УПРАВЛЕНИЕ ОБРАЗОВАНИЯ ГОРОДА ПЕНЗЫ

П Р И К А З

__30.12.2013___ № _370_

**Об организации и проведении работ
по обеспечению безопасности персональных данных
при их обработке в информационных системах персональных данных**

В соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», Перечнем сведений конфиденциального характера, утвержденным Указом Президента РФ от 06.03.1997 №188, Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», «Рекомендациями по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК России от 15.02.2008, руководствуясь положением об Управлении образования города Пензы,

П Р И К А З Ы В А Ю:

1. Утвердить Положение об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в Управлении образования города Пензы (Приложение 1).

2. Общее руководство за обеспечением требований по защите конфиденциальной информации, в том числе, содержащей персональные данные, возложить на начальника информационно-аналитического отдела Управления образования города Пензы (О.В. Шулякова).

3. Назначить ответственными за организацию и выполнение мероприятий по защите конфиденциальной информации, в том числе, содержащей персональные данные, начальников отделов Управления образования города Пензы, эксплуатирующих объекты информации и ведущих обработку этой информации (М.М. Авдонина, Л.Б. Савина, И.В. Трошина).

4. Возложить обязанности администратора безопасности информационных систем персональных данных на главного специалиста информационно-аналитического отдела Управления образования города Пензы (И.Н. Ведышев).

5. Возложить обязанности администратора безопасности информационных систем персональных данных отдела учета и отчетности Управления образования

на главного специалиста отдела учета и отчетности Управления образования города Пензы (А.Л. Вакин).

6. Ответственность за методическое руководство и контроль за эффективностью предусмотренных мер защиты возложить на главного специалиста информационно-аналитического отдела Управления образования города Пензы (И.Н. Ведышев).

7. Отделу кадрового и правового обеспечения (Л.Б. Савина) внести изменения в должностные обязанности работников, предусматривающие права и обязанности по вопросам защиты конфиденциальной информации, в том числе персональных данных.

8. Утвердить Инструкцию ответственного за организацию обработки персональных данных в Управлении образования города Пензы (Приложение 2).

9. Утвердить Инструкцию пользователя информационной системы персональных данных Управления образования города Пензы (Приложение 3).

10. Утвердить Инструкцию администратора безопасности информационной системы персональных данных Управления образования города Пензы (Приложение 4).

11. Администраторам безопасности информационных систем персональных данных (И.Н. Ведышев, А.Л. Вакин) разработать: частную модель угроз безопасности персональных данных, инструкцию по проведению антивирусного контроля, инструкцию администратора информационной безопасности, инструкцию ответственного за эксплуатацию объекта вычислительной техники и иную нормативно-распорядительную документацию обеспечения безопасности информационных систем персональных данных.

12. Запретить обработку персональных данных работникам, не допущенным к информационным системам Управления образования города Пензы, в которых ведется обработка персональных данных.

13. Начальникам отделов Управления образования города (М.М. Авдонина, Л.Б. Савина, И.В. Трошина) ознакомить работников с настоящим приказом.

14. Контроль за исполнением настоящего приказа возложить на заместителя начальника Управления образования города Пензы М.К. Шарошкину.

Начальник Управления Ю.А. Голодяев

Приложение № 1
к приказу начальника Управления
образования города Пензы
от 30.12.2013 № 370

ПОЛОЖЕНИЕ
об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации», Перечнем сведений конфиденциального характера, утвержденным Указом Президента РФ от 06.03.1997 №188, Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», «Рекомендациями по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК России от 15.02.2008 и иными нормативными актами, действующими на территории Российской Федерации.

Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации (далее - информационные системы).

1.2. Настоящее Положение вступает в силу с момента его утверждения начальником Управления образования города Пензы. Положение доводится до сведения всех работников отделов Управления образования, осуществляющих обработку ПДн в ИСПДн персонально под роспись.

1.3. В ИСПДн должны использоваться только сертифицированные технические и программные средства защиты информации.

1.4. Контроль за выполнением настоящего положения возлагается на заместителя начальника Управления образования города Пензы.

