Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»

Высшая школа электроники и компьютерных наук

Кафедра «Защита информации»

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2017 г.

Модернизация защиты информационной системы персональных данных в Областном казенном учреждении Центр занятости населения города Аши

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ

Автор проекта,
студент группы КЭ- 501
_____ Пикунов, К. А.
_____ 2017 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2017 г.

Челябинск 2017

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

АРМ - автоматизированное рабочее место;
БД – базы данных;
ЗИ – защита информации;
ИБ – информационная безопасность;
ИСПДн - информационная система персональных данных;
ОКУ ЦЗН – областное казенное учреждение Центр занятости населения;
НСД – несанкционированный доступ;
ПДн – персональные данные;
ПК – персональный компьютер;
ПО – программное обеспечение;
РД – руководящие документы;
РФ – Российская Федерация;
ФЗ – Федеральный закон;
ФСБ – Федеральная служба безопасности;
ФСТЭК - Федеральная служба по техническому и экспортному контролю;
СЗИ – система защиты информации.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных[10].

Угроза (безопасности информации) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации[13].

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных[10].

Уязвимость – недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации[11].

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы[10].

ВВЕДЕНИЕ

С развитием информационных технологий, с ростом технических возможностей по копированию и распространению информации, она подвергается воздействию различных процессов (неисправностям и сбоям оборудования, ошибкам операторов и т.д.), которые могут привести к ее разрушению, изменению, а также создать предпосылки к доступу к ней третьих лиц.

С появлением сложных автоматизированных систем управления, связанных с вводом, хранением, обработкой и выводом информации, проблемы ее защиты приобретают еще большее значение для организаций. Этому способствует: увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью автоматизированной информационной системы; сосредоточение в единых базах данных информации различного назначения и принадлежности; расширение круга пользователей, имеющих доступ к ресурсам информационной системы, и находящимся в ней данных.

Постоянно совершенствующееся законодательство в области защиты персональных данных обуславливает необходимость организациям обновлять меры по защите сведений, содержащих персональные данные.

В ОКУ ЦЗН города Аши хранится информация, напрямую связанная с субъектами персональных данных (безработными гражданами и сотрудниками ЦЗН).

Таким образом, актуальность данной работы обусловлена необходимостью модернизации защиты информационной системы персональных данных в ОКУ ЦЗН города Аши.

Объектом выпускной квалификационной работы является ОКУ ЦЗН города Аши.

Предметом выпускной квалификационной работы является информационная система персональных данных в ОКУ ЦЗН города Аши.

Целью дипломной работы является обоснование ряда мер по модернизации защиты информационной системы персональных данных.

В соответствии с поставленной целью необходимо решить следующие задачи:

1) Провести предпроектное обследование информационной системы ОКУ ЦЗН города Аши с целью обоснования мер по модернизации защиты информационной системы персональных данных.

2) Провести теоретическое обоснование выбора средств защиты информации в ОКУ ЦЗН города Аши.

3) Разработать проект по модернизации защиты информационной системы персональных данных в ОКУ ЦЗН города Аши.

1. АНАЛИЗ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОКУ ЦЗН ГОРОДА АШИ И СУЩЕСТВУЮЩИЕ ПРОБЛЕМЫ

1.1. Описание информационной системы

Объектами защиты в органах исполнительной власти субъектов Российской Федерации, осуществляющих переданные полномочия в области содействия занятости населения, являются сети, системы и комплексы, задействованные в обработке персональных данных населения.

В соответствии со статьей 16.1 Закона Российской Федерации от 19 апреля 1991 года № 1032-1 "О занятости населения в Российской Федерации", Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных данных", требованиями нормативных документов ФСТЭК и ФСБ России, Федеральной службой по труду и занятости разработаны рекомендации по защите информации в органах исполнительной власти субъектов Российской Федерации, осуществляющих переданные полномочия в области содействия занятости населения и государственных учреждениях центрах занятости населения в процессе информационного взаимодействия с автоматизированной информационной системой формирования и ведения регистров получателей государственных услуг в сфере занятости населения.

Для определения комплекса мероприятий по защите информации сначала необходимо сформировать общее представление об объекте защиты. Для этого был составлен паспорт предприятия (Приложение А). В паспорте перечислены реквизиты, определен вид деятельности, виды защищаемой информации, организационная структура, перечень поставщиков.

В информационной системе ОКУ ЦЗН города Аши можно выделить организационные, правовые, программно-аппаратные аспекты защиты информации.

Организационное обеспечение включает в себя такие документы как должностные инструкции персонала, отделов; эксплуатационная документация на средства защиты информации, инструкции пользователей ИСПДн, инструкции о порядке работы с персональными данными; особых режимах, системах взаимодействия с персоналом.

Правовое обеспечение включает в себя свод определенных нормативно-правовых документов, регулирующих деятельность организации, а также информационных процессов, протекающих в ней относительно обеспечения защиты информации: Конституция Российской Федерации; Федеральный закон «О персональных данных»; Федеральный закон «О занятости населения в Российской Федерации»; Федеральный закон «Об информации, информационных технологиях и о защите информации»; Трудовой кодекс Российской Федерации и т.д.

Программно-аппаратное обеспечение - это комплекс программно-аппаратных средств, обеспечивающих работу центра.

Основным назначением информационной системы центра занятости является: ведение кадрового учета; ведение бухгалтерского учета; сбор, накопление, хранение, и обработка персональных данных сотрудников организации и

безработных граждан; формирование отчетов, относящихся к деятельности центра занятости, организация электронного документооборота.

ИСПДн ОКУ ЦЗН города Аши взаимодействует с другими информационными системами с применением криптографических средств защиты информации.

Информация, хранимая и обрабатываемая в информационной системе ОКУ ЦЗН города Аши, востребована рядом информационных систем органов государственной власти и учреждений. В частности, информационная система ОКУ ЦЗН города Аши осуществляет посредством сети Интернет информационный обмен с Федеральной налоговой службой; Пенсионным фондом Российской Федерации; Сбербанком РФ.

Таким образом, все информационные потоки в информационной системе ОКУ ЦЗН города Аши можно разделить на две основные группы: внутренние и внешние.

К внешним информационным потокам относится передача информации во внешние информационные системы (Федеральную налоговую службу, Сбербанк РФ, Пенсионный фонд РФ и др.).

К внутренним информационным потокам относятся:

- сбор (ввод) целевой информации, первичных бухгалтерских данных, данных кадрового учета, персональных данных безработных граждан;
- просмотр, создание архивных копий, вывод на печать и др.;
- обмен служебной информации (приказы, распоряжения и др.);
- разрешения на доступ к целевой информации;
- передача запрошенной целевой информации;
- процессы авторизации пользователей информационной системы, запросы на получение доступа к целевой информации в соответствии с правилами доступа на предоставление целевой информации.

1.2. Анализ технологического процесса обработки информации

В ИСПДн осуществляется работа с локальными файлами и базами данных, содержащими ПДн на АРМ. Загрузка компьютеров осуществляется по персональному идентификатору и паролю конкретного пользователя. По окончании загрузки компьютера пользователь получает права доступа к устройствам, каталогам, файлам и программам ИСПДн. Функции, права, обязанности и порядок работы на ПК регламентируются специально разработанными инструкциями ответственного за обеспечение безопасности ПДн и пользователя ИСПДн. В целях фильтрации исходящего и входящего трафика, циркулирующего между сетью ЛВС и внешней сетью, на границе ЛВС установлен межсетевой экран в состав программного комплекса ViPNet Coordinator 3.2, а на АРМ установлены персональные межсетевые экраны в составе программных комплексов ViPNet Client 3.2.

1.3. Анализ информационных потоков

Документы, содержащие ПДн, предоставляются гражданами при поступлении на работу в ОКУ ЦЗН города Аши. Документы, содержащие ПДн, предоставляются гражданами, обращающимися в ОКУ ЦЗН города Аши за содействием в поиске работы. Специалисты ОКУ ЦЗН города Аши вносят ПДн в ИСПДн и обрабатывают полученные данные в целях, указанных в Положении об обработке персональных данных (Приложение Б). При обращении в ОКУ ЦЗН города Аши граждане дают свое согласие на обработку персональных данных (Приложение Г).

ПДн безработных граждан передаются в Главное управление по труду и занятости населения Челябинской области по защищенным каналам связи посредством ПК ViPNet Client 3.2 (хранение ПДн осуществляется на сервере СОИ СЗН).

ПДн сотрудников передаются в УПФР, ФНС и ФСС Ашинского района по открытому каналу с использованием шифрования СКЗИ КриптоПро CSP3.6. ПДн граждан и сотрудников также передаются в ПАО «Сбербанк России» с использованием шифрования СКЗИ «Бикрипт-КСБ-С», встроенным в Sbersign 5.7.

1.4. Выявление защищаемой информации

В ходе аналитической работы с информацией, обрабатываемой в ОКУ ЦЗН города Аши и с организационно-распорядительной документацией организации, была выявлена следующая защищаемая информация:

- сведения, содержащие персональные данные (на основании Федерального закона от 27 июля 2006 №152-ФЗ «О персональных данных»);
- общедоступная информация, располагаемая в общедоступных источниках и сети интернет (на основании Федерального закона от 27.07.2006 № 149-ФЗ (ред. от 21.07.2014) «Об информации, информационных технологиях и о защите информации»).

Информация о персональных данных содержится в «Перечне сведений, содержащих персональные данные» (Приложение В), который устанавливается и закрепляется в «Положении об обработке персональных данных» (Приложение Б).

1.5. Выявление объектов защиты

Объектами защиты являются – информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты. Перечень персональных данных, подлежащих защите, определен в Перечне персональных данных, подлежащих защите в ИСПД.

В результате был составлен следующий перечень объектов защиты:

- помещения для хранения и работы с важной защищаемой информацией;
- сервер;
- автоматизированные рабочие места;
- средства ввода-вывода и отображения информации;
- системы бесперебойного питания сервера и АРМ;

- системы дублирования и хранения информации;
- линии и средства связи, системы обеспечения функционирования СВТ и деятельности организации;
- носители информации;
- информационная инфраструктура;
- персонал.

1.6. Разработка модели угроз и уязвимостей для важных объектов защиты

1.6.1. Анализ угроз безопасности ИСПДн ОКУ ЦЗН города Аши

Анализ угроз безопасности ИСПДн ОКУ ЦЗН города Аши проводится в соответствии с «Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной заместителем директора ФСТЭК России 15 февраля 2008 года.

Модель угроз предназначена для решения следующих задач:

- анализ защищенности ИСПДн от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;
- разработка системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
- контроль за обеспечением уровня защищенности персональных данных.

ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей», утвержденный Приказом Федерального агентства по техническому регулированию и метрологии от 19 августа 2015 г. № 1180-ст дает следующее определение: «Уязвимость - недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации». Оценка уязвимости информации дает возможность выявить характерные особенности и недостатки объекта защиты, которые могут облегчить проникновение противника к информационной системе персональных данных. Главный результат такой работы — выявление возможных источников и каналов утечки информации. Виды уязвимости информации соответствуют видам информационных угроз.

Оценка актуальности угроз персональных данных осуществляется в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной приказом ФСТЭК России от 14 февраля 2008 г.

Она включает в себя:

- определение уровня исходной защищенности информационной системы как ИСПДн;
- определение вероятности реализации угроз в ИСПДн;
- определение возможности реализации угрозы в ИСПДн;
- оценку опасности угроз в ИСПДн;
- перечень актуальных угроз безопасности ПДн в ИСПДн;
- меры по противодействию угрозе.

Уровень исходной защищенности. Под уровнем исходной защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y1).

ИСПДн ОКУ ЦЗН города Аши имеет следующие технические и эксплуатационные характеристики:

а) территориальное размещение ИСПДн – распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом. Уровень защищенности – низкий.

б) наличие соединения с сетями связи общего пользования – ИСПДн, имеющая многоточечный выход в сеть общего пользования. Уровень защищенности – низкий.

в) встроенные (легальные) операции с записями баз персональных данных – модификация, передача. Уровень защищенности – низкий.

г) разграничение доступа к персональным данным – ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн. Уровень защищенности – средний.

д) наличие соединений с другими базами персональных данных иных ИСПДн – интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн). Уровень защищенности – низкий.

е) уровень обобщения (обезличивания) персональных данных – ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн). Уровень защищенности – низкий.

ж) объем персональных данных, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки – ИСПДн, предоставляющая часть ПДн. Уровень защищенности – средний.

Таблица 1. Исходная степень защищенности

№ п/п	Значение характеристики (уровень защищенности)	Количество значений	Процент значений не ниже данного уровня
1.	Высокий	0	0%
2.	Средний	2	29%
3.	Низкий	5	-

Т.о., по каждому фактору оценивается решение, в том числе на высоком, среднем и низком уровнях. Далее рассматривается отношение суммы положительных решений соответствующему среднему уровню защищенности, к общему количеству решений. В информационной системе ОКУ ЦЗН города Аши менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний». В соответствии с полученными данными устанавливается низкий показатель исходной защищенности. Устанавливается значение коэффициента Y1=10.

Определение вероятности реализации угроз в ИСПДн. Под вероятностью реализации угрозы поднимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализации конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя. При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y2:

- маловероятно (Y_2 =0) – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);
- низкая вероятность (Y_2 = 2) – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);
- средняя вероятность (Y_2 = 5) - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;
- высокая вероятность (Y_2 =10) - объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности ПДн не приняты.

По итогам оценки уровня защищенности (Y_1) и вероятности реализации угрозы (Y_2), коэффициент реализуемости угрозы Y будет определяться соотношением

$$Y = (Y1 + Y2) / 20.$$

Оценка вероятности реализации угрозы безопасности рассчитываются для каждой угрозы со стороны каждой категории нарушителей: внешние нарушители, пользователи, посетители.

Угроза безопасности ПДн считается актуальной, если она имеет возможность реализации - не ниже средней, а также степень опасности - не ниже средней (по трем градациям: низкая, средняя, высокая).

Таблица 2. Правила отнесения угрозы безопасности ПДн к актуальной

Возможность реализации угрозы	Показатель опасности угрозы		
	низкая	средняя	высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Таблица 3. Актуальность угроз

Вид угрозы безопасности ПДн	Вероятность реализации угроз	Коэффициент реализуемости угрозы (Y)	Возможность реализации угроз	Опасность	Актуальность
1	2	3	4	5	6
1. Угрозы утечки информации по техническим каналам					
1.1. Угрозы утечки акустической информации	низкая вероятность ($Y_2 = 2$)	0,6	средняя	низкая	неактуальная
1.2. Угрозы утечки видовой информации	низкая вероятность ($Y_2 = 2$)	0,6	средняя	низкая	неактуальная
1.3. Угрозы утечки информации по каналам ПЭМИН	низкая вероятность ($Y_2 = 2$)	0,6	средняя	низкая	неактуальная
2. Угрозы несанкционированного доступа к информации					
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн					
2.1.1. Кража ПЭВМ	низкая вероятность ($Y_2 = 2$)	0,6	средняя	средняя	актуальная
2.1.2. Кража носителей информации	низкая вероятность ($Y_2 = 2$)	0,6	средняя	средняя	актуальная
2.1.3. Кража ключей доступа	низкая вероятность ($Y_2 = 2$)	0,6	средняя	средняя	актуальная
2.1.4. Кражи, модификации, уничтожение информации	низкая вероятность ($Y_2 = 2$)	0,6	средняя	средняя	актуальная
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	низкая вероятность ($Y_2 = 2$)	0,6	средняя	низкая	неактуальная

Продолжение таблицы 3

1	2	3	4	5	6
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	высокая вероятность ($Y_2 = 10$)	1,00	очень высокая	средняя	актуальная
2.1.7. Несанкционированное отключение средств защиты	средняя вероятность ($Y_2 = 5$)	0,75	высокая	средняя	актуальная
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)					
2.2.1. Действия вредоносных программ (вирусов)	высокая вероятность ($Y_2 = 10$)	1,00	очень высокая	средняя	актуальная
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	низкая вероятность ($Y_2 = 2$)	0,6	средняя	низкая	неактуальная
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей	низкая вероятность ($Y_2 = 2$)	0,6	средняя	средняя	актуальная
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера					

Продолжение таблицы 3

1	2	3	4	5	6
2.3.1. Утрата ключей и атрибутов доступа	низкая вероятность ($Y_2 = 2$)	0,6	средняя	средняя	актуальная
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	средняя вероятность ($Y_2 = 5$)	0,75	высокая	средняя	актуальная
2.3.3. Непреднамеренное отключение средств защиты	средняя вероятность ($Y_2 = 5$)	0,75	высокая	средняя	актуальная
2.3.5. Сбой системы электроснабжения	низкая вероятность ($Y_2 = 2$)	0,6	средняя	низкая	неактуальная
2.3.6. Стихийное бедствие	низкая вероятность ($Y_2 = 2$)	0,6	средняя	низкая	неактуальная
2.4. Угрозы преднамеренных действий внутренних нарушителей					
2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке	средняя вероятность ($Y_2 = 5$)	0,75	высокая	средняя	актуальная
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	низкая вероятность ($Y_2 = 2$)	0,6	средняя	средняя	актуальная

Продолжение таблицы 3

1	2	3	4	5	6
2.5.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	высокая вероятность (Y_2 = 10)	1,00	очень высокая	средняя	актуальная
2.5.3. Угрозы выявления паролей по сети	низкая вероятность (Y_2 = 2)	0,6	низкая	средняя	неактуальная
2.5.4. Угроза навязывания ложного маршрута сети	низкая вероятность (Y_2 = 2)	0,6	низкая	средняя	неактуальная
2.5.5. Угрозы получения несанкционированного доступа путем подмены доверенного объекта в сети	низкая вероятность (Y_2 = 2)	0,6	средняя	средняя	актуальная
2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	низкая вероятность (Y_2 = 2)	0,6	низкая	средняя	неактуальная
2.5.7. Угрозы типа «Отказ в обслуживании»	низкая вероятность (Y_2 = 2)	0,6	средняя	средняя	актуальная
2.5.8. Угрозы удаленного запуска приложений	низкая вероятность (Y_2 = 2)	0,6	низкая	средняя	неактуальная

Продолжение таблицы 3

1	2	3	4	5	6
2.5.9. Угрозы внедрения по сети вредоносных программ	средняя вероятность (Y_2 = 5)	0,75	высокая	средняя	актуальная

Для ИСПДн ОКУ ЦЗН города Аши актуальны угрозы 2 типа – угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе. Учитывая исходные данные ИСПДн и тип актуальных угроз для ИСПДн, устанавливается 4-й уровень защищенности ПДн.[5]

Примерный перечень мер по противодействию актуальной угрозе информационной системы ОКУ ЦЗН города Аши представлен в таблице 4.

