ОТДЕЛ ОБРАЗОВАНИЯ
КУЗНЕЦКОГО РАЙОНА ПЕНЗЕНСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

от 12 апреля 2011 года №201

г. Кузнецк

О введении режима обработки и защиты персональных данных в Отделе образования Кузнецкого района Пензенской области

В целях исполнения требований Федерального закона от 27.06.2006 № 152-ФЗ «О персональных данных» (с последующими изменениями),

1. Ввести в Отделе образования Кузнецкого района Пензенской области режим обработки и защиты персональных данных.

2. Утвердить:

2.1. Разрешительную систему доступа к обрабатываемым персональным данным в Отделе образования Кузнецкого района Пензенской области (приложение № 1).

2.2. Инструкцию о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения информационных систем персональных данных Отдела образования Пензенской области (приложение № 2).

2.3. Инструкцию об антивирусной защите информационных систем персональных данных Отдела образования Пензенской области (приложение № 3).

2.4. Инструкцию о парольной защите информационных систем персональных данных Отдела образования Пензенской области (приложение № 4).

2.5. Журнал учета мероприятий по контролю за соблюдением режима защиты персональных данных Отдела образования Пензенской области (приложение № 5).

2.6. Журнал учета материальных носителей персональных данных (приложение № 6).

3. Руководителям структурных подразделений Отдела образования Пензенской области:

3.1. До 15 апреля 2011 года довести инструкции, указанные в подпунктах 2.2., 2.3., 2.4. пункта 2 настоящего распоряжения до лиц, ответственных за обработку персональных данных, подлежащих защите.

3.2. До 15 апреля 2011 года разработать и утвердить в установленном порядке описание технологического процесса обработки информации в информационной системе персональных данных подразделения Отдела образования Пензенской области согласно образцу (приложение № 7).

3.3. Учёт мероприятий по контролю за соблюдением режима защиты персональных данных Отдела образования Пензенской области и материальных носителей персональных данных вести в указанных в подпунктах 2.5. и 2.6. журналах.

4. Контроль за исполнением настоящего распоряжения оставляю за собой.

Начальник Отдела образования
Кузнецкого района **Т.В.Широкова**

Приложение № 1
к распоряжению Отдела образования
Кузнецкого района Пензенской области от
_____ № _____

Разрешительная система доступа
к обрабатываемым персональным данным
в Отделе образования Пензенской области

Группа	Уровень доступа к ПДн	Разрешенные действия	Сотрудники
Администраторы безопасности информационной системы персональных данных (далее – ИСПДн)	Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладает полной информацией о технических средствах и конфигурации ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн. Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Казаркина Е.С.
Пользователь ИСПДн	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Голованцева С.В. Курамшин Р.И. Макарова М.Н. Юрасова Е.В. Горбачева Н.Л. Минина Ю.В. Радаева Ю.Н. Горина Н.А. Маликова Л.Н. Баранова С.А.

Приложение № 2
к распоряжению Отдела образования
Кузнецкого района Пензенской области от
_____ № _____

ИНСТРУКЦИЯ
о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения информационных систем персональных данных Отдела образования Кузнецкого района Пензенской области

1.Назначение и область действия

1.1. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и систем защиты информации (далее – СЗИ) определяет действия, связанные с функционированием информационной системы персональных данных (далее – ИСПДн) подразделения, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

1.2. В настоящей Инструкции используются следующие термины:

- персональные данные (далее – ПДн) - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу;
- информационная система персональных данных (далее – ИСПДн) – информационная система, представляющая собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таких средств;
- система защиты информации (далее – СЗИ) – совокупность организационных мер и технических средств защиты информации, а также используемых в информационной системе информационных технологий, в рамках которых реализуются организационные и технические мероприятия, обеспечивающие безопасность информации;
- пользователь ИСПДн – лицо, участвующее в функционировании ИСПДн или использующее результаты её функционирования;
- администратор безопасности ИСПДн – гражданский служащий, в должностные обязанности которого входит обеспечение защиты ПДн в ИСПДн;
- резервное копирование – процесс создания копии данных на носителе (жёстком диске, дискете и т. д.), предназначенном для восстановления данных в оригинальном месте их расположения в случае их повреждения или разрушения.

1.3. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и систем

защиты информации определяет действия, связанные с функционированием ИСПДн подразделения, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

1.4. Действие настоящей Инструкции распространяется на всех пользователей подразделений, имеющих доступ к ресурсам ИСПДн, а также 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.

