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»

РАБОТА ПРОВЕРЕНА
Рецензент, начальник отдела кадров
ГБУЗ «ОПТД № 8» г. Южноуральск
_____ Е.Ю. Федорова
_____ 2018 г.

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2018 г.

Разработка системы защиты персональных данных в государственном бюджетном учреждении здравоохранения «Областной противотуберкулезный диспансер № 8» города Южноуральска

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.05.03.2018.273.ПЗ ВКР

Консультант

Безопасность жизнедеятельности,
к.т.н., доцент
_____ Н.В. Глотова
_____ 2018 г.

Руководитель проекта,
ген. директор ООО «Диджитер»
_____ С.А. Сабельников
_____ 2018 г.

Автор проекта,
студент группы КЭ-530
_____ О.И. Суркова
_____ 2018 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2018 г.

Челябинск 2018

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»

Специальность 10.05.03 «Информационная безопасность автоматизированных систем»

УТВЕРЖДАЮ

Заведующий кафедрой

_____ А.Н. Соколов

_____ 2018 г.

З А Д А Н И Е

на выпускную квалификационную работу студента

Сурковой Оксаны Игоревны

Группа *КЭ-530*

1 Тема работы

Разработка системы защиты персональных данных в государственном бюджетном учреждении здравоохранения «Областной противотуберкулезный диспансер № 8» города Южноуральска

Утверждена приказом ректора ЮУрГУ от _____ № _____
(утверждена, прот. заседания кафедры от _____ № _____)

2 Срок сдачи студентом законченной работы *30.05.2018*

3 Исходные данные к работе

Отчет о преддипломной практике, нормативно-правовые документы в области защиты информации, документация учреждения-базы практики

4 Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов)

4.1 Анализ состояния защиты ГБУЗ «ОПТД № 8» и существующие проблемы;

4.2 Теоретическое обоснование выбора средств защиты;

4.3 Разработка проекта создания системы защиты персональных данных в ГБУЗ «ОПТД № 8»

5 Перечень графического материала (с точным указанием обязательных чертежей, плакатов в листах формата А1)

Презентация «Разработка системы защиты персональных данных в государственном бюджетном учреждении здравоохранения «Областной противотуберкулезный диспансер № 8» города Южноуральска» в формате PowerPoint 2007 (pptx).

Всего ___ листов

6 Консультанты по работе (проекту), с указанием относящихся к ним разделов работы (проекта)

Раздел	Консультант	Подпись, дата	
		Задание выдал (консультант)	Задание принял (студент)
Безопасность жизнедеятельности	Н.В. Глотова		

7 Дата выдачи задания *25 января 2018*

Руководитель,
ген. директор ООО «Диджитер» _____ С.А. Сабельников

Задание принял к исполнению _____О.И. Суркова

КАЛЕНДАРНЫЙ ПЛАН

Наименование этапов выпускной квалификационной работы (проекта)	**Срок выполнения этапов работы**	**Отметки о выполнении руководителя**
Введение		
1 Анализ состояния защиты ГБУЗ «ОПТД № 8» и существующие проблемы		
2 Теоретическое обоснование выбора средств защиты		
3 Разработка проекта создания системы защиты персональных данных в ГБУЗ «ОПТД № 8»		
4 Безопасность жизнедеятельности		
Заключение		
Библиографический список		
Предзащита ВКР		
Защита ВКР		

Заведующий кафедрой _____ А.Н. Соколов

Руководитель работы _____ С.А. Сабельников

Студент _____ О.И. Суркова

АННОТАЦИЯ

Суркова О.И. Разработка системы защиты персональных данных в государственном бюджетном учреждении здравоохранения «Областной противотуберкулезный диспансер № 8» города Южноуральска – Челябинск: ЮУрГУ, КЭ-530, 135 с., 3 ил., 17 табл., библиогр. список – 16 наим., 15 прил.

Выпускная квалификационная работа выполнена с целью разработки системы защиты персональных данных в государственном бюджетном учреждении здравоохранения «Областной противотуберкулезный диспансер № 8» города Южноуральска. Работа состоит из четырех глав.

В первой главе были проанализированы процессы обработки информации, определены информационные системы персональных данных «Бухгалтерия и кадры» и «Медицина» и реализованные в них меры по защите информации. Рассмотрены актуальные угрозы безопасности персональных данных, а также составлены технические задания на создание системы защиты персональных данных и перечень обрабатываемых персональных данных.

Во второй главе было приведено теоретическое обоснование выбора средств защиты информации в соответствии с актуальными угрозами безопасности персональных данных.

В третьей главе был разработан проект создания системы защиты персональных данных. Определены основные этапы реализации проекта и проведен расчет рисков.

В четвертой главе обозначены требования по безопасности жизнедеятельности.

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ 9
ВВЕДЕНИЕ 10
1. АНАЛИЗ СОСТОЯНИЯ ЗАЩИТЫ ГБУЗ «ОПТД № 8» И СУЩЕСТВУЮЩИЕ ПРОБЛЕМЫ 11
1.1. Определение информационных систем 11
1.2. Разработка моделей деятельности 11
1.3. Выявление защищаемой информации 11
1.4. Описание информационных систем 12
1.5. Реализованные меры по защите персональных данных 16
1.6. Выявление объектов защиты 17
1.7. Разработка моделей угроз и уязвимостей 17
1.7.1. Угрозы безопасности персональных данных 18
1.7.2. Расчет рисков важных объектов защиты 23
1.7.2.1. Исходный уровень защищенности 23
1.7.2.2. Реализуемость угроз 24
1.7.2.3. Оценка опасности угроз 26
1.7.2.4. Определение актуальных угроз 28
1.8. Разработка технических заданий 29
1.9. Вывод по первой главе 29
2. ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ ВЫБОРА СРЕДСТВ ЗАЩИТЫ 31
2.1. Требуемые меры по защите персональных данных 31
2.2. Обзор возможных методов устранения уязвимостей 31
2.2.1. Угрозы, связанные с несанкционированным доступом 31
2.2.1.1. Кража носителей информации 31
2.2.1.2. Действия вредоносных программ (вирусов) 32
2.2.1.3. Установка ПО, не связанного с исполнением служебных обязанностей на рабочем месте 33
2.2.2. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн 34
2.2.2.1. Утрата ключей и атрибутов доступа 35
2.2.2.2. Непреднамеренная модификация или уничтожение информации сотрудниками 35
2.2.2.3. Непреднамеренное отключение средств защиты 36
2.3. Вывод по второй главе 36
3. РАЗРАБОТКА ПРОЕКТА СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГБУЗ «ОПТД № 8» 38
3.1. Описание объекта 38
3.2. Резюме проекта 38
3.3. Цели и задачи проекта 38
3.4. Объекты поставки проекта 39
3.5. Расчет рисков проекта 40
3.6. Структура разбиения работ 41

3.7. Структурная схема организации проекта 42
3.8. Матрица ответственности 42
3.9. Диаграмма Ганта и сетевой график 43
3.10. Вывод по третьей главе 44
4. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ 45
4.1. Требования к организации рабочего места 45
4.2. Требования к микроклимату 47
4.3. Требования к уровню шума 48
4.4. Требования к освещенности 48
4.5. Требования по электробезопасности 49
4.6. Требования по пожарной безопасности 49
4.7. Рекомендации по организации режима труда и отдыха 51
4.8. Вывод о соответствии рабочего места требованиям по охране труда 52
4.9. Вывод по четвертой главе 53
ЗАКЛЮЧЕНИЕ 54
БИБЛИОГРАФИЧЕСКИЙ СПИСОК 55
ПРИЛОЖЕНИЕ А 57
ПРИЛОЖЕНИЕ Б 58
ПРИЛОЖЕНИЕ В 59
ПРИЛОЖЕНИЕ Г 66
ПРИЛОЖЕНИЕ Д 79
ПРИЛОЖЕНИЕ Е 82
ПРИЛОЖЕНИЕ Ж 86
ПРИЛОЖЕНИЕ З 98
ПРИЛОЖЕНИЕ И 109
ПРИЛОЖЕНИЕ К 112
ПРИЛОЖЕНИЕ Л 114
ПРИЛОЖЕНИЕ М 115
ПРИЛОЖЕНИЕ Н 125
ПРИЛОЖЕНИЕ О 129
ПРИЛОЖЕНИЕ П 133

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

АРМ – автоматизированное рабочие место;
ВТСС – вспомогательные технические средства и системы;
ИСПДн – информационная система персональных данных;
НДВ – недекларированные возможности;
НСД – несанкционированный доступ;
ОС – операционная система;
ГБУЗ «ОПТД № 8» – государственное бюджетное учреждение здравоохранения «Областной противотуберкулезный диспансер № 8»;
ОТСС – основные технические средства и системы;
ПДн – персональные данные;
ПО – программное обеспечение;
ПЭВМ – персональная электронно-вычислительная машина;
РФ – Российская Федерация;
СВТ – средства вычислительной техники;
СЗПДн – система защиты персональных данных;
ТУ – технические условия;
УБПДн – угрозы безопасности персональных данных;
ФАПСИ – Федеральное агентство правительственной связи и информации при Президенте Российской Федерации;
ФЗ – Федеральный закон;
ФСБ – Федеральная служба безопасности;
ФСТЭК – Федеральная служба по техническому и экспортному контролю.

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 [1].

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств [5].

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) [5].

Угроза – действие, которое потенциально может привести к нарушению безопасности. Свойством угрозы является перечень уязвимостей, при помощи которых может быть реализована угроза [1].

Уязвимость – это слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы. Свойствами уязвимости являются: вероятность (простота) реализации угрозы через данную уязвимость и критичность реализации угрозы через данную уязвимость [1].

ВВЕДЕНИЕ

Деятельность медицинских учреждений невозможно представить без обработки персональных данных, так как они работают с пациентами, а также ведут бухгалтерский и кадровый учет. При этом обработка персональных данных сейчас осуществляется как с использованием электронных, так и с использованием бумажных документов.

Государственное бюджетное учреждение здравоохранения «Областной противотуберкулезный диспансер № 8» города Южноуральска (далее – ГБУЗ «ОПТД № 8») оказывает специализированную туберкулезную (противотуберкулезную) медицинскую помощь населению. Учреждение организует профилактическую работу, а также проводит обследования, лечение и реабилитацию больных в амбулаторных и стационарных условиях.

Актуальность данной работы обусловлена необходимостью разработки системы защиты персональных данных в ГБУЗ «ОПТД № 8».

Объектом выпускной квалификационной работы является ГБУЗ «ОПТД № 8».

Предметом выпускной квалификационной работы являются информационные системы персональных данных в данном учреждении.

Целью дипломной работы является организация защиты персональных данных в ГБУЗ «ОПТД № 8».

В соответствии с поставленной целью необходимо решить следующие задачи:

1. Определить информационные системы персональных данных ГБУЗ «ОПТД № 8» и проанализировать их с целью определения актуальных угроз и уязвимостей;
2. Провести анализ и теоретическое обоснование выбора средств защиты информации;
3. Разработать проект по созданию системы защиты персональных данных в ГБУЗ «ОПТД № 8».

1 АНАЛИЗ СОСТОЯНИЯ ЗАЩИТЫ ГБУЗ «ОПТД № 8» И СУЩЕСТВУЮЩИЕ ПРОБЛЕМЫ

1.1 Определение информационных систем

В целях создания системы защиты персональных данных было проведено предпроектное обследование ГБУЗ «ОПТД № 8». В ходе данного обследования в качестве объектов защиты были выделены 2 информационные системы:

– ИСПДн «Бухгалтерия и кадры»;

– ИСПДн «Медицина».

Для данных информационных систем были составлены акты определения уровня защищенности персональных данных (Приложение А, Приложение Б) на основе Постановления Правительства РФ № 1119 от 01.11.2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [14].

ИСПДн «Бухгалтерия и Кадры» присвоен 4 уровень защищенности персональных данных.

ИСПДн «Медицина» присвоен 3 уровень защищенности персональных данных.

1.2 Разработка моделей деятельности

В ходе анализа работы ГБУЗ «ОПТД № 8» были построены модели деятельности для каждой информационной системы (Приложение Д). В моделях деятельности отражаются основные бизнес-процессы учреждения, процессы управления, входная и выходная информация.

Данная модель окажется полезной при построении эффективной системы защиты процессов и ее модернизации в дальнейшем.

1.3 Выявление защищаемой информации

Информацией, подлежащей защите в ИСПДн "Бухгалтерия и кадры", являются персональные данные работников, бывших работников, родственников работников, кандидатов на замещение вакантных должностей, контрагентов и представителей юридических лиц.

В ИСПДн "Медицина" подлежат защите персональные данные пациентов и их законных представителей.

В ходе аналитической работы с информацией, обрабатываемой в ГБУЗ «ОПТД №8», а также с организационно-распорядительной документацией медицинской организации был определен перечень обрабатываемых персональных данных (Приложение Е «Перечень обрабатываемых персональных данных»).

1.4 Описание информационных систем

Система защиты персональных данных в ГБУЗ "ОПТД №8" должна основываться на организационных, правовых и программно-аппаратных мерах.

К организационным мерам относится определение актуальных угроз безопасности персональных данных при обработке в ИСПДн, определение контролируемой зоны, назначение должностного лица, ответственного за организацию обработки персональных данных, назначение должностного лица, ответственного за обеспечение безопасности персональных данных в информационных системах, утверждение перечня лиц, доступ которых к персональным данным необходим для выполнения ими служебных (трудовых) обязанностей.

Также должны быть разработаны и утверждены следующие документы:

– политика обработки и защиты персональных данных;

– должностные инструкции персонала;

– инструкция пользователей ИСПДн;

– инструкция ответственного за организацию обработки персональных данных;

– инструкция ответственного за обеспечение безопасности персональных данных в информационных системах;

– инструкция по организации парольной защиты;

– инструкция по организации антивирусной защиты;

– а также другие организационно-распорядительные документы.

К правовым мерам относятся нормативно-правовые документы, которые регулируют деятельность учреждения в области обеспечения защиты информации.

К таким документам относятся:

1) Федеральные законы:

– Федеральный закон № 152-ФЗ от 27.07.2006 «О персональных данных» [5];

– Федеральный закон № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации» [7].

2) Документы, устанавливающие требования к мерам и средствам защиты персональных данных:

– Постановление Правительства РФ № 1119 от 01.11.2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [14];

– Приказ ФСТЭК № 21 от 18.02.2013 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [10].

3) Документы, регламентирующие неавтоматизированную обработку персональных данных:

– Постановление Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» [13].

4) Документы, регламентирующие деятельность медицинских учреждений:

– Федеральный закон № 323-ФЗ от 21.11.2011 «Об основах охраны здоровья граждан в Российской Федерации» [8].

5) Документы, необходимые для составления моделей угроз:

– «Базовая модель угроз персональных данных при их обработке в ИСПДн» (Утверждена Заместителем директора ФСТЭК России 15.02.2008) [1];

– «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Утверждена Заместителем директора ФСТЭК России 14.02.2008) [4].

6) Документы, регламентирующие применение средств криптографической защиты информации:

– Приказ ФСБ № 378 от 10.07.2014 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» [11];

– Приказ ФАПСИ № 152 от 13.06.2001 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» [9].

К программно-аппаратным мерам относится комплекс программно-аппаратных средств, обеспечивающих работу ИСПДн и защиту информации. В ходе выполнения ВКР была проведена инвентаризация всего оборудования и программного обеспечения ГБУЗ «ОПТД №8». Состав ОТСС, ВТСС и сетевого оборудования отображен в Таблицах 1 и 2, перечень ПО – в Таблице 3.

Таблица 1 – Аппаратное обеспечение ИСПДн «Бухгалтерия и кадры»

№	Тип	Наименование (модель)
1	2	3
ОТСС		
АРМ Кадры		
1.1	Системный блок	Intel(R) Celeron(R) CPU E1600 @ 2.40GHz/ 2048MB/ 149.0GB
1.2	Монитор	Acer V206HQLBb
1.3	Мышь	A4tech OP-620D
1.4	Клавиатура	Genius KB-M200
1.5	Принтер	Canon Laser Shot LBP1120
АРМ Главный бухгалтер		
2.1	Системный блок	Intel(R) Core(TM) i3-2100 CPU @ 3.10GHz/ 3816MB / 232.9GB
2.2	Монитор	Acer V206HQLBb
2.3	Мышь	Logitech M100

Продолжение таблицы 1.

1	2	3
2.4	Клавиатура	Sven Standard 307M
2.5	Принтер	Canon i-SENSYS LBP6200d
АРМ Бухгалтер		
3.1	Системный блок	Intel(R) Celeron(R) CPU G530 @ 2.40GHz/ 1762MB/ 232.9GB
3.2	Монитор	Acer V206HQLBb
3.3	Мышь	A4tech OP-620D
3.4	Клавиатура	Defender Element HB-520
3.5	Принтер	Canon i-SENSYS LBP6200d
Сетевое оборудование		
4.1	Роутер	TP-Link TL-WR841N
ВТСС		
5	Телефонный аппарат	Panasonic KX-TS2352RU
6	Телефонный аппарат	Panasonic KX-TG1611RUH
7	Извещатель охранный объемный оптико-электронный	Астра-517
8	Прибор приемно-контрольный охранно-пожарный	Астра-712/1
9	Оповещатель охранно-пожарный комбинированный свето-звуковой	МАЯК-12К

Таблица 2 – Аппаратное обеспечение ИСПДн «Медицина»

№	Тип	Наименование (модель)
1	2	3
ОТСС		
АРМ Фтизиатр		
1.1	Системный блок	Intel(R) Celeron(R) CPU E3400 @ 2.60GHz/ 1024MB/ 149.0GB
1.2	Монитор	Acer V206HQLBb
1.3	Мышь	A4tech OP-620D
1.4	Клавиатура	Genius KB-M200
1.5	Принтер	Canon Laser Shot LBP1120
АРМ Фтизиатр 2		
2.1	Системный блок	Intel(R) Celeron(R) CPU E3400 @ 2.60GHz/ 1024MB/ 149.0GB
2.2	Монитор	Acer V206HQLBb
2.3	Мышь	Logitech M100
2.4	Клавиатура	Sven Standard 307M
АРМ Детский фтизиатр		
3.1	Системный блок	Intel(R) Celeron(R) CPU E3400 @

Продолжение таблицы 2.