Таблица 4. Примерный перечень мер по противодействию актуальной угрозе

Угроза безопасности ПДн	Степень актуальности	Меры по противодействию угрозе	
		Технические	Организационные
1	2	3	4
Кража ПЭВМ	актуальная	Видеонаблюдение, охранная сигнализация, разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации	Инструкция для персонала, установка решеток на окнах, закрывание дверей на замок
Кража носителей информации	актуальная	Реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам	Инструкция пользователя, установка решеток на окнах, закрывание дверей на замок, учет и хранение носителей

Продолжение таблицы 4

1	2	3	4
Кража ключей доступа	актуальная	Реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам	Инструкция пользователя, учет паролей, хранение ключей и введение политики безопасности
Кражи, модификации, уничтожение информации	актуальная	Решетки на окнах, кодовый замок, шифрование данных, система защиты от НСД, запрет загрузки с отчуждаемых носителей информации; запрет самостоятельного изменения аппаратно-программной конфигурации; использование систем обнаружения вторжений; использование средств анализа защищенности.	Резервное копирование, инструкция пользователя, реализация разрешительной системы допуска пользователей и обслуживающего персонала к рабочим станциям в составе ИСПДн
Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	актуальная	Реализация разрешительной системы допуска пользователей и обслуживающего персонала к рабочим станциям в составе ИСПДн, разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации	Инструкция администратора безопасности

Продолжение таблицы 4

1	2	3	4
Несанкционированное отключение средств защиты	актуальная	Настройка средств защиты, разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации	Инструкция администратора безопасности,
Действия вредоносных программ (вирусов)	актуальная	Использование средств антивирусной защиты; регулярное обновление ПО, используемого в серверных компонентах ИСПДн и АРМ	Инструкция по антивирусной защите
Недекларированные возможности ПО и ПО для обработки персональных данных	актуальная	Настройка средств защиты, разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации	Сертификация
Установка ПО, не связанного с исполнением обязанностей	актуальная	Настройка средств защиты, политика безопасности, использование систем обнаружения вторжений; использование средств анализа защищенности; использование систем доверенной загрузки	Инструкция пользователя, инструкция администратора безопасности, назначение пользователям ИСПДн прав, минимально необходимых для выполнения служебных обязанностей
Утрата ключей и атрибутов доступа	актуальная		Инструкция пользователя, введение парольной политики

Продолжение таблицы 4

1	2	3	4
Непреднамеренная модификация (уничтожение) информации сотрудниками	актуальная	Настройка средств защиты, политика безопасности, разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации	Инструкция пользователя, резервное копирование обрабатываемых ПДн
Непреднамеренное отключение средств защиты	актуальная	Разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации	Инструкция пользователя, инструкция администратора безопасности
Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке	актуальная	Разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации	Инструкция администратора безопасности, охранная сигнализация, установка решеток на окна, закрывание дверей на замок
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	актуальная	Настройка средств защиты, политика безопасности, доведение до пользователей ИСПДн информации об обязанности обеспечения безопасности ПДн; контроль действий пользователей ИСПДн и вводимых ими данных; предоставление персоналу ИСПДн привилегий, минимально необходимых для выполнения ими своих функциональных обязанностей	Инструкция для персонала, соглашение о неразглашении обрабатываемой информации, проведение занятий по повышению осведомленности в области защиты информации; проведение тестирований и опросов для оценки текущего уровня осведомленности в области ЗИ

Продолжение таблицы 4

1	2	3	4
Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	актуальная	Использование систем обнаружения вторжений; использование средств анализа защищенности; применение средств межсетевого экранирования; фильтрация сетевых пакетов по правилам, заданным оператором.	
Угрозы получения несанкционированного доступа путем подмены доверенного объекта в сети	актуальная	Межсетевой экран	Инструкция администратора безопасности
Угрозы типа «Отказ в обслуживании»	актуальная	Применение стойких алгоритмов идентификации и аутентификации хостов, пользователей и т.д.; применение средств межсетевого экранирования; использование систем обнаружения вторжений; использование средств анализа защищенности; фильтрация сетевых пакетов по правилам, заданным оператором	Инструкция пользователя, инструкция администратора безопасности

Продолжение таблицы 4

1	2	3	4
Угрозы внедрения по сети вредоносных программ	актуальная	Использование средств антивирусной защиты; регулярное обновление ПО, используемого в серверных компонентах ИСПДн и АРМ; анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности); использование систем обнаружения вторжений	Инструкция по антивирусной защите

1.6.2. Разработка модели угроз и уязвимостей для ИСПДн ОКУ ЦЗН города Аши

Для того чтобы выявить наиболее важные угрозы информационной безопасности ОКУ ЦЗН города Аши из большого количества возможных угроз, выделим наиболее важные объекты защиты персональных данных:

- персонал;
-автоматизированные рабочие места сотрудников, на которых обрабатываются персональные данные;
- сервер.

Таким образом, мы можем выделить наиболее значительные угрозы и уязвимости информационной безопасности относительно этих объектов. Выявленные угрозы и уязвимости представлены в Таблице – 5.

Таблица 5. Модель угроз и уязвимостей

Объект	Угроза	Уязвимость
Персонал (уровень критичности информации 66,66%)	1.Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	1.Несоблюдение соглашения о неразглашении обрабатываемой информации, инструкций для персонала
		2.Неактуальность документов по защите персональных данных, нарушение политики «чистого стола»

Продолжение таблицы 5

Объект	Угроза	Уязвимость
		3.Отсутствие регламента доступа в помещение, в котором обрабатываются персональные данные
	2. Утрата ключей и атрибутов доступа, вынос носителей информации за пределы контролируемой зоны	1.Отсутствие учета носителей информации, хранения ключей
		2.Отсутствие пропускного режима, видеонаблюдения
	3.Непреднамеренная модификация (уничтожение) информации сотрудниками	1.Отсутствие мероприятий по повышению информационной грамотности сотрудников
		2.Отсутствие инструкции по эксплуатации аппаратно-программных средств, АРМ и серверного оборудования, обрабатывающих персональные данные
	4. Кража, модификация, уничтожение информации (несанкционированное копирование, печать и размножение)	1.Нечеткая организация документооборота
		2.Неконтролируемый доступ сотрудников к копировальной и множительной технике
Автоматизированные рабочие места сотрудников, на которых обрабатываются персональные данные (уровень критичности информации 66,66%)	1.Несанкционированный доступ к АРМ	1.Отсутствие системы контроля доступа к АРМ
		2.Отсутствие видеонаблюдения в помещении
		3.Отсутствие пломбировки корпуса персонального компьютера
		4.Отсутствие авторизации на аппаратном уровне
	2. Разрушение защищаемой информации при помощи специальных программ и вирусов	1.Отсутствие или некорректная работа антивирусного ПО
		2.Отсутствие ограничения доступа пользователей к внешней сети
	3. Разглашение информации, модификация, уничтожение сотрудниками,	1.Несоблюдение соглашения о неразглашении обрабатываемой информации

Продолжение таблицы 5

Объект	Угроза	Уязвимость
	допущенными к ее обработке	2.Нечеткое распределение ответственности между сотрудниками
Сервер (уровень критичности информации 100%)	1.Несанкционированное проникновение нарушителя в помещение	1.Отсутствие видеонаблюдения в помещении
		2.Отсутствие регламента доступа в помещение
		3.Отсутствие выделенного помещения для сервера или физической защиты сервера
	2.Несанкционированный доступ к базам данных, хранящимся на сервере	1.Установка программного обеспечения, которое может создать условия для НСД
		2.Отсутствие регламента эксплуатации средств антивирусной защиты
	3.Утечка носителей информации за пределы контролируемой зоны (жестких дисков)	1.Отсутствие учета носителей информации
		2.Отсутствие пропускного режима
		3.Отсутствие пломбировки корпуса компьютера

1.7. Расчет рисков важных объектов защиты

Расчет рисков один из важнейших этапов обеспечения защиты информации в организации. С помощью расчета рисков выявляются наиболее вероятные угрозы для объектов информации через анализ этих угроз, действующих на конкретный ресурс, и уязвимостей, через которые данные угрозы могут быть реализованы.

Для расчета рисков важных объектов была использована модель оценки рисков российской консалтинговой компании в области аудита информационной безопасности «Digital Security Office» с программным обеспечением «ГРИФ 2006».

Также была использована методика, полученная в рамках курса “Экономика защиты информации”, разработанная на основе данной модели оценки рисков.

Для того, чтобы оценить риск информации, необходимо проанализировать все угрозы, действующие на информационную систему, и уязвимости, через которые возможна реализация угроз. На основе модели угроз и уязвимостей, актуальных для информационной системы ОКУ ЦЗН города Аши, будет проведен анализ вероятности реализации угроз информационной безопасности на каждый ресурс и, исходя из этого, рассчитаны риски.

Принцип работы алгоритма.

Входные данные:
ресурсы;
критичность ресурса;
отделы, к которым относятся ресурсы;
угрозы, действующие на ресурсы;
уязвимости, через которые реализуются угрозы;
вероятность реализации угрозы через данную уязвимость;
критичность реализации угрозы через данную уязвимость.

Расчет рисков по угрозе информационной безопасности.

1. На первом этапе рассчитывается уровень угрозы по уязвимости Th на основе критичности и вероятности реализации угрозы через данную уязвимость по формуле (1). Уровень угрозы показывает, насколько критичным является воздействие данной угрозы на ресурс с учетом вероятности ее реализации.

$$\mathrm{Th} = \frac{\mathrm{ER}}{100} \cdot \frac{\mathrm{P(V)}}{100}, \quad (1)$$

где
ER - критичность реализации угрозы (указывается в %);
P(V) - вероятность реализации угрозы через данную уязвимость (указывается в %).
Полученное значение уровня угрозы по уязвимости лежит в интервале от 0 до 1.

2. Для расчета уровня угрозы по всем уязвимостям CTh, через которые возможна реализация данной угрозы на ресурсе (формула (2)), необходимо просуммировать полученные уровни угроз через конкретные уязвимости по следующей формуле:

$$CTh = 1 - \prod_{i=1}^{n} (1 - Th_i), \quad (2)$$

где Th - уровень угрозы по уязвимости.
Значение уровня угрозы по всем уязвимостям лежит в интервале от 0 до 1.

3. Аналогично рассчитывается общий уровень угроз по ресурсу CThR (учитывая все угрозы, действующие на ресурс) по формуле (3).

$$\mathrm{CThR} = 1 - \prod_{i=1}^{n} (1 - CTh_i), \quad (3)$$

где CTh - уровень угрозы по всем уязвимостям.
Значение общего уровня угрозы лежит в интервале от 0 до 1.

4. Риск по ресурсу R рассчитывается в соответствии с формулой (4):
$R = \mathrm{CThR} \times D$, (4)
где D - критичность ресурса (задается в уровнях);
CThR - общий уровень угроз по ресурсу.

На основе данной методики были получены следующие результаты расчета рисков, представленные в Таблице 6.1, Таблице 6.2, Таблице 6.3.

Таблица 6.1. Расчет рисков (персонал)

Угроза/Уязвимость	Вероятность реализации угрозы через данную уязвимость в течение года (%), P(V)	Критичность реализации угрозы через данную уязвимость в течение года (%), ER
1	2	3
Персонал		
Угроза 1/Уязвимость 1	30	50
Угроза 1/Уязвимость 2	20	50
Угроза 1/Уязвимость 3	30	50
Угроза 2/Уязвимость 1	20	50
Угроза 2/Уязвимость 2	20	50
Угроза 3/Уязвимость 1	30	50
Угроза 3/Уязвимость 2	40	50
Угроза 4/Уязвимость 1	40	50
Угроза 4/Уязвимость 2	40	50

Таблица 6.2. Расчет рисков (АРМ)

Угроза/Уязвимость	Вероятность реализации угрозы через данную уязвимость в течение года (%), P(V)	Критичность реализации угрозы через данную уязвимость в течение года (%), ER
1	2	3
Автоматизированные рабочие места сотрудников, на которых обрабатывается защищаемая информация		
Угроза 1/Уязвимость 1	20	60
1	2	3
Угроза 1/Уязвимость 2	30	70
Угроза 1/Уязвимость 3	30	70
Угроза 1/Уязвимость 4	20	60
Угроза 2/Уязвимость 1	20	70
Угроза 2/Уязвимость 2	30	70
Угроза 3/Уязвимость 1	20	70
Угроза 3/Уязвимость 2	20	70

Таблица 6.3. Расчет рисков (сервер)

Угроза/Уязвимость	Вероятность реализации угрозы через данную уязвимость в течение года (%), P(V)	Критичность реализации угрозы через данную уязвимость в течение года (%), ER
1	2	3
Сервер		
Угроза 1/Уязвимость 1	30	80
Угроза 1/Уязвимость 2	20	70
Угроза 1/Уязвимость 3	30	80
Угроза 2/Уязвимость 1	20	80
Угроза 2/Уязвимость 2	20	70
Угроза 3/Уязвимость 1	20	80
Угроза 3/Уязвимость 2	20	70
Угроза 3/Уязвимость 3	30	80

1. Уровень угрозы:

Таблица 7. Уровень угрозы

Угроза/Уязвимость	Уровень угрозы (%), Th	Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза (%), CTh
1	2	3
Персонал		
Угроза 1/Уязвимость 1	0,15	0,35
Угроза 1/Уязвимость 2	0,1	
Угроза 1/Уязвимость 3	0,15	
Угроза 2/Уязвимость 1	0,1	0,19
Угроза 2/Уязвимость 2	0,1	
Угроза 3/Уязвимость 1	0,15	0,32
Угроза 3/Уязвимость 2	0,2	
Угроза 4/Уязвимость 1	0,2	0,36
Угроза 4/Уязвимость 2	0,2	
Автоматизированные рабочие места сотрудников, на которых обрабатывается защищаемая информация		
Угроза 1/Уязвимость 1	0,12	0,52
Угроза 1/Уязвимость 2	0,21	
Угроза 1/Уязвимость 3	0,21	
Угроза 1/Уязвимость 4	0,12	
Угроза 2/Уязвимость 1	0,14	0,32
Угроза 2/Уязвимость 2	0,21	

Продолжение таблицы 7

Угроза/Уязвимость	Уровень угрозы (%), Th	Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза (%), CTh
1	2	3
Угроза 3/Уязвимость 1	0,14	0,26
Угроза 3/Уязвимость 2	0,14	
Сервер		
Угроза 1/Уязвимость 1	0,24	0,50
Угроза 1/Уязвимость 2	0,14	
Угроза 1/Уязвимость 3	0,24	
Угроза 2/Уязвимость 1	0,16	0,28
Угроза 2/Уязвимость 2	0,14	
Угроза 3/Уязвимость 1	0,16	0,45
Угроза 3/Уязвимость 2	0,14	
Угроза 3/Уязвимость 3	0,24	

2. Общий уровень угроз, действующих на ресурс:

Таблица 8. Общий уровень угроз

Угроза/Уязвимость	Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза (%), CTh	Общий уровень угроз по ресурсу (%), CThR
1	2	3
Персонал		
Угроза 1/Уязвимость 1	0,35	0,77
Угроза 1/Уязвимость 2		
Угроза 1/Уязвимость 3		
Угроза 2/Уязвимость 1	0,19	
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1	0,32	
Угроза 3/Уязвимость 2		
Угроза 4/Уязвимость 1	0,36	
Угроза 4/Уязвимость 2		
Автоматизированные рабочие места сотрудников, на которых обрабатывается защищаемая информация		
Угроза 1/Уязвимость 1	0,52	0,76
Угроза 1/Уязвимость 2		
Угроза 1/Уязвимость 3		
Угроза 1/Уязвимость 4		

Продолжение таблицы 8

Угроза/Уязвимость	Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза (%), CTh	Общий уровень угроз по ресурсу (%), CThR
Угроза 2/Уязвимость 1	0,32	
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1	0,26	
Угроза 3/Уязвимость 2		
Сервер		
Угроза 1/Уязвимость 1	0,50	0,80
Угроза 1/Уязвимость 2		
Угроза 1/Уязвимость 3		
Угроза 2/Уязвимость 1	0,28	
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1	0,45	
Угроза 3/Уязвимость 2		
Угроза 3/Уязвимость 3		

3. Риск ресурса:

Таблица 9. Риск ресурса

Угроза/Уязвимость	Общий уровень угроз по ресурсу (%), CThR	Риск ресурса (уровень), R
1	2	3
Персонал		
Угроза 1/Уязвимость 1	0,77	51
Угроза 1/Уязвимость 2		
Угроза 1/Уязвимость 3		
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1		
Угроза 3/Уязвимость 2		
Угроза 4/Уязвимость 1		
Угроза 4/Уязвимость 2		
Автоматизированные рабочие места сотрудников, на которых обрабатывается защищаемая информация		
Угроза 1/Уязвимость 1	0,76	51
Угроза 1/Уязвимость 2		
Угроза 1/Уязвимость 3		
Угроза 1/Уязвимость 4		
Угроза 1/Уязвимость 5		

Продолжение таблицы 9

Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1		
Угроза 3/Уязвимость 2		
Сервер		
Угроза 1/Уязвимость 1	0,80	80
Угроза 1/Уязвимость 2		
Угроза 1/Уязвимость 3		
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1		
Угроза 3/Уязвимость 2		
Угроза 3/Уязвимость 3		

Таким образом, проанализировав все угрозы, действующие на информационную систему, и уязвимости, через которые возможна реализация угроз, произведен расчет риска информации, то есть вероятного ущерба, который понесет организация при реализации угроз информационной безопасности, зависящий от защищенности системы. По объекту «Персонал» наиболее высокий риск ИСПДн при реализации угрозы «Кража, модификация, уничтожение информации (несанкционированное копирование, печать и размножение)», наименее вероятен риск при реализации угрозы «Утрата ключей и атрибутов доступа, вынос носителей информации за пределы контролируемой зоны». По объекту «Автоматизированные рабочие места сотрудников, на которых обрабатывается защищаемая информация» наиболее высокий риск ИСПДн при реализации угрозы «Несанкционированный доступ к АРМ», наименее вероятен риск при реализации угрозы «Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке». По объекту «Сервер» наиболее высокий риск ИСПДн при реализации угроз «Несанкционированное проникновение нарушителя в помещение» и «Утечка носителей информации за пределы контролируемой зоны (жестких дисков)», наименее вероятен риск при реализации угрозы «Несанкционированный доступ к базам данных, хранящимся на сервере».

1.8. Разработка технического задания на модернизацию защиты ИСПДн

В ходе проведенного анализа и на основе полученной информации необходимо разработать техническое задание на модернизацию защиты информационной системы персональных данных (приложение Ж).

Содержание технического задания разрабатывалось на основании ГОСТ 34.602-1989 «Техническое задание на создание автоматизированной системы» и содержит следующие разделы:

1) общие сведения;
2) назначение и цели модернизации защиты ИСПДн;

3) характеристика объектов защиты;
4) требования к ИСПДн;
5) состав и содержание работ по модернизации защиты ИСПДн;
6) порядок контроля и приемки системы;
7) требования к составу и содержанию работ по подготовке объекта защиты к вводу защиты ИСПДн в действие;
8) требования к документированию;
9) источники разработки.

1.9. Безопасность жизнедеятельности

Сегодня невозможно представить свою жизнь без персонального компьютера. Они позволяют автоматизировать труд работников, снизить ручную работу до минимума. Но использование компьютера имеет не только положительную сторону. Пользователи ПК подвергаются воздействию опасных и вредных факторов, таких как повышенный уровень шума, электрический ток, электромагнитное излучение, статические и психологические нагрузки, и другие факторы.

Вредные факторы воздействуют на здоровье и самочувствие человека, приводят к снижению работоспособности, вызывают повышенное утомление. Снижают производительность труда и высокий уровень шума, который ухудшает слух, и электромагнитное излучение, которое также неблагоприятно влияет на здоровье. Персональный компьютер является источником опасности поражения электрическим током, а также может стать причиной пожара.

Все опасные и вредные производственные факторы в соответствии со ст. 13 Федерального закона от 28.12.2013 N 426-ФЗ (ред. от 01.05.2016) "О специальной оценке условий труда" подразделяются на физические, химические и биологические.

Условия труда специалистов ОКУ ЦЗН города Аши характеризуются возможностью воздействия на них комплекса следующих опасных и вредных производственных факторов:

- освещенность рабочей поверхности;
- температура воздуха;
- скорость движения воздуха;
- относительная влажность воздуха;
- уровень звука;
- вибрация общая и локальная.

Условия труда по степени вредности и (или) опасности подразделяются на четыре класса - оптимальные, допустимые, вредные и опасные условия труда.

Риск повреждения здоровья можно значительно снизить, если со всей ответственностью отнестись к организации рабочего места работника, а также соблюдать определенные организационно - технические защитные меры. Уменьшить возможные последствия от потенциального воздействия электромагнитных полей поможет правильно выбранный ПК, у которого есть гигиенический сертификат. Также необходимо строго соблюдать все правила и требования при организации рабочего

места и при необходимости применять защитные меры, чтобы свести к минимуму риск воздействия вредных факторов.

Организация рабочего места при работе с компьютером

Объектом анализа являются кабинеты сотрудников ОКУ ЦЗН города Аши, в которых обрабатываются персональные данные безработных граждан.

Анализ опасных и вредных факторов на рабочих местах проводится в соответствии с СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» и включает комплексную оценку вредности факторов производственной среды.

На рабочем месте сотрудников должны учитываться напряженность и тяжесть труда и производиться оценка опасных и вредных факторов.

При организации рабочего места специалистов центра занятости большое внимание уделяется эргономическим аспектам.

Согласно СанПиН 2.2.2/2.4.1340-03 предъявляются следующие требования к рабочему месту сотрудников.

При размещении в помещении нескольких рабочих мест с ПК необходимо учитывать, что расстояние между боковыми поверхностями соседних мониторов должно составлять не менее 1,2 м, а между тыльной поверхностью одного монитора и экраном другого - не менее 2,0 м.

Рабочие места с ПЭВМ при выполнении работы, требующей значительного умственного напряжения или высокой концентрации внимания, рекомендуется изолировать друг от друга перегородками высотой 1,5-2,0 м.

Экран видеомонитора должен находиться от глаз пользователя на расстоянии 600-700 мм, но не ближе 500 мм с учетом размеров алфавитно-цифровых знаков и символов.

Площадь на одно рабочее место пользователей ПЭВМ с ВДТ на базе плоских дискретных экранов (жидкокристаллические, плазменные) - 4,5 м2.