1.5. Пересмотр настоящей Инструкции осуществляется по мере необходимости, но не реже одного раза в два года.

1.6. Ответственным за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается администратор безопасности ИСПДн.

2.Порядок реагирования на инцидент

2.1. В настоящей Инструкции под инцидентом понимается любое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также потерей защищаемой информации.

2.2. Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;
- в результате преднамеренных действий пользователей и третьих лиц;
- в результате нарушения правил эксплуатации технических средств ИСПДн;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.3. Все действия в процессе реагирования на инцидент должны документироваться администратором безопасности ИСПДн в журнале по учету мероприятий по контролю за соблюдением режима защиты персональных данных Отдела образования Кузнецкого района.

2.4. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники (администратор безопасности и пользователь ИСПДн) предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с непосредственным руководителем. По необходимости, иерархия согласования может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1. Техническими мерами для обеспечения непрерывной работы и восстановления являются программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как:

- системы жизнеобеспечения ИСПДн;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

3.2. Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

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

3.4. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

3.5. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн: ПЭВМ, сетевое и коммуникационное оборудование должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.).

3.6. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

3.7. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (жесткий магнитный диск и т.п.).

3.8. Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых персональных данных – не реже раза в неделю;
- для технологической информации – не реже раза в месяц;

- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

3.9. Данные о проведении процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

3.10. Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения.

Приложение № 3
к распоряжению Отдела образования
Кузнецкого района Пензенской области
от _____ № _____

ИНСТРУКЦИЯ
об антивирусной защите информационных систем персональных данных Отдела образования Кузнецкого района Пензенской области

1. Общие положения

1.1. Компьютерный вирус является разрушающей программной закладкой и характеризуется значительным деструктивным потенциалом для программ, данных и любой информации, хранящейся на компьютерах и магнитных носителях. Особую опасность представляет то обстоятельство, что компьютерные вирусы могут скрытно и постепенно уничтожать, либо мгновенно разрушать хранящуюся в компьютере и магнитных носителях информацию, при этом также могут пострадать аппаратные средства.

1.2. Основными путями вирусного вторжения являются неквалифицированное обращение пользователей с компьютерной техникой при использовании ими зараженных машинных носителей информации и программ, либо целенаправленное спланированное воздействие извне с использованием компьютерных вирусов. При любых обстоятельствах это затрагивает вопросы защиты информации и интересы собственной безопасности Отдела образования Пензенской области.

1.3. В настоящей Инструкции используются следующие термины:

- антивирусная программа (антивирус) - программа для выявления и удаления компьютерных вирусов и других вредоносных программ, предотвращения их распространения, а также восстановления программ зараженных ими;
- антивирусный контроль – проверка информации на отсутствие компьютерных вирусов и вредоносных программ.

2. Порядок, обеспечивающий безопасную работу на компьютере и с магнитными носителями

2.1. Приобретение средств вычислительной техники (дате - СВТ) и программных продуктов подразделениями Отдела образования Кузнецкого района Пензенской области осуществляется исключительно через администратора безопасности информационных систем персональных данных, а их установка и техническая поддержка производятся ответственным лицом. Там же осуществляется проверка, настройка и тестовые испытания СВТ и программных продуктов.

2.2. Вновь поступающее программное обеспечение должно быть подвергнуто входному контролю – проверке на отсутствие вирусов и проверке соответствия длины и контрольных сумм, если таковые указаны в сопроводительных документах, полученным длинам и контрольным суммам.

2.3. Каждый компьютер решением начальника подразделения Отдела образования Кузнецкого района Пензенской области персонально закрепляется за ответственным за его эксплуатацию подготовленным работником.

2.4. Допуск сотрудников к самостоятельной работе на компьютерах и с внешними носителями осуществляется только после овладения ими навыками в работе с компьютером, антивирусными пакетами программ.

2.5. Запрещается использовать на компьютерах программные и аппаратные средства, не согласованные с документами ФСТЭК, а для систем, обрабатывающих информацию ограниченного доступа, с документами ФСТЭК и ФСБ.

2.6. На любом, работающем компьютере, в обязательном порядке должен быть установлен и активирован пакет антивирусных программ. Ответственность за это несет конкретный, отвечающий за его работоспособность сотрудник, а также администратор безопасности подразделения.