1	2	3
		2.60GHz/ 1024MB/ 149.0GB
3.2	Монитор	Acer V206HQLBb
3.3	Мышь	Logitech M100
3.4	Клавиатура	Sven Standard 307M
АРМ Медстатистик		
4.1	Системный блок	Intel(R) Celeron(R) CPU G530 @ 2.40GHz/ 2048MB/ 698.6GB
4.2	Монитор	Acer V206HQLBb
4.3	Мышь	Logitech M100
4.4	Клавиатура	Sven Standard 307M
4.5	Принтер	Canon i-SENSYS LBP6200d
АРМ Регистратура		
5.1	Системный блок	Intel(R) Celeron(R) CPU G530 @ 2.40GHz/ 1762MB/ 232.9GB
5.2	Монитор	Acer V206HQLBb
5.3	Мышь	A4tech OP-620D
5.4	Клавиатура	Defender Element HB-520
5.5	Принтер	Canon i-SENSYS MF4410
АРМ Старшая медсестра		
6.1	Системный блок	Intel(R) Celeron(R) CPU E3400 @ 2.60GHz/ 1024MB/ 149.0GB
6.2	Монитор	Acer V206HQLBb
6.3	Мышь	Logitech M100
6.4	Клавиатура	Sven Standard 307M
6.5	Принтер	Canon i-SENSYS LBP6200d
АРМ Ординаторская		
7.1	Системный блок	Intel(R) Celeron(R) CPU E3400 @ 2.60GHz/ 1024MB/ 149.0GB
7.2	Монитор	Acer V206HQLBb
7.3	Мышь	Logitech M100
7.4	Клавиатура	Sven Standard 307M
Сетевое оборудование		
8.1	Роутер	D-Link DIR-632
8.2	Роутер	D-Link DIR-300
ВТСС		
9	Телефонный аппарат	Panasonic KX-TG1711
10	Телефонный аппарат	Panasonic KX-TG1611RUH
11	Извещатель охранный объемный оптико-электронный	Астра-517
12	Прибор приемно-контрольный охранно-пожарный	Астра-712/1

Продолжение таблицы 2.

1	2	3
13	Оповещатель охранно-пожарный комбинированный свето-звуковой	МАЯК-12К

Таблица 3 – Программное обеспечение

№	Название	Версия
ИСПДн «Бухгалтерия и кадры»		
1	Microsoft Windows 7 Professional	6.1.7601.23403
2	Microsoft Office	2007
3	Mozilla Firefox	52.2.1
4	АРМ Медицинский персонал	1.5.6
5	VipNet Client	3.2
6	КриптоПро CSP	4.0.9758
7	1С: Предприятие	8.3.9.1818
8	Налогоплательщик ЮЛ	4.54
9	АРМ "Подготовка расчётов для ФСС"	2.0.4.03
ИСПДн «Медицина»		
1	Mozilla Firefox	52.2.1
2	VipNet Client	3.2
3	Microsoft Windows 7 Professional	6.1.7601.23403
4	OpenOffice	4.1.1
5	Microsoft Office	2007
6	КриптоПро CSP	4.0.9758

1.5 Реализованные меры по защите персональных данных

На момент проведения предпроектного обследования в ГБУЗ «ОПТД № 8» были внедрены средства криптографической защиты информации:

В ИСПДн «Бухгалтерия и кадры» - КриптоПро CSP 4.0 на АРМ Главного бухгалтера и АРМ Бухгалтера.

В ИСПДн «Медицина» - КриптоПро CSP 4.0 на АРМ Старшей медсестры.

На всех АРМ ИСПДн «Бухгалтерия и кадры» и «Медицина» - ViPNet Client 3.2 (КС 2).

Сертификат соответствия ФСБ на программный комплекс ViPNet Client 3.2 (КС 2) истек 30 ноября 2017 года. Работами по обновлению данного средства криптографической защиты в медицинских учреждениях Челябинской области занимается ГБУЗ «Челябинский областной медицинский информационно-аналитический центр», поэтому переход на актуальную версию ViPNet Client не будет рассматриваться в выпускной квалификационной работе.

В ГБУЗ «ОПТД № 8» выполняются требования Приказа ФСБ России от 10 июля 2014 №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» [11] и Приказа ФАПСИ от 13 июня 2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» [9].

Также в зданиях ГБУЗ «ОПТД № 8» установлены охранная и пожарная сигнализации.

1.6 Выявление объектов защиты

На основе изучения технологического процесса обработки информации, составления перечней аппаратного и программного обеспечения, моделей деятельности и перечня обрабатываемых персональных данных можно выделить следующие важные объекты защиты:

– автоматизированные рабочие места, на которых обрабатываются персональные данные: в ИСПДн «Бухгалтерия и кадры» - 3, в ИСПДн «Медицина» - 7;

– средства ввода-вывода информации;

– носители информации;

– линии и средства связи, обеспечивающие беспрерывное функционирование организации;

– персонал.

1.7 Разработка моделей угроз и уязвимостей

На основании анализа ИСПДн составляется модель угроз безопасности персональных данных. В данном документе дается описание угроз безопасности, которым подвержена информационная система. При этом в модели угроз безопасности персональных данных учитываются особенности ИСПДн, такие как программные, программно-технические, технические средства, а также процессы обработки информации.

Для создания моделей угроз и уязвимостей были использованы следующие документы:

– «Базовая модель угроз персональных данных при их обработке в ИСПДн» (Утверждена Заместителем директора ФСТЭК России 15.02.2008) [1];

– «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Утверждена Заместителем директора ФСТЭК России 14.02.2008) [4].

1.7.1 Угрозы безопасности персональных данных

Подробное описание угроз приведено в Таблице 4. Вероятность реализации угроз рассматривалась сразу для обеих ИСПДн.

Таблица 4 – Описание и вероятность реализации угроз безопасности

№	Наименование угрозы	Описание	Вероятность реализации
1	2	3	4
1	Угрозы утечки по техническим каналам		
1.1	Угроза утечки видовой информации	Данная угроза реализуется, когда внешнему или внутреннему нарушителю удается несанкционированно подсмотреть информацию у пользователя ИСПДн	Маловероятна
1.2	Угроза утечки акустической информации	Данная угроза реализуется, когда внешнему или внутреннему нарушителю удается подслушать речь пользователя ИСПДн при обработке данных	Маловероятна
1.3	Угрозы утечки информации по каналам ПЭМИН	Данная угроза реализуется, когда внешний нарушитель перехватывает побочные электромагнитные излучения элементов ИСПДн	Маловероятна
2	Угрозы НСД к информации		
2.1	Угрозы уничтожения, хищения аппаратных средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн		
2.1.1	Кража ПЭВМ	Данная угроза реализуется, когда внешнему или внутреннему нарушителю удается украсть ПЭВМ	Маловероятна
2.1.2	Кража носителей информации	Данная угроза реали-	Высокая

Продолжение таблицы 4.

1	2	3	4
		зуется, когда внешнему или внутреннему нарушителю удается завладеть носителями персональных данных	вероятность
2.1.3	Кражи ключей и атрибутов доступа	Данная угроза реализуется, когда внешнему или внутреннему нарушителю удается завладеть ключами или иными паролями для доступа к ИСПДн	Маловероятна
2.1.4	Кража, модификация, уничтожение информации	Данная угроза реализуется, когда внешнему или внутреннему нарушителю удается завладеть информацией ограниченного доступа	Маловероятна
2.1.5	Вывод из строя узлов ПЭВМ, каналов связи	Данная угроза осуществляется при непосредственном доступе внешнего или внутреннего нарушителя к узлам и каналам связи ИСПДн	Маловероятна
2.2	Угрозы хищения, несанкционированного изменения или блокирования информации за счет НСД с применением программно-аппаратных и программных средств		
2.2.1	Действия вредоносных программ (вирусов)	Данная угроза реализуется в случае, когда вредоносная программа попадает на ПЭВМ, входящую в состав ИСПДн	Высокая вероятность
2.2.2	Недекларированные возможности системного ПО и ПО для обработки ПДн	Данная угроза реализуется в случае, когда у ПО есть функции, которые не	Маловероятна

Продолжение таблицы 4.

1	2	3	4
		описаны в документах к этому ПО	
2.2.3	Установка ПО, не связанного с исполнением служебных обязанностей на рабочем месте	Данная угроза реализуется внутренними нарушителями путем установки на ПЭВМ постороннего ПО, которое не требуется для выполнения своих рабочих обязанностей	Высокая вероятность
2.3	Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и системы защиты из-за сбоев в ПО, а также от угроз неантропогенного и стихийного характера		
2.3.1	Утрата ключей и атрибутов доступа	Данная угроза реализуется в случае, когда пользователь ИСПДн по неосторожности теряет ключи или атрибуты доступа (пароли, личный идентификатор)	Высокая вероятность `
2.3.2	Непреднамеренная модификация или уничтожение информации сотрудниками	Данная угроза реализуется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения правил работы с ИСПДн	Высокая вероятность
2.3.3	Непреднамеренное отключение средств защиты	Данная угроза реализуется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения правил работы с ИСПДн	Высокая вероятность
2.3.4	Выход из строя аппаратно-программных средств	Данная угроза реализуется за счет несовершенства	Средняя вероятность

Продолжение таблицы 4.

1	2	3	4
		аппаратно-программных средств, из-за которых может происходить нарушение целостности и доступности защищаемой информации	
2.3.5	Сбой системы электроснабжения	Данная угроза реализуется за счет несовершенства системы электропитания	Маловероятна
2.3.6	Стихийные бедствия	Данная угроза реализуется в случае стихийных бедствий (пожары, наводнения, землетрясения)	Маловероятна
2.4	Угрозы преднамеренных действий внутренних нарушителей		
2.4.1	Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	Данная угроза реализуется в случае, если внешний или внутренний нарушитель осуществляет НСД к информации ограниченного доступа	Маловероятна
2.4.2	Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Данная угроза реализуется в случае, если пользователь ИСПДн не соблюдает требования по защите информации	Средняя вероятность
2.5	Угрозы несанкционированного доступа по каналам связи		
2.5.1	Угроза "Анализ сетевого трафика"	Данная угроза реализуется в случае использования нарушителем специальной программы-анализатора (сниффера)	Средняя вероятность
2.5.2	Угроза «сканирование сети»	Данная угроза реализуется в случае, когда нарушитель передает запросы се-	Средняя вероятность

Продолжение таблицы 4.

1	2	3	4
		тевым службам хостов ИСПДн и анализирует ответы от них с целью выявления используемых протоколов и доступных портов	
2.5.3	Угроза выявления паролей по сети	Данная угроза реализуется в случае, когда нарушитель пытается совершить взлом парольной защиты	Маловероятна
2.5.4	Угрозы навязывание ложного маршрута сети	Данная угроза реализуется в случае, когда нарушитель производит внутрисегментное или межсегментное навязывание ложного маршрута сети	Маловероятна
2.5.5	Угрозы подмены доверенного объекта в сети	Данная угроза реализуется в случае, когда нарушитель передает данные под именем доверенного пользователя	Маловероятна
2.5.6	Угрозы внедрения ложного объекта	Данная угроза подразумевает использование недостатков алгоритма удаленного поиска и изменение маршрутно-адресных данных, что может привести к перехвату всего потока информации	Маловероятна
2.5.7	Угрозы типа "Отказ в обслуживании"	Данная угроза реализуется в случае, когда нарушитель перегружает систему пакетами запросов	Маловероятна

Продолжение таблицы 4.

1	2	3	4
2.5.8	Угрозы удаленного запуска приложений	Данная угроза реализуется в случае, когда нарушитель пытается через хост запустить предварительно внедренные вредоносные программы	Средняя вероятность
2.5.9	Угрозы внедрения по сети вредоносных программ	Данная угроза реализуется в случае внедрения вредоносных программ через сеть Интернет	Средняя вероятность

1.7.2 Расчет рисков важных объектов защиты

На основе «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК был выполнен расчет рисков важных объектов защиты ГБУЗ «ОПТД № 8». С помощью этих расчетов можно определить наиболее уязвимые места информационных систем.

1.7.2.1 Исходный уровень защищенности

Для оценки актуальности угроз необходимо учитывать уровень исходной защищенности ИСПДн. В Таблице 5 представлены показатели исходной защищенности ИСПДн «Бухгалтерия и кадры», а в Таблице 6 – ИСПДн «Медицина».

Таблица 5 – Исходный уровень защищенности ИСПДн «Бухгалтерия и кадры»

Технические и эксплуатационные характеристики	Уровень защищенности
По территориальному размещению	Высокий
По наличию соединения с сетями общего пользования	Средний
По встроенным операциям с записями баз ПДн	Низкий
По разграничению доступа к персональным данным	Средний
По наличию соединений с другими базами ПДн иных ИСПДн	Высокий
По уровню (обезличивания) ПДн	Низкий
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	Средний

Таблица 6 – Исходный уровень защищенности ИСПДн «Медицина»

Технические и эксплуатационные характеристики	Уровень защищенности
По территориальному размещению	Средний
По наличию соединения с сетями общего пользования	Средний
По встроенным операциям с записями баз ПДн	Низкий
По разграничению доступа к персональным данным	Средний
По наличию соединений с другими базами ПДн иных ИСПДн	Высокий
По уровню (обезличивания) ПДн	Низкий
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	Средний

Согласно данным, отображенным в Таблицах 5 и 6, ИСПДн «Бухгалтерия и кадры» и ИСПДн «Медицина» имеют средний уровень исходной защищенности. Такой вывод основан на том, что более 70% характеристик соответствуют уровню не ниже «средний», но менее 70% характеристик ИСПДн соответствуют уровню «высокий». Числовой коэффициент среднего уровня исходной защищенности равен 5 (Y1 = 5).

1.7.2.2 Реализуемость угроз

Далее определяется вероятность реализации угрозы. Числовой коэффициент вероятности реализации угрозы определяется по четырем вербальным показателям вероятности реализации угрозы:

– маловероятно - отсутствие объективных предпосылок для осуществления угроз (Y2 = 0);

– низкая вероятность - существуют объективные предпосылки угрозы, однако, реализация такой угрозы затруднена ввиду принятых мер (Y2 = 2);

– средняя вероятность - существуют объективные предпосылки угрозы, однако принятые меры обеспечения безопасности ПДн недостаточны (Y2 = 5);

– высокая вероятность - существуют объективные предпосылки угрозы и не приняты меры по обеспечению безопасности ПДн (Y2 = 10).

После определения числового коэффициента уровня исходной защищенности и вероятностей реализации угроз необходимо определить коэффициенты реализуемости угрозы *Y*. Для этого используют формулу (1).

$$Y = (Y_1 + Y_2)/20 \qquad (1)$$

где:

Y_1 – коэффициент уровня исходной защищенности;

Y_2 – вероятность реализации угрозы.

После подстановки полученных значений в формулу, были рассчитаны коэффициенты реализуемости для каждой угрозы. Результаты отображены в Таблице 7.

Таблица 7 - Коэффициенты реализуемости угроз в обеих ИСПДн

Наименование угрозы	Коэффициент реализуемости угрозы	Возможность реализации
1	2	3
Угрозы утечки по техническим каналам		
Угроза утечки видовой информации	0,25	низкая
Угроза утечки акустической информации	0,25	низкая
Угрозы утечки информации по каналам ПЭМИН	0,25	низкая
Угрозы НСД к информации		
Угрозы уничтожения, хищения аппаратных средств ИСПДН, носителей информации путем физического доступа к элементам ИСПДН		
Кража ПЭВМ	0,25	низкая
Кража носителей информации	0,75	высокая
Кражи ключей и атрибутов доступа	0,25	низкая
Кража, модификация, уничтожение информации	0,25	низкая
Вывод из строя узлов ПЭВМ, каналов связи	0,25	низкая
Угрозы хищения, несанкционированного изменения или блокирования информации за счет НСД с применением программно-аппаратных и программных средств		
Действия вредоносных программ (вирусов)	0,25	низкая
Недекларированные возможности системного ПО и ПО для обработки ПДн	0,25	низкая
Установка ПО, не связанного с исполнением служебных обязанностей на рабочем месте	0,75	высокая
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и системы защиты из-за сбоев в ПО, а также от угроз неантропогенного и стихийного характера		
Утрата ключей и атрибутов доступа	0,75	высокая
Непреднамеренная модификация или уничтожение информации сотрудниками	0,75	высокая

Продолжение таблицы 7.

1	2	3
Непреднамеренное отключение средств защиты	0,75	высокая
Выход из строя аппаратно-программных средств	0,5	средняя
Сбой системы электроснабжения	0,25	низкая
Стихийные бедствия	0,25	низкая
Угрозы преднамеренных действий внутренних нарушителей		
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	0,25	низкая
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	0,25	низкая
Угрозы несанкционированного доступа по каналам связи		
Угроза "Анализ сетевого трафика"	0,5	средняя
Угроза «сканирование сети»	0,5	средняя
Угроза выявления паролей по сети	0,25	низкая
Угрозы навязывание ложного маршрута сети	0,25	низкая
Угрозы подмены доверенного объекта в сети	0,25	низкая
Угрозы внедрения ложного объекта	0,25	низкая
Угрозы типа "Отказ в обслуживании"	0,25	низкая
Угрозы удаленного запуска приложений	0,5	средняя
Угрозы внедрения по сети вредоносных программ	0,5	средняя

1.7.2.3 Оценка опасности угроз

Оценка опасности УБПДн производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

– низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

– средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

– высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Оценка опасности угроз приведена в Таблице 8.

Таблица 8 - Опасность угроз персональных данных для обеих ИСПДн

Наименование угрозы	Опасность угрозы
1	2
Угрозы утечки по техническим каналам	
Угроза утечки видовой информации	низкая
Угроза утечки акустической информации	низкая
Угрозы утечки информации по каналам ПЭМИН	низкая
Угрозы НСД к информации	
Угрозы уничтожения, хищения аппаратных средств ИСПДН, носителей информации путем физического доступа к элементам ИСПДН	
Кража ПЭВМ	низкая
Кража носителей информации	средняя
Кражи ключей и атрибутов доступа	низкая
Кража, модификация, уничтожение информации	низкая
Вывод из строя узлов ПЭВМ, каналов связи	низкая
Угрозы хищения, несанкционированного изменения или блокирования информации за счет НСД с применением программно-аппаратных и программных средств	
Действия вредоносных программ (вирусов)	средняя
Недекларированные возможности системного ПО и ПО для обработки ПДн	низкая
Установка ПО, не связанного с исполнением служебных обязанностей на рабочем месте	средняя
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и системы защиты из-за сбоев в ПО, а также от угроз неантропогенного и стихийного характера	
Утрата ключей и атрибутов доступа	средняя
Непреднамеренная модификация или уничтожение информации сотрудниками	средняя
Непреднамеренное отключение средств защиты	низкая
Выход из строя аппаратно-программных средств	низкая
Сбой системы электроснабжения	низкая
Стихийные бедствия	низкая
Угрозы преднамеренных действий внутренних нарушителей	

Продолжение таблицы 8.

1	2
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	средняя
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	средняя
Угрозы несанкционированного доступа по каналам связи	
Угроза "Анализ сетевого трафика"	низкая
Угроза «сканирование сети»	низкая
Угроза выявления паролей по сети	низкая
Угрозы навязывание ложного маршрута сети	низкая
Угрозы подмены доверенного объекта в сети	низкая
Угрозы внедрения ложного объекта	низкая
Угрозы типа "Отказ в обслуживании"	низкая
Угрозы удаленного запуска приложений	низкая
Угрозы внедрения по сети вредоносных программ	низкая

1.7.2.4 Определение актуальных угроз

В соответствии с правилами отнесения угрозы безопасности к актуальной, для ИСПДн определяются актуальные и неактуальные угрозы. Правила приведены в Таблице 9.

Таблица 9 – Определение актуальности угроз

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

Перечень актуальных угроз:

– Кража носителей информации;

– Действия вредоносных программ (вирусов);

– Установка ПО, не связанного с исполнением служебных обязанностей на рабочем месте;

– Утрата ключей и атрибутов доступа;

– Непреднамеренная модификация или уничтожение информации сотрудниками;

– Непреднамеренное отключение средств защиты.