1.5. Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой системы (подсистемы) защиты персональных данных (СЗПДн). Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн. СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

1.6. При обнаружении нарушений порядка предоставления персональных данных оператор или уполномоченное лицо незамедлительно приостанавливают предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

Лица, виновные в нарушении требований Федерального закона от 27 июля 2006 № 152-ФЗ «О персональных данных», несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

2. Замысел обеспечения безопасности ПДн

Конечной целью проведения мероприятий по защите ИСПДн является:

- предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа (НСД) к ПДн;
- недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие НСД к ним;
- постоянный контроль над обеспечением уровня защищенности ПДн;
- защита конституционных прав граждан на сохранение конфиденциальности персональных данных, имеющихся в информационных системах.

3. Организация работ по обеспечению безопасности ПДн

3.1. Обязанности и права должностных лиц в части обеспечения безопасности ПДн:

а) начальник Управления образования города Пензы:

- несет персональную ответственность за организацию и состояние работ по защите информации в Управлении;
- организует работы по защите конфиденциальной информации;
- несет персональную ответственность за непосредственное руководство и координацию работ, проводимых в соответствии с руководящими и нормативно-методическими документами по защите информации;
- организует разработку организационно-распорядительных документов по вопросам защиты информации в Управлении;
- утверждает списки сотрудников, допущенных к информационным системам персональных данных (к обработке персональных данных);

б) заместители начальника Управления:

- несут персональную ответственность за непосредственное руководство и координацию работ, проводимых в Управлении в соответствии с

руководящими и нормативно-методическими документами по защите информации;

в) начальники отделов Управления

- организуют выполнение мероприятий по защите информации, содержащей сведения, отнесенные к информации с ограниченным распространением;

- осуществляют текущий контроль за обеспечением конфиденциальности информации и соблюдением требований по защите информации в отделах;

- предоставляют на утверждение начальнику Управления списки сотрудников, допущенных к информационным системам персональных данных (к обработке персональных данных);

- доводят под роспись до работников, допущенных к информационным системам персональных данных (к обработке персональных данных) требования по безопасности информации;

д) начальник информационно-аналитического отдела, администратор безопасности информационных систем:

- обеспечивают защиту информации, циркулирующей в классифицированных информационных системах персональных данных и автоматизированных системах Управления образования города Пензы;

имеют право:

- проводить систематический контроль работы средств защиты информации, применяемых в информационных системах персональных данных, выполнение комплекса мероприятий по обеспечению безопасности информации;

- осуществлять плановые и внеплановые проверки состояния защиты информации, контролировать состояние защищенности информационных систем персональных данных, требовать от пользователей информационных систем персональных данных безусловного соблюдения и выполнения требований по информационной безопасности;

е) пользователи (муниципальные служащие), осуществляющие обработку персональных данных:

- несут персональную ответственность за соблюдение требований по защите конфиденциальной информации;

- обработку конфиденциальной информации производят в соответствии с принятыми положениями, инструкциями, иными нормативно-правовыми актами.

3.2. Организационно-распорядительные документы Управления образования города Пензы:

- приказ об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

- приказ начальника Управления о проведении проверки состояния обеспечения безопасности персональных данных.

Организационно-распорядительные документы по обеспечению безопасности персональных данных разработаны в соответствии с Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации», Перечнем сведений конфиденциального характера, утвержденным Указом Президента РФ от 06.03.1997 №188, Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», «Рекомендациями по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК России от 15.02.2008 и иными нормативными актами, действующими на территории Российской Федерации, и утверждены приказом начальника Управления образования.

Список лиц, допущенных к работе с ПДн, определение их полномочий утверждается приказом Управления города Пензы.

3.3. Организация работ по подготовке и вводу в эксплуатацию ИСПДн:

3.3.1. Для проведения классификации информационных систем ПДн в Управлении города Пензы приказом создается комиссия. Классификация ИСПДн проводится членами комиссии в соответствии с «Порядком проведения классификации информационных систем персональных данных».

3.3.2. Техническое задание на систему защиты ПДн в ИСПДн для 3 (локальные и автономные системы) и 4 класса разрабатывается администратором безопасности, назначенного приказом начальника Управления образования. Требования к содержанию технического задания определены «Основными мероприятиями по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» ФСТЭК России.

3.3.3. Модель угроз применительно к конкретной ИСПДн разрабатывается администратором безопасности в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Модель угроз может быть пересмотрена администратором безопасности в связи с изменением класса и структуры ИСПДн.

3.3.4. Аттестация ИСПДн по требованиям безопасности информации проводится в соответствии с порядком проведения аттестации и контроля «Положения по аттестации объектов информатизации по требованиям безопасности информации», утвержденного Гостехкомиссией России 25 ноября 1994 пункт 3.1.