2.7. Периодически, не реже 1 раза в неделю, работник, ответственный за компьютер, проверяет его дисковое пространство с использованием антивирусного пакета программ на возможное наличие компьютерного вируса.

2.8. Пользователь (в случае необходимости совместно с администратором безопасности подразделения) обязан проводить антивирусный контроль любой электронной информации (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивируемые/разархивируемые файлы и т.д.), получаемой и передаваемой по телекоммуникационным каналам, а также информации на съемных носителях (магнитных дисках, оптических носителях, Flash - память и т.п.).

2.9. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов специалистов по антивирусной защите, администратора безопасности информационной системы персональных данных, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь специалистов по информационным технологиям, по защите информации).

3. Ответственность

3.1. Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на

администратора безопасности в структурном подразделении Отдела образования Кузнецкого района Пензенской области.

3.2. Пользователь и администратор безопасности несут ответственность за качество и своевременность выполнения задач и функций, возложенных на них в соответствии с настоящей Инструкцией.

Приложение № 4
к распоряжению Отдела образования
Кузнецкого района Пензенской области от
_____ № _____

ИНСТРУКЦИЯ
о парольной защите информационных систем персональных данных Отдела образования Кузнецкого района Пензенской области

1. Общие положения

1.1. Данная Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных (далее – ИСПДн) Отдела образования Кузнецкого района Пензенской области, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.2. В настоящей Инструкции используются следующие термины:

- персональные данные (далее – ПДн) - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу;
- информационная система персональных данных (далее – ИСПДн) – информационная система, представляющая собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таких средств;
- пользователь ИСПДн – лицо, участвующее в функционировании ИСПДн или использующее результаты её функционирования;
- администратор безопасности ИСПДн – ~~государственный~~ гражданский служащий, в должностные обязанности которого входит обеспечение защиты ПДн в ИСПДн;
- пароль – последовательность знаков, позволяющая пользователям ИСПДн входить в компьютер, получать доступ к файлам, программам и другим ресурсам.

2. Порядок парольной защиты

2.1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в ИСПДн возлагается на администратора безопасности ИСПДн подразделения Отдела образования Кузнецкого района Пензенской области.

2.2. Личные пароли должны генерироваться и распределяться централизованно с учетом следующих требований:

- длина пароля должна быть не менее 7 символов;

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения;

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

- личный пароль пользователь не имеет права сообщать никому.

2.3. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

2.4. Формирование личных паролей пользователей осуществляется централизованно. Ответственность за правильность их формирования и распределения возлагается на администратора безопасности ИСПДн. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления (самих, допущенных к обработке персональных данных, сотрудников, а также руководителей подразделений) с паролями других сотрудников подразделения.

2.5. Полная плановая смена паролей пользователей должна проводиться регулярно.

2.6. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться администратором безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой.

2.7. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры по смене пароля.

2.8. Компрометацией личного пароля является утрата доверия к тому, что используемый личный пароль недоступен посторонним лицам. К событиям, связанным с компрометацией личного пароля, относятся, в том числе следующие:

- утрата материального носителя пароля;

- утрата материального носителя пароля с последующим его обнаружением;

- нарушение целостности печати на сейфе с материальным носителем пароля, либо на конверте или пенале с паролем;

- утрата ключей от сейфа с материальным носителем пароля;

- утрата ключей от сейфа с материальным носителем пароля с последующим их обнаружением;

- доступ посторонних лиц к информации о пароле.

2.8. Хранение сотрудником (исполнителем) значений своих паролей на материальном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя подразделения в опечатанном конверте или пенале.

2.9. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены и использования в подразделениях возлагается на администратора безопасности подразделения.

3. Ответственность

3.1. Пользователь и администратор безопасности несут ответственность за качество и своевременность выполнения задач и функций, возложенных на них в соответствии с настоящей Инструкцией.

Приложение № 5
к распоряжению Отдела образования
Кузнецкого района Пензенской области от
_____ № _____

Журнал
учета мероприятий по контролю за соблюдением режима защиты персональных данных подразделения Отдела образования Кузнецкого района Пензенской области

Мероприятие	Дата	Исполнитель	Результат

Приложение № 6
к распоряжению Отдела образования
Кузнецкого района
Пензенской области от _____ № _____

ЖУРНАЛ
учета материальных носителей персональных данных

Начат « __»_____2011г.