1.8 Разработка технических заданий

По результатам предпроектного обследования были составлены технические задания на создание системы защиты для ИСПДн «Медицина» и «Бухгалтерия и кадры» (Приложение Ж, Приложение З).

Для составления технических заданий использовался ГОСТ 34.602-1989 «Техническое задание на создание автоматизированной системы» [3] и приказ ФСТЭК № 21 от 18.02.2013 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [10].

В данном ГОСТе отображены разделы, которые должны быть в технических заданиях, а также требования к оформлению разделов. Любое техническое задание должно включать в себя:

– общие сведения;
– назначение и цели создания системы;
– характеристика объектов защиты;
– требования к системе;
– состав и содержание работ по созданию системы;
– порядок контроля и приемки системы;
– требования к составу и содержанию работ по подготовке объекта защиты к вводу системы в действие;
– требования к документированию;
– источники разработки.

1.9 Вывод по первой главе

В результате проведения обследования ГБУЗ "ОПТД № 8" были выделены две информационные системы персональных данных: "Бухгалтерия и кадры" и "Медицина".

В ИСПДн «Бухгалтерия и кадры» обрабатываются иные категории персональных данных, тип актуальных угроз – 3, уровень защищенности персональных данных – 4.

В ИСПДн «Медицина» обрабатываются специальные категории персональных данных, тип актуальных угроз – 3, уровень защищенности персональных данных – 3.

Для данных ИСПДн были разработаны акты определения уровня защищенности, составлены перечни аппаратного и программного обеспечения и перечень обрабатываемых персональных данных.

Была разработана модель деятельности предприятия, которая необходима для создания эффектной системы защиты персональных данных.

Приведено описание информационных систем и их компонентов. Это позволило выявить перечень объектов защиты.

Были составлены модели угроз, которые отображают уязвимости и позволяют грамотно распределить ресурсы. К актуальным угрозам безопасности персональных данных для обеих ИСПДн относятся:

– Кража носителей информации;

– Действия вредоносных программ (вирусов);

– Установка ПО, не связанного с исполнением служебных обязанностей на рабочем месте;

– Утрата ключей и атрибутов доступа;

– Непреднамеренная модификация или уничтожение информации сотрудниками;

– Непреднамеренное отключение средств защиты.

Результатом проделанной работы являются сформированные технические задания на создание систем защиты ИСПДн «Бухгалтерия и кадры» и «Медицина».

2 ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ ВЫБОРА СРЕДСТВ ЗАЩИТЫ

2.1 Требуемые меры по защите персональных данных

В соответствии с Техническими заданиями на создание системы защиты для ИСПДн «Медицина» и «Бухгалтерия и кадры»(Приложение Ж, Приложение З) определен Перечень требований к функционалу системы защиты персональных данных в ГБУЗ «ОПТД № 8»(Приложение И).

Принимаемые меры в ИСПДн «Бухгалтерия и кадры» и ИСПДн «Медицина» будут различны, так как информационные системы имеют разные уровни защищенности персональных данных.

По требованиям указанного выше Приказа, для обеспечения 4 уровня защищенности персональных данных должны применяться средства вычислительной техники от несанкционированного доступа, сертифицированные по требованиям безопасности информации не ниже 6 класса, а для 3 уровня защищенности – не ниже 5 класса. Для обоих уровней защищенности должны использоваться средства защиты информации, сертифицированные по требованиям безопасности информации не ниже 6 класса.

Различия мер также будут обусловлены тем, что персональные данные в ИСПДн «Медицина» составляют врачебную тайну.

2.2 Обзор возможных методов устранения уязвимостей

При создании системы защиты персональных данных необходимо учитывать имеющиеся актуальные угрозы безопасности персональных данных, определенные в модели угроз (п. 1.7.2.4). На основе их анализа выбираются методы и средства, которые необходимы для устранения угроз и безопасного функционирования информационных систем.

2.2.1 Угрозы, связанные с несанкционированным доступом

В ГБУЗ «ОПТД № 8» были выявлены следующие угрозы, связанные с несанкционированным доступом к информации:

– кража носителей информации;

– действия вредоносных программ (вирусов);

– установка ПО, не связанного с исполнением служебных обязанностей на рабочем месте.

2.2.1.1 Кража носителей информации

Данная угроза может реализоваться в случае, если злоумышленник сможет похитить носитель информации и вынести его за пределы контролируемой зоны.

Многие носители информации хранятся в кабинетах на рабочих столах, в картотеках. Так как помещения ГБУЗ «ОПТД № 8» посещает множество пациентов и

их родственников, перемещение которых не всегда можно отследить, то появляется возможность реализации угрозы. Также нельзя отрицать вероятность того, что и работник лечебного учреждения может случайно или преднамеренно совершить кражу носителя информации. Для снижения вероятности такой угрозы, были выполнены следующие действия:

– организация учета хранения носителей персональных данных;

– разработка инструкции ответственного за безопасность информации в информационных системах;

– разработка инструкции ответственного за организацию обработки персональных данных;

– разработка инструкции пользователя.

В рамках ВКР были разработаны документы:

– Инструкция пользователя (Приложение Н).

2.2.1.2 Действия вредоносных программ (вирусов)

В ГБУЗ «ОПТД № 8» на автоматизированных рабочих местах пользователей отсутствуют сертифицированные средства антивирусной защиты.

Для снижения вероятности реализации угрозы, в учреждении были выполнены следующие действия:

– внедрение антивирусного ПО;

– разработка инструкции пользователя;

– разработка инструкции ответственного за безопасность информации в информационных системах;

– разработка инструкции ответственного за организацию обработки персональных данных;

– разработка инструкции по организации антивирусной защиты;

– обучение пользователей.

В рамках ВКР были разработаны документы:

– Инструкция пользователя (Приложение Н).

– Инструкция по организации антивирусной защиты (Приложение П).

Выбор средства антивирусной защиты основывался на сравнительном анализе существующих продуктов. Критерии сравнения показаны в Таблице 10.

По результатам анализа в качестве антивирусного ПО был выбран Dr.Web Desktop Security Suite исходя из экономической целесообразности.

После ввода данных мер угроза со стороны вредоносного ПО стала минимальной.

Таблица 10 – Сравнение средств антивирусной защиты

Критерии сравнения	Kaspersky Endpoint Security 10 для Windows	ESET NOD32 Secure Enterprise Pack 5.0	Dr.Web Desktop Security Suite
Сертификат ФСТЭК	№3025 до 25.11.2019 ИТ.САВЗ.Б2.ПЗ, ИТ.САВЗ.В2.ПЗ, ИТ.САВЗ.Г2.ПЗ	№3243 до 13.10.2020 ИТ.САВЗ.А4.ПЗ, ИТ.САВЗ.Б4.ПЗ, ИТ.САВЗ.В4.ПЗ, ИТ.САВЗ.Г4.ПЗ	№3509 до 27.01.2019 ИТ.САВЗ.А2.ПЗ, ИТ.САВЗ.Б2.ПЗ, ИТ.САВЗ.В2.ПЗ, ИТ.САВЗ.Г2.ПЗ
Особые условия	Снижение стоимости для медицинских учреждений на 30%	Снижение стоимости для медицинских учреждений на 30%	Снижение стоимости для медицинских учреждений на 50%
Стоимость (за 10 рабочих мест, на 1 год)	13 447	19 075	5 895

2.2.1.3 Установка ПО, не связанного с исполнением служебных обязанностей на рабочем месте

Данная угроза реализуется при установке на АРМ работниками стороннего ПО, которое не требуется для исполнения их служебных обязанностей. Часто такое ПО не является лицензионным или скаченным с проверенных ресурсов.

Для того, чтобы обезопасить ИСПДн от данной угрозы, были выполнены следующие действия:

– внедрение средств защиты информации от несанкционированного доступа;

– внедрение средств анализа защищенности в ИСПДн «Медицина»;

– разработка инструкции пользователя;

– разработка инструкции ответственного за безопасность информации в информационных системах;

– разграничение прав пользователей;

– обучение пользователей.

В рамках ВКР были разработаны документы:

– Инструкция пользователя (Приложение Н).

Выбор средства защиты информации от несанкционированного доступа основывался на сравнительном анализе существующих продуктов. Критерии сравнения показаны в Таблице 11.

По результатам анализа в качестве средства защиты от НСД был выбран Dallas Lock 8.0-K за счет более выгодной стоимости.

Таблица 11 – Сравнение средств защиты от НСД

Критерии сравнения	Secret Net Studio	Dallas Lock 8.0-K	Страж NT 4.0.
Сертификат ФСТЭК	№ 3745 до 16.05.2020 СВТ – 5 НДВ – 4	№ 2720 до 25.09.2018 СВТ – 5 НДВ – 4	№ 3553 до 20.04.2019 СВТ – 3 НДВ – 2
Обеспечиваемый уровень защищенности ПДн	До 1 уровня защищенности включительно	До 1 уровня защищенности включительно	До 1 уровня защищенности включительно
Стоимость (за 10 рабочих мест, бессрочная лицензия)	79 000	69 000	75 000

Внедрение средства анализа защищенности планируется только в ИСПДн «Медицина», так как в ней обрабатываются персональные данные третьего уровня защищенности. Выбор данного продукта основывался на сравнительном анализе существующих продуктов. Критерии сравнения показаны в Таблице 12.

Таблица 12 – Сравнение средств анализа защищенности

Критерии сравнения	XSpider 7.8	RedCheck	Сканер-ВС
Сертификат ФСТЭК	№ 3247 до 24.10.2020 НДВ – 4 ТУ	№ 3172 до 23.06.2020 НДВ – 4 ТУ	№ 2204 до 13.11.2019 НДВ – 4 ТУ
Удобство пользовательского интерфейса	+/-	+	+/-
Стоимость (за 7 ip-адресов, на 1 год)	19 200	11 080	10 000

По результатам анализа в качестве средства анализа защищенности был выбран RedCheck за счет более удобного пользовательского интерфейса.

2.2.2 Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДН

В ГБУЗ «ОПТД № 8» были выявлены следующие угрозы, связанные с непреднамеренными действиями пользователей и нарушений безопасности функционирования ИСПДн:

– утрата ключей и атрибутов доступа;

– непреднамеренная модификация или уничтожение информации сотрудниками;

– непреднамеренное отключение средств защиты.

2.2.2.1 Утрата ключей и атрибутов доступа

Данная угроза реализуется за счет человеческого фактора, когда сотрудники из-за своей халатности теряют ключи или другие атрибуты доступа, к чему также относится компрометация паролей. Работа в информационных системах ГБУЗ «ОПТД № 8» невозможна без аутентификации.

Для сведения данной угрозы к минимуму были выполнены следующие действия:

– разработка инструкции пользователя;

– разработка инструкции по организации парольной защиты

– разработка инструкции ответственного за безопасность информации в информационных системах;

– разработка инструкции ответственного за организацию обработки персональных данных.

В рамках ВКР были разработаны документы:

– Инструкция пользователя (Приложение Н);

– Инструкция по организации парольной защиты (Приложение О).

2.2.2.2 Непреднамеренная модификация или уничтожение информации сотрудниками

Данная угроза также реализуется за счет человеческого фактора, когда работники по неосторожности уничтожают информацию или же модифицируют ее таким образом, что она становится некорректной.

Для снижения вероятности возникновения угроз данного вида были выполнены следующие действия:

– внедрение средств защиты от несанкционированного доступа;

– разработка политики обработки и защиты персональных данных;

– разработка инструкции ответственного за безопасность информации в информационных системах;

– разработка инструкции ответственного за организацию обработки персональных данных;

– разграничение прав пользователей;

– разработка инструкции пользователя;

– обучение пользователей.

В рамках ВКР были разработаны документы:

– Политика обработки и защиты персональных данных (Приложение М);

– Инструкция пользователя (Приложение Н).

Выбор средства защиты информации от несанкционированного доступа основывался на сравнительном анализе существующих продуктов. Критерии сравнения показаны в Таблице 11.

2.2.2.3 Непреднамеренное отключение средств защиты

Данная угроза реализуется в результате халатного отношения сотрудника к правилам работы со средствами защиты информации.

Для сведения данной угрозы к минимуму в ГБУЗ «ОПТД № 8» были предприняты следующие меры:

– внедрение средств анализа защищенности в ИСПДн «Медицина»;

– разработка инструкции пользователя;

– разработка инструкции ответственного за безопасность информации в информационных системах;

– разработка инструкции по организации антивирусной защиты;

– обучение пользователей.

В рамках ВКР были разработаны документы:

– Инструкция пользователя (Приложение Н);

– Инструкция по организации антивирусной защиты (Приложение П).

Выбор средства анализа защищенности основывался на сравнительном анализе существующих продуктов. Критерии сравнения показаны в Таблице 12.

2.3 Вывод по второй главе

В данной главе были определены требуемые меры для нейтрализации актуальных угроз безопасности персональных данных с учетом требований законодательства.

Для снижения вероятности возникновения угроз, связанных с несанкционированным доступом, были выполнены следующие задачи:

– внедрение средств защиты от несанкционированного доступа Dallas Lock 8.0-K;

– внедрение антивирусного ПО Dr.Web Desktop Security Suite;

– внедрение средств анализа защищенности RedCheck (В ИСПДн «Медицина»);

– организация учета хранения носителей персональных данных;

– разработка инструкции пользователя;

– разработка инструкции ответственного за безопасность информации в информационных системах;

– разработка инструкции ответственного за безопасность информации в информационных системах;

– разработка инструкции по организации антивирусной защиты;

– разграничение прав пользователей;

– обучение пользователей.

Для снижения вероятности возникновения угроз, связанных с непреднамеренными действиями пользователей и нарушениями безопасности функционирования ИСПДн, было выполнено:

– внедрение средств защиты от несанкционированного доступа Dallas Lock 8.0-K;

– внедрение средств анализа защищенности RedCheck (В ИСПДн «Медицина»);

– разработка инструкции пользователя;

– разработка инструкции ответственного за безопасность информации в информационных системах;

– разработка инструкции ответственного за безопасность информации в информационных системах;

– разработка инструкции по организации парольной защиты;

– разработка инструкции по организации антивирусной защиты;

– разработка политики обработки и защиты персональных данных;

– разграничение прав пользователей;

– обучение пользователей.

3 РАЗРАБОТКА ПРОЕКТА СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГБУЗ «ОПТД № 8»

3.1 Описание объекта

ГБУЗ «ОПТД № 8» - это государственное учреждение, входящее в систему здравоохранения, и предоставляющее туберкулезную (противотуберкулезную) медицинскую помощь. Деятельность учреждения сопровождается большим количеством информационных потоков. Потоки защищаемой информации представлены в Таблице 13.

Таблица 13 –Потоки защищаемой информации

Входящая	Исходящая
Данные о работниках, родственниках работников, бывших работниках	База данных работников
	Документы по бухгалтерскому учету
	Налоговая отчетность
	Документы по кадровому учету
Данные о пациентах и их законных представителях	База данных пациентов
	Медицинская документация
Данные о контрагентах и представителях юридических лиц	Документы по бухгалтерскому учету
	Налоговая отчетность
	Контракты и договоры
Данные о кандидатах на замещение вакантных должностей	-

3.2 Резюме проекта

Разработка проекта создания системы защиты персональных данных в ГБУЗ «ОПТД № 8» проводилась согласно утвержденным техническим заданиям (Приложение Ж, Приложение З).

В рамках реализации проекта был реализован комплекс организационных и программно-аппаратных мер. Была разработана матрица ответственности, в которой обозначены ответственные лица за выполнение различных этапов проекта. Также были определены объекты поставки и объем поставляемого аппаратно-программного обеспечения.

Результат проекта – система защиты персональных данных в ГБУЗ «ОПТД № 8», состоящая из двух ИСПДн: «Бухгалтерия и кадры» и «Медицина», которые удовлетворяют требованиям нормативных документов по обеспечению информационной безопасности. Данная система сведет к минимуму возможность утечки информации ограниченного доступа.

3.3 Цели и задачи проекта

Цели создания системы защиты персональных данных в ГБУЗ «ОПТД № 8»:

– защита персональных данных в соответствии с требованиями законодательства;

– обеспечение защищенности ИСПДн в процессе обработки и хранения персональных данных, а также обеспечение конфиденциальности, целостности и доступности персональных данных.

Задачи создания системы защиты персональных данных в ГБУЗ «ОПТД № 8»:

– нейтрализация актуальных угроз информационной безопасности.

3.4 Объекты поставки проекта

3.4.1 Организационно-распорядительная документация

Проект создания системы защиты персональных данных предусматривает разработку следующих документов:

– Акты определения уровня защищенности персональных данных информационной системы персональных данных (Приложение А, Приложение Б);

– Технические паспорта (Приложение В, Приложение Г);

– Перечень обрабатываемых персональных данных (Приложение Е);

– Приказ об утверждении списка лиц, доступ которых к защищаемой информации необходим для выполнения служебных (трудовых) обязанностей;

– Инструкция пользователя ИСПДн (Приложение Н);

– Приказ о назначении ответственного за организацию обработки персональных данных;

– Инструкция ответственного за организацию обработки персональных данных;

– Приказ о назначении ответственного за безопасность информации в информационных системах;

– Инструкция ответственного за безопасность информации в информационных системах;

– Инструкция по организации антивирусной защиты (Приложение П);

– Инструкция по организации парольной защиты (Приложение О);

– Приказ об определении границ контролируемой зоны;

– Приказ об утверждении списка мест хранения материальных носителей персональных данных;

– Журнал учета хранения носителей персональных данных;

– Политика обработки и защиты персональных данных (Приложение М);

– Формы согласий на обработку персональных данных;

– а также другие организационно-распорядительные документы.

3.4.2 Программно-аппаратные меры

Проект создания системы защиты персональных данных предусматривает покупку и установку следующих программно-аппаратных средств:

– Средство защиты от НСД Dallas Lock 8.0-K – на 10 АРМ;

– Антивирусное ПО Dr.Web Desktop Security Suite – на 10 АРМ;
– Средство анализа защищенности RedCheck – на 7 ip-адресов.

3.4.3 Обучение персонала

В рамках реализации проекта по созданию системы защиты персональных данных в ГБУЗ «ОПТД № 8» необходимо провести обучение работников учреждения по новым требованиям защиты информации с обоснованием их значимости, разъяснить положения новых организационно-распорядительных документов и ознакомить их с внедренными средствами защиты информации.

3.5 Расчет рисков проекта

Для расчета рисков проекта по созданию системы защиты персональных воспользуемся формулой (2).

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

где Th – уровень угрозы.

Для определения уровня угрозы Th (%) необходимо использовать формулу (3).

$$Th = \frac{ER}{100} * \frac{P(V)}{100}, \quad (3)$$

где: ER (%) – критичность реализации угрозы.
P(V) (%) – вероятность реализации угрозы.

Результаты расчета рисков представлены в Таблице 14.