В ИСПДн, установленный класс которой не требует обязательной аттестации, проводится оценка соответствия (декларирование) ИСПДн требованиям безопасности информации. Декларирование соответствия — это подтверждение соответствия характеристик информационной системы персональных данных предъявляемым к ней требованиям, установленным законодательством Российской Федерации, руководящими и нормативно-методическими документами ФСТЭК России и ФСБ России. Декларирование соответствия может осуществляться на основе собственных доказательств или на основании доказательств, полученных с участием привлеченных

организаций, имеющих необходимые лицензии. Оценку соответствия проводит комиссия по обследованию и классификации ИСПДн, по результатам работы которой выявляется несоответствие требованиям по обеспечению безопасности ПДн в ИСПДн. Все обнаруженные недостатки заносятся в акт работы комиссии и подлежат устранению. После устранения всех недостатков и оформления документации на ИСПДн, указанной в данном положении, проводится пробная эксплуатация системы. Если все недостатки устранены, издается приказ о вводе в эксплуатацию ИСПДн и назначение ответственных за эксплуатацию лиц (п. 3.1.3) система вводится эксплуатацию.

Декларация о соответствии должна содержать:

- наименование и местонахождение ИСПДн;
- информацию об объекте подтверждения соответствия, позволяющую идентифицировать этот объект, класс ИСПДн;
- наименование документов, на соответствие требованиям которых подтверждается ИСПДн;
- указание на схему декларирования соответствия;
- сведения о документах, послуживших основанием для подтверждения соответствия ИСПДн необходимым требованиям;
- срок действия декларации о соответствии;

3.4. Порядок обеспечения сохранности носителей ПДн:

3.4.1. Физическая охрана здания Управления образования и помещений организации осуществляется круглосуточно сотрудниками лицензированного охранного предприятия.

3.4.2. Уборка помещения, в котором ведется обработка ПДн либо сервер ИСПДн должна осуществляться в рабочее время под присмотром сотрудника, за которым закреплено данное помещение. В нерабочее время помещение закрываться на ключ.

Повседневный контроль за выполнением требований по защите помещений осуществляет начальник отдела.

3.4.3. Доступ к серверному оборудованию разрешается только администратору безопасности, назначенному приказом по Управлению образования (лицу, его заменяющему).

3.4.4. Все носители информации на бумажной, магнитной, оптической (магнитно-оптической) основе, съемные накопители информации, используемые в технологическом процессе обработки ПДн подлежат учету в соответствующем отделе Управления. Учет съемных носителей информации осуществляется по журналу установленной формы. При этом перед выполнением работ сотрудником, ответственным за их учет, на этих носителях информации предварительно проставляются любым доступным способом следующие учетные реквизиты: учетный номер, дата, пометка «Для служебного пользования», номер экземпляра, подпись сотрудника, а также другие возможные реквизиты, идентифицирующие носитель информации. Носители информации должны учитываться и храниться в

отделах в порядке, установленном для конфиденциальной информации. Временно неиспользуемые носители информации должны храниться в сейфе.

3.5 Порядок обмена информацией со сторонними организациями:

3.5.1. Передача (получение) ПДн осуществляется с письменного разрешения субъекта персональных данных (за исключением случаев, предусмотренных частью 2 федерального закона «О персональных данных») с условием, что все требования по обеспечению конфиденциальности информации будут соблюдены обеими сторонами.

3.5.2. При обмене информацией в случаях предусмотренных федеральными законами со сторонними организациями с руководителем организации (организацией) заключается соглашение об обеспечении конфиденциальности персональных данных. Если потребность в том, чтобы передаваемая информация содержала персональные данные отсутствует, то ПДн из передаваемой информации извлекаются (обезличивание). В случаях, непредусмотренных федеральными законами, передача персональных данных осуществляется с согласия субъекта персональных данных.

3.5.3. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств.

3.6. При проведении работ с участием сторонних организаций, в договоре предусматривается пункт (пункты) об обеспечении конфиденциальности ПДн, ставших известными организациям и их сотрудникам в процессе проведения работ.

4. Контроль состояния работ по обеспечению безопасности ПДн

4.1. Целью контроля является своевременное выявление и предотвращение утечки информации по техническим каналам, исключение или существенное затруднение несанкционированного доступа к ней и предотвращение специальных программно-технических воздействий, вызывающих нарушение конфиденциальности, целостности или доступности информации.