По отношению к световым проемам, ПК должны располагаться так, чтобы естественный свет падал сбоку, преимущественно слева. Свет, падающий спереди на рабочее место, утомляет зрение. Свет, падающий сзади, ухудшает видимость, создает блики на экране. Не следует размещать рабочие места с ПК вблизи силовых кабелей и вводов, высоковольтных трансформаторов, технологического оборудования, создающего помехи в работе ПК.

Конструкция рабочего стола должна обеспечивать оптимальное размещение на рабочей поверхности используемого оборудования с учетом его количества и конструктивных особенностей, характера выполняемой работы.

Конструкция рабочего стула (кресла) должна обеспечивать поддержание рациональной рабочей позы при работе на ПК, позволять изменять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления. Тип рабочего стула (кресла) следует выбирать с учетом роста пользователя, характера и продолжительности работы с ПК. Рабочий стул (кресло) должен быть обеспечен подъемно-поворотным механизмом,

также он должен быть регулируемым по высоте и углам наклона сиденья и спинки, а также расстояния спинки от переднего края сиденья, при этом регулировка каждого параметра должна быть независимой, легко осуществляемой и иметь надежную фиксацию. Поверхность сиденья, спинки и других элементов стула (кресла) должна быть полумягкой, с нескользящим, слабо электризующимся и воздухопроницаемым покрытием, обеспечивающим легкую очистку от загрязнений.

Высота рабочей поверхности стола для взрослых пользователей должна регулироваться в пределах 680 - 800 мм; при отсутствии такой возможности высота рабочей поверхности стола должна составлять 725 мм. Рабочее место пользователя ПК следует оборудовать подставкой для ног. Клавиатуру следует располагать на поверхности стола на расстоянии 100 - 300 мм от края, обращенного к пользователю или на специальной, регулируемой по высоте рабочей поверхности, отделенной от основной столешницы.

Рабочее место с ПК должно быть автономным.

Основные источники импульсных электрических и магнитных, а также электростатических полей - монитор и системный блок ПК - должны быть максимально удалены от пользователя.

Необходимо обеспечить надежное заземление (зануление) системного блока и источника питания ПК, а также заземление защитного фильтра и локальной сети.

Обязательно проведение периодического контроля сопротивления заземления (зануления). Необходимо занулять системный блок не только через зануляющий контакт трехконтактной вилки питания, но путем соединения отдельным проводником корпуса системного блока с контуром заземления помещения.

Должно быть обеспечено надежное заземление защитного фильтра монитора ПК. Наиболее правильным способом является соединение фильтра с корпусом системного блока ПК. Не рекомендуется соединение защитного экранного фильтра с другими зануленными электроустановками.

Необходимо обеспечить наибольшее удаление пользователя от сетевых розеток и проводов электропитания. Не рекомендуется использование двухпроводных удлинителей, переносок и сетевых фильтров, а также подобных устройств с трехконтактными розетками и вилками питания, но с незадействованным контактом зануления. Использование таких устройств можно допустить при наличии отдельно выполненного заземления (зануления) системного блока ПК.

При организации электропитания рабочего места целесообразно предусмотреть возможность изменения полярности включения в розетку сетевой вилки питания системного блока и монитора ПК и маркировку фазового и нулевого проводов. Это позволит при проведении измерений электромагнитных полей оперативно выбрать и зафиксировать ту ориентацию подключения вилки питания, при которой поля на рабочем месте минимальны.

При организации рабочего места с большим числом периферийных устройств, когда пользователь практически окружен различной оргтехникой, необходимо надежно занулять (заземлять) каждое периферийное устройство, следить за исправностью шины информационных цепей, связывающих эти устройства.

Оптимальная планировка рабочего места - планировка, при которой полностью разделены зоны местонахождения пользователя ПК и зоны расположения кабелей электропитания технических средств рабочего места, включая розетки сетевого электропитания.

При размещении в помещении нескольких рабочий мест с ПК необходимо учитывать, что расстояние между боковыми поверхностями соседних мониторов должно составлять не менее 1,2 м, а между тыльной поверхностью одного монитора и экраном другого - не менее 2,0 м.

При размещении значительного числа рабочих мест в помещении для обеспечения электромагнитной безопасности необходимо обеспечивать:

- автономное размещение отдельных рабочих мест, их автономное электропитание;
- максимально возможная удаленность от каждого пользователя сетевых элементов и аппаратуры соседних рабочих мест.

По результатам специальной оценки условий труда в ОКУ ЦЗН города Аши на рабочих местах не выявлены вредные и (или) опасные производственные факторы, все рабочие места признаны с оптимальными и допустимыми условиями труда, соответствующими государственным нормативным требованиям охраны труда. Итоговый класс условий труда – 2, то есть «условия труда, при которых на работника воздействуют вредные и (или) опасные производственные факторы, уровни воздействия которых не превышают уровни, установленные нормативами (гигиеническими нормативами) условий труда, а измененное функциональное состояние организма работника восстанавливается во время регламентированного отдыха или к началу следующего рабочего дня (смены)» (Ст. 14. Федерального закона от 28.12.2013 N 426-ФЗ (ред. от 01.05.2016) "О специальной оценке условий труда").

Санитарно-гигиенические параметры рабочего места

Требования к микроклимату рабочих мест

Для рабочих мест, на которых работа с ПЭВМ производится сидя и не требует физического напряжения, а также является основным видом выполняемых работ и связана с непрерывным эмоциональным напряжением, согласно СанПиН 2.2.2/2.4.1340-03 должны быть обеспечены оптимальные параметры микроклимата для работ категории 1а. Работа в ОКУ ЦЗН по СанПиН 2.2.4.3359-16 относится к работам категории 1а. (К категории 1а относятся работы с интенсивностью энергозатрат до 120 ккал/ч (до 139 Вт), производимые сидя и сопровождающиеся незначительным физическим напряжением (ряд профессий в сфере управления и т.п.).

Показателями, характеризующими микроклимат в производственных помещениях, являются:

- температура воздуха;
- температура поверхностей;
- относительная влажность воздуха;
- скорость движения воздуха;

- интенсивность теплового облучения.

Таблица 10. Гигиенические требования к микроклимату помещений, в которых установлены компьютеры (СанПиН 2.2.4.3359-16)

Период года	Категория работ по уровням энергозатрат, Вт	Температура воздуха, °С	Температура поверхностей, °С	Относительная влажность воздуха, %	Скорость движения воздуха, м/с
Холодный	1а (до 139)	22−24	21−25	60−40	0,1
Теплый	1а (до 139)	23−25	22−26	60−40	0,1

При наличии теплового облучения работающих при категории работ 1а температура воздуха на рабочих местах не должна превышать 25 °С.

Для обеспечения комфортных условий должны использоваться как организационные методы (рациональная организация проведения работ в зависимости от времени года и суток, чередование труда и отдыха), так и технические средства (вентиляция, кондиционирование воздуха, отопительная система).

В помещениях, оборудованных ПЭВМ, должна проводиться ежедневная влажная уборка, а также проветривание после каждого часа работы на ПЭВМ.

По результатам специальной оценки условий труда в ОКУ ЦЗН города Аши по микроклимату присвоен 2 класс условий труда.

Требования к освещению рабочих мест

При работе с вычислительной техникой важным фактором, обеспечивающим высокий уровень работоспособности, является правильно спроектированное освещение, не вызывающее раннего переутомления.

Согласно СанПиН 2.2.2/2.4.1340-03 рабочие столы следует размещать таким образом, чтобы ВДТ были ориентированы боковой стороной к световым проемам, чтобы естественный свет падал преимущественно слева. Оконные проемы должны быть оборудованы регулируемыми устройствами типа занавесей, внешних козырьков, жалюзи и т.д. Искусственное освещение в помещениях для эксплуатации ПЭВМ должно осуществляться системой общего равномерного освещения. В производственных и административно-общественных помещениях, в случаях преимущественной работы с документами и бумагами, следует применять системы комбинированного освещения.

Освещенность на поверхности рабочего стола должна быть 300−500 люкс. Освещенность поверхности экрана не должна быть более 300 лк, освещение не должно создавать бликов на поверхности экрана.

Для освещения помещений с ПЭВМ рекомендуется применять светильники с зеркальными параболическими решетками, укомплектованными электронными пускорегулирующими аппаратами (ЭПРА). Общее освещение при использовании люминесцентных светильников следует выполнять в виде сплошных или прерывистых линий светильников, расположенных сбоку от рабочих мест, параллельно линии зрения пользователя и линии оконных проёмов при рядном расположении рабочих мест, оснащённых ПЭВМ с ВДТ. При периметральном расположении компьютеров линии светильников должны располагаться локализовано над рабочим столом ближе к его переднему краю, обращенному к оператору. Коэффициент пульсации не должен превышать 5%.

Для обеспечения нормируемых значений освещенности в помещениях для использования ПЭВМ следует проводить чистку стекол оконных рам и светильников не реже двух раз в год и проводить своевременную замену перегоревших ламп.

По результатам специальной оценки условий труда в ОКУ ЦЗН города Аши по световой среде - освещенность рабочей поверхности (общая) - присвоен 3.1 класс условий труда, то есть «вредные условия труда (3 класс), при которых уровни воздействия вредных и (или) опасных производственных факторов превышают уровни, установленные нормативами (гигиеническими нормативами) условий труда, в том числе подкласс 3.1 (вредные условия труда 1 степени) - условия труда, при которых на работника воздействуют вредные и (или) опасные производственные факторы, после воздействия которых измененное функциональное состояние организма работника восстанавливается, как правило, при более длительном, чем до начала следующего рабочего дня (смены), прекращении воздействия данных факторов, и увеличивается риск повреждения здоровья» (Ст. 14. Федерального закона от 28.12.2013 N 426-ФЗ (ред. от 01.05.2016) "О специальной оценке условий труда"); освещенность рабочей поверхности (комбинированная) - присвоен 2 класс условий труда. Фактический уровень вредного фактора соответствует гигиеническим нормам. Итоговый класс условий труда – 2.

Требования к уровням шума и вибрации на рабочих местах

Уровень шума на рабочих местах, при выполнении основных и вспомогательных производственных работ с использованием ПЭВМ не должен превышать показателей, устанавливаемых нормами СанПиН 2.2.2/2.4.1340-03 предельно допустимых значений для данных видов работ в соответствии с действующими санитарно-эпидемиологическими нормативами. А именно должен соответствовать нормам СанПиН 2.2.4.3359-16 для высококвалифицированной работы, требующей сосредоточенности, в рабочих комнатах. Эквивалентные уровни звука на рабочих местах приведены в Таблице 11.

Таблица 11. Эквивалентные уровни звука на рабочих местах

Предельно допустимые эквивалентные уровни звука, дБА			
Категории напряженности трудового процесса	Категории тяжести трудового процесса		
	легкая и средняя физическая нагрузка	тяжелый труд 1 степени	тяжелый труд 2 степени
Напряженность легкой и средней степени	80	75	75
Напряженный труд 1 степени	70	65	65
Напряженный труд 2 степени	60	-	-
Напряженный труд 3 степени	50	-	-

В соответствии с нормами, ограничивающими предельно допустимое звуковое давление для рабочих мест, оснащённых ПЭВМ шумящее оборудование, уровни шума которого превышают нормативные, должно размещаться вне помещений с ПЭВМ.

По результатам специальной оценки условий труда в ОКУ ЦЗН города Аши в кабинете ответственного за обеспечение безопасности ПДн по шуму присвоен 3 класс условий труда, то есть «вредные условия труда, при которых уровни воздействия вредных и (или) опасных производственных факторов превышают уровни, установленные нормативами (гигиеническими нормативами) условий труда» (Ст. 14. Федерального закона от 28.12.2013 N 426-ФЗ (ред. от 01.05.2016) "О специальной оценке условий труда"), в остальных кабинетах – 2.

Режим труда и отдыха при работе с ПК

Режимы труда и отдыха при работе с ПЭВМ и ВДТ должны организовываться в зависимости от вида и категории трудовой деятельности в соответствии с приложением 7 к СанПиН 2.2.2/2.4.1340-03.

По виду трудовой деятельности работу оператора можно отнести к группе «А» – работа по считыванию информации с экрана ВДТ или ПЭВМ с предварительным запросом.

Для видов трудовой деятельности устанавливается три категории тяжести и напряженности работы с ВДТ и ПЭВМ.

Для группы «А» категории определяются по суммарному числу считываемых знаков за рабочую смену, но не более 60 000 знаков за смену:

1 категория – до 20 000 знаков;
2 категория – до 40 000 знаков;
3 категория – до 60 000 знаков.

Согласно ст. 108 ТК РФ в течение рабочего дня (смены) работнику должен быть предоставлен перерыв для отдыха и питания продолжительностью не более двух часов и не менее 30 минут, который в рабочее время не включается.

Время предоставления перерыва и его конкретная продолжительность устанавливаются правилами внутреннего трудового распорядка или по соглашению между работником и работодателем.

В соответствии со ст. 25 Федерального закона от 30.03.1999 N 52-ФЗ (ред. от 03.07.2016) "О санитарно-эпидемиологическом благополучии населения" условия труда, рабочее место и трудовой процесс не должны оказывать вредное воздействие на человека. Юридические лица обязаны выполнять требования санитарных правил к режиму труда и отдыха работников «в целях предупреждения травм, профессиональных заболеваний, инфекционных заболеваний и заболеваний (отравлений), связанных с условиями труда».

По результатам специальной оценки условий труда в ОКУ ЦЗН по тяжести труда присвоен 1 класс условий труда, то есть оптимальные условия труда, «при которых воздействие на работника вредных и (или) опасных производственных факторов отсутствует или уровни воздействия которых не превышают уровни, установленные нормативами (гигиеническими нормативами) условий труда и принятые в качестве безопасных для человека, и создаются предпосылки для поддержания высокого уровня работоспособности работника» (Ст. 14. Федерального закона от 28.12.2013 N 426-ФЗ (ред. от 01.05.2016) "О специальной оценке условий труда"), по напряженности труда – 2 класс.

Электробезопасность

В помещениях, где установлены ПЭВМ, особое внимание уделяется электробезопасности. Для питания электроприборов используется напряжение 220 В. В ОКУ ЦЗН на всех электрических розетках указывается их номинальное напряжение.

В соответствии с ГОСТ Р 12.1.019-2009 «Система стандартов безопасности труда. Электробезопасность. Общие требования и номенклатура видов защиты» опасные и вредные воздействия на людей электрического тока, электрической дуги и электромагнитных полей проявляются в виде электротравм и профессиональных заболеваний.

Степень опасного и вредного воздействия на человека электрического тока, электрической дуги и электромагнитных полей зависит от:

- рода и величины напряжения и тока;
- частоты электрического тока;
- пути тока через тело человека;
- продолжительности воздействия электрического тока или электромагнитного поля на организм человека;
- условий внешней среды.

Для обеспечения защиты от случайного прикосновения к токоведущим частям необходимо применять следующие способы и средства:

- защитные оболочки;

- защитные ограждения (временные или стационарные);
- защитные барьеры;
- безопасное расположение токоведущих частей;
- изоляция токоведущих частей (основная, дополнительная, усиленная, двойная);
- изоляция рабочего места;
- малое напряжение;
- защитное отключение;
- электрическое разделение;
- предупредительная сигнализация, блокировки, знаки безопасности.

Пожарная безопасность

Пожары в помещениях с ПК представляют особую опасность, так как сопряжены с большими материальными потерями. Характерная особенность помещений с ПК - небольшие площади помещений. Как известно пожар может возникнуть при взаимодействии горючих веществ, окисления и источников зажигания. В помещениях с ПК присутствуют все три основных фактора, необходимых для возникновения пожара.

В соответствии с Федеральным законом от 22 июля 2008 г. № 123-ФЗ «Технический регламент о требованиях пожарной безопасности» каждый объект защиты должен иметь систему обеспечения пожарной безопасности. Целью создания системы обеспечения пожарной безопасности объекта защиты является предотвращение пожара, обеспечение безопасности людей и защита имущества при пожаре. Система обеспечения пожарной безопасности объекта защиты включает в себя систему предотвращения пожара, систему противопожарной защиты, комплекс организационно-технических мероприятий по обеспечению пожарной безопасности. Система обеспечения пожарной безопасности объекта защиты в обязательном порядке должна содержать комплекс мероприятий, исключающих возможность превышения значений допустимого пожарного риска, установленного настоящим Федеральным законом, и направленных на предотвращение опасности причинения вреда третьим лицам в результате пожара.

Оповещение людей о пожаре, управление эвакуацией людей и обеспечение их безопасной эвакуации при пожаре в зданиях и сооружениях должны осуществляться одним из следующих способов или комбинацией следующих способов:

1) подача световых, звуковых и (или) речевых сигналов во все помещения с постоянным или временным пребыванием людей;

2) трансляция специально разработанных текстов о необходимости эвакуации, путях эвакуации, направлении движения и других действиях, обеспечивающих безопасность людей и предотвращение паники при пожаре;

3) размещение и обеспечение освещения знаков пожарной безопасности на путях эвакуации в течение нормативного времени;

4) включение эвакуационного (аварийного) освещения;

5) дистанционное открывание запоров дверей эвакуационных выходов;

6) обеспечение связью пожарного поста (диспетчерской) с зонами оповещения людей о пожаре;

7) иные способы, обеспечивающие эвакуацию.

Информация, передаваемая системами оповещения людей о пожаре и управления эвакуацией людей, должна соответствовать информации, содержащейся в разработанных и размещенных на каждом этаже зданий и сооружений планах эвакуации людей.

Пожарные оповещатели, устанавливаемые на объекте, должны обеспечивать однозначное информирование людей о пожаре в течение времени эвакуации, а также выдачу дополнительной информации, отсутствие которой может привести к снижению уровня безопасности людей.

В любой точке защищаемого объекта, где требуется оповещение людей о пожаре, уровень громкости, формируемый звуковыми и речевыми оповещателями, должен быть выше допустимого уровня шума. Речевые оповещатели должны быть расположены таким образом, чтобы в любой точке защищаемого объекта, где требуется оповещение людей о пожаре, обеспечивалась разборчивость передаваемой речевой информации. Световые оповещатели должны обеспечивать контрастное восприятие информации в диапазоне, характерном для защищаемого объекта.

При разделении здания и сооружения на зоны оповещения людей о пожаре должна быть разработана специальная очередность оповещения о пожаре людей, находящихся в различных помещениях здания и сооружения.

Размеры зон оповещения, специальная очередность оповещения людей о пожаре и время начала оповещения людей о пожаре в отдельных зонах должны быть определены исходя из условия обеспечения безопасной эвакуации людей при пожаре.

Системы оповещения людей о пожаре и управления эвакуацией людей должны функционировать в течение времени, необходимого для завершения эвакуации людей из здания, сооружения.

Технические средства, используемые для оповещения людей о пожаре и управления эвакуацией людей из здания, сооружения при пожаре, должны быть разработаны с учетом состояния здоровья и возраста эвакуируемых людей.

Звуковые сигналы оповещения людей о пожаре должны отличаться по тональности от звуковых сигналов другого назначения.

Звуковые и речевые устройства оповещения людей о пожаре не должны иметь разъемных устройств, возможности регулировки уровня громкости и должны быть подключены к электрической сети, а также к другим средствам связи. Коммуникации систем оповещения людей о пожаре и управления эвакуацией людей допускается совмещать с радиотрансляционной сетью здания и сооружения.

Системы оповещения людей о пожаре и управления эвакуацией людей должны быть оборудованы источниками бесперебойного электропитания.

Здания медицинских организаций, учреждений социальной защиты населения и учреждений социального обслуживания с пребыванием людей на постоянной основе или стационарном лечении с учетом индивидуальных способностей людей к восприятию сигналов оповещения должны быть дополнительно оборудованы (ос-

нащены) системами (средствами) оповещения о пожаре, в том числе с использованием персональных устройств со световым, звуковым и с вибрационным сигналами оповещения. Такие системы (средства) оповещения должны обеспечивать информирование дежурного персонала о передаче сигнала оповещения и подтверждение его получения каждым оповещаемым.

Одним из наиболее часто встречающихся первичных средств пожаротушения являются огнетушители. Их легко привести в действие, они не требуют специальных навыков работы и прекрасно справляются с начальными стадиями возгорания. Поэтому огнетушителями оборудуют любые типы зданий, будь то общественные, производственные или складские помещения.

Виды огнетушителей:

- углекислотные;
- порошковые;
- воздушно-пенные;
- самосрабатывающие;
- хладоновые.

Руководитель организации обеспечивает объект огнетушителями по нормам согласно приложений № 1 и 2 Правил противопожарного режима в РФ, Основание: п.70 в зависимости от огнетушащей способности огнетушителя, предельной площади помещения, а также класса пожара. Выбор огнетушителя (передвижной или ручной) обусловлен размерами возможных очагов пожара.