Таблица 14 – Риски проекта

Риски	Критичность, ER	Вероятность, P(V)	Уровень угрозы, Th	Риски проекта, CTh
1	2	3	4	5
1 Риски, связанные с изменением законодательства				
Изменение законодательства в области защиты информации	30	25	0,075	0,089
Реформы в экономике	15	10	0,015	
2 Риски, связанные с чрезвычайными ситуациями				
Стихийные бедствия	70	1	0,007	0,007
3 Организационные риски				
Задержка финансирования	70	10	0,07	0,206
Отсутствие резерва финансирования	50	10	0,05	
Нехватка рабочей силы	30	10	0,03	
Увеличение срока выполнения работ	30	15	0,045	

Продолжение таблицы 14.

1	2	3	4	5
Недооценка стоимости работ и использование финансов для других целей	30	10	0,03	
4 Риски, связанные с человеческим фактором				
Влияние личностных факторов	20	10	0,02	0,106
Ошибки персонала	30	20	0,06	
Риск недоступности персонала, которому трудно подобрать замену	30	10	0,03	

Согласно Таблице 14, наиболее актуальные риски проекта - организационные. В частности, к ним относятся проблемы с финансированием и затягивание сроков выполнения работ. Наименее опасные риски проекта – риски, связанные с чрезвычайными ситуациями.

3.6 Структура разбиения работ

Для повышения эффективности реализации проекта по созданию системы защиты персональных данных необходимо воспользоваться процессом разбиения работ.

Структура разбиения работ по разработке СЗПДн:

СЗПДн 1 Проектирование;

СЗПДн 1.1 определение процессов деятельности учреждения и информационных систем;

СЗПДн 1.2 анализ проблем и слабых мест в выделенных информационных системах;

СЗПДн 1.3 анализ и выбор способов и методов улучшения СЗПДн;

СЗПДн 1.4 разработка и согласование структуры СЗПДн;

СЗПДн 2 Разработка организационно-распорядительной документации;

СЗПДн 2.1 выполнение документов согласно п. 3.4.1;

СЗПДн 2.2 согласование и утверждение организационно-распорядительных документов;

СЗПДн 2.3 внесение изменений в трудовые договоры;

СЗПДн 3 Подготовка реализации проекта;

СЗПДн 3.1 определение ответственных лиц и исполнителей проекта;

СЗПДн 3.2 приобретение антивирусного ПО;

СЗПДн 3.3 приобретение средств защиты информации от НСД;

СЗПДн 3.4 приобретение средств анализа защищенности;

СЗПДн 4 Внедрение;

СЗПДн 4.1 установка и настройка антивирусного ПО;

СЗПДн 4.2 установка и настройка средств защиты информации от НСД;

СЗПДн 4.3 установка и настройка средств анализа защищенности;

СЗПДн 4.4 контроль защищенности;

СЗПДн 4.5 обучение персонала.

Общая структура разбиения работ представлена на Рисунке 1.

Рисунок 1 – Структура разбиения работ

3.7 Структурная схема организации проекта

Для выполнения поставленных задач в срок и в полном объеме необходима скоординированная работа всех задействованных работников. Все сотрудники, участвующие в выполнении проекта по созданию системы защиты персональных данных, отображены в структурной схеме организации проекта на Рисунке 2.

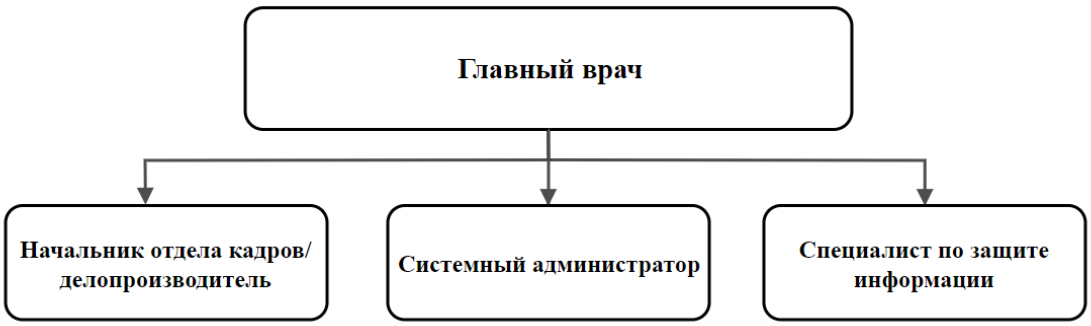


Рисунок 2 – Структурная схема организации проекта

3.8 Матрица ответственности

При реализации проекта исполнители выполняют разные функции, которые можно разделить на условные группы:

– управление (У);

– контроль (К);
– исполнение (И).

В соответствии с структурой разбиения работ и структурной схемой организации проекта определена матрица ответственности, которая представлена в Таблице 15.

Таблица 15 – Матрица ответственности

Исполнитель / Этапы	Главный врач	Начальник отдела кадров/ делопроизводитель	Системный администратор	Специалист по защите информации
СЗПДн 1	У/К			И
СЗПДн 1.1	У/К			И
СЗПДн 1.2	К		И	И
СЗПДн 1.3	К			И
СЗПДн 1.4	У/К			И
СЗПДн 2	К			И
СЗПДн 2.1	К	К		И
СЗПДн 2.2	К	И		К
СЗПДн 2.3	К	И		И/К
СЗПДн 3	К			И
СЗПДн 3.1	К/И			К
СЗПДн 3.2	К			И
СЗПДн 3.3	К			И
СЗПДн 3.4	К			И
СЗПДн 4	К			И
СЗПДн 4.1	К			И
СЗПДн 4.2	К			И
СЗПДн 4.3	К		И	И
СЗПДн 4.4	К		К/И	И
СЗПДн 4.5	У/К	У/К		И/К

3.9 Диаграмма Ганта и сетевой график

Для определения точных сроков выполнения проекта воспользуемся диаграммой Ганта (Приложение К) и сетевым графиком (Приложение Л).

Диаграмма Ганта– это инструмент планирования, который представляет собой столбчатые диаграммы и наглядно показывает календарный план выполнения работ. Согласно диаграмме Ганта, срок выполнения проекта по созданию системы защиты персональных данных – 31 день.

Сетевой график — это также инструмент планирования, который представляет собой динамическую модель проекта. В нем отражаются зависимости этапов выполнения проекта друг от друга.

3.10 Вывод по третьей главе

По результатам выполненных работ был разработан проект создания системы защиты персональных данных в ГБУЗ «ОПТД № 8», определены цели и задачи проекта.

Были определены объекты поставки, к которым относятся организационно-распорядительная документация, обучение персонала и программно-аппаратные меры.

Были рассчитаны риски проекта. Выявлено, что наиболее актуальные риски проекта – организационные.

Для повышения эффективности выполнения проекта было произведено разбиение работ, определены сотрудники, задействованные в выполнении проекта. На основе этих данных была определена матрица ответственности для всех исполнителей.

При помощи диаграммы Ганта и сетевого графика был определен срок выполнения проекта – 31 день.

Итогом выполнения проекта является организация системы защиты персональных данных в ГБУЗ «ОПТД № 8», которая удовлетворяет требованиям российского законодательства.

4 БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

Для работы сотрудников на автоматизированных рабочих местах информационных систем необходима правильная организация рабочих мест, позволяющая снизить негативное воздействие опасных и вредных производственных факторов.

Вредный производственный фактор - производственный фактор, воздействие которого на работника может привести к его заболеванию.

Опасный производственный фактор - производственный фактор, воздействие которого на работника может привести к его травме.

Вредные факторы воздействуют на здоровье и самочувствие человека, приводят к снижению работоспособности, могут вызывать 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 № 426-ФЗ «О специальной оценке условий труда» [6] подразделяются на физические, химические и биологические.

Условия труда работников ГБУЗ «ОПТД № 8», использующих персональные компьютеры, должны соответствовать:

– требованиям к организации рабочего места;
– требованиям к микроклимату;
– требованиям к уровню шума;
– требованиям к освещенности;
– требованиям по электробезопасности;
– требованиям по пожарной безопасности;
– рекомендациям по организации режима труда и отдыха.

4.1 Требования к организации рабочего места

ГБУЗ «ОПТД № 8» - учреждение здравоохранения, деятельность которого подразумевает использование ПЭВМ и других технических средств. Для правильной организации рабочего места с ПЭВМ, необходимо, чтобы помещение соответствовало требованиям, описанных в СанПиН 2.2.2/2.4.1340-03 [15]. Данный документ содержит следующие положения:

– площадь на одно рабочее место пользователей ПЭВМ на базе плоских дискретных экранов (жидкокристаллические, плазменные) должно быть– 4,5 м^2;

– для внутренней отделки интерьера помещений, где расположены ПЭВМ, должны использоваться диффузно-отражающие материалы с коэффициентом отражения для потолка – 0,7−0,8; для стен – 0,5−0,6; для пола – 0,3−0,5;

– помещения, где размещаются рабочие места с ПЭВМ, должны быть оборудованы защитным занулением или заземлением в соответствии с техническими требованиями по эксплуатации;

– не допускается расположение рабочих кабинетов, оборудованных ПЭВМ, в полуподвальных и подвальных помещениях.

При размещении рабочих мест с ПЭВМ расстояние между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора и экрана другого видеомонитора), должно быть не менее 2,0 м, а расстояние между боковыми поверхностями видеомониторов – не менее 1,2 м.

Рабочие места с ПЭВМ в помещениях с источниками вредных производственных факторов должны размещаться в изолированных кабинах с организованным воздухообменом.

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.

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

При этом допускается использование рабочих столов различных конструкций, отвечающих современным требованиям эргономики. Поверхность рабочего стола должна иметь коэффициент отражения 0,5−0,7.

При организации рабочих мест необходимо использовать рабочий стул (кресло), обеспечивающий поддержание рациональной рабочей позы при работе на ПЭВМ, позволяющий 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 ПЭВМ.

Рабочий стул (кресло) должен быть обеспечен подъемно-поворотным механизмом, а также должен быть регулируемым по высоте и углам наклона сиденья и спинки, расстояния спинки от переднего края сиденья, при этом регулировка каждого параметра должна быть независимой, легко осуществляемой и надежно фиксируемой.

Поверхность сиденья, спинки и других элементов стула (кресла) должна быть полумягкой, с нескользящим, слабо электризующимся и воздухопроницаемым покрытием, обеспечивающим легкую очистку от загрязнений.

Нормированные значения для рабочего стола и стульев из документа СанПиН 2.2.2/2.4.1340-03 [15]:

Высота рабочей поверхности стола должна регулироваться в пределах 680−800 мм; при отсутствии такой возможности высота рабочей поверхности стола должна составлять 725 мм.

Модульными размерами рабочей поверхности стола для ЭВМ, на основании которых должны рассчитываться конструктивные размеры, следует считать: ширину 800, 1000, 1200 и 1400 мм, глубину 800 и 1000 мм.

Рабочий стол должен иметь пространство для ног высотой не менее 600 мм, шириной – не менее 500 мм, глубиной на уровне колен – не менее 450 мм и на уровне вытянутых ног – не менее 650 мм.

Конструкция рабочего стола должна обеспечивать оптимальное размещение на рабочей поверхности используемого оборудования с учетом его количества и конструктивных особенностей (размер ПЭВМ, клавиатуры, и др.), характера выполняемой работы. При этом допускается использование рабочих столов различных конструкций, отвечающих современным требованиям эргономики.

Конструкция стула (кресла) должна обеспечивать:

– ширину и глубину поверхности сиденья не менее 400 мм;

– поверхность сиденья с закругленным передним краем;

– регулировку высоты поверхности сиденья в пределах 400−550 мм и углам наклона вперед до 15°, и назад до 5°;

– высоту опорной поверхности спинки 300±20 мм, ширину – не менее 380мм и радиус кривизны горизонтальной плоскости – 400 мм;

– угол наклона спинки в вертикальной плоскости в пределах ±30°;

– регулировку расстояния спинки от переднего края сиденья в пределах 260−400 мм;

– стационарные или съемные подлокотники длиной не менее 250 мм и шириной – 50−70 мм;

– регулировку подлокотников по высоте над сиденьем в пределах 230±30 мм и внутреннего расстояния между подлокотниками в пределах 350−500 мм.

4.2 Требования к микроклимату

При работе с ПЭВМ, также необходимо поддерживать микроклимат в помещениях. При его отсутствии работники могут получить нервно-эмоциональное напряжение и ряд подобных расстройств. Оптимальные параметры микроклимата описаны в СанПиН 2.2.4.3359-16 «Санитарно-эпидемиологические требования к физическим факторам на рабочих местах» [16]. Требования данного документа приведены в Таблице 15.

Показателями, характеризующими микроклимат в помещениях, являются:

– температура воздуха;

– температура поверхностей;

– относительная влажность воздуха;

– скорость движения воздуха;

– интенсивность теплового облучения.

Работа в ГБУЗ «ОПТД № 8» относится к категории 1а по уровню энергозатрат. Оптимальные параметры микроклимата на рабочих местах для данной категории работ приведены в Таблице 16.

Таблица 16 – Оптимальные параметры микроклимата на рабочих местах

Период года	Температура воздуха, °С	Температура поверхностей, °С	Относительная влажность воздуха, %	Скорость движения воздуха, м/с
Холодный	22−24	21−25	60−40	0,1
Теплый	23−25	22−26	60−40	0,1

Также в соответствии с приведенным СанПиНом необходимо в помещении, где работают ПЭВМ, проводить ежедневно влажную уборку, а также проветривать помещение после каждого часа работы.

4.3 Требования к уровню шума

При работе на ПЭВМ источниками шума являются:

– системный блок ПЭВМ;

– работающие принтеры и многофункциональные устройства.

Требования по уровню шума указаны в нормативном документе СанПиН 2.2.4.3359-16 «Санитарно-эпидемиологические требования к физическим факторам на рабочих местах» [16]. Согласно данному документу, нормативным эквивалентным уровнем звука на рабочих местах является 80 дБА.

4.4 Требования к освещенности

При работе на ПЭВМ одним из важных факторов является уровень освещенности помещения, так как пользователю ПЭВМ приходится большую часть времени проводить возле экрана монитора. Поэтому необходимо спроектировать освещение, которые позволит не вызвать раннего переутомления. Для этого необходимо применять совокупность искусственного и естественного света.

Требования к освещенности рабочих мест, оборудованных ПЭВМ, описаны в СанПиНе 2.2.2/2.4.1340-03 [15]:

– в помещениях должно присутствовать естественное и искусственное освещение, которые должны соответствовать требования нормативной документации;

– рабочие столы следует размещать таким образом, чтобы экраны были ориентированы боковой стороной к световым проемам (окнам), чтобы естественный свет падал преимущественно слева;

– 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 лк;

– 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. 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 ЖК - мониторами.

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.

4.5 Требования по электробезопасности

По степени опасности поражения электрическим током рабочие помещения относятся к классу помещений с повышенной опасностью, ввиду возможности прикосновения сотрудника к металлоконструкциям с заземлением сооружений и зданий и одновременно к металлическим элементам оборудования.

Обычно доступ к токопроводящим элементам затруднен. Однако, большая вероятность получить поражение электрическим током от прикосновения к устройству, корпус которого не проводит ток. Такое событие может случится в случае нарушения изоляции проводящих элементов. Поэтому необходимо производить постоянный контроль целостности оборудования, в частности изоляции токопроводящих элементов.

Для защиты от случайного прикосновения к металлическим нетоковедущим частям оборудования, которые могут оказаться под напряжение применяют следующие меры:

– защитное заземление;
– зануление;
– изоляцию нетоковедущих частей;
– защитное экранирование.

Данные меры описаны в ГОСТ Р 12.1.019-2009 «ССБТ. Электробезопасность. Общие требования и номенклатура видов защиты» [15].

4.6 Требования по пожарной безопасности

Все правила и требования в области обеспечения пожарной безопасности описаны в нормативном документе Постановление Правительства №390 от 25.04.2012 «О противопожарном режиме» [12].

Согласно данным правилам и требованиям, руководителем учреждения утверждается инструкция о мерах пожарной безопасности в соответствии с требованиями настоящего документа.

Лица допускаются к работе на объекте только после прохождения обучения мерам пожарной безопасности.

Обучение лиц мерам пожарной безопасности осуществляется путем проведения противопожарного инструктажа и прохождения пожарно-технического минимума.

Порядок и сроки проведения противопожарного инструктажа и прохождения пожарно-технического минимума определяются руководителем организации. Обучение мерам пожарной безопасности осуществляется в соответствии с нормативными документами по пожарной безопасности.

Руководитель организации назначает лицо, ответственное за пожарную безопасность, которое обеспечивает соблюдение требований пожарной безопасности на объекте.

Во всех помещениях и зданиях предприятия должны располагаться специальные таблички с номерами вызова пожарной охраны, а также утвержденные планы эвакуации персонала.

На объекте с массовым пребыванием людей руководитель организации обеспечивает наличие инструкции о действиях персонала по эвакуации людей при пожаре, а также проведение не реже 1 раза в полугодие учебных тревог.

Запрещается курение на территории предприятия, не оборудованных табличками «Место для курения». Руководитель организации обеспечивает размещение на указанных территориях знаков пожарной безопасности "Курение табака и пользование открытым огнем запрещено".

Руководитель организации организует проведение работ по заделке негорючими материалами, обеспечивающими требуемый предел огнестойкости и дымогазонепроницаемости, образовавшихся отверстий и зазоров в местах пересечения противопожарных преград различными инженерными (в том числе электрическими проводами, кабелями) и технологическими коммуникациями.

Следует отметить, что данный нормативный документ накладывает ряд запретов на организацию в области пожарной безопасности. К ним относятся:

– снимать предусмотренные проектной документацией двери эвакуационных выходов из поэтажных коридоров, холлов, фойе, тамбуров и лестничных клеток, другие двери, препятствующие распространению опасных факторов пожара на путях эвакуации;

– производить изменение объемно-планировочных решений и размещение инженерных коммуникаций и оборудования, в результате которых ограничивается доступ к огнетушителям, пожарным кранам и другим системам обеспечения пожарной безопасности или уменьшается зона действия автоматических систем противопожарной защиты (автоматической пожарной сигнализации, стационарной автоматической установки пожаротушения, системы дымоудаления, системы оповещения и управления эвакуацией);

– загромождать мебелью, оборудованием и другими предметами двери;

– загромождать и закрывать проходы к местам крепления спасательных устройств.

Руководитель организации обеспечивает содержание наружных пожарных лестниц и ограждений на крышах (покрытиях) зданий и сооружений в исправном

состоянии, организует не реже 1 раза в 5 лет проведение эксплуатационных испытаний пожарных лестниц и ограждений на крышах с составлением соответствующего протокола испытаний, а также периодического освидетельствования состояния средств спасения с высоты в соответствии с технической документацией или паспортом на такое изделие.

Руководитель организации при выполнении планового ремонта или профилактического осмотра технологического оборудования обеспечивает соблюдение необходимых мер пожарной безопасности.

Руководитель организации в соответствии с технологическим регламентом обеспечивает выполнение работ по очистке вытяжных устройств (шкафов, окрасочных, сушильных камер и др.), аппаратов и трубопроводов от пожароопасных отложений.

Так как в рабочих помещениях присутствует электротехника, то, возможный пожар будет иметь класс Е (пожар электроустановок). Пожары такого класса тушат инертными разбавителями и порошками.

