73

УПРАВЛЕНИЕ ОБРАЗОВАНИЯ
АДМИНИСТРАЦИИ
АНЖЕРО-СУДЖЕНСКОГО ГОРОДСКОГО ОКРУГА

П Р И К А З

от 30.04.2014г. **№356**

Об утверждении Положения о порядке организации и проведении работ по защите конфиденциальной информации

Руководствуясь требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных", Постановления Правительства Российской Федерации от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Постановления Правительства Российской Федерации от 21.03.2012 N 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 в целях защиты персональных данных граждан, обрабатываемых в управлении образования администрации Анжеро-Судженского городского округа,
приказываю:

1. Утвердить прилагаемое Положение о порядке организации и проведении работ по защите конфиденциальной информации в управлении образования администрации Анжеро-Судженского городского округа (далее - Положение).
2. Руководителям структурных подразделений управления образования администрации Анжеро-Судженского городского округа ознакомить подчинённых им сотрудников с настоящим руководством и обеспечить его исполнение.
4. Контроль за исполнением приказа возложить на заместителя начальника управления образования Анжеро-Судженского городского округа – Семкину М.В.

Начальник управления образования О.Н.Овчинникова

Утверждено
Приказом управления образования
администрации Анжеро-Судженского
городского округа
от 30 апреля 2014 № 356

Положение о порядке организации и проведении работ по защите конфиденциальной информации

1.Термины и определения

Перечень сокращений:

ПДн	Персональные данные
НСД	Несанкционированный доступ
АИС	Автоматизированная информационная система
ИСПДн	Информационная (-ые) система (-ы) персональных данных
ПО	Программное обеспечение
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ОТСС	Основные технические средства и системы
ВТСС	Вспомогательные технические средства и системы

В рамках данного документа используются следующие термины и определения:

Вспомогательные технические средства и системы (ВТСС) - технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с ОТСС или в выделенных помещениях.

Доступ к информации – возможность получения информации и ее использования.

Защита информации от несанкционированного доступа (защита от НСД) или воздействия – деятельность, направленная на предотвращение получения информации заинтересованным субъектом (или воздействия на информацию) с нарушением установленных прав или правил.

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

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных (ИСПДн) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Основные технические средства и системы (ОТСС) - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной (секретной) информации

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Конфиденциальность информации – обязательное для соблюдения оператором или иным получившим доступ к конфиденциальной информации лицам требование не допускать их распространения.

ИСПДН – объединение информационных систем, в том числе информационных систем персональных данных, компьютерного, телекоммуникационного и офисного оборудования всех подразделений управления образования администрации Анжеро-Судженского городского округа, посредством их подключения к единой компьютерной сети передачи данных с использованием различных физических и логических каналов связи.

Нарушение информационной безопасности – событие, при котором компрометируется один или несколько аспектов безопасности информации (доступность, конфиденциальность или целостность).

Обработка конфиденциальной информации - действия (операции) с конфиденциальной информацией, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание (персональных данных), блокирование, уничтожение;

Оператор обработки конфиденциальной информации – юридическое лицо, организующее и (или) осуществляющее обработку конфиденциальной информации, а также определяющее цели и содержание обработки конфиденциальной информации.

Пользователь информационной системы – сотрудник управления образования администрации Анжеро-Судженского городского округа (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированные в ИСПДн в установленном порядке.

2. Общие положения

2.1. Настоящее Положение определяет порядок организации и проведения работ по защите конфиденциальной информации в управлении образования администрации Анжеро-Судженского городского округа. Данное Положение используется совместно с «Руководством пользователя по обеспечению безопасности ИСПДн», «Порядком обеспечения безопасности ПДн при помощи криптосредств» и другими нормативными документами принятыми в управлении образования администрации Анжеро-Судженского городского округа.

2.2. Конфиденциальная информация должна обрабатываться (передаваться) с использованием защищенных систем и средств информатизации и связи или с

использованием технических и программных средств технической защиты конфиденциальной информации, сертифицируемых в установленном порядке.