Пунктом 468 Правил противопожарного режима (ППР) указано на необходимость оборудования каждого этажа общественного здания и сооружения не менее, чем двумя ручными огнетушителями; при этом, максимальное расстояние от возможного очага пожара до места установки огнетушителя для общественных зданий и сооружений не должно превысить 20 метров. Основание: пункт 474 ППР. Но если в общественном здании есть помещения с установленными стационарными автоматическими установками пожаротушения, то такие помещения оборудуются 50-тью процентами огнетушителей от расчетного числа.

Наиболее часто встречаются следующие типы огнетушителей: порошковый ОП-4 и углекислотный ОУ-3.

При выборе огнетушителя в первую очередь необходимо учитывать специфику помещения и материалов, которые в нем хранятся. При решении какой огнетушитель лучше, углекислотный или порошковый, следует учитывать класс пожара, эффективность используемого состава в каждом конкретном случае и возможные последствия.

Углекислотные огнетушители предназначены для тушения загораний различных веществ и материалов, электроустановок под напряжением до 1000 В, двигателей внутреннего сгорания, горючих жидкостей. Порошковые огнетушители предназначены для тушения пожаров и загораний нефтепродуктов, ЛВЖ и ГЖ, растворителей, твердых веществ, а также электроустановок под напряжением до 10000В.

Мероприятия, устраняющие причины пожара, разделяются на организационные, эксплуатационные, технические и режимные.

Организационные мероприятия: обучение рабочих и служащих противопожарным правилам, проведение бесед, лекций, инструкций и т. п.

Эксплуатационные мероприятия предусматривают правильную эксплуатацию машин, транспорта, правильное содержание зданий, территорий.

К техническим мероприятиям относится соблюдение противопожарных правил и норм, при выборе электрооборудования, вентиляции, освещения и т. д., при устройстве отопления.

К мероприятиям режимного характера относится запрещение курения в неустановленных местах, проведение электросварочных работ в пожароопасных помещениях и т. д.

В ОКУ ЦЗН установлена автоматическая пожарная сигнализация Протон 16 с дымовыми пожарными извещателями с источником резервного питания Скат 1200. Система оповещения о пожаре звуковая и по городской телефонной связи. Установлен пожарный щит с пожарным рукавом и огнетушителями. Первичные средства пожаротушения – огнетушители - расположены в общедоступных местах с указанием в плане эвакуации и с помощью указателей в местах размещения. Приняты меры по ликвидации возможного загорания, используя углекислотные огнетушители типа ОУ-3 (до 10000 В) в количестве 5 шт., 1 порошковый огнетушитель ОП-4 (до 1000 В). Данными огнетушителями допускается тушение электрооборудования, находящегося в помещении под напряжением до 380 В.

ВЫВОДЫ ПО ПЕРВОЙ ГЛАВЕ

В ходе проведенного обследования существующей ИСПДн ОКУ ЦЗН города Аши был составлен паспорт предприятия. Выявлены объекты защиты информации, составлена модель угроз и рассчитаны риски для выделенных объектов защиты.

В результате анализа информационной системы ОКУ ЦЗН города Аши были выявлены сведения, подлежащие защите – сведения, содержащие персональные данные.

Проведен анализ угроз безопасности ИСПДн ОКУ ЦЗН города Аши. Осуществлена оценка актуальности угроз: по уровню исходной защищенности информационной системы как ИСПДн (низкий показатель, коэффициент Y1=10); по вероятности реализации угроз в ИСПДн; по возможности реализации угрозы в ИСПДн; по степени опасности угроз в ИСПДн. Для ИСПДн ОКУ ЦЗН города Аши актуальны угрозы 2 типа. Учитывая исходные данные ИСПДн и тип актуальных угроз для ИСПДн, устанавливается 3-й уровень защищенности ПДн.

Определен примерный перечень мер по противодействию актуальным угрозам информационной системы ОКУ ЦЗН города Аши. Разработана модель угроз и уязвимостей при обработке персональных данных в ИСПДн ОКУ ЦЗН города Аши, в которой выделены наиболее важные объекты защиты персональных данных: персонал; автоматизированные рабочие места сотрудников, на которых обрабатываются персональные данные; сервер.

В результате произведенного расчета рисков на выделенных объектах установлен высокий уровень информационного риска.

Из результатов проведенной работы следует, что необходимо принимать контрмеры по снижению вероятности реализации угроз безопасности ИСПДн, продолжить работу по модернизации защиты ИСПДн. Это:

а) разработка новых организационно-распорядительных документов, так как обнаружено их несоответствие существующему законодательству в сфере защиты информации, содержащей персональные данные;

б) внедрение программно-аппаратных средств резервного копирования на АРМ сотрудников;

в) внедрение дополнительных технических средств защиты от НСД на АРМ сотрудников.

Также в ходе собеседования с сотрудниками и анализа происшествий информационной безопасности были выявлены недостатки помещения серверной комнаты, а именно, отсутствие отдельного помещения для сервера. Комната, в которой находится сервер, расположена рядом с бывшей туалетной комнатой, где проложены водопроводные трубы, а сам сервер находится рядом с батареей отопления. Поэтому есть риск затопления серверной комнаты. В результате чего было предложено разработать организационные меры по их устранению.

В главе «Безопасность жизнедеятельности» проанализированы требования безопасности в соответствии с санитарными нормами, государственными стандартами и правилами техники безопасности. Приведены результаты

специальной оценки условий труда на рабочих местах сотрудников ОКУ ЦЗН города Аши по степени вредности и (или) опасности.

Итогом первой главы является разработка технического задания по модернизации ИСПДн ОКУ ЦЗН города Аши (Приложение Ж).

2. ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ ВЫБОРА СРЕДСТВ ЗАЩИТЫ

2.1. Обзор возможных методов устранения угроз, связанных с НСД

Одним из основных этапов работы по модернизации защиты информационной системы персональных данных является определение и анализ используемых в настоящее время методов и средств, необходимых для устранения выявленных угроз и уязвимостей, актуальных для ИСПДн ОКУ ЦЗН города Аши. На данном этапе необходимо выявить наиболее эффективные варианты для решения поставленной задачи.

Выбор в пользу тех или иных средств защиты информации при разработке информационных систем, обрабатывающих персональные данные – ключевая процедура, определяющая не только будущий уровень защищенности и надежности системы, но и законность дальнейшей эксплуатации с точки зрения российского законодательства.

В соответствии с законодательством Российской Федерации, организационно-распорядительными и нормативными документами ФСТЭК и ФСБ России в государственных информационных системах, обрабатывающих персональные данные, использование сертифицированных программных продуктов по требованиям информационной безопасности является обязательным.

Применение в информационной системе сертифицированных средств защиты не является достаточным условием выполнения требований законодательных и нормативных актов, важно чтобы параметры безопасности соответствовали требованиям Руководящих документов к системе безопасности автоматизированных систем, но и могли быть подтверждены уполномоченными органами при аттестации объекта информатизации.

Если использование сертифицированных средств защиты информации не обязательно, то выбор в пользу сертифицированных средств защиты предпочтителен, поскольку наличие сертификата является важным фактором обеспечения доверия к приобретаемым программным продуктам, а также гарантия безопасности и качества.

В настоящее время среди всех сертифицированных СЗИ от НСД можно выделить следующие продукты:

- SecretNet и Соболь (Код Безопасности);
- Аккорд (ОКб САПР);
- Dallas Lock (НПП ИТБ);
- КРИПТОН (Анкад);

Сравнение возможностей продуктов представлено в таблице 12

Таблица 12

Характеристика	Secret Net 7 (лок)	Аккорд	Dallas Lock 7.7	КРИПТОН
Наличие сертификата по РД	да	да	да	да
Идентификация и аутентификация пользователей до загрузки ОС	да	да	да	да
Возможность аппаратной идентификации	да	нет	да	нет
Защита от обхода загрузки СЗИ	да	да	да	да
Контроль целостности до загрузки ОС	да	да	да	да
Обеспечение целостности информационной системы и информации	да	да	да	да
Автоматическая очистка дискового пространства при удалении информации	да	нет	да	нет
Зачистка дискового пространства при удалении произвольных файлов	да	да	нет	да
Кодирование данных	да	нет	да	нет
Разграничение доступа к внешним носителям, устройствам	да	да	да	да
Контроль аппаратной конфигурации	да	да	частично	да
Интеграция с доменом в режиме рабочей станции домена	да	да	да	да
Регистрация событий безопасности	да	нет	да	нет
Совместимость с ОС Windows 7	да	нет	да	нет
Средняя стоимость, руб.	5100	9089	6000	6100

По таблице видно, что из числа рассмотренных средств защиты информации, бесспорным преимуществом обладает СЗИ от НСД «Secret Net 7».

Сравнение наиболее востребованных на рынке антивирусных программ Kaspersky, ESET NOD32, McAfee, Symantec, Dr. Web, AVG, TrustPort приведено в таблице 13.

Таблица 13

Антивирус / Характеристика	Найдено угроз	% определения	Время на поиск	Загрузка ЦП, %	Цена, руб.
Касперский	3695	96,3	23 мин	80-95	4479
McAfee	3489	90,1	12 мин	60-80	1432
Dr. Web	2968	77,3	1 мин 10 сек	50-60	6123
AVG	2840	74	5 мин 32 сек	15-30	1740
Symantec	2497	65	6 мин 10 сек	40-50	666
TrustPort	2107	54,9	45 сек	40-50	1295
ESET NOD32	1949	50,8	1 мин 10 сек	40-50	1600

Из таблицы видно, что самым надежным является антивирус Касперского по такому важному показателю, как процент определения угроз, несмотря на то, что время, потраченное на поиск зараженных файлов и потребляемые ресурсы персонального компьютера, оказались самыми большими среди всех тестируемых продуктов.

2.2. Угрозы, связанные с НСД

Угрозы несанкционированного доступа к обрабатываемым в информационной системе персональным данным могут быть осуществлены при помощи программных и программно-аппаратных средств. В случае неправомерного копирования и/или распространения персональных данных происходит нарушение режима конфиденциальности ПД. Также привести к серьезным последствиям может изменение или уничтожение нарушителем защищаемых персональных данных. Для кражи информации или воздействия на нее удаленно нарушитель может создать во время реализации угрозы НСД нештатные режимы работы операционной среды или ПО.

Несанкционированный доступ является одним из основных методов получения злоумышленником доступа к конфиденциальной информации.

Для выбора наиболее эффективных средств и методов защиты информации от несанкционированного доступа в рамках рассматриваемой организации необходимо определить актуальные угрозы, связанные с несанкционированным доступом, для данного объекта.

К таким угрозам относятся:

- несанкционированный доступ к АРМ;
- несанкционированное проникновение нарушителя в помещение;
- несанкционированный доступ к базам данных, хранящимся на сервере;
- утечка носителей информации за пределы контролируемой зоны (жестких дисков);
- кража, модификация, уничтожение информации.

Также в организации были выявлены уязвимости, которые могут привести к данным угрозам.

2.2.1. Несанкционированный доступ к АРМ

К уязвимостям, которые могут привести к реализации угрозы несанкционированного доступа к АРМ, относятся:

- отсутствие видеонаблюдения в помещении;
- отсутствие пломбировки корпуса персонального компьютера;
- отсутствие авторизации на аппаратном уровне.

Решением первой проблемы является установка камер видеонаблюдения в помещении.

Чтобы решить вторую проблему, необходимо осуществить пломбировку корпуса персонального компьютера.

Путем решения третьей проблемы является авторизация пользователя с помощью установки паролей на рабочих станциях, в качестве программного средства ЗИ от НСД рекомендуется использовать "Secret Net 7" для авторизации пользователей в системе и разграничения прав доступа пользователей к устройствам и защищаемой информации.

2.2.2. Несанкционированное проникновение нарушителя в помещение

Уязвимостями, которые могут привести к реализации угрозы несанкционированного проникновения нарушителя в помещение, являются:

- отсутствие видеонаблюдения в помещении;
- отсутствие регламента доступа в помещение;
- отсутствие выделенного помещения для сервера или физической защиты сервера.

Для решения первой проблемы необходимо установить камеры видеонаблюдения в помещении.

В качестве решения второй проблемы может послужить мероприятие по разработке матрицы доступа. В данном документе будет содержаться список лиц, допущенных в режимные помещения предприятия. Также назначается лицо, ответственное за исполнение этого документа.

Путем решения третьей проблемы является выделение отдельного закрытого помещения для сервера и пломбировка корпуса сервера.

2.2.3. Несанкционированный доступ к базам данных, хранящимся на сервере

К уязвимостям, приводящим к реализации угрозы несанкционированного доступа к базам данных, хранящимся на сервере, относятся:

- установка программного обеспечения, которое может создать условия для НСД;
- отсутствие регламента эксплуатации средств антивирусной защиты;
- отсутствие регламента доступа в помещение, в котором находится сервер;
- отсутствие пломбирования корпуса сервера.

Решением первой проблемы является установка антивирусного ПО "Kaspersky Endpoint Security 10", которое обеспечивает комплексную защиту компьютеров и файловых серверов от интернет-атак, финансового онлайн-мошенничества, программ-вымогателей и потери данных.

Вторая и третья проблемы аналогичны проблеме угрозы неавторизированного проникновения нарушителя, поэтому пути решения проблемы схожи. Необходимо также разработать матрицы доступа и назначить лица, ответственные за исполнение этих документов.

Последняя проблема решается путем пломбировки корпуса серверов и назначением лица, ответственного за ее сохранность.

2.2.4. Утечка носителей информации за пределы контролируемой зоны (жестких дисков)

Уязвимости, приводящие к угрозе утечки носителей информации за пределы контролируемой зоны (жестких дисков):

- отсутствие учета носителей информации;
- отсутствие видеонаблюдения;
- отсутствие пломбировки корпуса сервера.

Для решения первой проблемы необходимо вести журнал учета носителей информации. На самих машинных носителях проставляются их учетные номера. Листы журналов учета носителей должны быть перед заведением пронумерованы, прошиты и опечатаны печатью. На обратной стороне последнего листа журнала проставляется заверительная подпись с указанием количества листов, подписываемая сотрудником, ответственным за ведение журнала.

Решением второй и третьей проблемы является установка камер видеонаблюдения и пломбировка корпуса сервера.

2.2.5. Кража, модификация, уничтожение информации (несанкционированное копирование, печать и размножение)

Уязвимости, приводящие к угрозе кражи, модификации и уничтожению информации:

- нечеткая организация документооборота;
- неконтролируемый доступ сотрудников к копировальной и множительной технике.

Для исключения данных уязвимостей необходимо соблюдать основные принципы организации документооборота:

- прохождение документов должно быть оперативным. Чтобы сократить время их пребывания в сфере делопроизводства, следует:

- различные операции по обработке документов выполнять параллельно (например, копирование и раздача копий документа лицам, в исполнении которого они участвуют одновременно и т. д.);

- порядок прохождения и процессы обработки основных видов документов должны быть единообразными.

Необходимо разработать матрицу доступа и назначить лицо, ответственное за доступ к копировальной и множественной технике.

ВЫВОДЫ ПО ВТОРОЙ ГЛАВЕ

Для выявления наиболее эффективных средств защиты информации при разработке информационных систем, обрабатывающих персональные данные, была составлена сравнительная таблица сертифицированных СЗИ от НСД и наиболее востребованных на рынке антивирусных программ. Наибольшим преимуществом обладает СЗИ от НСД «Secret Net 7». Самым надежным среди антивирусных программ является средство антивирусной защиты информации Касперского.

В результате выявления уязвимостей на рассматриваемом объекте, приводящих к возможной реализации той или иной угрозы, была выявлена наиболее значительная угроза, связанная с НСД и наиболее эффективные варианты решения проблем, препятствующие возникновению неблагоприятных последствий от воздействия угрозы:

1) несанкционированный доступ к АРМ: установка камер видеонаблюдения в помещении; пломбировку корпуса персонального компьютера, сотрудников, обрабатывающих персональные данные; авторизация пользователя с помощью установки паролей на рабочих станциях; установка СЗИ от НСД "Secret Net 7";

2) несанкционированное проникновение нарушителя в помещение: установка системы видеонаблюдения в помещении; разработка матрицы доступа; выделение отдельного закрытого помещения для сервера и пломбировка корпуса сервера; назначение ответственного за список лиц, допущенных в режимные помещения организации;

3) несанкционированный доступ к базам данных, хранящимся на сервере: установка антивирусного ПО " Kaspersky Endpoint Security 10"; разработка матрицы доступа; пломбировка корпуса сервера и назначение лица, ответственного за ее сохранность;

4) утечка носителей информации за пределы контролируемой зоны (жестких дисков): ведение журнал учета носителей информации; установка камер видеонаблюдения; пломбировка корпуса сервера.

5) кража, модификация, уничтожение информации (несанкционированное копирование, печать и размножение): соблюдение основных принципов организации документооборота (оперативное прохождение документов, единообразные порядок и процессы обработки основных видов документов); разработка матрицы доступа и назначение лица, ответственного за доступ к копировальной и множественной технике.

3 РАЗРАБОТКА ПРОЕКТА МОДЕРНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОКУ ЦЗН ГОРОДА АШИ

3.1 Описание объекта защиты

Областное казенное учреждение Центр занятости населения города Аши является организацией, осуществляющей переданные полномочия в области содействия занятости населения, в которой хранятся и обрабатываются персональные данные сотрудников и безработных граждан.

3.2 Резюме проекта

Проект разработан согласно утвержденному техническому заданию по модернизации защиты ИСПДн ОКУ ЦЗН города Аши (Приложение Ж).

Для достижения поставленной цели, необходимо разработать ряд организационных и программно-аппаратных мер. С помощью матрицы ответственности за каждым конкретным этапом работы зафиксированы ответственные лица, также определены основные объекты поставки. Результатом проекта является модернизированная ИСПДн, включающая внедрение программного средства, обеспечивающего защиту от НСД, соответствующая требованиям нормативно-правовых актов в этой области и целям внедрения.

3.3 Цели и задачи проекта

Целями модернизации защиты информационной системы персональных данных ОКУ ЦЗН города Аши являются:

- предотвращение утечки, хищения, утраты, искажения, подделки информации.
- предотвращение других форм незаконного вмешательства в информационные ресурсы и системы, обеспечение правового режима информации как объекта собственности.
- обеспечение защищенности ИСПДн в процессе обработки и хранения ПДн, обеспечение защиты ПДн при их обработке, а также других необходимых свойств информации (целостности, доступности и т.п.).
- снижение вероятности реализации актуальных угроз несанкционированного доступа (НСД) к ПДн, обрабатываемым в ОКУ ЦЗН города Аши.
- соответствие требованиям обеспечения информационной безопасности при обработке ПДн в ИСПДн, регламентируемых руководящими документами ФСТЭК России и ФСБ России.

3.4 Объекты поставки проекта

3.4.1 Организационно-распорядительная документация

Данным проектом предусмотрено изменение или уточнение уже существующих в организации документов в области информационной безопасности:

- положение об обработке персональных данных (Приложение Б);
- инструкция пользователя о порядке работы с персональными данными (Приложение Е);
- должностная инструкция ответственного за обеспечение безопасности персональных данных (Приложение Д).

Необходимо разработать документ, определяющий политику обработки и защиты персональных данных.

3.4.2 Программно-аппаратные меры

Система защиты информации от несанкционированного доступа СЗИ от НСД «Secret Net 7»;

Антивирусное ПО Kaspersky Endpoint Security 10.

3.4.3 Обучение персонала

Обучение сотрудников новым требованиям защиты информации с обоснованием их необходимости и значимости для организации по результатам внедрения новых организационно-распорядительных документов, предусмотренных проектом, а также программно-аппаратных решений.