4.2. Начальники отделов осуществляют текущий контроль за обеспечением конфиденциальности информации и соблюдением требований по защите информации в отделе.

Начальник информационно-аналитического отдела, администраторы безопасности информационных систем:

- осуществляют плановые и внеплановые проверки состояния защиты информации, контролируют состояние защищенности информационных систем персональных данных, требуют от пользователей информационных систем персональных данных безусловного соблюдения и выполнения требований по информационной безопасности;
- проводят систематический контроль работы средств защиты информации, применяемых в информационных системах персональных данных,

выполнения комплекса мероприятий по обеспечению безопасности информации

Постоянный контроль выполнения пользователями инструкций по обеспечению безопасности ПДн осуществляется начальниками отделов Управления, эксплуатирующих ИСПДн, администраторами безопасности.

Постоянный контроль состояния технической защиты информации в ИСПДн осуществляется администраторами безопасности.

4.3. Периодический контроль проводит комиссия по проверке состояния обеспечения безопасности персональных данных, созданная в Управлении. По результатам контроля составляется акт, в котором отображается:

соблюдение требований нормативно – методических документов по обеспечению безопасности персональных данных и защите конфиденциальной информации;

работоспособность применяемых средств защиты информации в соответствии с их эксплуатационной документацией;

знание и выполнение персоналом своих функциональных обязанностей в части защиты информации.

4.4. По решению заместителя начальника Управления могут быть приняты дополнительные организационно-технические меры по обеспечению безопасности ПДн, содержащейся в ИСПДн Управления образования.

5. Планирование мероприятий по обеспечению безопасности ПДН

5.1 План мероприятий по обеспечению безопасности ПДн в ИСПДн разрабатывается ежегодно администратором безопасности информационных систем, подписывается начальником информационно-аналитического отдела и утверждается заместителем начальника Управления.

5.2 План мероприятий по обеспечению безопасности ИСПДн должен содержать:

перечень мероприятий;

сроки проведения мероприятий;

ответственных за выполнение запланированных мероприятий;

возможные затраты на проведение мероприятий.

5.3. Контроль за выполнением плана осуществляет начальник информационно-аналитического отдела, начальники отделов Управления, осуществляющих обработку ПДн в ИСПДн. Отчет о выполнение плана заслушивается на планерках Управления образования города Пензы.

Начальник
информационно-аналитического отдела О.В.Шулякова

Приложение № 2
к приказу начальника Управления
образования города Пензы
от 30.12.2013 № 370

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных в Управлении образования города Пензы

1. Общие положения

1. Настоящая инструкция разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

2. Назначение ответственного за организацию обработки персональных данных производится приказом Управления образования города Пензы.

3. Ответственный за организацию обработки персональных данных, получает указания непосредственно от начальника Управления образования города Пензы, и подотчетен ему.

4. Ответственный за организацию обработки персональных данных:

4.1. Осуществляет внутренний контроль за соблюдением работниками Управления образования города Пензы законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.

4.2. Доводит до сведения муниципальных служащих положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

4.3. Организует мероприятия по приему и обработке обращений и запросов субъектов персональных данных или их представителей и (или) осуществлению контроля за приемом и обработкой таких обращений и запросов.

4.4. Организует разработку документов, определяющих политику Управления образования города Пензы в отношении обработки персональных данных, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

4.5. Организует работы по применению организационных и технических мер для обеспечения защиты персональных данных, обрабатываемых в Управлении образования города Пензы, от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

4.6. Организует мероприятия по оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального

закона от 27.07.2006 № 152-ФЗ «О персональных данных», соотношение указанного вреда и принимаемых в администрации города Пензы мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

4.7. Возглавляет комиссию для проведения проверки состояния обеспечения безопасности персональных данных в отделах Управления образования города.

4.8. Вносит предложения по совершенствованию организационных и технических мер защиты персональных данных в Управлении образования города Пензы.

4.9. Имеет право запрашивать и получать необходимые материалы для организации и проведения работ по вопросам организации обработки и обеспечения безопасности персональных данных.

4.10. Утверждает план мероприятий по обеспечению безопасности персональных данных в Управлении образования города Пензы.

4.11. Принимает в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

4.12. Информирует начальника Управления образования города Пензы о фактах нарушения порядка обращения с персональными данными, о попытках несанкционированного доступа к ним.