2.3.Уровень технической защиты конфиденциальной информации, а также перечень необходимых мер защиты определяется по результатам обследования объекта информатизации.

Проведение любых мероприятий и работ с конфиденциальной информацией, без принятия необходимых мер технической защиты информации не допускается.

2.4. Объектами защиты в управлении образования администрации Анжеро-Судженского городского округа являются:

- средства и системы информатизации и связи ИСПДн, используемые для обработки, хранения и передачи конфиденциальной информации (ОТСС);
- технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается конфиденциальной информация (ВТСС);
- помещения (служебные кабинеты, конференц-залы и т.п.), специально предназначенные для проведения конфиденциальных мероприятий.

2.5. Ответственность за выполнение требований настоящего Положения возлагается на *ответственного за организацию работ и обеспечение безопасности персональных данных в управлении образования администрации Анжеро-Судженского городского округа*.

3. Охраняемые сведения

Охраняемые сведения содержатся в «Перечне сведений конфиденциального характера, обрабатываемых в ИСПДн».

4. Технические каналы утечки конфиденциальной информации, несанкционированного доступа и специальных воздействий на нее

4.1. Доступ к конфиденциальной информации, нарушение ее целостности и доступности возможно реализовать за счет:

- несанкционированного доступа к конфиденциальной информации при ее обработке в информационных системах и ресурсах;
- утечки конфиденциальной информации по техническим каналам.

4.2. Описание возможных технических каналов утечки информации, несанкционированного доступа к информации и специальных воздействий на нее содержится в Моделях угроз ИСПДн.

5. Организационные и технические мероприятия по технической защите конфиденциальной информации

5.1. Разработка мер, и обеспечение защиты конфиденциальной информации осуществляются *ответственным за выполнение работ по технической и криптографической защите персональных данных*. Разработка мер защиты информации также может осуществляться сторонними предприятиями, имеющими соответствующие лицензии ФСТЭК России и ФСБ России на право осуществления таких работ.

5.2. Для защиты конфиденциальной информации, используются сертифицированные по требованиям безопасности технические средства защиты.

5.3. Техническая защита информации в защищаемых помещениях:

5.3.1. Перечень защищаемых помещений определяется по результатам анализа циркулирующей в них конфиденциальной информации.

5.3.2. Обеспечение эффективного контроля за доступом в защищаемые помещения.

5.3.3. Инструктирование сотрудников, работающих в защищаемых помещениях о правилах эксплуатации ПЭВМ, других технических средств обработки информации, средств связи с соблюдением требований по технической защите конфиденциальной информации.

5.3.4. Проведение в защищаемых помещениях обязательных проверок на наличие внедренных закладных устройств.

5.3.5. Исключение неконтролируемого доступа к линиям связи, управления и сигнализации в защищаемых помещениях.

5.3.6. Осуществление *ответственным за выполнение работ по технической и криптографической защите персональных данных* контроля за проведением всех монтажных и ремонтных работ в защищаемых помещениях.

5.3.7. Обеспечение требуемого уровня звукоизоляции входных дверей и окон защищаемых помещений.

5.3.8. Отключение при проведении совещаний в защищаемых помещениях всех неиспользуемых электро- и радиоприборов от сетей питания и трансляции.

5.3.9. Выполнение перед проведением совещаний следующих условий:

окна должны быть плотно закрыты и зашторены;

двери плотно прикрыты.

5.4. Защита информации, циркулирующей в ОТСС и наводящейся в ВТСС.

5.4.1. При эксплуатации ОТСС и ВТСС необходимо неукоснительное выполнение требований, определенных в предписании на эксплуатацию.

5.4.2. Техническая защита информации в средствах вычислительной техники (СВТ) и автоматизированных системах (АС) от несанкционированного доступа обеспечиваться путем:

- проведения классификации АС;
- выполнения необходимых организационных мер защиты;
- установки сертифицированных программных и аппаратно-технических средств защиты информации от НСД.
- защита каналов связи, предназначенных для передачи конфиденциальной информации.
- защиты информации от воздействия программ-закладок и компьютерных вирусов.