К первичным средствам пожаротушения относятся специальные емкости с песком, лопаты, ведра, ломы, багры, асбестовые полотна, грубошерстные ткани и войлок, огнетушители. Первичные средства пожаротушения размещаются в легкодоступных местах и не должны быть помехой при эвакуации персонала из помещений.

4.7 Рекомендации по организации режима труда и отдыха

Руководитель любого учреждения обязан организовать режим труда и отдыха на своем предприятии. Большая часть работы в ГБУЗ «ОПТД № 8» предполагает работу за ПЭВМ, поэтому необходимо воспользоваться СанПиНом 2.2.2./2.4. 1340-03 [15]. Согласно данному документу, трудовую деятельность можно отнести к группе «Б». Данная деятельность подразумевает ввод информации.

Для видов трудовой деятельности устанавливается три категории тяжести и напряженности работы ПЭВМ. Для группы «Б» категории определяются по суммарному числу считываемых знаков за рабочую смену, но не более 40 000 знаков за смену:

1 категория – до 15 000 знаков;
2 категория – до 30 000 знаков;
3 категория – до 40 000 знаков.

Продолжительность обеденного перерыва определяется действующим законодательством о труде и правилами внутреннего распорядка предприятия.

Для обеспечения оптимальной работоспособности и сохранения здоровья профессиональных пользователей, на протяжении рабочей смены должны устанавливаться регламентированные перерывы. Время регламентированных перерывов в течении рабочей смены следует устанавливать в зависимости от ее продолжительности, вида и категории трудовой деятельности. Продолжительность непрерывной работы без регламентированного перерыва не должна превышать одного часа. При

восьмичасовой рабочей смене и работе на ПЭВМ суммарная длительность регламентированных перерывов должна составлять:

–для 1 категории работ 50 минут;

–для 2 категории работ 70 минут;

–для 3 категории работ 90 минут.

Во время регламентированных перерывов с целью снижения нервно эмоционального напряжения, утомления зрительного анализатора, устранения влияния гиподинамии и гипокинезии, предотвращения развития познотонического утомления целесообразно выполнять комплексы упражнений для глаз, для улучшения мозгового кровообращения, для снятия утомления с плечевого пояса и рук, а также общего воздействия.

В случаях возникновения у пользователя зрительного дискомфорта и других неблагоприятных субъективных ощущений, несмотря на соблюдение санитарно-гигиенических, эргономических требований, режимов труда и отдыха следует применять индивидуальный подход в ограничении времени работ с ПЭВМ. Коррекцию длительности перерывов для отдыха или проводить смену деятельности на другую, не связанную с использованием ПЭВМ.

4.8 Вывод о соответствии рабочего места требованиям по охране труда

Для анализа условий рабочего места рассмотрим рабочее место начальника отдела кадров (Рисунок 3).

Измеренные параметры для данного рабочего места представлены в Таблице 17.

Таблица 17 – Измеренные параметры

Параметр	Значение	Соответствие нормативным требованиям
1	2	3
Высота рабочего стола	725 мм	соответствует
Ширина рабочего стола	1200 мм	соответствует
Глубина рабочего стола	800 мм	соответствует
Наличие регулировки сиденья	есть	соответствует
Высота пространства для ног	700 мм	соответствует
Ширина пространства для ног	1150 мм	соответствует
Наличие подставки для ног	есть	соответствует
Ширина подставки для ног	300 мм	соответствует
Глубина подставки для ног	400 мм	соответствует
Площадь рабочего места	4,5 $м^2$	соответствует
Положение естественного света относительно пользователя	слева	соответствует
Освещенность на поверхности рабочего стола	380 лк	соответствует

Продолжение таблицы 17.

1	2	3
Уровень шума	45 ДбА	соответствует
Температура воздуха (теплый период года)	24 °С	соответствует
Температура поверхностей (теплый период года)	22 °С	соответствует
Относительная влажность воздуха	50 %	соответствует

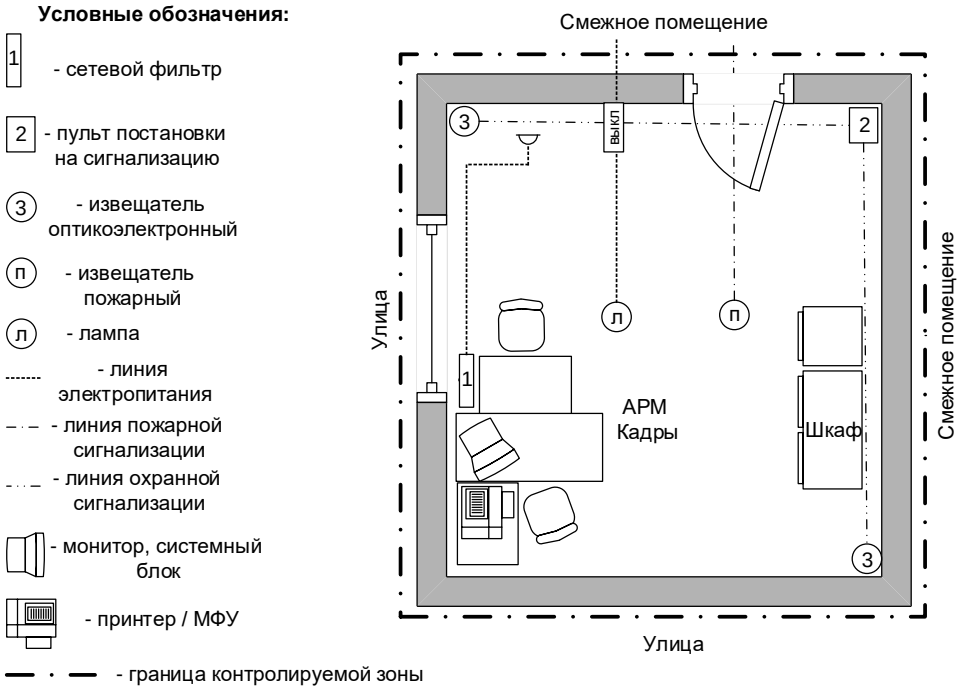


Рис. 3 – Рабочее место начальника отдела кадров

Таким образом, рабочее место соответствует требованиям по охране труда.

4.9 Вывод по четвертой главе

Работа на электронно-вычислительных машинах несет за собой множество опасных и вредных производственных факторов, которые могут пагубно повлиять на здоровье человека, его работоспособность, трудовую пригодность и эффективность.

Для снижения негативного воздействия этих факторов необходима правильная организация рабочих мест, соответствующая всем требованиям по охране труда.

Был проведен анализ условий рабочего места ГБУЗ «ОПТД № 8», который показал, что данное рабочее место соответствует требованиям безопасности жизнедеятельности.

ЗАКЛЮЧЕНИЕ

Результатом выполнения выпускной квалификационной работы является созданная система защиты персональных данных в ГБУЗ «ОПТД № 8», которая удовлетворяет требованиям законодательства Российской Федерации в области защиты персональных данных.

В ходе выполнения выпускной квалификационной работы были выполнены следующие задачи:

1) Проведен анализ состояния защиты ГБУЗ «ОПТД № 8», в ходе которого были определены 2 информационные системы: ИСПДн «Бухгалтерия и кадры» и ИСПДн «Медицина».

В ИСПДн «Бухгалтерия и кадры» обрабатываются иные категории персональных данных, тип актуальных угроз – 3, уровень защищенности персональных данных – 4.

В ИСПДн «Медицина» обрабатываются специальные категории персональных данных, тип актуальных угроз – 3, уровень защищенности персональных данных – 3.

Для данных информационных систем были разработаны модели угроз и технические задания на создание системы защиты персональных данных.

2) Сформировано теоретическое обоснование выбора средств защиты, в процессе выполнения которого были рассмотрены актуальные угрозы безопасности персональных данных, и определены средства и меры защиты:

– Разработана организационно-распорядительная документация;

– Внедрены программно-аппаратные средства защиты (Dallas Lock 8.0-K, Dr.Web Desktop Security Suite и RedCheck);

– Проведено обучение персонала.

3) Разработан проект введения системы защиты персональных данных в ГБУЗ «ОПТД № 8», для которого были рассчитаны риски, определены основные этапы, ответственные лица и срок выполнения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1) «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК от 15.02.2008: (ред. от 09.01.2008) // ФСТЭК: Интернет-версия [электронный ресурс]. – Электрон. дан. и прогр. – М., 2018.

2) ГОСТ Р 12.1.019–2009 «ССБТ. Электробезопасность. Общие требования и номенклатура видов защиты». — М.: Стандатинформ, 2010. — 32 с.

3) ГОСТ 34.602–1989 «Техническое задание на создание автоматизированной системы». — М.: Изд-во стандартов, 1989. — 12 с.

4) «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК от 14.02.2008: (ред. от 14.02.2008) // ФСТЭК: Интернет-версия [электронный ресурс]. – Электрон. дан. и прогр. – М., 2018.

5) «О персональных данных»: федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2018.

6)) «О специальной оценке условий труда»: федеральный закон Российской Федерации от 28.12.2013 № 426-ФЗ // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2018.

7) «Об информации, информационных технологиях и о защите информации»: федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ: (ред. от 24.11.2014) // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2018.

8) «Об основах охраны здоровья граждан в Российской Федерации»: федеральный закон Российской Федерации от 21.11.2011 № 323-ФЗ: (ред. от 07.03.2018) // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2018.

9) «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»: приказ ФАПСИ от 13.06.2001 г. № 152 // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2018.

10) «Об Утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработки в информационных системах персональных данных»: приказ ФСТЭК от 18.02.2013 г. № 21: (ред. от 14.11.2017) // ФСТЭК: Интернет-версия [электронный ресурс]. – Электрон. дан. и прогр. – М., 2018.

11) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ин-

формационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»: приказ ФСБ от 10.07.2014 г. № 378 // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2018.

12) Постановление Правительства РФ «О противопожарном режиме» от 25.04.2012 № 390 // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «Консультант-Плюс». – Электрон. дан. и прогр. – М., 2018.

13) Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 № 687 // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2018.

14) Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119 // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2018.

15) СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы». – М.: Минздрав России, 2003.– 42 с.

16) СанПиН 2.2.4.3359-16 «Санитарно-эпидемиологические требования к физическим факторам на рабочих местах». – М.: Минздрав России, 2016.– 64 с.

ПРИЛОЖЕНИЕ А

Государственное бюджетное учреждение здравоохранения
«Областной противотуберкулезный диспансер № 8»

УТВЕРЖДАЮ

Главный врач
ГБУЗ «ОПТД № 8»

_____А.С. Куликова
___ _____ _____г.

АКТ

от ___ _____ №_____
_____г.

г. Южноуральск

определения уровня защищенности персональных данных информационной системы персональных данных «Бухгалтерия и кадры»

Составлен комиссией:

Председатель:
Главный врач Фамилия И.О.
Члены комиссии:
Начальник отдела кадров Фамилия И.О.
Программист Фамилия И.О.
Главный бухгалтер Фамилия И.О.

Комиссия установила, что согласно постановлению Правительства РФ от 01.11.12 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», следующие исходные данные ИСПДн «Бухгалтерия и кадры»:

— является информационной системой, обрабатывающей иные категории персональных данных менее 100 000 субъектов персональных данных, не являющихся сотрудниками ГБУЗ «ОПТД № 8»;

— актуальными являются угрозы 3 типа.

На основании анализа исходных данных комиссия решила, что для персональных данных ИСПДн «Бухгалтерия и кадры» необходимо обеспечить уровень защищенности: 4.

Председатель:
Главный врач _____ И.О. Фамилия
Члены комиссии:
Начальник отдела кадров _____ И.О. Фамилия
Программист _____ И.О. Фамилия
Главный бухгалтер _____ И.О. Фамилия

ПРИЛОЖЕНИЕ Б

Государственное бюджетное учреждение здравоохранения
«Областной противотуберкулезный диспансер № 8»

УТВЕРЖДАЮ

Главный врач
ГБУЗ «ОПТД № 8»

_____А.С. Куликова
___ _____ _____г.

АКТ

от ___ _____ №_____
_____г.

г. Южноуральск

определения уровня защищенности персональных данных информационной системы персональных данных «Медицина»

Составлен комиссией:

Председатель:
Главный врач Фамилия И.О.
Члены комиссии:
Начальник отдела кадров Фамилия И.О.
Программист Фамилия И.О.
Главный бухгалтер Фамилия И.О.

Комиссия установила, что согласно постановлению Правительства РФ от 01.11.12 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», следующие исходные данные ИСПДн «Медицина»:

— является информационной системой, обрабатывающей специальные категории персональных данных менее 100 000 субъектов персональных данных, не являющихся сотрудниками ГБУЗ «ОПТД № 8»;

— актуальными являются угрозы 3 типа.

На основании анализа исходных данных комиссия решила, что для персональных данных ИСПДн «Медицина» необходимо обеспечить уровень защищенности: 3.

Председатель:
Главный врач _____ И.О. Фамилия
Члены комиссии:
Начальник отдела кадров _____ И.О. Фамилия
Программист _____ И.О. Фамилия
Главный бухгалтер _____ И.О. Фамилия

ПРИЛОЖЕНИЕ В

Государственное бюджетное учреждение здравоохранения
«Областной противотуберкулезный диспансер № 8»

ТЕХНИЧЕСКИЙ ПАСПОРТ

Информационная система персональных данных

«Бухгалтерия и кадры»

на базе автоматизированных рабочих мест

2018 г.

1. Общие сведения об информационной системе персональных данных (ИСПДн)

1.1 Наименование ИСПДн: «Бухгалтерия и кадры» ГБУЗ «ОПТД №8» на базе автоматизированных рабочих мест.

1.2. Уровень защищенности персональных данных: 4 («Акт определения уровня защищенности персональных данных», № _____-дсп от __.__.20__).

2. Состав оборудования ИСПДн

2.1 Перечень основных технических средств и систем, входящих в состав ИСПДн:

№ п.п.	Тип ОТСС	Наименование (модель)	Заводской номер
АРМ Кадры			
1	Системный блок	Intel(R) Celeron(R) CPU E1600 @ 2.40GHz/ 2048MB/ 149.0GB	
2	Монитор	Acer V206HQLBb	ETLBN0C03792600BA34041
3	Мышь	A4tech OP-620D	Q1008
4	Клавиатура	Genius KB-M200	WE150FA03488
5	Принтер	Canon Laser Shot LBP1120	NTBS38502
АРМ Главный бухгалтер			
1	Системный блок	Intel(R) Core(TM) i3-2100 CPU @ 3.10GHz/ 3816MB / 232.9GB	
2	Монитор	Acer V206HQLBb	ETLBN0C03792600BA34041
3	Мышь	Logitech M100	831566-0000
4	Клавиатура	Sven Standard 307M	SV1105AR00003
5	Принтер	Canon i-SENSYS LBP6200d	NOAD95482
АРМ Бухгалтер			
1	Системный блок	Intel(R) Celeron(R) CPU G530 @ 2.40GHz/ 1762MB/ 232.9GB	
2	Монитор	Acer V206HQLBb	ETLBN0C03792600BA34041
3	Мышь	A4tech OP-620D	Q1212
4	Клавиатура	Defender Element HB-520	647SX13051505579

5	Принтер	Canon i-SENSYS LBP6200d	NOAD95482

2.2 Перечень вспомогательных технических средств, входящих в состав ИСПДн (средств вычислительной техники, не участвующих в обработке персональных данных)

№ п.п.	Тип ВТСС	Модель, заводской номер	Примечание
Прочее			
1	Телефонный аппарат	Panasonic KX-TS2352RU	Расположено в пределах контролируемой зоны
2	Телефонный аппарат	Panasonic KX-TG1611RUH	Расположено в пределах контролируемой зоны
3	Извещатель охранный объемный оптико-электронный	Астра-517	Расположено в пределах контролируемой зоны
4	Прибор приемно-контрольный охранно-пожарный	Астра-712/1	Расположено в пределах контролируемой зоны
5	Оповещатель охранно-пожарный комбинированный свето-звуковой	МАЯК-12К	Расположено в пределах контролируемой зоны
6	Линия электропитания		Выходит к электрощитку, находящемуся в пределах контролируемой зоны
7	Линия охранно-пожарной сигнализации		Выходит к пульту, находящемуся в пределах контролируемой зоны

2.3 Структура, топология и размещение технических средств ИСПДн относительно границ контролируемой зоны объекта:

ИСПДн состоит из трех АРМ, подключенных к сети общего пользования.

ИСПДн расположена на первом этаже здания, принадлежащего ГБУЗ «ОПТД №8». Контролируемой зоной являются кабинеты 1 и 4 противотуберкулезного диспансера.

Схемы размещения и расположения ОТСС, ВТСС, а также проводящих линий и коммуникаций объекта с привязкой к границам контролируемой зоны приведены в приложении 1.

2.4. Системы электропитания и заземления.

Для электропитания технических средств ИСПДн применена схема TN-C-S с глухозаземленной нейтралью на трансформаторной подстанции (ТП). ТП расположена за пределами контролируемой зоны и имеет подключения сторонних потребителей со стороны низшего напряжения. Питающие кабели от ТП к ИСПДн проходят за пределами

контролируемой зоны. Вводно-распределительное устройство расположено за пределами контролируемой зоны.

Выделенный контур заземления отсутствует. Заземляющее устройство повторного заземления здания расположено за пределами КЗ.

План размещения розеток электропитания, прокладки кабелей электропитания приведен в приложении 1.

2.5 Перечень средств защиты информации, установленных в ИСПДн.

№ п.п.	**Наименование СЗИ**	**Заводской номер**	**Сведения о сертификате**	**Место, дата установки**
1	ViPNet Client 3.2	28602-6036-756	ФСТЭК России № 1549/1 до 26.05.2019	АРМ Кадры, 31.05.2015
2	ViPNet Client 3.2	28602-6656-753	ФСТЭК России № 1549/1 до 26.05.2019	АРМ Бухгалтер, 31.05.2015
3	ViPNet Client 3.2	27602-6656-786	ФСТЭК России № 1549/1 до 26.05.2019	АРМ Главный бухгалтер, 31.05.2015
4	КриптоПро CSP 4.0	BBIK-SK29-94J7	ФСБ России № СФ/124-2864 до 31.12.2018	АРМ Главный бухгалтер, 27.09.2016
5	КриптоПро CSP 4.0	TUIK-WK29-14S0	ФСБ России № СФ/124-2864 до 31.12.2018	АРМ Бухгалтер, 27.09.2016
6	Dallas Lock 8.0-K	99099-7643-640	ФСТЭК России № 2720 до 25.09.2018	АРМ Кадры, 08.04.2018
7	Dallas Lock 8.0-K	99099-2948-245	ФСТЭК России № 2720 до 25.09.2018	АРМ Бухгалтер, 08.04.2018
8	Dallas Lock 8.0-K	99099-9287-284	ФСТЭК России № 2720 до 25.09.2018	АРМ Главный бухгалтер, 08.04.2018
9	Dr.Web Desktop Security Suite	6TU9-A9D9-DJSM-2VMF	ФСТЭК России № 3509 до 27.01.2019	АРМ Кадры, 09.04.2018

10	Dr.Web Desktop Security Suite	JD89-7SJW-4JE8-MS7S	ФСТЭК России № 3509 до 27.01.2019	АРМ Бухгалтер, 09.04.2018
11	Dr.Web Desktop Security Suite	8DJF-8SHJ-3JDK-S4SG	ФСТЭК России № 3509 до 27.01.2019	АРМ Главный бухгалтер, 09.04.2018

2.6. Перечень используемых в ИСПДн программных средств.

