

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

2.6. **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.

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

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

3.1. 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 со-

гласно 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.

4. ОБЕСПЕЧЕНИЕ СОХРАННОСТИ ИНФОРМАЦИИ

4.1. 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.

4.2. 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;

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

4.3. 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

Проректор по информационным
технологиям
«28» 12 2015 г.



Е.В. Яковлев

Начальник отдела кадров
«28» 12 2015 г.



Г.В. Привалова