5.5. Организации антивирусной защиты информации на объектах информатизации достигается путём:

- установки и применения средств антивирусной защиты информации;
- обновления баз данных средств антивирусной защиты информации;
- действий должностных лиц при обнаружении заражения информационно-вычислительных ресурсов программными вирусами.

5.5.1. Организация работ по антивирусной защите информации возлагается на *ответственного за выполнение работ по технической и криптографической защите персональных данных*

5.5.2. Защита информации от воздействия программных вирусов должна осуществляться посредством применения средств антивирусной защиты. Порядок применения средств антивирусной:

- обязательный входной контроль на отсутствие программных вирусов всех поступающих в управление образования администрации Анжеро-Судженского городского округа носителей информации, информационных массивов, программных средств общего и специального назначения;
- периодическая проверка пользователями жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка используемых в работе носителей информации перед началом работы с ними на отсутствие программных вирусов;
- внеплановая проверка носителей информации на отсутствие программных вирусов в случае подозрения на наличие программного вируса;
- восстановление работоспособности программных средств и информационных массивов в случае их повреждения программными вирусами.

5.5.3. К использованию допускается только лицензированные, сертифицированные по требованиям ФСТЭК России антивирусные средства.

5.5.4. Порядок применения средств антивирусной защиты определяется «Инструкцией по организации антивирусной защиты в ИСПДн».

5.6. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в управлении образования администрации Анжеро-Судженского городского округа «Руководством пользователя по обеспечению безопасности ИСПДн»

6. Обязанности и права должностных лиц

6.1. Руководство технической защитой конфиденциальной информации в управлении образования администрации Анжеро-Судженского городского округа возлагается на *ответственного за выполнение работ по технической и криптографической защите персональных данных*.

6.2. *Ответственный за выполнение работ по технической и криптографической защите персональных данных* управления образования администрации Анжеро-Судженского городского округа организует и обеспечивает техническую защиту информации, циркулирующую в технических средствах и помещениях подчиненных им подразделений.

6.3. *Ответственный за выполнение работ по технической и криптографической защите персональных данных* осуществляет непосредственное руководство разработкой мероприятий по технической защите конфиденциальной информации и контролю в органе исполнительной власти.

6.4. Руководители подразделений и сотрудники управления образования администрации Анжеро-Судженского городского округа обязаны вносить предложения о приостановке работ с использованием конфиденциальной

информации в случае обнаружения утечки (или предпосылок к утечке) этих сведений. Предложения докладываются непосредственно *ответственному за выполнение работ по технической и криптографической защите персональных данных*

7. Планирование работ по технической защите конфиденциальной информации и контролю

7.1. *Ответственный за выполнение работ по технической и криптографической защите персональных данных* составляет годовые планы работ по технической защите конфиденциальной информации и контролю. Сроки разработки, представления и утверждения планов устанавливаются *ответственным за организацию работ и обеспечение безопасности персональных данных в управлении образования администрации Анжеро-Судженского городского округа*.

7.2. В годовые планы по технической защите конфиденциальной информации и контролю включаются:

- подготовка проектов распорядительных документов по вопросам организации технической защиты информации в управлении образования администрации Анжеро-Судженского городского округа, инструкций, рекомендаций, памяток и других документов по обеспечению безопасности информации при использовании технических средств обработки и передачи информации;
- аттестация вводимых в эксплуатацию ОТСС и защищаемых помещений, а также периодическая переаттестация находящихся в эксплуатации ОТСС и защищаемых помещений на соответствие требованиям по технической защите конфиденциальной информации;
- проведение периодического контроля состояния технической защиты информации;
- мероприятия по устранению нарушений и выявленных недостатков по результатам контроля;
- мероприятия по совершенствованию технической защиты информации на объектах органа исполнительной власти.

7.3. Контроль выполнения планов и отчетность по ним возлагается на *ответственного за организацию работ и обеспечение безопасности персональных данных в управлении образования администрации Анжеро-Судженского городского округа*..