№ п.п.	**Наименование и тип программного средства**	**Серийный номер (номер лицензии)**
АРМ Кадры		
1	Microsoft Windows 7 Professional	D2Q4Q-T9QWW-P32TM-PX4BB-M9FJ9
2	АРМ Медицинский персонал	
3	Mozilla Firefox	
4	Microsoft Office 2007	
АРМ Главный бухгалтер		
1	Microsoft Windows 7 Professional	D8K4Y-T9QWW-P32TM-PX4BB-M9FJ9
2	1С: Предприятие	
3	Microsoft Office 2007	
4	Mozilla Firefox	
5	Налогоплательщик ЮЛ	
6	АРМ "Подготовка расчётов для ФСС"	
АРМ Бухгалтер		
1	Microsoft Windows 7 Professional	N7Q4Q-T9QTW-P32TM-PX4BB-M9FJ9
2	1С: Предприятие	
3	Microsoft Office 2007	
4	Mozilla Firefox	

3. Сведения об аттестации объекта информатизации на соответствие требованиям по безопасности информации

_____

_____

_____

_____

4. Результаты периодического контроля

№, п/п	Дата проведения проверки	Наименование организации, проводящей проверку	Результаты проверки, номер отчетного документа

5.Лист регистрации изменений.

№, п/п	Дата внесения изменения	Описание вносимого изменения	Подпись ответственного за эксплуатацию

ПРИЛОЖЕНИЕ 1

Схема расположения ОТСС и ВТСС и проводных линий в помещении

Кабинет 1

Условные обозначения:

1 - сетевой фильтр

2 - пульт постановки на сигнализацию

(з) - извещатель оптикоэлектронный

(п) - извещатель пожарный

(л) - лампа

------ - линия электропитания

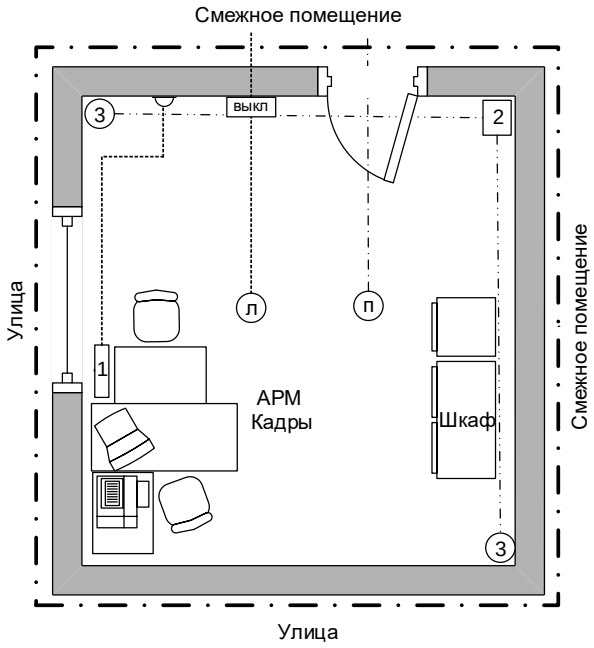
– · – · – - линия пожарной сигнализации

– · · – · · – - линия охранной сигнализации

- монитор, системный блок

- принтер / МФУ

— · — · — - граница контролируемой зоны



Кабинет 4

Условные обозначения:

1 - сетевой фильтр

2 - пульт постановки на сигнализацию

(з) - извещатель оптикоэлектронный

(п) - извещатель пожарный

(л) - лампа

------ - линия электропитания

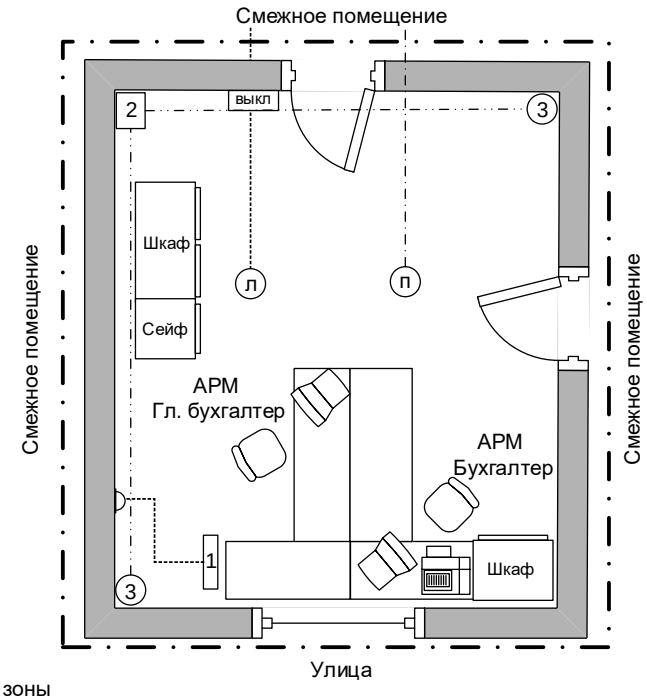
– · – · – - линия пожарной сигнализации

– · · – · · – - линия охранной сигнализации

- монитор, системный блок

- принтер / МФУ

— · — · — - граница контролируемой зоны



ПРИЛОЖЕНИЕ Г

Государственное бюджетное учреждение здравоохранения
«Областной противотуберкулезный диспансер № 8»

ТЕХНИЧЕСКИЙ ПАСПОРТ

Информационная система персональных данных

«Медицина»

на базе автоматизированных рабочих мест

2018 г.

1. Общие сведения об информационной системе персональных данных (ИСПДн)

1.1 Наименование ИСПДн: «Медицина» ГБУЗ «ОПТД №8» на базе автоматизированных рабочих мест.

1.2. Уровень защищенности персональных данных: 3 («Акт определения уровня защищенности персональных данных», № _____-дсп от __.__.20__).

2. Состав оборудования ИСПДн

2.1 Перечень основных технических средств и систем, входящих в состав ИСПДн:

№ п.п.	Тип ОТСС	Наименование (модель)	Заводской номер
АРМ Фтизиатр			
1	Системный блок	Intel(R) Celeron(R) CPU E3400 @ 2.60GHz/ 1024MB/ 149.0GB	
2	Монитор	Acer V206HQLBb	ETLBN0C03792600BA34941
3	Мышь	A4tech OP-620D	Q1008
4	Клавиатура	Genius KB-M200	WE150FA03488
5	Принтер	Canon Laser Shot LBP1120	NTBS38502
АРМ Фтизиатр 2			
1	Системный блок	Intel(R) Celeron(R) CPU E3400 @ 2.60GHz/ 1024MB/ 149.0GB	
2	Монитор	Acer V206HQLBb	ETLBN0C03772600BA34B82
3	Мышь	Logitech M100	831566-0000
4	Клавиатура	Sven Standard 307M	SV1105AR00003
АРМ Детский фтизиатр			
1	Системный блок	Intel(R) Celeron(R) CPU E3400 @ 2.60GHz/ 1024MB/ 149.0GB	
2	Монитор	Acer V206HQLBb	EYRBN0C00472670BA34B87
3	Мышь	Logitech M100	831896-0000
4	Клавиатура	Sven Standard 307M	SV1105AR00006

АРМ Медстатистик			
1	Системный блок	Intel(R) Celeron(R) CPU G530 @ 2.40GHz/ 2048MB/ 698.6GB	
2	Монитор	Acer V206HQLBb	YRTLMN3C03742600BA34B95
3	Мышь	Logitech M100	838666-0000
4	Клавиатура	Sven Standard 307M	SV1105RR00043
5	Принтер	Canon i-SENSYS LBP6200d	NOAD95482
АРМ Регистратура			
1	Системный блок	Intel(R) Celeron(R) CPU G530 @ 2.40GHz/ 1762MB/ 232.9GB	
2	Монитор	Acer V206HQLBb	YRTLTN3C03742600BA34B91
3	Мышь	A4tech OP-620D	Q1007
4	Клавиатура	Defender Element HB-520	647SX13051505579
5	Принтер	Canon i-SENSYS MF4410	DOAN05681
АРМ Старшая медсестра			
1	Системный блок	Intel(R) Celeron(R) CPU E3400 @ 2.60GHz/ 1024MB/ 149.0GB	
2	Монитор	Acer V206HQLBb	RTLEBN0C03757600BA34G83
3	Мышь	Logitech M100	831596-0070
4	Клавиатура	Sven Standard 307M	SV1125AR00083
5	Принтер	Canon i-SENSYS LBP6200d	DOBN05631
АРМ Ординаторская			
1	Системный блок	Intel(R) Celeron(R) CPU E3400 @ 2.60GHz/ 1024MB/ 149.0GB	
2	Монитор	Acer V206HQLBb	NLEVN0C03772600BA34FN94
3	Мышь	Logitech M100	831366-0300
4	Клавиатура	Sven Standard 307M	SV1905AR00099

2.2 Перечень вспомогательных технических средств, входящих в состав ИСПДн (средств вычислительной техники, не участвующих в обработке персональных данных)

№ п.п.	Тип ВТСС	Модель, заводской номер	Примечание
Прочее			
1	Телефонный аппарат	Panasonic KX-TG1711	Расположено в пределах контролируемой зоны
2	Телефонный аппарат	Panasonic KX-TG1611RUH	Расположено в пределах контролируемой зоны
3	Извещатель охранный объемный оптико-электронный	Астра-517	Расположено в пределах контролируемой зоны
4	Прибор приемно-контрольный охранно-пожарный	Астра-712/1	Расположено в пределах контролируемой зоны
5	Оповещатель охранно-пожарный комбинированный свето-звуковой	МАЯК-12К	Расположено в пределах контролируемой зоны
6	Линия электропитания		Выходит к электрощитку, находящемуся в пределах контролируемой зоны
7	Линия охранно-пожарной сигнализации		Выходит к пульту, находящемуся в пределах контролируемой зоны

2.3 Структура, топология и размещение технических средств ИСПДн относительно границ контролируемой зоны объекта:

В ИСПДн входит 2 сети, расположенные в разных зданиях. Все АРМ подключены к сети общего пользования.

ИСПДн расположена на первых этажах зданий, принадлежащих ГБУЗ «ОПТД №8». Контролируемой зоной являются кабинеты 6, 7, 10, 12 противотуберкулезного диспансера, а также ординаторская и кабинет старшей медсестры противотуберкулезного отделения.

Схемы размещения и расположения ОТСС, ВТСС, а также проводящих линий и коммуникаций объекта с привязкой к границам контролируемой зоны приведены в приложении 1.

2.4. Системы электропитания и заземления.

Для электропитания технических средств ИСПДн применена схема TN-C-S с глухозаземленной нейтралью на трансформаторной подстанции (ТП). ТП расположена за преде-

лами контролируемой зоны и имеет подключения сторонних потребителей со стороны низшего напряжения. Питающие кабели от ТП к ИСПДн проходят за пределами контролируемой зоны. Вводно-распределительное устройство расположено за пределами контролируемой зоны.

Выделенный контур заземления отсутствует. Заземляющее устройство повторного заземления здания расположено за пределами КЗ.

План размещения розеток электропитания, прокладки кабелей электропитания приведен в приложении 1.

2.5 Перечень средств защиты информации, установленных в ИСПДн.

№ п.п.	**Наименование СЗИ**	**Заводской номер**	**Сведения о сертификате**	**Место, дата установки**
1	ViPNet Client 3.2	28602-6036-756	ФСТЭК России № 1549/1 до 26.05.2019	АРМ Фтизиатр, 31.05.2015
2	ViPNet Client 3.2	74937-3748-384	ФСТЭК России № 1549/1 до 26.05.2019	АРМ Фтизиатр 2, 31.05.2015
3	ViPNet Client 3.2	29487-4947-394	ФСТЭК России № 1549/1 до 26.05.2019	АРМ Детский фтизиатр, 31.05.2015
4	ViPNet Client 3.2	24049-3947-273	ФСТЭК России № 1549/1 до 26.05.2019	АРМ Медстатистик, 31.05.2015
5	ViPNet Client 3.2	34947-9833-894	ФСТЭК России № 1549/1 до 26.05.2019	АРМ Регистратура, 31.05.2015
6	ViPNet Client 3.2	38394-4949-384	ФСТЭК России № 1549/1 до 26.05.2019	АРМ Старшая медсестра, 31.05.2015
7	ViPNet Client 3.2	94847-3834-876	ФСТЭК России № 1549/1 до 26.05.2019	АРМ Ординаторская, 31.05.2015

8	КриптоПро CSP 4.0	YBIK-SK29-94J1	ФСБ России № СФ/124-2864 до 31.12.2018	АРМ Старшая медсестра, 27.09.2016
9	Dallas Lock 8.0-K	99099-8474-733	ФСТЭК России № 2720 до 25.09.2018	АРМ Фтизиатр, 08.04.2018
10	Dallas Lock 8.0-K	99099-7439-374	ФСТЭК России № 2720 до 25.09.2018	АРМ Фтизиатр 2, 08.04.2018
11	Dallas Lock 8.0-K	99099-8374-246	ФСТЭК России № 2720 до 25.09.2018	АРМ Детский фтизиатр, 08.04.2018
12	Dallas Lock 8.0-K	99099-8395-328	ФСТЭК России № 2720 до 25.09.2018	АРМ Медстатистик, 08.04.2018
13	Dallas Lock 8.0-K	99099-2748-212	ФСТЭК России № 2720 до 25.09.2018	АРМ Регистратура, 08.04.2018
14	Dallas Lock 8.0-K	99099-1739-134	ФСТЭК России № 2720 до 25.09.2018	АРМ Старшая медсестра, 09.04.2018
15	Dallas Lock 8.0-K	99099-1834-837	ФСТЭК России № 2720 до 25.09.2018	АРМ Ординаторская, 09.04.2018
16	Dr.Web Desktop Security Suite	8DFJ-FR9S-HJEW-734F	ФСТЭК России № 3509 до 27.01.2019	АРМ Фтизиатр, 08.04.2018
17	Dr.Web Desktop Security Suite	D7JR-JD78-37FH-5CB3	ФСТЭК России № 3509 до 27.01.2019	АРМ Фтизиатр 2, 08.04.2018
18	Dr.Web Desktop Security Suite	7SH3-AN2K-MSU6-S7W3	ФСТЭК России № 3509 до 27.01.2019	АРМ Детский фтизиатр, 08.04.2018

19	Dr.Web Desktop Security Suite	94KJ-FDKD-3J0D-IJ4H	ФСТЭК России № 3509 до 27.01.2019	АРМ Медстатистик, 08.04.2018
20	Dr.Web Desktop Security Suite	6S9E-93J0-SK73-S7WK	ФСТЭК России № 3509 до 27.01.2019	АРМ Регистратура, 08.04.2018
21	Dr.Web Desktop Security Suite	W9RK-S9KW-29EJ-SJD9	ФСТЭК России № 3509 до 27.01.2019	АРМ Старшая медсестра, 09.04.2018
22	Dr.Web Desktop Security Suite	9SJ3-AJ29-SOW0-N2S9	ФСТЭК России № 3509 до 27.01.2019	АРМ Ординаторская, 09.04.2018
23	RedCheck	3849-2949-2913	ФСТЭК России № 3172 до 23.06.2020	АРМ Фтизиатр, 08.04.2018
24	RedCheck	0492-4942-1939	ФСТЭК России № 3172 до 23.06.2020	АРМ Фтизиатр 2, 08.04.2018
25	RedCheck	2943-2948-2940	ФСТЭК России № 3172 до 23.06.2020	АРМ Детский фтизиатр, 08.04.2018
26	RedCheck	2839-2940-1849	ФСТЭК России № 3172 до 23.06.2020	АРМ Медстатистик, 08.04.2018
27	RedCheck	8275-2984-2949	ФСТЭК России № 3172 до 23.06.2020	АРМ Регистратура, 08.04.2018
28	RedCheck	8362-6254-7252	ФСТЭК России № 3172 до 23.06.2020	АРМ Старшая медсестра, 09.04.2018
29	RedCheck	3958-3932-1904	ФСТЭК России № 3172 до 23.06.2020	АРМ Ординаторская, 09.04.2018

2.6. Перечень используемых в ИСПДн программных средств.

№ п.п.	Наименование и тип программного средства	Серийный номер (номер лицензии)
АРМ Фтизиатр		
1	Microsoft Windows 7 Professional	G7Q4Q-T9QTW-P32TM-PX4BB-M9RJ9
2	Mozilla Firefox	
3	OpenOffice 4.1.1	
АРМ Фтизиатр 2		
1	Microsoft Windows 7 Professional	N7U4W-T9QTW-P32TM-PX4BW-M9WJ9
2	Mozilla Firefox	
3	OpenOffice 4.1.1	
АРМ Детский фтизиатр		
1	Microsoft Windows 7 Professional	N7H4Q-T9QTW-Q32TM-PX4BH-M9FJ5
2	Mozilla Firefox	
3	OpenOffice 4.1.1	
АРМ Медстатистик		
1	Microsoft Windows 7 Professional	V3Q4Q-T9QTW-P32TM-PX3BB-M9FJ3
2	Mozilla Firefox	
3	Microsoft Office 2007	
АРМ Регистратура		
1	Microsoft Windows 7 Professional	V8Q4K-T9QTW-P32TM-PX3BB-M9FJ8
2	Mozilla Firefox	
АРМ Старшая медсестра		
1	Microsoft Windows 7 Professional	R7Q4Q-T9QTB-P32TM-EX4BB-M9FT5
2	Mozilla Firefox	

3	OpenOffice 4.1.1	
АРМ Ординаторская		
1	Microsoft Windows 7 Professional	M0Q4Q-T9QRW-P32UM-PX4BB-Y9FR2
2	Mozilla Firefox	

3. Сведения об аттестации объекта информатизации на соответствие требованиям по безопасности информации

_____

_____

_____

_____

_____

4. Результаты периодического контроля

№, п/п	Дата проведения проверки	Наименование организации, проводящей проверку	Результаты проверки, номер отчетного документа

5. Лист регистрации изменений.