Дата поступ-ления	Рег. №	Откуда поступил	Вид носителя	Коли-чество носителей	№ и дата сопроводитель-ного документа	Учётные номера носителя	Кому передан носитель	Дата передачи носителя	Дата и № акта уничто-жения	Ф.И.О. передавшего	Ф.И.О. получившего	Роспись

Приложение № 7
к распоряжению Отдела образования
Пензенской области от _____ № _____

ОПИСАНИЕ
технологического процесса обработки информации в информационных системах персональных данных подразделений Отдела образования Кузнецкого района Пензенской области

1. Расположение объекта

Объект расположен по адресу: г. Кузнецк, ул. Комсомольская, д.51,

2. Назначение, решаемые задачи

Информационная система персональных данных (далее – ИСПДн) отдела предназначена для разработки, хранения, печати конфиденциальной информации, в том числе персональных данных, а также общедоступной информации.

3. Основные элементы системы

В состав системы входят:
- системный блок – 1 шт.;
- монитор – 1 шт.;
- клавиатура – 1 шт.;
- манипулятор «мышь» – 1 шт.;
- принтер – 1 шт.
- прочее – _____

4. Программное обеспечение

Для осуществления технологического процесса обработки информации, в ИСПДн используется следующее программное обеспечение (далее - ПО):

№ п/п	Название ПО	Назначение, наличие лицензии	Место установки (папка на ЖМД)	Инв. № ПЭВМ ИСПДн, на которых установлено данное ПО
1.	Windows XP Pro	операционная система, имеет лицензию	C:\Windows	

2.	MS Office 2007	текстовый, табличный редактор, имеет лицензию	C:\Program files	
3.	Антивирус Касперского 6.0	антивирусная программа, имеет лицензию	C:\Program files	

Копии лицензионной версии операционной системы и средств защиты информации от несанкционированного доступа (далее – НСД) хранятся у ответственного за эксплуатацию объекта информатизации.

На ПЭВМ ИСПДн установлена операционная система MS Windows XP.

Для разработки документов пользователей на ПЭВМ ИСПДн установлен программный пакет Microsoft Office 2007.

5. Режим работы системы и разграничение прав доступа

ИСПДн предназначена для работы в многопользовательском режиме, доступ исполнителей к работе в ИСПДн, осуществляется по утвержденному списку, пользователи имеют различные права доступа к информации.

Доступ к работе на ПЭВМ ИСПДн осуществляется по предъявлению персонального идентификатора (имени пользователя) и ввода пароля конкретного пользователя. При этом пользователь получает установленные Администратором безопасности права доступа к устройствам, каталогам, файлам и программам ИСПДн.

Права доступа пользователей к программам, каталогам и файлам ИСПДн определены в разрешительной системе доступа и реализованы в ИСПДн средства защиты информации от несанкционированного доступа.

6. Получение и добавление персональных данных в систему

Персональные данные субъекта вносятся в систему:

- лично субъектом путем заполнения анкет, предоставления копий документов, написания заявлений и передачи их работнику кадрового подразделения;
- работником кадрового подразделения, в процессе обработки данных, предоставленных субъектом, либо данных, касающихся субъекта персональных данных, появляющихся/изменяющихся в процессе конкурсных мероприятий или трудовой деятельности субъекта.

7. Работа с персональными данными

В процессе жизненного цикла персональных данных субъекта в кадровом подразделении производится обновление данных субъекта. При обновлении данных вносятся изменения в электронную копию документа, хранятся руководящие документы, породившие изменение.

Все руководящие документы готовятся в электронном виде, сохраняются на ПЭВМ либо съемных носителях информации, распечатываются. Хранятся электронные и бумажные копии документов.

8. Хранение персональных данных

Пользователи имеют право хранения файлов с конфиденциальными данными на жестком магнитном диске ПЭВМ, в специально выделенных администратором безопасности каталогах, а также дискетах, дисках CD, DVD и других съемных носителях информации. Хранение информации осуществляется в соответствии с разрешительной системой доступа.

Материальные носители информации, содержащие персональные данные, учтены и хранятся в сейфе.

9. Настройка и обслуживание системы

Настройку системы защиты от несанкционированного доступа и контроль ее работы осуществляет администратор безопасности. Функции, права, обязанности и порядок работы в ИСПДн администратора безопасности и пользователей регламентируется специально разработанными инструкциями администратору безопасности и пользователю.

Антивирусная защита осуществляется пользователями ИСПДн с применением программного средства Антивирус Касперского в соответствии с инструкцией по антивирусной защите.