3.5 Риски проекта

Вероятность реализации угрозы через данную уязвимость в течение года: P(V), (%)

Критичность реализации угрозы через уязвимость: ER, (%)

Уровень угрозы Th (%), рассчитывается по формуле (1).

$$Th = \frac{ER}{100} \times \frac{P(V)}{100}$$

Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза CTh (%), рассчитывается по формуле (2):

$$CTh = 1 - \prod_{i=1}^{n} (1 - Th)$$

Таблица 14– Потоки защищаемой информации

Риски / пути их реализации	Критичтич-ность ER	Вероятность P(V)	h	CTh
1	2	3	4	5
1. Риски изменений в стране, обществе				
1.1. Ухудшение политических и экономических характеристик и факторов:				0,020
– изменения в экономике и политике	15	10	0,008	
– перемены в законодательстве	30	10	0,015	
1.2. Изменение человеческих характеристик:				0,506
– условия отдыха, здравоохранение и медицина	25	5	0,012	
– негативный настрой сотрудников и их отношение к работе	80	50	0,4	
2. Риски окружения проекта в составе организации				
2.1. Изменение или недостаток бюджета проекта:				0,835
– задержки финансирования	90	10	0,09	
– недостаток бюджетных средств	90	90	0,81	
2.2. Недостаточная организованность работ				0,032
– срыв графиков работ, невыполнение сроков	15	10	0,015	
– нехватка рабочей силы	35	50	0,017	
– недооценка стоимости работ и использование финансов для других целей	35	20	0,007	
2.3. Риски персонала				0,045
– влияние личностных факторов (неумеренные амбиции участников проекта, переоценка собственных возможностей, преувеличение роли технологической стороны в ущерб менеджменту)	20	10	0,030	
– риск недоступности персонала, которому сложно подобрать замену (болезнь, увольнение и другие непредвиденные обстоятельства)	30	50	0,015	

3.6 Структура разбиения работ

Структура разбиения работ позволяет согласовать план проекта с потребностями заказчика, представленными в виде описаний работ. Структура разбиения работ представлена на рисунке 1.

Структура разбиения работ по модернизации защиты ИСПДн:

ИСПДн 1. Проектирование;

ИСПДн 1.1. Определение ключевых показателей существующих бизнес-процессов с точки зрения ИБ;

ИСПДн 1.2. Анализ проблем и слабых мест существующих бизнес-процессов;

ИСПДн 1.3. Разработка значений ключевых показателей новых бизнес-процессов;

ИСПДн 1.4. Анализ и выбор наилучших способов и методов улучшения значений ключевых показателей бизнес-процессов;

ИСПДн 1.5. Разработка и согласование структуры новых бизнес-процессов;

ИСПДн 2. Совершенствование организационно-распорядительной документации;

ИСПДн 2.1. Положение «Об обработке персональных данных»;

ИСПДн 2.2. Перечень сведений, содержащих персональные данные;

ИСПДн 2.3. Внесение изменений в должностные инструкции;

ИСПДн 2.4. Согласование и утверждение организационно-распорядительной документации;

ИСПДн 3. Подготовка реализации проекта модернизации защиты ИСПДн;

ИСПДн 3.1. Определение ответственных лиц и исполнителей проекта;

ИСПДн 3.2. Приобретение антивирусного ПО;

ИСПДн 3.3. Приобретение программно-аппаратного средства защиты от НСД;

ИСПДн 4. Внедрение;

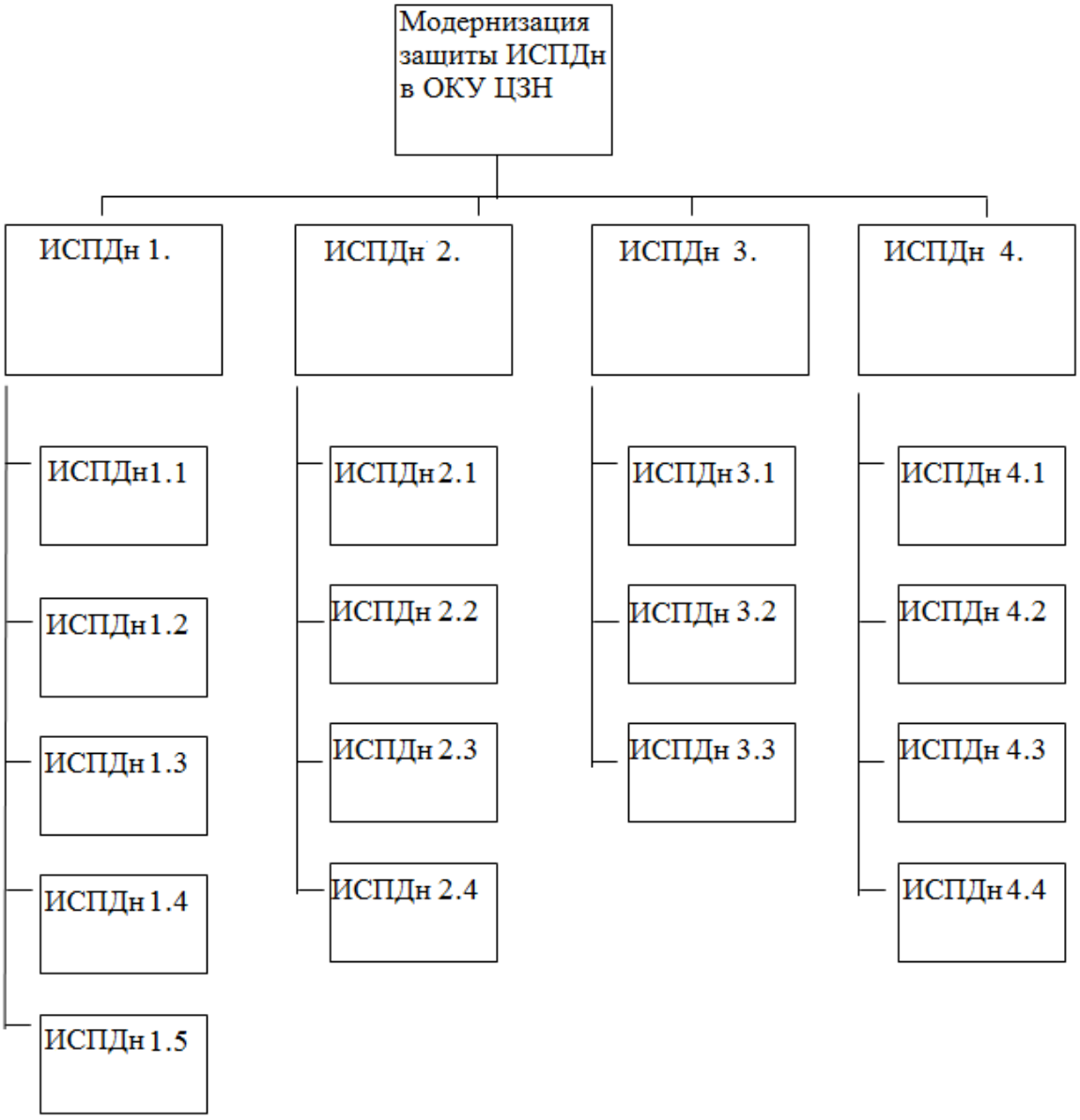
ИСПДн 4.1. Установка и настройка антивирусного ПО;

ИСПДн 4.2. Установка и настройка программно-аппаратного средства защиты от НСД;

ИСПДн 4.3. Контроль защищенности;

ИСПДн 4.4. Обучение пользователей.

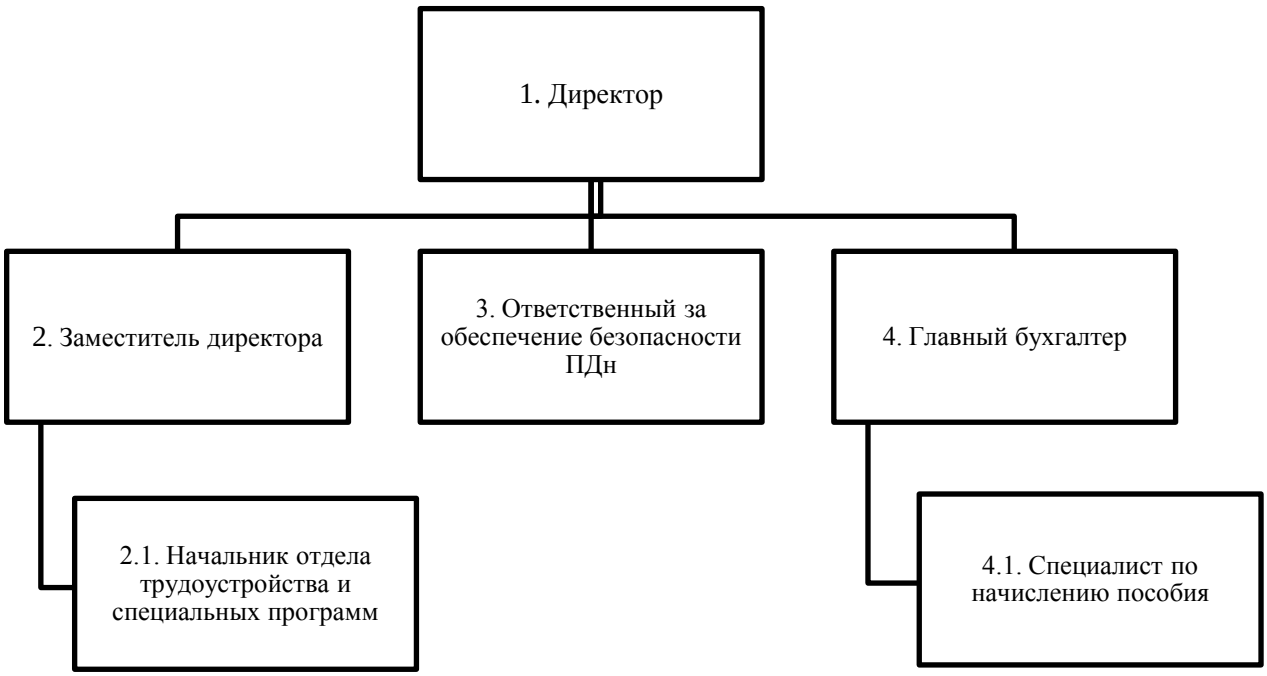
Рисунок 1 – Структура разбиения работ



3.7 Структурная схема организации проекта

Для точного и своевременного выполнения проекта, необходима скоординированная работа всех задействованных сотрудников. Для этого была определена структурная схема организации проекта. Структурная схема организации представлена на рисунке 2.

Рисунок 2 – Структурная схема организации проекта



3.8 Матрица ответственности

Все действия исполнителей по работам делятся на условные группы:

- управление (У);
- исполнение (И);
- контроль (К).

Матрица ответственности представлена в Таблице 15.

Таблица 15 – Матрица ответственности

Исполнитель/Работа	1	2	2.1	3	4	4.1
ИСПДн 1.	К					
ИСПДн 1.1.	К/У			И		
ИСПДн 1.2.	И			К		
ИСПДн 1.3.	И			К		
ИСПДн 1.4.	К/У			И		
ИСПДн 1.5.	И			К		
ИСПДн 2.	К			У/И		
ИСПДн 2.1.	К			У/И		
ИСПДн 2.2.	К			У/И		
ИСПДн 2.3.	К			У/И		
ИСПДн 2.4.	К			У/И		
ИСПДн 3.	К					
ИСПДн 3.1.	К			И		
ИСПДн 3.2.	К					
ИСПДн 3.3.	К					
ИСПДн 4.	К		И			
ИСПДн 4.1.	К		И			
ИСПДн 4.2.	К		И			
ИСПДн 4.3.	К		И			
ИСПДн 4.4.	И			К		К

3.9 Диаграмма Ганта и сетевой график

Диаграмма Ганта используется для иллюстрации плана, графика работ по выбранному проекту. Является одним из методов планирования проектов. Используется в приложениях по управлению проектами. Диаграмма Ганта для проекта модернизации защиты ИСПДн ОКУ ЦЗН города Аши представлена в Приложении З.

Сетевой график это динамическая модель производственного процесса, отражающая технологическую зависимость и последовательность выполнения комплекса работ, увязывающая их свершение во времени с учётом затрат ресурсов и стоимости работ с выделением при этом узких (критических) мест.

Сетевой график является детализированным наглядным представлением обо всех работах проекта, включая временные и ресурсные оценки. Сетевой график для проекта модернизации защиты ИСПДн ОКУ ЦЗН города Аши представлена в Приложении И.

По итогам составления диаграммы Ганта и сетевого графика можно определить точные сроки выполнения проекта.

ВЫВОДЫ ПО ТРЕТЬЕЙ ГЛАВЕ

По результатам выполненных работ разработан проект модернизации защиты информационной системы персональных данных в ОКУ ЦЗН города Аши, поставлены цели проекта модернизации. Определены объекты поставки проекта путем внедрения новых организационно-распорядительных документов, предусмотренных проектом, а также программно-аппаратных мер и обучения персонала.

Построена структура разбиения работ. Для понимания роли каждого участника в реализации цели проекта составлена матрица ответственности проекта.

Работы были разбиты в последовательности и иерархически структурированы. Каждой работе назначен ответственный за неё или исполнитель. Структура разбиения работ наглядно представлена на сетевых графиках и диаграмме Ганта.

ЗАКЛЮЧЕНИЕ

В результате выполнения выпускной квалификационной работы был проведен анализ информационной системы ОКУ ЦЗН города Аши. Это государственная организация, в которой обрабатывается информация, содержащая персональные данные. В ходе предпроектного обследования было установлено, что часть организационно – распорядительных документов не соответствует требованиям современного законодательства в этой области. В связи с этим был разработан пакет организационно-распорядительных документов по защите персональных данных в организации.

В ходе выполнения выпускной квалификационной работы были освоены технологии подготовки документов для принятия решений по созданию защиты информационной системы персональных данных в организации. Было проведено предпроектное обследование, которое включает в себя:

- разработку паспорта предприятия с точки зрения обеспечения информационной безопасности – были проанализированы организационно-правовая форма и организационная структура, виды деятельности, предполагаемые виды защищаемой информации, информационная среда предприятия, строительная инфраструктура здания и местоположение предприятия;
- разработку модели деятельности предприятия – построенные диаграммы позволяют выявить циркулирующие потоки информации, которая нуждается в защите на предприятии;
- описание информационной системы – были проанализированы программное, аппаратное обеспечение и обеспечение инфраструктуры ИС;
- выявление объектов защиты – на основе результатов проведенной инвентаризации были выделены объекты, нуждающиеся в защите, которые обрабатывают и в которых циркулирует защищаемая информация, содержащая персональные данные;
- разработку модели угроз и уязвимостей для важных объектов защиты и расчет рисков для них – на основе накопленных статистических данных о вероятностях и критичности возможных угроз безопасности объектов защиты была составлена их модель и подсчитаны риски по предварительно выбранной методике расчета рисков;

На основе полученной информации было подготовлено техническое задание на модернизацию защиты информационной системы персональных данных ОКУ ЦЗН города Аши. Реализация данного проекта позволит добиться снижения рисков безопасности персональных данных.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Нормативно-правовые документы

1. Федеральный закон Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных данных";
2. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 21.07.2014) «Об информации, информационных технологиях и о защите информации»;
3. Закон Российской Федерации от 19 апреля 1991 года № 1032-1 "О занятости населения в Российской Федерации";
4. Трудовой кодекс Российской Федерации;
5. Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
6. Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 23.03.2017) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
7. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная приказом ФСТЭК России от 14 февраля 2008 г.;
8. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная заместителем директора ФСТЭК России от 15 февраля 2008 г.;
9. ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей», утвержденный Приказом Федерального агентства по техническому регулированию и метрологии от 19 августа 2015 г. № 1180-ст.;
10. ГОСТ 34.602-1989 «Техническое задание на создание автоматизированной системы»;
11. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;
12. Федеральный закон от 28.12.2013 № 426-ФЗ (ред. от 01.05.2016) "О специальной оценке условий труда";
13. Федеральный закон от 30.03.1999 № 52-ФЗ (ред. от 03.07.2016) "О санитарно-эпидемиологическом благополучии населения" (с изм. и доп., вступ. в силу с 04.07.2016);
14. ГОСТ Р 12.1.019-2009 Система стандартов безопасности труда. Электробезопасность. Общие требования и номенклатура видов защиты. Межгосударственный стандарт;
15. Санитарно-эпидемиологические правила и нормативы "Гигиенические требования к персональным электронно-вычислительным машинам и организации работы. СанПиН 2.2.2/2.4.1340-03", утвержденные Главным государственным

санитарным врачом Российской Федерации 30 мая 2003 года (с изменениями на 21 июня 2016 года);

16. Постановление Главного государственного санитарного врача РФ от 21.06.2016 № 81 "Об утверждении СанПиН 2.2.4.3359-16 "Санитарно-эпидемиологические требования к физическим факторам на рабочих местах" (вместе с "СанПиН 2.2.4.3359-16. Санитарно-эпидемиологические правила и нормативы...") (Зарегистрировано в Минюсте России 08.08.2016 № 43153);

17. СанПиН 2.2.1/2.1.1.1278-03, утвержденные Постановлением Главного государственного санитарного врача Российской Федерации от 08 апреля 2003 года № 34;

18. Федеральный закон от 22 июля 2008 г. № 123-ФЗ «Технический регламент о требованиях пожарной безопасности» (в редакции, актуальной с 15 июля 2016 г.).

ПРИЛОЖЕНИЕ А

ГЛАВНОЕ УПРАВЛЕНИЕ
ПО ТРУДУ И ЗАНЯТОСТИ НАСЕЛЕНИЯ
ЧЕЛЯБИНСКОЙ ОБЛАСТИ

Областное казенное учреждение
Центр занятости населения
города Аши

УТВЕРЖДАЮ
Директор ОКУ ЦЗН

_____И.И. Иванов

Дата_____

ПАСПОРТ ПРЕДПРИЯТИЯ
с точки зрения обеспечения информационной безопасности

15.02.2017 № 1
г. Аша

Паспорт предприятия ОКУ ЦЗН города Аши

Содержание паспорта предприятия:

1.1.1. Организационно-правовая форма предприятия (организации, учреждения) и его реквизиты

1. Название организации: Областное казенное учреждение Центр занятости населения города Аши (далее – ОКУ ЦЗН города Аши)
2. Численность сотрудников: 21 человек
3. Банковские реквизиты:

ОГРН: 1027400507991
ОКПО: 12602709
ИНН: 7401007800
КПП: 745701001
УФК по Челябинской области (Минфин Челябинской области, ОКУ ЦЗН города Аши, л/счет 03103200060ОБ)
Р/счет: 40201810900000100027
БАНК: Отделение Челябинск г. Челябинск
БИК: 047501001

1.1.2. Виды деятельности предприятия (в соответствии с Уставом), наличие лицензий ФСБ, ФСТЭК.

- Деятельность в области обязательного социального обеспечения.

2. Сертификат соответствия ФСБ России:

СФ/124-2073, СФ/525-2075- «Программный комплекс ViPNet Coordinator 3.2», используется для криптографической информации, не содержащей сведения, составляющие государственную тайну;

СФ/124-2072; СФ/525-74; СФ/121-2251 – «Программный комплекс ViPNet Client 3.2»;

СФ/114-2737 Средство криптографической защиты информации КриптоПро SCP 3.6.

3. Лицензионные соглашения:

ПО Microsoft Windows Server Standard 2008;

ПО САСНЕ.

1.1.3. Предполагаемые виды защищаемой информации

Персональные данные

1.1.4. Перечень предприятий поставщиков и клиентов.

Клиентами ОКУ ЦЗН города Аши являются как физические, так и юридические лица.

Поставщиками ОКУ ЦЗН города Аши являются:

- ПАО «Ростелеком»
- ООО “Майкрософт Рус”
- ООО “КРИПТО-ПРО”
- ЗАО «ПФ «СКБ Контур»
- ООО «НПЦ «АИР»
- ИТ «Энигма»
-

1.1.5. Описание организационной структуры предприятия.

Организационная структура ОКУ ЦЗН города Аши включает в себя:

1. Директор

1.1. Заместитель директора

1.1.1. Отдел трудоустройства и специальных программ

1.1.2. Отдел профессионального обучения и профессиональной ориентации и психологической поддержки

1.1.3. Отдел рынка труда

1.2. Главный бухгалтер

1.2.1. Бухгалтерия

1.3. Технический отдел
1.4. Архив

1.1.6. Описание организационной структуры предприятия.

Организационная структура ОКУ ЦЗН города Аши включает в себя:

2. Директор
2.1. Заместитель директора
2.1.1. Отдел трудоустройства и специальных программ
2.1.2. Отдел профессионального обучения и профессиональной ориентации и психологической поддержки
2.1.3. Отдел рынка труда
2.2. Главный бухгалтер
2.2.1. Бухгалтерия
2.3. Технический отдел
2.4. Архив

1.1.7. Описание информационной среды организации.

ОКУ ЦЗН города Аши работает как с физическими, так и с юридическими лицами. Поэтому в информационную среду организации входят базы данных сотрудников и клиентов. Также по специфике работы организации в информационную среду входят локально-вычислительные и телефонные сети, как между клиентами, так и внутри организации.