8. Контроль состояния технической защиты конфиденциальной информации

8.1. Основными задачами контроля состояния технической защиты конфиденциальной информации являются оценка уровня принятых мер защиты, своевременное выявление и предотвращение утечки по техническим каналам информации, составляющей конфиденциальную информацию, НСД к информации, преднамеренных программно-технических воздействий на

информацию с целью ее уничтожения, искажения, блокирования, нарушения правового режима использования информации.

8.2. Контроль осуществляется:

ФСТЭК России (силами Управления по соответствующему федеральному округу);

Управлением Федеральной службы безопасности;

Ответственным за организацию работ и обеспечение безопасности персональных данных в управлении образования администрации Анжеро-Судженского городского округа.

8.3. Контроль заключается в проверке выполнения актов законодательства Российской Федерации по вопросам защиты конфиденциальной информации, решений ФСТЭК России, руководителя управления образования администрации Анжеро-Судженского городского округа, наличия соответствующих документов по технической защите конфиденциальной информации, в инструментальной и визуальной проверке ОТСС и защищаемых помещений на наличие каналов утечки информации, на соответствие требованиям и нормам технической защиты информации.

9. Взаимодействие с предприятиями, учреждениями и организациями

9.1. При проведении совместных работ управление образования администрации Анжеро-Судженского городского округа с предприятиями, учреждениями и организациями должна быть обеспечена техническая защита конфиденциальной информации независимо от места проведения работ.

9.2. В технических заданиях на выполнение совместных работ с использованием конфиденциальной информации, должны быть предусмотрены требования (или меры) по ее технической защите, которые должны выполняться каждой из сторон. Технические задания на выполнение совместных работ согласовываются с *ответственным за выполнение работ по технической и криптографической защите персональных данных в управлении образования администрации Анжеро-Судженского городского округа*.

9.3. Организация технической защиты информации возлагается на руководителей совместных работ, а ответственность за обеспечение технической защиты информации - на исполнителей работ.

10. Ответственность за разглашение конфиденциальной информации

За разглашение информации конфиденциального характера, нарушение порядка обращения с документами и машинными носителями информации, содержащими такую информацию, а также за нарушение или неисполнение требований режима защиты, обработки и порядка использования этой информации сотрудник может быть привлечен к дисциплинарной или иной

ответственности, предусмотренной действующим законодательством.

С приказом № 356 **от «** 30 **»** апреля **2014 ознакомлен:**

N п/п	Фамилия, имя, отчество работника	Дата ознакомления	Роспись в ознакомлении
1	Семенкина М.В.	30.04.14г	
2	Вейс С.А.	30.04.14г	
3	Резникова Е.А.	30.04.2014	
4	Федоренко Т.А.	30.04.2014	
5	Шумахер О.Г.	30.04.2014г	
6	Порфирьевич Ю.А.	30.04.2014	
7	Частикин А.М.	30.04.2014	
8	Латтова А.Р.	30.04.2014	
9	Лукарева О.А.	30.04.2014	
10	Крупаченко А.А.	30.04.2014	
11	Мещерина О.В.	30.04.2014	
12	Головина К.П.	30.04.2014	
13	Ульянина Л.А.	30.04.2014	
14	Вакуленко Ж.С.	30.04.2014	
15	Колесова Я.В.	30.04.2014	
16	Бутинцева Е.А.	30.04.2014	
17	Боровкова Г.И.	30.04.2014	
18	Сапожникова О.П.	30.04.2014	
19	Кузьменко А.Ю.	30.04.2014	
20	Голорова Е.П.	30.04.2014г	
21	Акуличева О.А.	30.04.2014	
22	Жиленко Л.В.	30.04.2014	
23	Порфирьевич Ю.А.	30.04.2014г	
24	Шафрина И.П.	30.04.2014.	
25	Нетяга Н.В.	30.04.2014	
26	Толстуук Е.А.	30.04.2014	
26	Шумейко Л.И.	30.04.2014	
28	Тодоренко А.С.	30.04.2014	
29	Пуха В.В.	30.04.2014	
30	Тимофеева С.В.	30.04.2014	
31	Шестеренко М.В.	30.04.2014	
32	Станкевич Г.А.	30.04.2014г	
33			
34			
35			