4.13. Организует служебное расследование по факту нарушений условий обработки персональных данных.

4.14. Организует повышение квалификации в области защиты персональных данных.

5. За неисполнение или ненадлежащее исполнение требований правовых актов, регулирующих отношения в сфере обработки персональных данных ответственный за организацию обработки персональных данных несет ответственность, установленную законодательством Российской Федерации.

Начальник информационно-аналитического отдела О.В. Шулякова

Приложение № 3
к приказу начальника Управления
образования города Пензы
от 30.12.2013 № 370

ИНСТРУКЦИЯ
пользователя информационной системы персональных данных Управления образования города Пензы

1. Общие положения

1.1. Настоящая Инструкция разработана для обеспечения защиты персональных данных в Управлении образования города Пензы.

1.2. Персональные данные (далее – ПДн) относятся к категории информации ограниченного распространения.

1.3. Наиболее вероятными каналами утечки информации для информационных систем персональных данных (далее – ИСПДн) являются:

- несанкционированный доступ к информации, обрабатываемой в ИСПДн;
- хищение технических средств с хранящейся в них информацией или отдельных носителей информации;
- просмотр информации с экранов дисплеев мониторов и других средств ее отображения с помощью оптических устройств;
- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности обмена, в том числе электромагнитного, через специально внедренные электронные и программные средства («закладки»).

2. Обязанности муниципальных служащих, имеющих доступ к ПДн

2.1. Муниципальные служащие, получившие доступ к персональным данным, обязаны хранить в тайне сведения ограниченного распространения, ставшие им известными во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки персональных данных немедленно информировать руководителя структурного подразделения.

2.2. Персональные данные не подлежат разглашению (распространению). Прекращение доступа к такой информации не освобождает работника от взятых им обязательств по неразглашению персональных данных.

2.3. В случае освобождения от занимаемой должности муниципальный служащий обязан вернуть все документы и материалы, относящиеся к деятельности подразделения, организации. В том числе: отчеты, инструкции, переписку, списки работников, компьютерные программы, а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к деятельности Управления образования города Пензы, полученные в течение срока работы.

2.4. Работники при работе с персональными данными обязаны:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

- выполнять требования нормативно-правовых актов Управления образования города Пензы в области защиты персональных данных;

- знать и строго выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемыми на персональных компьютерах;

- хранить в тайне свой аудентификатор (пароль доступа в автоматизированную систему, либо ключевой носитель), а также информацию о системе защиты, установленной в ИСПДн;

- использовать для работы только учтенные съемные накопители информации (гибкие магнитные диски, компакт диски и т.д.);

- контролировать обновление антивирусных баз и в случае необходимости сообщать о необходимости обновления администратору безопасности ИСПДН;

2.5. Немедленно ставить в известность начальника отдела, администратора безопасности ИСПДн:

- в случае утери носителя с персональными данными или при подозрении компрометации личных ключей и паролей;

- нарушений целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах ПЭВМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к защищенной ИСПДн;

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн.

- в случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию рабочей станции, выхода из строя или неустойчивого функционирования узлов ПЭВМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных в автоматизированной системе технических средств защиты ставить в известность администратора безопасности ИСПДн.

2.6. Ставить в известность администратора безопасности ИСПДн при:

- необходимости обновления антивирусных баз;

- обновлении программного обеспечения;

- проведении регламентных работ, модернизации аппаратных средств или изменении конфигурации ИСПДн;

- необходимости вскрытия системных блоков персональных компьютеров входящих в состав ИСПДн;

- резервном копировании информации;

- и в других случаях, связанных с обработкой и защитой персональных данных.

2.7. Уборка помещений должна производиться под контролем муниципального служащего, имеющего доступ в помещение и постоянно в нем работающего.

2.8. Вынос ПЭВМ, на которых проводилась обработка персональных данных, за пределы территории здания с целью их ремонта, замены и т. п. без согласования с начальником отдела запрещен. При принятии решения о выносе компьютеров, жесткие магнитные диски должны быть демонтированы и сданы на

хранение ответственному за организацию и выполнение мероприятий по защите конфиденциальной информации, в том числе содержащей персональные данные.

2.9. ПЭВМ, используемые для работы с персональными данными, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра экрана видеомонитора работниками, не имеющими отношения к конкретно обрабатываемой информации.