Программно-аппаратные средства:

- Пакет Microsoft Office, необходим при оформлении (дополнении и изменении) договоров, приказов, распоряжений, отчетности.
- Microsoft Office communicator – коммуникационная программа-клиент, позволяющая пользователям общаться друг с другом в реальном времени.
- ПТК Система обработки информации СЗН – единый многоуровневый программный комплекс корпоративной информационной сети региона с базами данных (БД) центров занятости населения (ЦЗН) и сводной БД регионального органа службы занятости населения (РОСЗН) и охватывает все структуры, входящие в систему службы занятости населения, создавая единое информационное пространство.
- ViPNet Client 3.2 — программный продукт для обмена сообщениями и совместной работы.
- КриптоПро – для работы с сертификатами и организации структуры PKI.
- Etoken, Rutoken – для усиленной аутентификации пользователей АРМ.
- Диадок – для организации электронного документооборота и отправки отчетности в контролирующие государственные органы.

- Active Directory – позволяет администраторам использовать групповые политики для обеспечения единообразия настройки пользовательской рабочей среды, разворачивать программное обеспечение на множестве компьютеров через групповые политики или посредством System Center Configuration Manager, устанавливать обновления операционной системы, прикладного и серверного программного обеспечения на всех компьютерах в сети, используя Службу обновления Windows Server.

1.1.8. Описание строительной инфраструктуры здания.

Организация располагается по адресу: 456010, г. Аша, ул. Озимина, д. 14.

- Наружные и капитальные стены выполнены из шлакоблока с облицовкой кирпичом, перегородки из железобетонных плит.
- Входная дверь металлическая, оборудованная наружными и внутренними замками и доводчиком, имеется тамбур с пластиковой дверью со стеклом с доводчиком и замками.
- Окна – пластиковые стеклопакеты с двойным остеклением. На окнах установлены декоративные распашные металлические решетки с замками.
- На крыльце имеется наружное освещение.
- Установлена охранно-пожарная сигнализация. Охранная сигнализация Протон 16 с датчиками движения; автоматическая пожарная сигнализация Протон 16 с дымовыми пожарными извещателями с источником резервного питания Скат 1200.
- Установлен пожарный щит с пожарным рукавом и огнетушителями.
- Система центрального водяного отопления.
- Помещение охраняется вневедомственной охраной.
- Общая и внутренняя телефонная сеть.
- Электропитание здания организовано от трансформаторной подстанции, которая находится за пределами контролируемой зоны. К трансформаторной подстанции подключены сторонние потребители.
- Проход персонала и посетителей производится через центральный вход, запасного выхода нет.

1.1.9. Описание местоположения организации.

Организация располагается на 1 этаже 3-х этажного жилого дома по адресу: 456010, г. Аша, ул. Озимина, д. 14.

Здание располагается около проезжей части. Напротив здания расположен цветочный магазин и автобусная остановка. Позади - находится внутренний жилой двор и здание администрации рынка. Слева от входа прилегает трехэтажный жилой дом, в котором расположены «Совкомбанк» и три магазина. Справа – рыночная площадь и рыночный павильон. Вокруг расположены многоэтажные жилые дома.

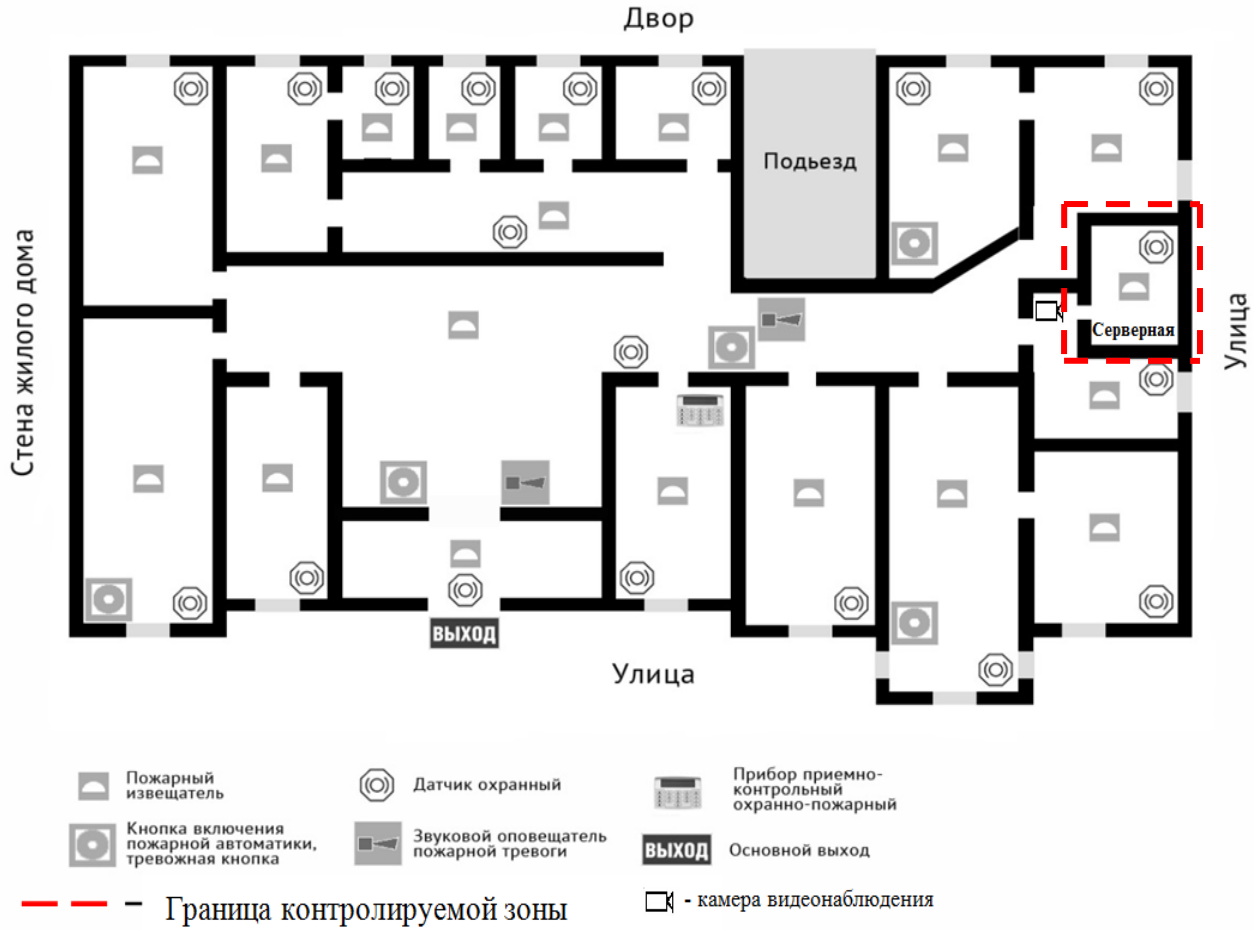
1.1.10. Описание информационной среды ОКУ ЦЗН города Аши:

Таблица 1

Программа	Назначение	Версия
ViPNet Client	Программный продукт для обмена сообщениями и совместной работы	3.2
Windows 7 Professional	Операционная система, установленная на АРМ сотрудников	6.1.7601.22616
Microsoft Office 2010	Офисный пакет для работы с документами	14.0.7015.1000 SP2
КриптоПро CSP	Программа для формирования ключей шифрования и ключей электронной цифровой подписи, шифрования и имитозащиты данных, обеспечения целостности и подлинности информации, не содержащей сведений, составляющих государственную тайну	4.0
ПТК Система обработки информации СЗН	Единый многоуровневый программный комплекс корпоративной информационной сети региона с базами данных (БД) центров занятости населения (ЦЗН) и сводной БД регионального органа службы занятости населения (РОСЗН) и охватывает все структуры, входящие в систему службы занятости населения, создавая единое информационное пространство.	

1.1.11. Схема территории:

Рисунок А.1 – Схема помещения



ПРИЛОЖЕНИЕ Б

ГЛАВНОЕ УПРАВЛЕНИЕ
ПО ТРУДУ И ЗАНЯТОСТИ НАСЕЛЕНИЯ
ЧЕЛЯБИНСКОЙ ОБЛАСТИ

Областное казенное учреждение
Центр занятости населения
города Аши

УТВЕРЖДАЮ
Директор ОКУ ЦЗН

_____И.И. Иванов

Дата_____

Положение об обработке персональных данных

15.02.2017 № 2
г. Аша

Положение об обработке персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение по обработке персональных данных (далее — Положение) Областного казенного учреждения Центр занятости населения города Аши (далее – ОКУ ЦЗН города Аши) разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149, Федеральным законом «О персональных данных» от 27.07.2006 №152-ФЗ, Правилами внутреннего трудового распорядка ОКУ ЦЗН города Аши.

1.2. Цель разработки Положения — определение порядка обработки персональных данных сотрудников ОКУ ЦЗН города Аши и иных субъектов, персональные данные которых подлежат обработке, на основании полномочий оператора; обеспечение защиты прав и свобод человека и гражданина, в т.ч. работника ОКУ ЦЗН города Аши, при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Порядок ввода в действие и изменения Положения.

1.3.1. Настоящее Положение вступает в силу с момента его утверждения директором ОКУ ЦЗН города Аши и действует бессрочно, до замены его новым Положением.

1.3.2. Все изменения в Положение вносятся приказом директора центра занятости населения.

1.4. Все работники ОКУ ЦЗН города Аши должны быть ознакомлены с настоящим Положением под роспись.

1.5. Режим неразглашения информации, содержащей персональные данные, снимается в случаях их обезличивания и по истечении 75 лет срока их хранения, или продлевается на основании заключения экспертной комиссии ОКУ ЦЗН города Аши, если иное не определено законом.

2. ОСНОВНЫЕ ПОНЯТИЯ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Состав персональных данных, обрабатываемых в ИСПДн ОКУ ЦЗН города Аши, определяется «Перечнем сведений, содержащих персональные данные».

2.2. Комплекс документов, сопровождающий процесс оформления трудовых отношений работника в ОКУ ЦЗН города Аши при его приеме, переводе и увольнении.

2.2.1. Информация, представляемая работником при поступлении на работу в ОКУ ЦЗН города Аши, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

– паспорт или иной документ, удостоверяющий личность;

– трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;

– страховое свидетельство государственного пенсионного страхования;

– документы воинского учета — для военнообязанных и лиц, подлежащих воинскому учету;

– документ об образовании, о квалификации или наличии специальных знаний — при поступлении на работу, требующую специальных знаний или специальной подготовки;

– справку о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям, выданную в порядке и по форме, которые устанавливаются федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, - при поступлении на работу, связанную с деятельностью, к осуществлению которой в соответствии с настоящим Кодексом, иным

федеральным законом не допускаются лица, имеющие или имевшие судимость, подвергающиеся или подвергавшиеся уголовному преследованию.

2.2.2. При оформлении работника в ОКУ ЦЗН города Аши специалистом заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:

– общие сведения (Ф.И.О. работника, дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);
– сведения о воинском учете;
– данные о приеме на работу;

В дальнейшем в личную карточку вносятся:

– сведения о переводах на другую работу;
– сведения об аттестации;
– сведения о повышении квалификации;
– сведения о профессиональной переподготовке;
– сведения о наградах (поощрениях), почетных званиях;
– сведения об отпусках;
– сведения о социальных гарантиях;
– сведения о месте жительства и контактных телефонах.

2.2.3. У специалиста ОКУ ЦЗН города Аши создаются и хранятся следующие группы документов, содержащие персональные данные работников в единичном или сводном виде:

2.2.3.1. Документы, содержащие персональные данные работников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству ОКУ ЦЗН города Аши, начальникам отделов; копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения).

2.2.3.2. Документация по ОКУ ЦЗН города Аши, работе отделов (Положения, должностные инструкции работников, приказы директора центра занятости населения); документы по планированию, учету, анализу и отчетности в части работы с персоналом ОКУ ЦЗН города Аши.

2.3. Комплекс документов, сопровождающий процесс оказания государственных услуг безработным гражданам.

2.3.1. Информация, представляемая безработными гражданами в ОКУ ЦЗН города Аши, должна иметь документальную форму. Граждане предъявляют следующие документы:

- паспорт или иной документ, удостоверяющий личность;
- страховое свидетельство государственного пенсионного страхования;
- ИНН;
- документ об образовании;
- номер лицевого счета;
- ИПР (для граждан, имеющих группу инвалидности);
- справку из УСВИ и ПФ;
- справку о заработной плате.

В дальнейшем в ИСПДн ОКУ ЦЗН города Аши вносятся:

- паспортные данные;
- сведения об образовании;
- сведения о трудовой деятельности;
- сведения об ограничениях по состоянию здоровья;
- сведения о льготах.

2.3.2. У сотрудников ОКУ ЦЗН города Аши создаются и хранятся следующие документы, содержащие персональные данные безработных граждан в единичном или сводном виде:

- справка из УСВИ;
- справка о заработной плате;
- карточка учета безработного гражданина (в соответствии с Законом «О занятости населения в Российской Федерации»);
- приказы (в соответствии с Законом «О занятости населения в Российской Федерации»).

3. СБОР, ОБРАБОТКА И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Порядок получения персональных данных.

3.1.1. Все персональные данные сотрудников ОКУ ЦЗН города Аши и безработных граждан следует получать у них самих. Если персональные данные возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Специалист ОКУ ЦЗН города Аши должен сообщить о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

3.1.2. ОКУ ЦЗН города Аши не имеет права получать и обрабатывать персональные данные сотрудников и безработных граждан об их расовой, национальной

принадлежности, политических взглядах, религиозных или философских убеждениях, интимной жизни.

3.1.3. ОКУ ЦЗН города Аши как работодатель вправе обрабатывать персональные данные сотрудников и безработных граждан только с их письменного согласия.

3.1.4. Письменное согласие субъекта на обработку своих персональных данных должно включать в себя:

– фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

– наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

– цель обработки персональных данных;

– перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

– перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

– срок, в течение которого действует согласие, а также порядок его отзыва.

3.1.5. Согласие субъекта не требуется в следующих случаях:

– обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия работодателя;

– обработка персональных данных осуществляется в целях исполнения трудового договора;

– обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

– обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работника, если получение его согласия невозможно.

3.2. Порядок обработки, передачи и хранения персональных данных.

3.2.1. Субъект предоставляет специалисту ОКУ ЦЗН города Аши достоверные сведения о себе. Специалист ОКУ ЦЗН города Аши проверяет достоверность сведений, сверяя данные, предоставленные субъектом, с имеющимися у субъекта документами.

3.2.2. Директор и сотрудники ОКУ ЦЗН города Аши при обработке персональных данных должны соблюдать следующие общие требования:

3.2.2.1. Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, оказания государственных услуг безработным гражданам, содействия

сотрудникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.2.2.2. При определении объема и содержания обрабатываемых персональных данных оператор должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом «О персональных данных» от 27.07.2006 №152-ФЗ и иными федеральными законами.

3.2.2.3. При принятии решений, затрагивающих интересы субъекта, ОКУ ЦЗН города Аши как оператор не имеет права основываться на персональных данных субъекта, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.2.2.4. Защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается ОКУ ЦЗН города Аши как оператором за счет своих средств и в порядке, установленном федеральным законом.

3.2.2.5. Сотрудники и их представители должны быть ознакомлены под расписку с документами ОКУ ЦЗН города Аши, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

3.2.2.6. Во всех случаях отказ субъекта от своих прав на сохранение и защиту персональных данных недействителен.

4. ПЕРЕДАЧА И ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. При передаче персональных данных субъекта ОКУ ЦЗН города Аши как работодатель должен соблюдать следующие требования:

4.1.1. Не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника, а также в случаях, установленных федеральным законом.

4.1.2. Не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия. Обработка персональных данных субъектов в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.

4.1.3. Предупредить лиц, получивших персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получившие персональные данные субъекта, обязаны соблюдать режим неразглашения информации. Данное Положение не распространяется на обмен персональными данными субъектов в порядке, установленном федеральными законами.

4.1.4. Осуществлять передачу персональных данных субъектов в пределах ОКУ ЦЗН города Аши в соответствии с настоящим Положением.

4.1.5. Разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные сотрудника, которые необходимы для выполнения конкретной функции.

4.1.6. Не запрашивать у субъектов информацию об их расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, интимной жизни.

4.1.7. Передавать персональные данные сотрудников представителям в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функции.

4.2. Хранение и использование персональных данных:

4.2.1. Персональные данные субъектов обрабатываются и хранятся в помещениях ОКУ ЦЗН города Аши и на учтённых машинных носителях в соответствии с Инструкцией по учёту машинных носителей.

4.2.2. Персональные данные субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде — в локальной компьютерной сети, в компьютерных программах и электронных базах данных.

4.3. При получении персональных данных не от субъекта (за исключением случаев, если персональные данные были предоставлены ОКУ ЦЗН города Аши на основании федерального закона или если персональные данные являются общедоступными), ОКУ ЦЗН города Аши до начала обработки таких персональных данных обязано предоставить субъекту следующую информацию:

– наименование (фамилия, имя, отчество) и адрес оператора или его представителя;

– цель обработки персональных данных и ее правовое основание;

– предполагаемые пользователи персональных данных;

– установленные Федеральным законом №152 «О персональных данных» права субъекта персональных данных.

5. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ СОТРУДНИКОВ

5.1. Перечень лиц, имеющих право доступа к персональным данным, определяется «Списком лиц, которым необходим доступ к персональным данным», утверждённым директором ОКУ ЦЗН города Аши.

5.2. Субъект персональных данных, чьи персональные данные обрабатываются в информационной системе ОКУ ЦЗН города Аши, имеет право:

5.2.1. Получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей персональные данные этого субъекта.

5.2.2. Требовать от ОКУ ЦЗН города Аши уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющих необходимыми для оператора персональных данных.

5.2.3. Получать от оператора:

– сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

– перечень обрабатываемых персональных данных и источник их получения;

– сроки обработки персональных данных, в том числе сроки их хранения;

– сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

5.2.4. Требовать извещения Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.3. Копировать и делать выписки персональных данных субъекта разрешается исключительно в служебных целях с письменного разрешения секретаря.

5.4. Передача информации третьей стороне возможна только при письменном согласии субъектов.

6. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Сотрудники ОКУ ЦЗН города Аши, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с федеральными законами.

6.2. Директор ОКУ ЦЗН города Аши за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.

Ответственный за обеспечение безопасности ПДн А.А.Петров

Окончание приложения Б

Приложение 1

Лист ознакомления с инструкцией

Дата ознакомления	**ФИО сотрудника, ознакомившегося с документом**	**Должность сотрудника, ознакомившегося с документом**	**Подпись сотрудника, ознакомившегося с документом**

ПРИЛОЖЕНИЕ В

ГЛАВНОЕ УПРАВЛЕНИЕ
ПО ТРУДУ И ЗАНЯТОСТИ НАСЕЛЕНИЯ
ЧЕЛЯБИНСКОЙ ОБЛАСТИ

Областное казенное учреждение
Центр занятости населения
города Аши

УТВЕРЖДАЮ
Директор ОКУ ЦЗН

_____И.И. Иванов

Дата_____

Перечень сведений, содержащих персональные данные

15.02.2017 № 3
г. Аша

Перечень сведений, содержащих персональные данные

№	Наименование	Типы документов, где возможно появление персональных данных
1.	Персональные данные сотрудников (паспортные данные, сведения о трудовой деятельности, образовании, сведения о семейном положении и составе семьи, месте жительства, сведения о доходах, получаемых льготах, уплачиваемых налогах и сборах)	
1.1.	Персональные данные сотрудников, необходимые для обеспечения кадровой деятельности	Бумажные носители, локальные файлы, СУБД Сервер БД «1С Предприятие», рабочие станции сотрудников
1.2.	Персональные данные сотрудников, необходимые для подготовки отчетов в ПФР и ФСС	Локальные файлы Рабочие станции сотрудников
1.3.	Персональные данные сотрудников, необходимые для подготовки отчетов для ФНС	Локальные файлы Рабочие станции сотрудников

1.4.	Персональные данные сотрудников, необходимые для выплаты заработной платы	Локальные файлы Рабочие станции сотрудников
2.	Персональные данные безработных (паспортные данные, сведения о трудовой деятельности, образовании, мест жительства, сведения о полученных выплатах, номера расчетных счетов, данные об обучении и переобучении)	
2.1.	Персональные данные безработных	Бумажные носители, СУБД Сервер БД «СОИ»
2.2.	Персональные данные безработных, необходимые для подготовки отчетов в ПФР	Локальные файлы Рабочие станции сотрудников
2.3.	Персональные данные безработных, необходимые для выплаты пособий	Локальные файлы Рабочие станции сотрудников
2.4.	Справки по безработным	Бумажные носители, локальные файлы Рабочие станции сотрудников

Ответственный за обеспечение безопасности ПДн А.А.Петров

ПРИЛОЖЕНИЕ Г

ГЛАВНОЕ УПРАВЛЕНИЕ
ПО ТРУДУ И ЗАНЯТОСТИ НАСЕЛЕНИЯ
ЧЕЛЯБИНСКОЙ ОБЛАСТИ

Областное казенное учреждение
Центр занятости населения
города Аши

УТВЕРЖДАЮ
Директор ОКУ ЦЗН

_____И.И. Иванов

Дата_____

Согласие на обработку персональных данных

15.02.2017 № 4
г. Аша

Согласие на обработку персональных данных

«___» _____ 20__года

Я, _____
(фамилия, имя, отчество субъекта)

_____
(основной документ, удостоверяющий личность)

_____
(номер, сведения о дате выдачи указанного документа и выдавшем его органе)

в дальнейшем «Субъект», дает согласие ОКУ ЦЗН города Аши, расположенному по адресу: РФ, Челябинская обл., г. Аша, ул. Озимина, д. 14, в лице ответственных лиц за обработку персональных данных, на обработку персональных данных (см. п.3) на следующих условиях:

1. Субъект дает согласие на обработку Оператором своих персональных данных, т.е. совершение, в том числе, следующих действий: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных, при этом общее описание вышеуказанных способов обработки данных приведено в ФЗ №152 от 27.07.2006, а также право на передачу такой информации третьим лицам, если это необходимо для осуществления переданных полномочий по решению вопросов социальной поддержки и социального

обслуживания граждан, охраны труда, функционирования информационных систем, организационной деятельности учреждения и в случаях, установленных нормативными документами вышестоящих органов и законодательством.

2. Оператор обязуется использовать данные Субъекта в целях реализации на территории муниципального района в рамках переданным органам местного самоуправления отдельных государственных полномочий единой государственной социальной политики в сфере социальной защиты населения (социальная поддержка отдельных категорий граждан, оказание государственной социальной помощи, социальное обслуживание населения), вопросов в сфере социальных отношений, не отнесенных к компетенции органов местного самоуправления других муниципальных образований, органов государственной власти и не исключенных из их компетенции федеральными законами и законами Челябинской области, а также исполнение иных полномочий в соответствии с законодательством Российской Федерации и Челябинской области, Положения об Управлении, муниципальными правовыми актами. Оператор может раскрыть правоохранительным органам любую информацию по официальному запросу в случаях, установленных законодательством в стране проживания Субъекта.

3. Перечень персональных данных, передаваемых Оператору на обработку:

- паспортные данные;
- сведения об образовании;
- сведения о трудовой деятельности;
- сведения о заработной плате
- сведения об ограничениях по состоянию здоровья;
- сведения о льготах;
- номер лицевого счета;
- контактная информация.

4. Субъект персональных данных по письменному запросу имеет право на получение информации, касающейся обработки его персональных данных (в соответствии с п.4 ст. 14 ФЗ №152 от 27.06.2006).

5. При поступлении Оператору письменного заявления Субъекта о прекращении действия Согласия, персональные данные уничтожаются установленным способом в 15-дневый срок.

6. Настоящее разрешение действует в течение срока хранения персональных данных Субъекта.

Субъект _____ /_____ /
(подпись) (И.О. Фамилия)

ПРИЛОЖЕНИЕ Д

ГЛАВНОЕ УПРАВЛЕНИЕ
ПО ТРУДУ И ЗАНЯТОСТИ НАСЕЛЕНИЯ
ЧЕЛЯБИНСКОЙ ОБЛАСТИ

Областное казенное учреждение
Центр занятости населения
города Аши

УТВЕРЖДАЮ
Директор ОКУ ЦЗН

_____И.И. Иванов

Дата_____

Должностная инструкция ответственного за обеспечение безопасности персональных данных

15.02.2017 № 5
г. Аша

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ

ответственного за обеспечение безопасности персональных данных

1. Общие положения

1.1. Данная Инструкция определяет основные обязанности и права ответственного за обеспечение безопасности персональных данных Областного казенного учреждения Центра занятости населения города Аши (далее – ОКУ ЦЗН).

1.2. Ответственный за обеспечение безопасности персональных данных является штатным сотрудником ОКУ ЦЗН.

1.3. Ответственный за обеспечение безопасности персональных данных назначается приказом директора.

1.4. Решение вопросов обеспечения информационной безопасности входит в прямые служебные обязанности ответственного за обеспечение безопасности персональных данных.

1.5. Ответственный за обеспечение безопасности персональных данных обладает правами доступа к любым программным и аппаратным ресурсам.

2. Должностные обязанности

Ответственный за обеспечение безопасности персональных данных обязан:

2.1. Знать перечень установленных в подразделениях автоматизированных рабочих мест (далее АРМ) и перечень задач, решаемых с их использованием.

2.2. Осуществлять учет и периодический контроль над составом и полномочиями пользователей различных АРМ информационной системы (далее ИС).

2.3. Осуществлять оперативный контроль над работой пользователей защищенных АРМ, анализировать содержимое системных журналов всех АРМ и адекватно реагировать на возникающие нештатные ситуации. Обеспечивать своевременное архивирование системных журналов АРМ и надлежащий режим хранения данных архивов.

2.4. Осуществлять непосредственное управление режимами работы и административную поддержку функционирования применяемых на АРМ ИС специальных технических средств защиты от несанкционированного доступа (далее НСД).

2.5. Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных АРМ и серверов, устанавливать и осуществлять настройку средств защиты АРМ.

2.6. Периодически проверять состояние используемых средств защиты информации (далее СЗИ) от НСД, осуществлять проверку правильности их настройки (выборочное тестирование).

2.7. Периодически контролировать целостность печатей (пломб, наклеек) на устройствах защищенных АРМ.

2.8. Проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИС и осуществления НСД к информации и техническим средствам АРМ.

2.9. По указанию руководства своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах по управлению средствами защиты от НСД, установленных на АРМ ИС.

2.10. Проводить занятия с сотрудниками и начальниками отделов по правилам работы на АРМ, оснащенных СЗИ от НСД, и по изучению руководящих документов по вопросам обеспечения безопасности информации.

2.11. Участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в результате НСД.

2.12. Участвовать в работе комиссий по пересмотру планов защиты

3. Порядок работы с ресурсами ИС

Перечень работ, производимых ответственным за обеспечение безопасности персональных данных ресурсами ИС.

3.1. Проверка работоспособности и настройка системы доступа к ресурсам ИС:

3.1.1. Ответственный за обеспечение безопасности персональных данных разрабатывает правила парольной защиты, отражает их в «Инструкции по организации парольной защиты» и контролирует их соблюдение;

3.1.2. Ответственный за обеспечение безопасности персональных данных сообщает пользователю его уникальное имя и предоставляет возможность задать пароль, кодирует аппаратный идентификатор пользователя (при наличии);

3.1.3. Изменение учетных данных пользователя производится по требованию начальника отдела, согласованному с ответственным за обеспечение безопасности персональных данных, а также периодически по утвержденному плану и в случае увольнения сотрудника;

3.1.4. Ответственный за обеспечение безопасности персональных данных имеет право в целях тестирования уязвимости системы доступа (выявление простейших паролей) производить попытки взлома паролей пользователей, если попытка взлома была успешной, ответственный за обеспечение безопасности персональных данных обязан потребовать у пользователя изменения пароля.

3.2. Проверка работоспособности и настройка аппаратных и программных средств защиты информации:

3.2.1. Ответственный за обеспечение безопасности персональных данных обязан перед началом работ включить и убедиться в работоспособности аппаратных СЗИ, в случае сбоя – прекратить работы.

3.2.2. В случае сбоя программных СЗИ, таких, как неправильная идентификация пользователей и их прав доступа, ответственный за обеспечение безопасности персональных данных обязан прекратить работы, но в случае производственной необходимости – отключить программное обеспечение (далее ПО) СЗИ и лично контролировать проведение работ пользователем.

3.3. Антивирусная защита ресурсов ИС. Ответственный за обеспечение безопасности персональных данных разрабатывает и контролирует реализацию антивирусной политики, а именно:

3.3.1. Настраивает параметры антивирусной программы;

3.3.2. Контролирует работоспособность антивирусной программы;

3.3.3. Немедленно реагирует на сообщения пользователей о подозрительном поведении ПО, а также, о появлении любых сообщений антивирусной программы;

3.3.4. Имеет право на проведение внеплановой проверки на присутствие вирусов;

3.3.5. Периодически обновляет антивирусные базы данных, а также исполняемые модули антивирусной программы.

3.4. Хранение дистрибутивов программного обеспечения СЗИ. Ответственный за обеспечение безопасности персональных данных должен хранить дистрибутивы программного обеспечения СЗИ, установленного на АРМ в месте, исключающем доступ других лиц.

3.5. Проверка целостности системного и прикладного ПО. Ответственный за обеспечение безопасности персональных данных должен периодически (не реже одного раза в квартал) производить проверку целостности системного и прикладного программного обеспечения с использованием специальных режимов работы СЗИ от НСД.

3.6. Резервное копирование и восстановление информации. В соответствии с утвержденным регламентом, а также по требованию пользователей, ответственный за обеспечение безопасности персональных данных проводит резервное копирование и восстановление пользовательской информации. При этом необходимо выполнять следующие требования:

3.6.1. Иметь в наличии регламент резервного копирования и перечня резервируемой информации, утверждаемых приказом директора;

3.6.2. Вне графика производить обязательное резервное копирование в случае обнаружения неисправностей в работе АРМ или отчуждаемых носителей;

3.6.3. Допускается обоснованное внеплановое резервное копирование информации по инициативе ответственного за обеспечение безопасности персональных данных, если это не нарушает технологию обработки информации;

3.6.4. Резервные копии хранятся на отдельных носителях в шифрованном виде в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение (ответственным за хранение является ответственный за обеспечение безопасности персональных данных);

3.6.5. При устранении неисправностей АРМ ответственный за обеспечение безопасности персональных данных производит восстановление важной информации с резервных копий.

3.7. Вывод ресурсов ИС из эксплуатации. При невозможности ремонта различных ресурсов ИС ответственный за обеспечение безопасности персональных данных обязан:

3.7.1. Физически уничтожать любые носители, независимо от содержащейся на них информации, отразить факт уничтожения носителя в «Журнале учета уничтоженных машинных носителей»;

3.7.2. Отразить факт выхода из строя и замены оборудования в «Техническом паспорте объекта информатизации».

4. Действия при обнаружении попыток несанкционированного доступа

4.1. К попыткам несанкционированного доступа относятся:

4.1.1. Сеансы работы с информационной системой персональных данных (далее ИСПДн) незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий которых истек, либо в состав полномочий которых не входят операции по доступу к данным или манипулирования ими;

4.1.2. Действия третьего лица, пытающегося получить доступ (или получившего доступ) к ИСПДн, при использовании учетной записи администратора или другого пользователя ИСПДн, в целях получения коммерческой или другой личной выгоды, методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.

4.2. При выявлении факта НСД ответственный за обеспечение безопасности персональных данных обязан:

4.2.1. Прекратить доступ к ИСПДн со стороны выявленного участка НСД;

4.2.2. Доложить директору служебной запиской о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;

4.2.3. Известить начальника отдела, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;

4.2.4. Проанализировать характер НСД;

4.2.5. Внести запись в «Журнал регистрации попыток несанкционированного доступа к ИСПДн».

5. Права

5.1. Требовать от пользователей информационных ресурсов выполнения инструкций по обеспечению безопасности и защите информации в ИС.

5.2. Проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИС.

5.3. Вносить свои предложения по совершенствованию мер защиты в ИС.

6. Ответственность

6.1. Несет персональную ответственность за программно-аппаратные, инженерно-технические и криптографические средства защиты информации, средства вычислительной техники, информационно - вычислительные комплексы, сети и информационные системы обработки информации, закрепленные за ним приказом директора и за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями.

6.2. Несет ответственность по действующему законодательству за разглашение информации, составляющей персональные данные, ставшие известными ему по роду работы.

6.3. Несет ответственность за все действия, совершенные от имени его учетной записи или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

С должностной инструкцией ознакомлен (а)

Ответственный за обеспечение безопасности ПДн А.А.Петров

ПРИЛОЖЕНИЕ Е

ГЛАВНОЕ УПРАВЛЕНИЕ
ПО ТРУДУ И ЗАНЯТОСТИ НАСЕЛЕНИЯ
ЧЕЛЯБИНСКОЙ ОБЛАСТИ

Областное казенное учреждение
Центр занятости населения
города Аши

УТВЕРЖДАЮ
Директор ОКУ ЦЗН

_____И.И. Иванов

Дата_____

Инструкция пользователя о порядке работы с персональными данными

15.02.2017 № 6
г. Аша

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ
о порядке работы с персональными данными

1. Общие понятия

1.1. Данная инструкция разработана с целью защиты интересов Областного казенного учреждения Центра занятости населения города Аши (далее ОКУ ЦЗН) и его сотрудников, а также безработных граждан, в целях предотвращения раскрытия (передачи) персональных данных, а также соблюдения надлежащих правил обращения с персональными данными.

1.2. Данная инструкция предназначена для использования всеми сотрудниками ОКУ ЦЗН и регулирует правила работы с персональными данными.

1.3. Сотрудники ОКУ ЦЗН, доступ которых к персональным данным необходим для выполнения ими своих служебных обязанностей, должны быть ознакомлены под роспись с данной инструкцией и предупреждены о возможной ответственности за его нарушение.

1.4. К работе со сведениями, содержащими персональные данные, допускаются сотрудники, заключившие трудовой договор, содержащий соответствующее «Обязательство о неразглашении информации, содержащей персональные данные».

1.5. Отнесение сведений к категории персональных данных осуществляется в соответствии с «Перечнем сведений, содержащих персональные данные».

2. Порядок работы с документами, содержащими информацию о персональных данных

2.1. Лица, поступающие на работу в ОКУ ЦЗН, должны быть ознакомлены с «Перечнем сведений, содержащих персональные данные» и предупреждены об ответственности за разглашение (утрату) сведений, содержащих персональные данные и дать письменное обязательство о неразглашении указанных сведений.

2.2. Право работы со сведениями, относящимися к персональным данным, сотрудники получают в пределах выполнения своих должностных (функциональных) обязанностей.

2.3. При работе с документами, магнитными, оптическими и флеш-носителями, содержащими персональные данные, сотрудники ОКУ ЦЗН обязаны следить как за сохранностью самих документов и носителей, так и за сохранностью, содержащейся в них информации (не допускать несанкционированного ознакомления с документами посторонних лиц, в том числе других сотрудников).

2.4. Носители с персональными данными следует убирать и запирать в шкаф или сейф, когда они не используются.

2.5. Все бумажные документы, содержащие персональные данные, не должны храниться в открытом виде, позволяющем визуальный съем информации, их фотографирование или несанкционированное создание копий.

2.6. Бумажные документы, ставшие ненужными, у которых истек срок хранения, испорченные бланки, лишние копии документов должны уничтожаться в специальных устройствах – шредерах, а при больших объемах уничтожаемых документов - путем сжигания в присутствии двух ответственных сотрудников.

2.7. Запрещается оставлять на рабочем месте документы, содержащие персональные данные, или носители с персональными данными без присмотра.

2.8. Запрещается выносить носители с персональными данными за пределы служебных помещений ОКУ ЦЗН.

2.9. Запрещается записывать персональные данные на съемные носители без прямой служебной необходимости.

2.10. При обработке персональных данных нельзя допускать возможность визуального просмотра персональных данных, зафиксированных на бумажных носителях или отображаемых на экране монитора, третьими лицами.

2.11. Персональные компьютеры и принтеры должны быть выключены по окончании работы. При кратковременном покидании рабочего места компьютеры должны быть заблокированы.

2.12. В нерабочее время фотокопировальные устройства должны быть защищены от доступа третьих лиц (заперты, убраны и т.п.).

2.13. Напечатанные документы с персональными данными должны изыматься из принтеров немедленно.

2.14. Запрещается выносить переносные компьютеры, содержащие персональные данные, за пределы служебных помещений.

2.15. Категорически запрещается упоминать в разговоре с третьими лицами сведения, содержащие персональные данные.

2.16. Запрещается в нерабочее время вне служебных помещений упоминать в разговоре с сотрудниками ОКУ ЦЗН сведения, содержащие персональные данные.

2.17. Запрещается обсуждать с кем-либо порядок доступа, места хранения, средства защиты систем обработки персональных данных, кроме обсуждения со специально допущенными к этой информации сотрудниками.

3. Ответственность за разглашение персональных данных

3.1. За нарушение правил работы с персональными данными сотрудник несет дисциплинарную, административную, гражданскую и уголовную ответственность в соответствии с действующим законодательством.

3.2. Нарушение правил работы с персональными данными может служить основанием для расторжения трудового договора.

3.3. Каждый сотрудник несет ответственность за любые неправомерные деяния, совершенные в рабочее время с использованием персонального компьютера, за который он является ответственным.

3.4. Сотрудники несут ответственность за деяния, совершенные с использованием их учетной записи в тех случаях, когда с их стороны не принимались достаточные меры по защите авторизационных данных.

3.5. В случае нарушения правил работы с персональными данными, повлекшего ущерб или нарушение работы информационной системы, сотрудник обязан собственными силами восстановить первоначальное состояние информационной системы либо возместить затраты на восстановление информационной системы.

4. Обязанности руководства по защите персональных данных

4.1. Директор ОКУ ЦЗН участвует в подготовке и последующей корректировке «Перечня сведений, содержащих персональные данные».

4.2. Директор ОКУ ЦЗН назначает сотрудника, ответственного за антивирусную защиту в соответствии с «Инструкцией по антивирусной защите».

4.3. Директор ОКУ ЦЗН назначает сотрудника, ответственного за поддержание работоспособности рабочих станций и локальной сети ОКУ ЦЗН.

4.4. Директор ОКУ ЦЗН совместно с администратором сети проводит контроль целевого использования сотрудниками ресурсов сети Internet.

4.5. Директор ОКУ ЦЗН участвует в проведении служебных расследований по фактам нарушения настоящей инструкции и принимает решение об ответственности сотрудников.

5. Общие обязанности сотрудников

5.1. Каждый сотрудник ОКУ ЦЗН, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным информационной системы персональных данных (далее ИСПДн), несет персональную ответственность за свои действия и обязан:

5.1.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

5.1.2. Знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте (далее АРМ);

5.1.3. Хранить в тайне свой пароль (пароли). В соответствии с «Инструкцией по организации парольной защиты» с установленной периодичностью менять свой пароль (пароли);

5.1.4. Выполнять требования «Инструкции по организации антивирусной защиты» в части касающейся действий пользователей АРМ ИСПДн;

5.2. Немедленно вызывать ответственного за обеспечение безопасности персональных данных и ставить в известность начальника отдела при обнаружении:

5.2.1. Нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее НСД) к защищаемой АРМ;

5.2.2. Несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;

5.2.3. Отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

5.2.4. Некорректного функционирования установленных на АРМ технических средств защиты;

5.2.5. Непредусмотренных отводов кабелей и подключенных к АРМ дополнительных устройств;

5.3. Присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию, закрепленной за ним АРМ в отделе.

6. Сотрудникам категорически запрещается

6.1. Использовать компоненты программного и аппаратного обеспечения ИСПДн ОКУ ЦЗН в неслужебных целях;

6.2. Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства, непредусмотренные формулярами рабочих станций;

6.3. Осуществлять обработку информации, содержащей персональные данные в присутствии посторонних (не допущенных к данной информации) лиц;

6.4. Записывать и хранить информацию, содержащую персональные данные на неучтенных носителях информации;

6.5. Оставлять включенной без присмотра свое АРМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

6.6. 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 ответственного за обеспечение безопасности персональных данных и начальника отдела.

Приложение 1
Лист ознакомления с инструкцией

Дата ознакомления	ФИО сотрудника, ознакомившегося с документом	Должность сотрудника, ознакомившегося с документом	Подпись сотрудника, ознакомившегося с документом

ПРИЛОЖЕНИЕ Ж

ГЛАВНОЕ УПРАВЛЕНИЕ
ПО ТРУДУ И ЗАНЯТОСТИ НАСЕЛЕНИЯ
ЧЕЛЯБИНСКОЙ ОБЛАСТИ

Областное казенное учреждение
Центр занятости населения
города Аши

УТВЕРЖДАЮ:
Директор ОКУ ЦЗН

_____И.И. Иванов

«___» _____2017 г.

УТВЕРЖДАЮ:
Ответственный за обеспечение безопасности ПДн

_____А.А.Петров

«___» _____2017 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
по модернизации защиты ИСПДн
в ОКУ ЦЗН города Аши

«СОГЛАСОВАНО»
Старший администратор ИС
ООО «Интеркомп-А»

_____В.В. Тимофеев

«___» _____2017 г.