Запрещается:

- передавать, кому бы то ни было (в том числе родственникам) устно или письменно сведения о персональных данных субъектов;
- использовать персональные данные, не являющиеся общедоступными, при подготовке открытых публикаций, докладов, сообщений и т.д.;
- обрабатывать персональные данные, не являющиеся общедоступными, на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения начальника отдела;
- накапливать ненужные для работы персональные данные;
- передавать или принимать без расписки материальные носители с персональными данными, не являющимися общедоступными;
- оставлять на рабочих столах, в столах и незакрытых сейфах материальные носители с персональными данными, не являющимися общедоступными, а также оставлять после окончания работы незапертыми и неопечатанными сейфы, помещения и хранилища с документами конфиденциального характера;
- использовать компоненты программного и аппаратного обеспечения ИСПДн отдела в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства;
- осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить персональные данные на неучтенных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенной без присмотра свою рабочую станцию (ПЭВМ), не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность начальника отдела, администратора безопасности ИСПДн.

3. Ответственность

3.1. Пользователь несет ответственность за соблюдение требований настоящей инструкции, а также других нормативных документов в области защиты информации.

3.2. За разглашение информации ограниченного распространения, нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники привлекаются к дисциплинарной или иной, предусмотренной законодательством, ответственности.

Начальник информационно-аналитического отдела О.В. Шулякова

Приложение № 4
к приказу начальника Управления
образования города Пензы
от 30.12.2013 № 370

ИНСТРУКЦИЯ
администратора безопасности информационной системы персональных данных Управления образования города Пензы

1. Общие положения

1.1. Администратор безопасности информационной системы персональных данных назначается приказом начальника Управления образования города Пензы и отвечает за обеспечение устойчивой работоспособности и информационной безопасности объекта информатизации.

1.2. Администратор безопасности информационной системы персональных данных несет ответственность за организацию работ по обеспечению безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники (СВТ) на объектах вычислительной техники (ОВТ), а также правильность использования и нормального функционирования средств защиты информации (СЗИ), подготовку сотрудников по вопросам безопасной обработки информации на СВТ.

2. Функции администратора информационной безопасности

2.1. Осуществляет настройку и сопровождение системы защиты от НСД на ОВТ, при этом:

- реализует полномочия доступа для каждого пользователя к элементам защищаемых информационных на основе утвержденного руководством списка сотрудников, допущенных к работе на ОВТ;
- вводит описание пользователей ОВТ в информационную базу системы защиты от НСД;
- назначает пароли к информационным ресурсам и вводит в базу данных системы защиты описание полномочий доступа пользователей к защищаемым ресурсам;
- своевременно удаляет описание пользователя из базы данных при увольнении или перемещении сотрудника;
- периодически производит смену паролей пользователями для доступа в систему обработки информации ОВТ.

2.2. Осуществляет настройку и сопровождение подсистемы регистрации и учета:

- вводит в базу данных системы защиты от НСД описания событий, подлежащих регистрации в системном журнале;
- проводит регулярный анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам;
- своевременно информирует руководство о несанкционированных действиях персонала и организует расследование попыток НСД.

2.3. Сопровождает подсистемы обеспечения целостности рабочего программного обеспечения (ПО):

- проводит периодическое тестирование функций системы защиты от НСД при изменении программной среды и полномочий исполнителей ОВТ;
- осуществляет восстановление системы защиты от НСД при сбоях;
- проводит контроль соответствия общесистемной программной среды эталону;
- обеспечивает поддержание установленного порядка и соблюдение требований инструкции по антивирусной защите.

2.4. Участвует в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

2.5. Производит выдачу исполнителям паролей для средств защиты информации (СЗИ) от несанкционированного доступа (НСД), а также осуществляет оперативный контроль за действиями пользователей ОВТ.

3. Администратор безопасности информационной системы персональных данных обязан:

3.1. Обеспечивать функционирование и поддерживать работоспособность средств защиты автоматизированных рабочих мест в пределах возложенных на них функций.

3.2. В случае отказа работоспособности технических средств и программного обеспечения СВТ, в том числе средств защиты АРМ принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.3. Информировать начальника информационно-аналитического отдела о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам АРМ.

4. Администратор безопасности информационной системы персональных данных имеет право:

4.1. Контролировать работу пользователей на автоматизированных рабочих местах АРМ.

4.2. Требовать прекращения обработки информации как в целом, так и отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования АРМ.

Начальник информационно-аналитического отдела О.В. Шулякова