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Полное наименование системы и ее условное обозначение

Полное наименование системы: Информационная система персональных данных в ОКУ ЦЗН.

Условное обозначение системы: ИСПДн в ОКУ ЦЗН города Аши.

1.2. Наименования предприятий разработчика и заказчика модернизации защиты ИСПДн.

Предприятие разработчик защиты ИСПДн: ОКУ ЦЗН города Аши, в лице ответственного за обеспечение безопасности ПДн.

Предприятие заказчик защиты ИСПДн: ОКУ ЦЗН города Аши, в лице директора.

1.3. Перечень документов, на основании которых создается защита ИСПДн:

- Конституция Российской Федерации;
- Федеральный закон Российской Федерации от 27.07. 2006 года № 152-ФЗ "О персональных данных";
- Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 21.07.2014) «Об информации, информационных технологиях и о защите информации»
- Трудовой кодекс РФ от 30.12.2001 № 197-ФЗ;

1.4. Порядок оформления и предъявления заказчику результатов работ по модернизации защиты ИСПДн (ее частей), по изготовлению и наладке отдельных средств (технических, программных, информационных) и программно-технических (программно-методических) комплексов защиты ИСПДн.

Результаты работы оформляются и предъявляются заказчику по мере исполнения в виде минимальных независимых частей проекта и/или предварительных проектов. Окончательный вариант проекта предоставляется на рассмотрение заказчику после ответственного за обеспечение безопасности ПДн ОКУ ЦЗН города Аши.

2. НАЗНАЧЕНИЕ И ЦЕЛИ МОДЕРНИЗАЦИИ ЗАЩИТЫ ИСПДн

2.1. Назначение модернизации защиты ИСПДн

Модернизация защиты информационной системы персональных данных необходимый процесс, обусловленный постоянными изменениями, как в правовой, так и в технической сфере информационных технологий. Для того, чтобы защита ИСПДн функционировала и была законодательно действительна, необходимо проводить постоянный анализ информационной среды организации и анализировать возможные угрозы и уязвимости.

2.2. Цели модернизации защиты ИСПДн

Основной целью проведения работ является обеспечение безопасности информации, обрабатываемой в информационной системе, приведение порядка обработки, хранения и передачи персональных данных ОКУ ЦЗН города Аши в соответствие с требованиями, перечисленными в данном Техническом задании.

3. ХАРАКТЕРИСТИКА ОБЪЕКТОВ ЗАЩИТЫ

3.1. Краткие сведения об объектах защиты

Объектом защиты являются информация, содержащая персональные данные, ее носители, места их обработки, а также информационные системы и помещения, в отношении которых необходимо обеспечивать защиту:

1. Автоматизированные рабочие места:

- АРМ сотрудников, на которых обрабатывается защищаемая информация

2. Помещения для хранения и работы с важной защищаемой информацией:

- Отдел трудоустройства и специальных программ;
- Отдел профессионального обучения и профессиональной ориентации и психологической поддержки;
- Бухгалтерия;
- Архив
- Серверная комната.

3. Линии и средства связи, системы обеспечения функционирования СВТ и деятельности организации:

- Линии городской телефонной станции;
- Система электропитания;
- Линии охранной и пожарной сигнализации;
- Телекоммуникационная инфраструктура локальной компьютерной сети;
- Система охлаждения и вентиляции серверов.

4. Средства ввода-вывода и отображения информации:

- Мониторы сотрудников, на которых обрабатывается защищаемая информация: LG Flatron L 1918S, BenQ G2420HDB, Benq T221W.
- Принтеры HP LaserJet P2055d, Canon LBP 2900.
- Оперативная память ПК, входящих в АРМ.

5. Сервер:

- ACER ALTOS 1100.

6. Системы бесперебойного питания сервера и рабочих станций:

- Источник бесперебойного питания в серверной комнате;
- Источники бесперебойного питания АРМ сотрудников, на которых обрабатывается защищаемая информация.

7. Носители информации:

- Бумажные носители информации ограниченного доступа;
- Электронные (дискеты, диски, флэш-накопители с документами, содержащими информацию ограниченного доступа);
- Персонал.

8. Персонал:

- Начальник отдела трудоустройства и специальных программ;
- Специалисты отдела трудоустройства и специальных программ (3 человека);
- Начальник отдела профессионального обучения и профессиональной ориентации и психологической поддержки;
- Специалисты отдела профессионального обучения и профессиональной ориентации и психологической поддержки (2 человека);
- Главный бухгалтер;
- Бухгалтер по начислению пособия;
- Архивариус.

3.2. Сведения об условиях эксплуатации объекта защиты и характеристиках окружающей информационной среды.

3.2.1. Объекты защиты подвержены воздействию следующих угроз:

3.2.1.1. Сервер с базами данных:

- Уничтожение информации в случае непреднамеренного выключения или уничтожения основных носителей информации;
- Неавторизованная модификация информации в системе, хранящейся на сервере;
- Разглашение информации, содержащей персональные данные сотрудниками организации;

3.2.1.2. АРМ начальника отдела и специалистов отдела трудоустройства и специальных программ:

- Уничтожение информации в случае непреднамеренного выключения или уничтожения основных носителей информации;
- Неавторизованная модификация информации в системе, хранящейся на АРМ начальника отдела и специалистов отдела трудоустройства и специальных программ;

3.2.2. Присутствуют следующие уязвимости:

3.2.2.1. Сервер с базами данных:

- Отсутствие регламента резервного копирования;
- Несоблюдение соглашений о неразглашении информации, содержащей персональные данные;
- Неактуальность документов по защите персональных данных и соблюдения режима защиты информации, содержащей персональные данные;
- Отсутствие инструкции по обращению с сервером при возникновении чрезвычайных ситуаций;
- Затопление серверной комнаты;
- Пожар в серверной комнате;
- Попадание пыли, загрязнение сервера;
- Отсутствие пломбировки корпуса сервера, а также отсутствие пломбировки внутренних функциональных элементов и, как следствие, возможность физического повреждения аппаратной части.

3.2.2.2. АРМ начальника отдела и специалистов отдела трудоустройства и специальных программ:

- Отсутствие регламента доступа к компьютеру специалистов отдела трудоустройства и специальных программ;
- Отсутствие регламента резервного копирования;
- Отсутствие пломбировки корпуса ПК и, как следствие, доступ к жестким магнитным дискам;
- Установка программного обеспечения, которое может создать условия для НСД к информации ограниченного доступа;
- Отсутствие авторизации на аппаратном уровне;
- Несоблюдение соглашений о неразглашении информации, содержащей персональные данные;
- Неактуальность документов по защите персональных данных и соблюдения режима защиты информации, содержащей персональные данные.

4. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО МОДЕРНИЗАЦИИ ЗАЩИТЫ ИСПДн

Работы должны проводиться в соответствии с положениями, перечисленными в данном Техническом задании.

Работы должны проводиться в один этап: приведение в соответствие порядка обработки персональных данных, а также оптимизация технических средств обработки информации.

4.1. Приведение в соответствие порядка обработки персональных данных.

Следующие работы должны быть проведены в отношении всех существующих у Заказчика систем обработки информации, содержащей персональные данные:

- Уточнение степени участия персонала организации в обработке персональных данных;
- Сбор сведений об имевших место инцидентах информационной безопасности, связанных с информацией, содержащей персональные данные;
- Изучение существующих организационных мер обеспечения безопасности информационной системы персональных данных;
- Разработка актуальной модели угроз;
- Разработка перечня требований по защите информации о персональных данных;
- Выявление имеющихся средств технической защиты информации, которые могут быть использованы для обеспечения безопасности информации, содержащей персональные данные;
- Изучение технических мер обеспечения безопасности информационной системы персональных данных, применяемых в организации;
- Анализ соответствия применяемых мер и средств технической защиты предъявляемым требованиям нормативно-правовой базы Российской Федерации в области защиты персональных данных;
- Разработка рекомендаций по технической защите ИСПДн;
- Определение необходимости сертификации имеющихся технических средств и программного обеспечения защиты ИСПДн;
- Доработка нормативной и рабочей документации по защите ИСПДн в части приведения в соответствие требованиям нормативно-правовых документов.

4.2. Приведение в соответствие (включая оптимизацию) технических средств обработки информации.

Модернизация защиты ИСПДн должна производится с учетом программных и программно-аппаратных средств защиты информации, имеющихся в наличии у Заказчика.

Следующие работы должны быть проведены в отношении всех существующих у Заказчика систем обработки персональных данных:

- Определение условий расположения информационной сети по передаче сведений, содержащих персональных данных относительно границ контролируемой зоны;
- Определение конфигурации и топологии информационной сети в целом и ее отдельных компонент, физических, функциональных и технологических связей как внутри этих систем, так и с другими системами различного уровня и назначения;
- Сбор сведений об имевших место инцидентах информационной безопасности, связанных с изменениями в работоспособности элементов информационной системы;
- Изучение существующих организационных мер обеспечения безопасности работоспособности и функционирования информационных систем;
- Поставка необходимого и/или недостающего оборудования для обеспечения повышения надежности и отказоустойчивости информационной системы;
- Обновление программных продуктов информационной системы до актуального состояния;
- Определение списка специализированных средств защиты информации и обеспечения сохранности данных.

4.3. Порядок проведения работ:

4.3.1. Для выполнения работ Исполнитель формирует команду из состава специалистов Заказчика, имеющих необходимую компетенцию.

4.3.2. Специалисты Заказчика на время проекта переходят под руководство Исполнителя.

4.3.3. Исходные данные Исполнителем собираются в ходе проведения работ путем:

- интервьюирования персонала Заказчика, в том числе руководителей и сотрудников организации;
- анализа результатов деятельности Исполнителя в составе организации Заказчика;
- анализа документов и записей результатов деятельности Заказчика в части обеспечения безопасности информационных систем персональных данных (нормативных документов, проектной и эксплуатационной документации, актов, журналов и пр.).

5. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ КСЗИ

5.1. Критериями для приемки работ является настоящее техническое задание и соответствующие частные Технические задания, разрабатываемые в процессе выполнения работ.

5.2. Приемка работ осуществляется единовременно.

5.3. Заказчик направляет замечания в письменном виде.

6. ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ ПРОЕКТА РАБОТ ПО ПОДГОТОВКЕ ОБЪЕКТА ЗАЩИТЫ К ВВОДУ ЗАЩИТЫ ИСПДн В ДЕЙСТВИЕ

При подготовке к проведению Исполнителем работ со стороны Заказчика необходимо обеспечить следующее:

- назначить ответственное лицо от Заказчика, наделенное соответствующими полномочиями, для обеспечения выполнения работ Исполнителем;
- определить ответственного от Заказчика для организации и проведения интервьюирования;
- обеспечить промежутки времени доступности лиц, с которыми необходимо провести интервьюирование (перечень лиц, подлежащих интервьюированию, определяется Исполнителем на основании письменного запроса в адрес Заказчика).

7. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

7.1. Исполнителем при разработке защиты ИСПДн должны быть подготовлены следующие документы:

- Положение об обработке персональных данных;
- Перечень сведений, содержащих персональные данные;
- Регламент по резервному копированию.

7.2. Отчетные документы предоставляются Заказчику в электронном виде в формате документов Microsoft Office и на бумажных носителях.

8. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ И ОГРАНИЧЕНИЯ

8.1. В случае поставки и внедрения технических средств защиты третьей стороной до начала работ по аттестации, Заказчик согласует с Исполнителем следующее:

- состав и спецификацию технических средств;
- состав сопроводительной документации к техническим средствам и сертификатов;

- схемы установки и подключения;
- настройки аппаратно-программных средств;
- рабочую документацию этапа внедрения.

8.2. Срок поставки и внедрения технических средств защиты не входит в расчет сроков этапов работ.

8.3. В случае задержки по срокам предоставления исходных данных при проведении работ, или неполного предоставления информации со стороны Заказчика, по согласованию сторон возможен перенос сроков выполнения работ по договору в сторону увеличения.

ПРИЛОЖЕНИЕ З

Для построения диаграммы Ганта сначала определим перечень задач и их сроки (с учетом выходных дней).

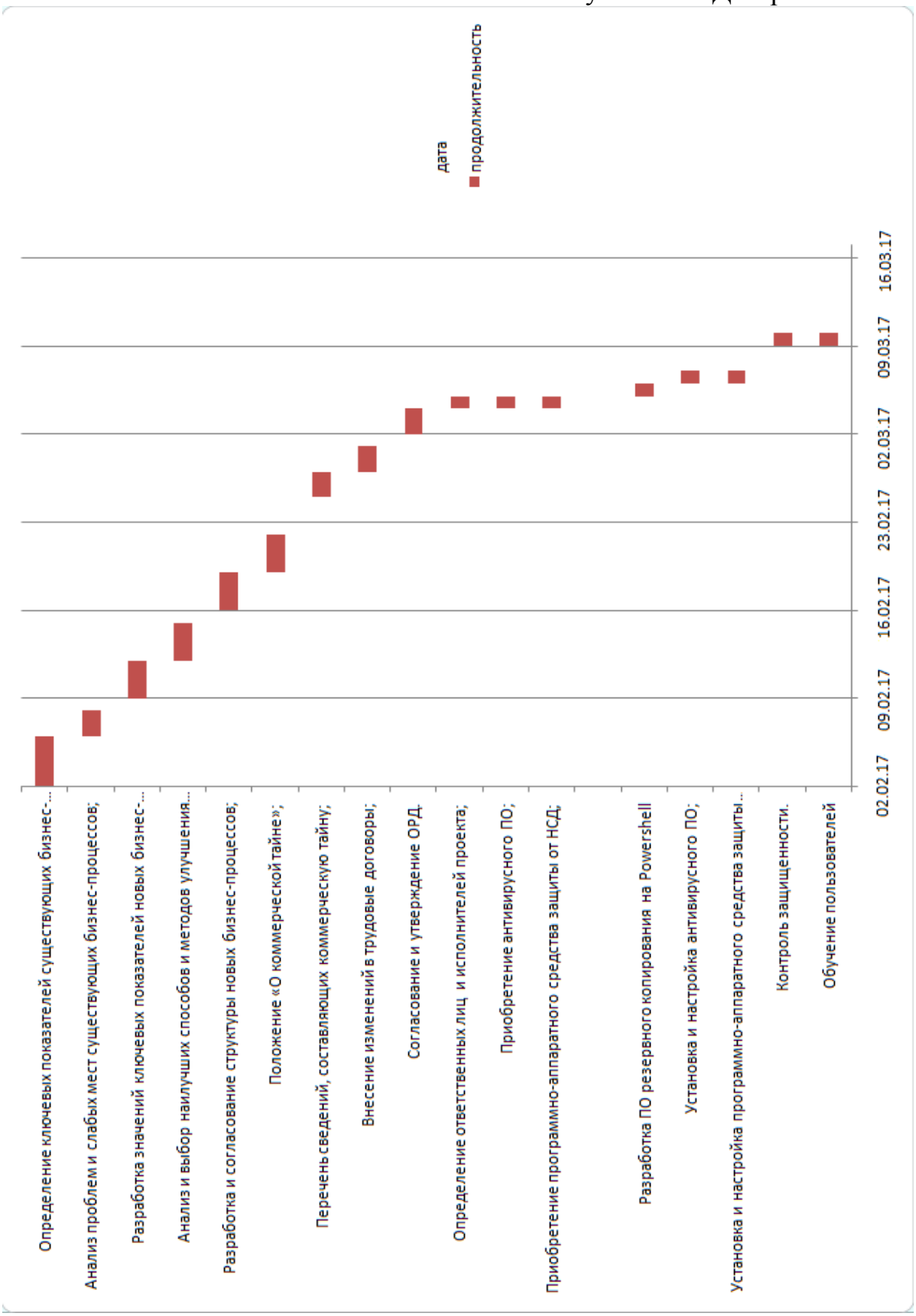
Таблица 3.1 Перечень задач и сроков

Работы	Название работы	Длительность	Начало	Окончание
1	Проектирование	15	02.02.2017	15.02.2017
1.1	Определение ключевых показателей существующих бизнес-процессов с точки зрения ИБ;	4	02.02.2017	06.02.2017
1.2	Анализ проблем и слабых мест существующих бизнес-процессов;	2	06.02.2017	09.02.2017
1.3	Разработка значений ключевых показателей новых бизнес-процессов;	3	09.02.2017	12.02.2017
1.4	Анализ и выбор наилучших способов и методов улучшения значений ключевых показателей бизнес-процессов;	3	12.02.2017	16.02.2017
1.5	Разработка и согласование структуры новых бизнес-процессов;	3	16.02.2017	19.02.2017
2	Совершенствование организационно-распорядительной документации	7	19.02.2017	26.02.2017
2.1	Положение «Об обработке персональных данных»;	3	19.02.2017	25.02.2017
2.2	Перечень сведений, содержащих персональные данные;	2	25.02.2017	27.02.2017
2.3	Внесение изменений в трудовые договоры;	2	27.02.2017	02.03.2017
2.4	Согласование и утверждение ОРД.	2	02.03.2017	04.03.2017
3	Подготовка реализации проекта модернизации защиты ИСПДн	2	04.03.2017	06.03.2017

Работы	Название работы	Длительность	Начало	Окончание
3.1	Определение ответственных лиц и исполнителей проекта;	1	04.03.2017	05.03.2017
3.2	Приобретение антивирусного ПО;	1	04.03.2017	05.03.2017
3.3	Приобретение программно-аппаратного средства защиты от НСД;	1	04.03.2017	05.03.2017
3.4	Разработка ПО резервного копирования на Powershell	1	05.03.2017	06.03.2017
4	Внедрение	2	06.03.2017	10.03.2017
4.1	Установка и настройка антивирусного ПО;	1	06.03.2017	09.03.2017
4.2	Установка и настройка программно-аппаратного средства защиты от НСД;	1	06.03.2017	09.03.2017
4.3	Контроль защищенности.	1	09.03.2017	10.03.2017
4.4	Обучение пользователей	1	09.03.2017	10.03.2017
Проект модернизации защиты ИСПДн		25	02.02.2017	10.03.2017

На основе этих данных мы можем построить диаграмму Ганта, представленную на рисунке 3.1.

Рисунок 3.1 – Диаграмма Ганта



ПРИЛОЖЕНИЕ И

Сетевой график

Для своевременного выполнения работ, а также соответствия плану работ необходимо определить сроки выполнения работ (составить расписание выполнения работ) (Таблица И.1).

i-j – Код работы

T – длительность работы, дней

$\mathbf{T_{рн}}$ – ранний срок начала работы

$\mathbf{T_{пн}}$ – поздний срок начала работы

$\mathbf{T_{ро}}$ – ранний срок окончания работы

$\mathbf{T_{по}}$ – поздний срок окончания работы

Таблица И.1 Расписание выполнения работ

i-j	Название работы	T	$T_{рн}$	$T_{пн}$	$T_{ро}$	$T_{по}$
	Проектирование	15	0	0	15	15
1-2	Определение ключевых показателей существующих бизнес-процессов с точки зрения ИБ;	4	0	0	4	4
2-3	Анализ проблем и слабых мест существующих бизнес-процессов;	2	4	4	6	6
3-4	Разработка значений ключевых показателей новых бизнес-процессов;	3	6	6	9	9
4-5	Анализ и выбор наилучших способов и методов улучшения значений ключевых показателей бизнес-процессов;	3	9	9	12	12
5-6	Разработка и согласование структуры новых бизнес-процессов;	3	12	12	15	15
	Совершенствование организационно-распорядительной документации	7	15	15	22	22

i-j	Название работы	T	$T_{рн}$	$T_{пн}$	$T_{ро}$	$T_{по}$
6-7	Положение «Об обработке персональных данных»;	3	15	15	18	18
7-8	Перечень сведений, содержащих персональные данные;	2	18	18	20	20
8-9	Внесение изменений в трудовые договоры;	2	20	20	22	22
9-10	Согласование и утверждение ОРД.	2	22	22	24	24
	Подготовка реализации проекта модернизации защиты ИСПДн	2	24	24	26	26
10-11	Определение ответственных лиц и исполнителей проекта;	1	24	24	25	25
10-12	Приобретение антивирусного ПО;	1	24	24	25	25
12-13	Приобретение программно-аппаратного средства защиты от НСД;	1	24	24	25	25
13-14	Разработка ПО резервного копирования на Powershell	1	25	25	26	26
	Внедрение	2	26	26	28	28
14-15	Установка и настройка антивирусного ПО;	1	26	26	27	27
15-16	Установка и настройка программно-аппаратного средства защиты от НСД;	1	26	26	27	27
16-17	Контроль защищенности.	1	27	27	28	28
17-18	Обучение пользователей	1	27	27	28	28