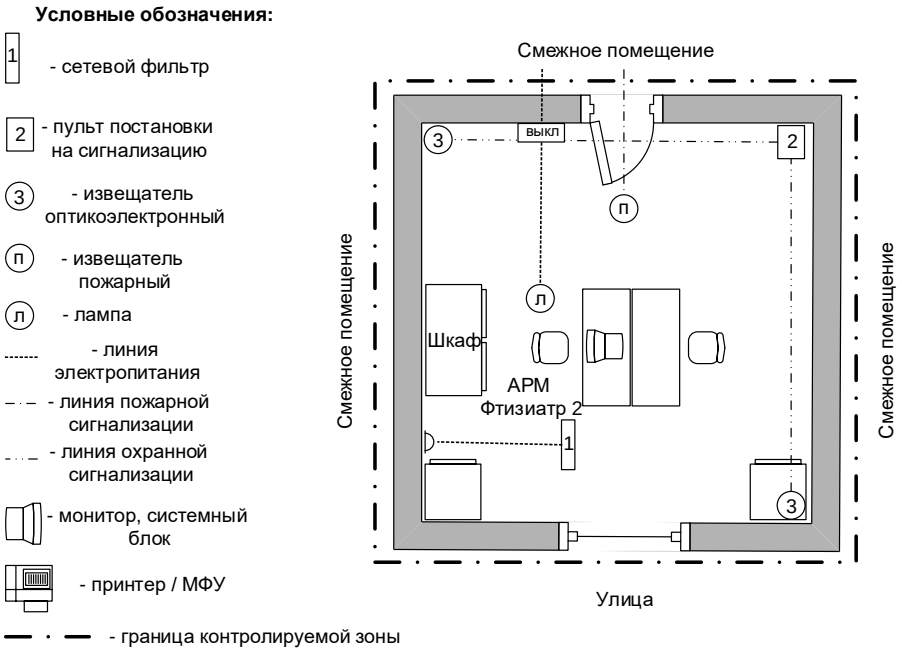
№, п/п	Дата внесения изменения	Описание вносимого изменения	Подпись ответственного за эксплуатацию

ПРИЛОЖЕНИЕ 1

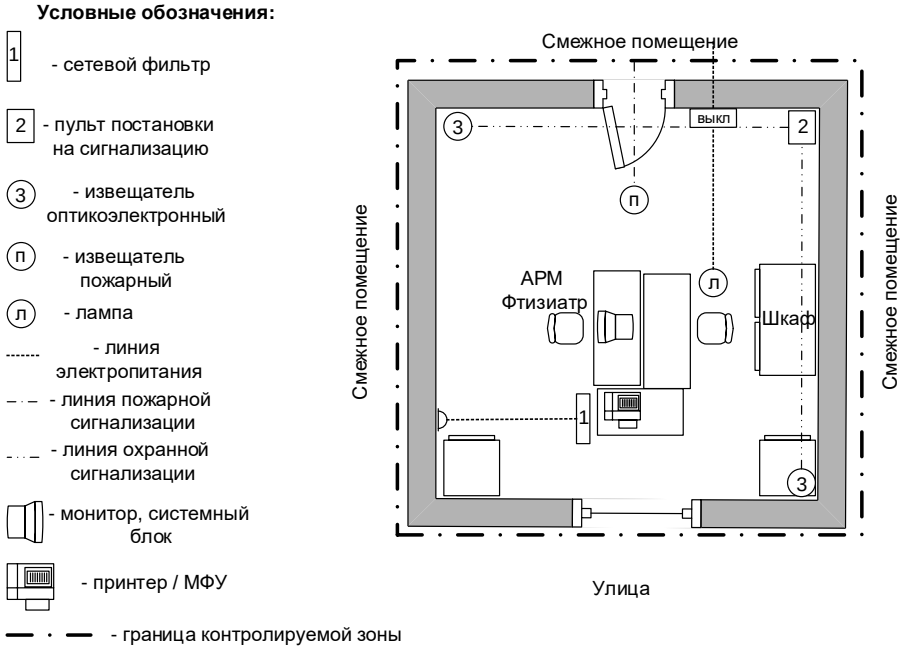
Схема расположения ОТСС и ВТСС и проводных линий в помещении

Противотуберкулезный диспансер:

Кабинет 6



Кабинет 7



Кабинет 10

Условные обозначения:

1 - сетевой фильтр

2 - пульт постановки на сигнализацию

(3) - извещатель оптикоэлектронный

(п) - извещатель пожарный

(л) - лампа

------ - линия электропитания

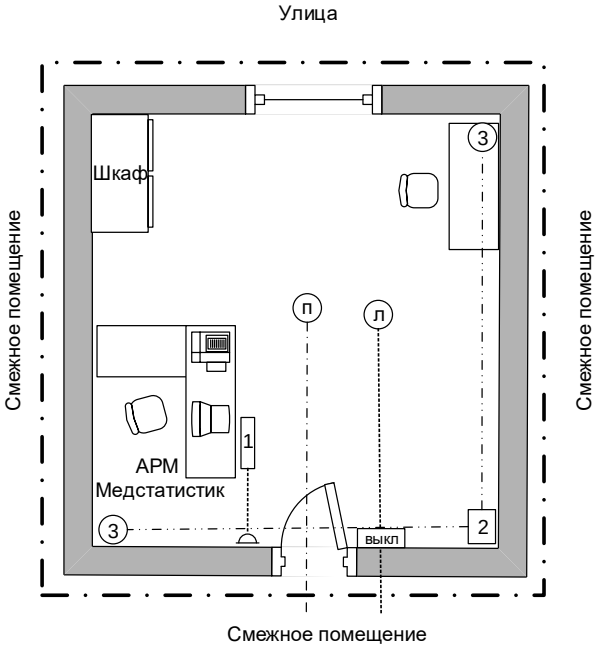
– · – - линия пожарной сигнализации

– · · – - линия охранной сигнализации

- монитор, системный блок

- принтер / МФУ

— · — - граница контролируемой зоны



Кабинет 12

Условные обозначения:

- сетевой фильтр

2 - пульт постановки на сигнализацию

(3) - извещатель оптикоэлектронный

(п) - извещатель пожарный

(л) - лампа

------ - линия электропитания

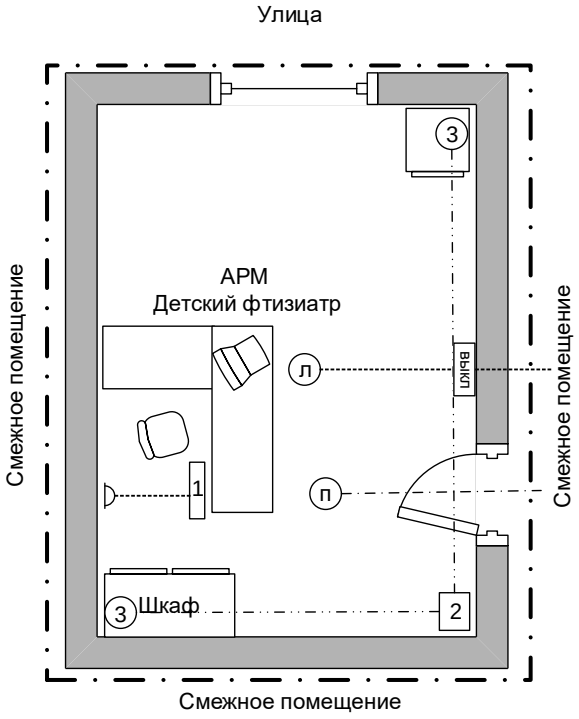
– · – - линия пожарной сигнализации

– · · – - линия охранной сигнализации

- монитор, системный блок

- принтер / МФУ

— · — - граница контролируемой зоны



Регистратура

Условные обозначения:

1 - сетевой фильтр

2 - пульт постановки на сигнализацию

З - извещатель оптикоэлектронный

п - извещатель пожарный

л - лампа

------ - линия электропитания

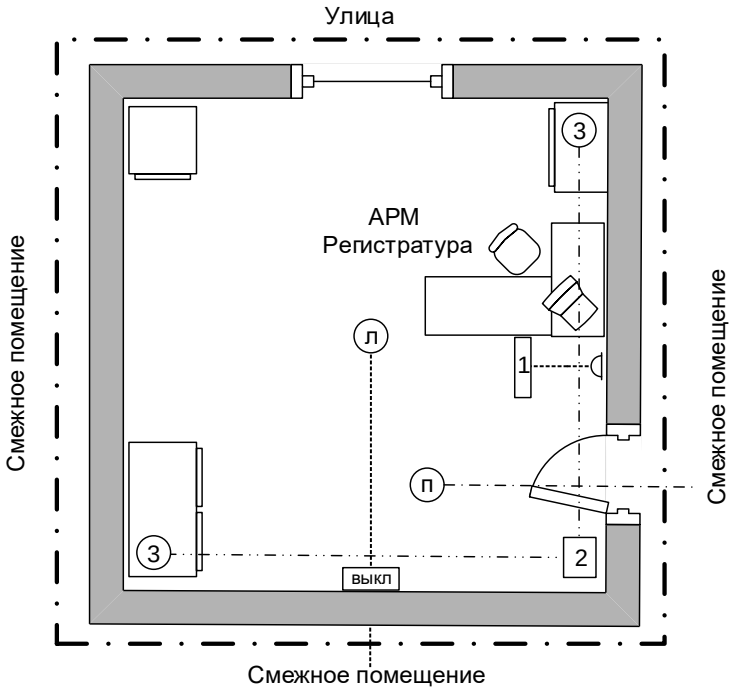
– · – - линия пожарной сигнализации

– ·· – - линия охранной сигнализации

- монитор, системный блок

- принтер / МФУ

— · — - граница контролируемой зоны

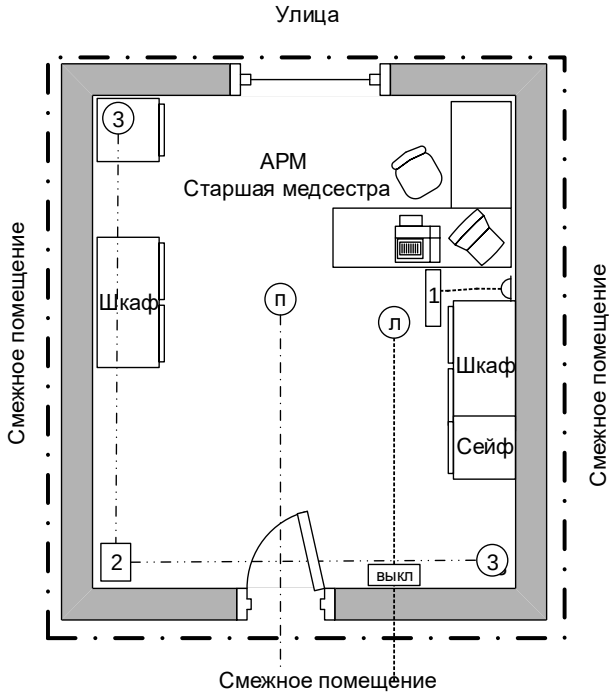


Противотуберкулезное отделение:

Кабинет старшей медсестры

Условные обозначения:

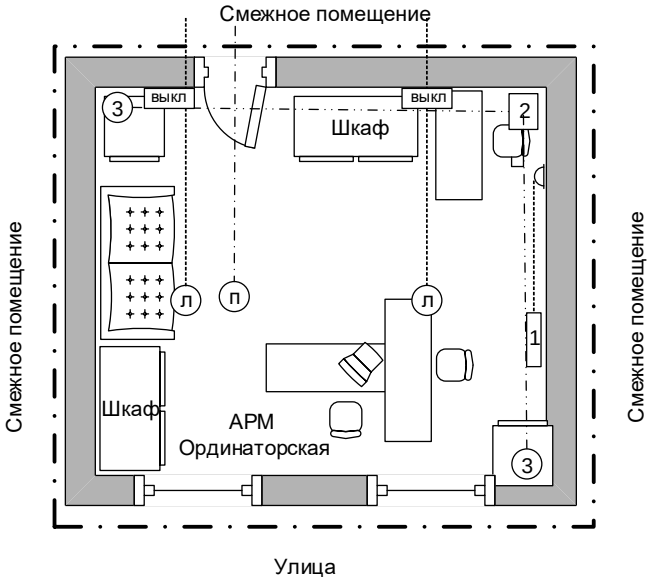
- 1 - сетевой фильтр
- 2 - пульт постановки на сигнализацию
- (3) - извещатель оптикоэлектронный
- (п) - извещатель пожарный
- (л) - лампа
- ------ - линия электропитания
- – · – - линия пожарной сигнализации
- – · _ - линия охранной сигнализации
- - монитор, системный блок
- - принтер / МФУ
- — · — - граница контролируемой зоны



Ординаторская

Условные обозначения:

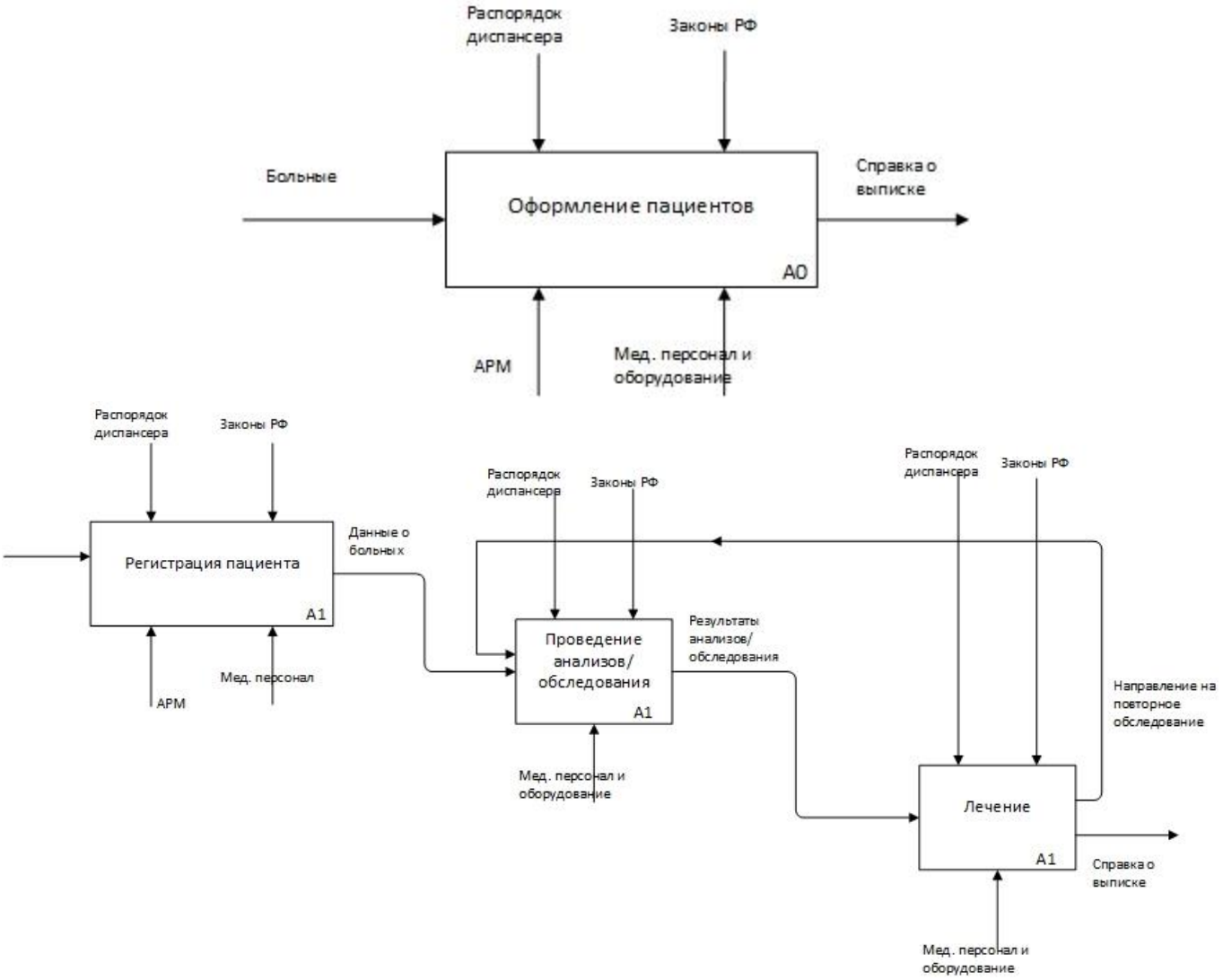
- 1 - сетевой фильтр
- 2 - пульт постановки на сигнализацию
- (3) - извещатель оптикоэлектронный
- (п) - извещатель пожарный
- (л) - лампа
- ------ - линия электропитания
- – · – - линия пожарной сигнализации
- – · _ - линия охранной сигнализации
- - монитор, системный блок
- - принтер / МФУ
- — · — - граница контролируемой зоны



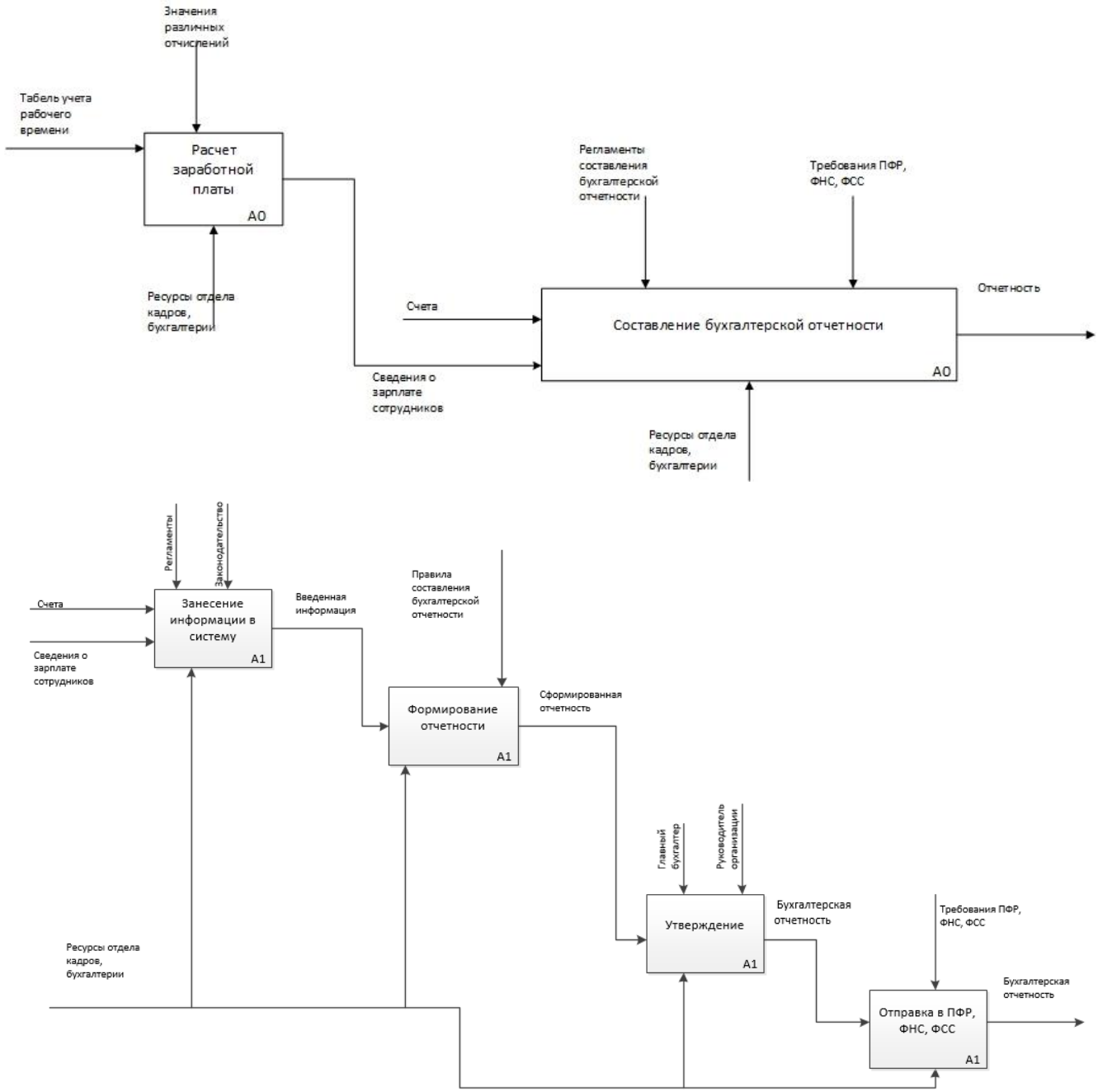
ПРИЛОЖЕНИЕ Д

Модели деятельности

Медицина:

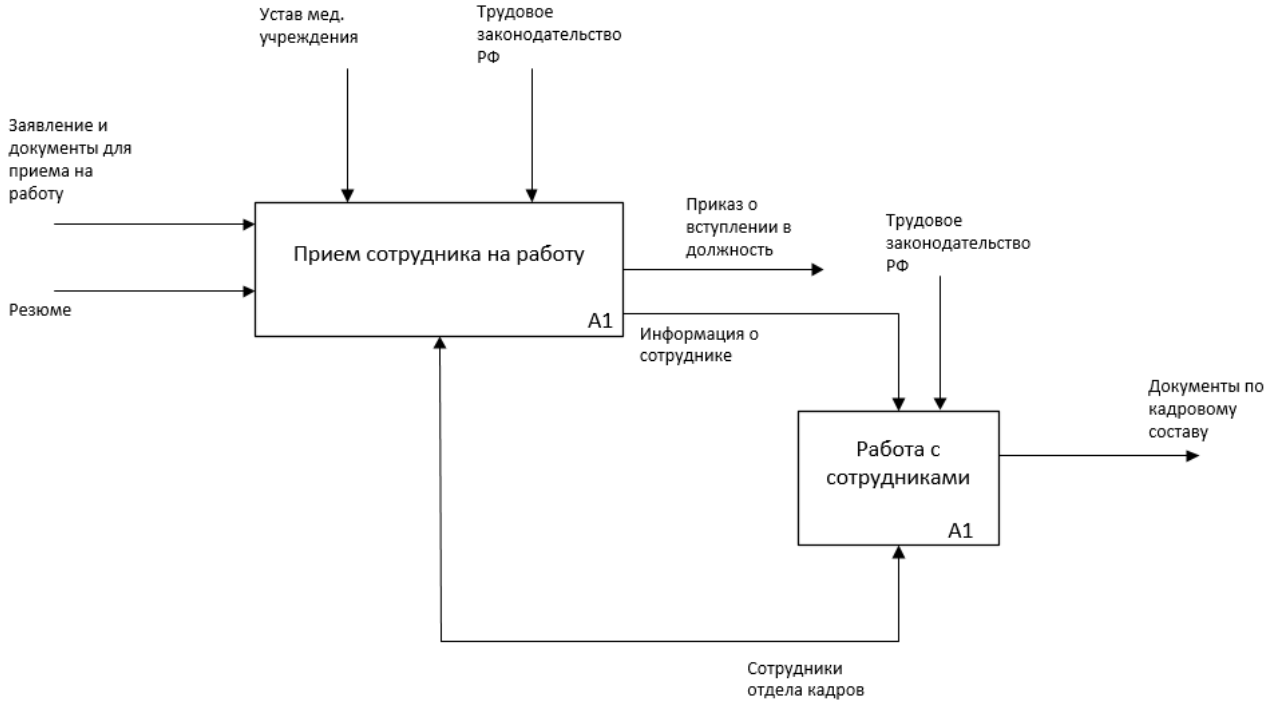


Бухгалтерия:



Кадры:


Устав мед. учреждения
Трудовое законодательство РФ
Заявление о приеме на работу
Резюме
Деятельность отдела кадров
A0
Приказы по кадровому составу
Сотрудники отдела кадров
Сотрудники бухгалтерии


Устав мед. учреждения
Трудовое законодательство РФ
Заявление и документы для приема на работу
Резюме
Прием сотрудника на работу
A1
Приказ о вступлении в должность
Трудовое законодательство РФ
Информация о сотруднике
Работа с сотрудниками
A1
Документы по кадровому составу
Сотрудники отдела кадров

ПРИЛОЖЕНИЕ Е

УТВЕРЖДЕН
приказом
главного врача
ГБУЗ «ОПТД № 8»
от _____ № _____

ПЕРЕЧЕНЬ
обрабатываемых персональных данных

ОБЩИЕ ПОЛОЖЕНИЯ

1. Перечень персональных данных, подлежащих защите в ГБУЗ «ОПТД № 8» (далее – Перечень), разработан в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» и Уставом ГБУЗ «ОПТД № 8».

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

2.1. Персональные данные работников:

2.1.1. Фамилия Имя Отчество;

2.1.2. ИНН;

2.1.3. СНИЛС (№ страхового пенсионного свидетельства);

2.1.4. табельный номер;

2.1.5. пол;

2.1.6. номер, дата трудового договора;

2.1.7. дата рождения;

2.1.8. место рождения;

2.1.9. гражданство;

2.1.10. образование (среднее (полное) общее, начальное профессиональное, среднее профессиональное, высшее профессиональное, аспирантура, адъюнктура, докторантура);

2.1.11. наименование образовательного учреждения;

2.1.12. наименование, серия, номер, дата выдачи, направление или специальность, код по ОКСО, ОКИН документа об образовании, о квалификации или наличии специальных знаний

2.1.13. профессия (в т.ч. код по ОКПДТР);

2.1.14. стаж работы;

2.1.15. состояние в браке;

2.1.16. состав семьи, с указанием степени родства, фамилии, имени, отчества, года рождения ближайших родственников;

2.1.17. данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ);

2.1.18. адрес и дата регистрации;

2.1.19. фактический адрес места жительства;

2.1.20. телефон;

2.1.21. сведения об отношении к воинской службе;

2.1.22. дата приема на работу;

2.1.23. характер работы;

2.1.24. вид работы (основной, по совместительству);

2.1.25. структурное подразделение;

2.1.26. занимаемая должность (специальность, профессия), разряд, класс (категория) квалификации;

2.1.27. ранее занимаемая должность;

2.1.28. тарифная ставка (оклад), надбавка, руб.;

2.1.29. номер лицевого банковского счета;

2.1.30. основание трудоустройства;

2.1.31. сведения об аттестации (дата, решение, номер и дата документа, основание);

2.1.32. сведения о профессиональной подготовке (дата начала и окончания переподготовки, специальность (направление, профессия, наименование, номер, дата документа, свидетельствующего о переподготовке, основание переподготовки);

2.1.33. сведения о наградах, поощрениях, почетных званиях (наименование, номер, дата награды);

2.1.34. сведения об отпусках (вид, период работы, количество дней, дата начала и окончания, основание);

2.1.35. сведения о социальных льготах, на которые работник имеет право в соответствии с законодательством (наименование льготы, номер, дата выдачи документа, основание);

2.1.36. сведения об увольнении (основания, дата, номер и дата приказа);

2.1.37. объем работы;

2.1.38. сведения из справки об инвалидности;

2.1.39. сведения из справки о состоянии здоровья;

2.1.40. сведения из водительского удостоверения;

2.1.41. сведения о доходах.

2.2. Персональные данные родственников работников:

2.2.1. Фамилия Имя Отчество;

2.2.2. степень родства;

2.2.3. год рождения.

2.3. Персональные данные бывших работников совпадают с пунктом 2.1.

2.4. Персональные данные пациентов и их законных представителей:

2.4.1. Фамилия Имя Отчество;

2.4.2. пол;

2.4.3. дата рождения;

2.4.4. место рождения;

2.4.5. фактический адрес жительства и адрес регистрации;

2.4.6. контактный телефон;

2.4.7. место работы;

2.4.8. СНИЛС;

2.4.9. данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ);

2.4.10. данные полиса ОМС;

2.4.11. сведения о состоянии здоровья;

2.4.12. сведения об оказанных медицинских услугах;

2.4.13. сведения об инвалидности;

2.4.14. семейное положение;

2.4.15. сведения о социальном положении.

2.5. Персональные данные кандидатов на замещение вакантных должностей:

2.5.1. Фамилия Имя Отчество;

2.5.2. образование (среднее (полное) общее, начальное профессиональное, среднее профессиональное, высшее профессиональное, аспирантура, адъюнктура, докторантура);

2.5.3. наименование образовательного учреждения;

2.5.4. наименование, направление или специальность документа об образовании, о квалификации или наличии специальных знаний;

2.5.5. сведения о предыдущем месте работы (дата поступления, дата окончания, организация, должность, заработная плата, причина увольнения, ФИО руководителя, должность, контактный телефон);

2.5.6. стаж работы;

2.5.7. контактный телефон,

2.5.8. адрес электронной почты.

2.6. Персональные данные контрагентов, представителей юридических лиц ГБУЗ «ОПТБ № 8»:

2.6.1. Фамилия Имя Отчество;

2.6.2. место работы;

2.6.3. должность;

2.6.4. контактный телефон;

2.6.5. e-mail.

ПРИЛОЖЕНИЕ Ж

УТВЕРЖДАЮ

Главный врач
ГБУЗ «ОПТД № 8»

_____А.С. Куликова
___ _____ _____г.

СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ДЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ
«МЕДИЦИНА»
Государственного бюджетного учреждения здравоохранения «Областной противотуберкулезный диспансер № 8»

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

На ___ листах
Действует с _____

г. Южноуральск
2018

1 ОБЩИЕ СВЕДЕНИЯ

1.1. Настоящее техническое задание разработано для информационной системы персональных данных «Медицина» Государственного бюджетного учреждения здравоохранения «Областной противотуберкулезный диспансер № 8» и описывает требования, предъявляемые к построению, внедрению системы защиты персональных данных.

1.2. Полное наименование и обозначение системы: Система защиты информации, обрабатываемой в информационной системе персональных данных «Медицина».

1.3. Сокращенное наименование системы: СЗПДн

1.4. Заказчик:

Заказчик	Государственное бюджетное учреждение здравоохранения «Областной противотуберкулезный диспансер № 8»
Юридический адрес	457040, Челябинская область, г. Южноуральск, ул. Мира, д. 4

1.5. Исполнитель: специалист по защите информации

1.6. Работы по созданию СЗПДн проводятся на основании настоящего технического задания

1.7. При разработке технического задания (далее - ТЗ) использовались следующие нормативно-технические документы и методические материалы:

а) Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
б) Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
в) Постановление Правительства РФ от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
г) Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
д) Приказ Гостехкомиссии России от 30 августа 2002 г. № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»;
е) Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
ж) Приказ ФСБ России от 10 июля 2014 г. №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
з) «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» №149/7/2/6-432 от 31.03.2015 г.
и) Руководящий документ ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

2 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1 **Назначение системы защиты персональных данных (далее - СЗПДн):**

2.1.1. Назначением СЗПДн является обеспечение информационной безопасности (далее - ИБ) персональных данных (далее - ПДн), обрабатываемых в информационной системе персональных данных (далее - ИСПДн).

2.1.2. СЗПДн призвана обеспечить конфиденциальность, целостность, доступность ПДн при их обработке в ИСПДн.

2.1.3. Объектом защиты СЗПДн является ИСПДн, описание которой приведено в частной модели угроз и модели нарушителя безопасности персональных данных информационной системы персональных данных (далее – Модель угроз).

2.2 **Цели создания СЗПДн:**

2.2.1 Целями создания СЗПДн являются:

а) обеспечение защищенности ИСПДн в процессе обработки и хранения ПДн, а также обеспечение конфиденциальности ПДн при их обработке, а также других необходимых характеристик защищенности информации;

б) соответствие требованиям обеспечения ИБ при обработке ПДн в ИСПДн, регламентируемых РД ФСТЭК России и ФСБ России.

2.2.2 В результате создания СЗПДн должно быть обеспечено:

а) нейтрализация актуальных угроз информационной безопасности ПДн;

б) определение подлинности субъекта доступа, отслеживание действий субъектов доступа.

2.3 **Критериями оценки достижения поставленных целей по созданию СЗПДн являются:**

а) соответствие требованиям по обеспечению безопасности ПДн в ИСПДн, согласно приказу ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», для которых определен уровень защищенности, согласно Постановлению Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

б) соответствие требованиям приказа ФСБ России от 10 июля 2014 г. №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

в) выполнение функциональных требований настоящего ТЗ.

3 ХАРАКТЕРИСТИКА ОБЪЕКТА ЗАЩИТЫ

3.1. Объектом защиты являются ПДн, обрабатываемые в ИСПДн «Медицина».

3.2. Категория обрабатываемых персональных данных – специальные;

3.3. Принадлежность обрабатываемых персональных данных – не сотрудники;

3.4. Объем обрабатываемых персональных данных в ИСПДн «Медицина» – менее 100 000 субъектов;

3.5. Тип актуальных угроз – 3;

3.6. Актуальные угрозы ИБ, которым подвержена ИСПДн «Медицина», определяются и обосновываются в Модели угроз, разрабатываемой Исполнителем на этапе проектирования ИСПДн на основе Руководящего документа ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

3.7. Для ПДн при их обработке в ИСПДн «Медицина» определен 3 уровень защищенности в соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3.8. Рабочие станции пользователей функционируют под управлением операционных систем Windows 7 Professional.

4 ТРЕБОВАНИЯ К СЗПДН

4.1 Требования к СЗПДн в целом

4.1.1 Требования к структуре и функционированию

4.1.1.1 В состав СЗПДн должны входить следующие подсистемы:

а) идентификации и аутентификации субъектов доступа и объектов доступа;

б) управления доступом субъектов доступа к объектам доступа;

в) защиты машинных носителей информации,

г) регистрации событий безопасности;

д) антивирусной защиты;

е) анализа защищенности;

ж) защиты технических средств;

з) защиты информационной системы, ее средств, систем связи и передачи данных;

и) управления конфигурацией информационной системы и системы защиты.

4.1.1.2 Структура СЗПДн может изменяться и уточняться по результатам разработки Модели угроз на предпроектной стадии с учетом обоснования необходимых изменений в ТЗ.

4.1.1.3 *Подсистема идентификации и аутентификации субъектов доступа и объектов доступа.* Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

4.1.1.4 *Подсистема управления доступом*. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

4.1.1.5 *Подсистема защиты машинных носителей информации*. Меры по защите машинных носителей информации (средства обработки (хранения) информации, съемные машинные носители информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных носителей информации.

4.1.1.6 *Подсистема регистрации и учета*. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

4.1.1.7 *Подсистема антивирусной защиты*. Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

4.1.1.8 *Подсистема контроля (анализа) защищенности информации*. Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

4.1.1.9 *Подсистема защиты технических средств*. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее – средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

4.1.1.10 *Подсистема защиты информационной системы, ее средств, систем связи и передачи данных*. Меры по защите информационной системы, ее средств, систем связи и передачи данных должны

обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

4.1.1.11 *Подсистема управления конфигурацией и системы защиты персональных данных*. Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

4.1.2 Требования к численности и квалификации персонала ИСПДн, режиму его функционирования

4.1.2.1 Квалификация персонала должна быть достаточной для осуществления им настройки общесистемных и сетевых сервисов СЗПДн и настройки СЗИ СЗПДн.

4.1.2.2 Персонал СЗПДн должен осуществлять обслуживание и эксплуатацию СЗПДн по рабочим дням в рабочее время, с возможностью выхода в нерабочее время для проведения сервисного обслуживания или восстановления работоспособности СЗПДн.

4.1.3 Показатели назначения

4.1.3.1 Системно-технические решения СЗПДн должны обеспечить минимизацию вероятности реализации угроз, описанных в Модели угроз для данной ИСПДн.

4.1.3.2 Экономический эффект от создания СЗПДн должен проявляться в снижении вероятной величины материального и морального ущерба по отношению к субъектам и оператору ПДн.

4.1.4 Требования к надежности

4.1.4.1 Должна быть обеспечена возможность резервного копирования конфигураций и журналов регистрации событий компонентов СЗПДн.

4.1.4.2 Аппаратно-программные компоненты СЗПДн должны функционировать в круглосуточном режиме и позволять осуществлять выполнение процедур резервирования и восстановления системы после сбоев.

4.1.5 Требования безопасности

4.1.5.1 Конструкция используемого оборудования должна обеспечивать защиту эксплуатирующего персонала от поражения электрическим током.

4.1.5.2 Размещение оборудования на штатных местах должно обеспечивать его безопасное обслуживание и эксплуатацию.

4.1.6 Требования к эргономике и технической эстетике

Автоматизированные рабочие места СЗПДн должны обеспечивать возможность непрерывной работы операторов в течение смены в соответствии с требованиями Постановления Главного государственного санитарного врача РФ от 3 июня 2003 г. № 118 «О введении в действие санитарно-эпидемиологических правил и нормативов СанПиН 2.2.2/2.4.1340-03» с изменениями от 25 апреля 2007 г.

4.1.7 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов СЗПДн

4.1.7.1 Эксплуатация программно-технических средств должна предусматривать следующие виды технического обслуживания:

а) оперативное обслуживание;

б) профилактические работы.

4.1.7.2 Оперативное обслуживание должно предусматривать ежедневный контроль функционирования аппаратно-технических средств. Оперативное обслуживание не должно нарушать выполнения функций СЗПДн в целом.

4.1.7.3 Профилактическое обслуживание должно предусматривать периодическую проверку и обслуживание составных частей СЗПДн, для которых такое обслуживание предусмотрено эксплуатационной документацией.

4.1.7.4 Объем и порядок выполнения технического обслуживания технических и программных средств СЗПДн должны определяться эксплуатационной документацией.

4.1.7.5 Физический доступ неуполномоченных лиц к сетевому и серверному оборудованию должен быть запрещен.

4.1.7.6 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению могут уточняться на этапе проектирования СЗПДн.

4.1.8 Требования по сохранности информации при авариях

Сохранность информации при авариях в СЗПДн должна обеспечиваться методом резервного копирования.

4.1.9 Требования к защите от влияния внешних воздействий

Защита ИСПДн от влияния внешних воздействий должна осуществляться в рамках общих организационно-технических мероприятий по обеспечению безопасности и физической защите на объектах заказчика.

4.1.10 Требования к патентной чистоте

4.1.10.1 При создании СЗПДн должны соблюдаться положения законодательных актов Российской Федерации по соблюдению авторских прав и защите специальных знаков.

4.1.10.2 При поставке программного обеспечения должны быть выполнены требования части IV Гражданского Кодекса Российской Федерации, а также международные патентные соглашения.

4.1.11 Требования к стандартизации и унификации

4.1.11.1 Решения по использованию технических средств и ПО в СЗПДн должны использовать однотипные компоненты в целях обеспечения снижения расходов на обслуживание и ремонт, взаимозаменяемости используемых компонентов, удобства эксплуатации.

4.1.11.2 Должна обеспечиваться совместимость технических средств и ПО СЗПДн с техническими средствами и ПО, используемыми в ИСПДн «ОПТД 8».

4.1.11.3 При применении технических средств и ПО особое внимание должно быть уделено унификации программных и аппаратных решений. Предпочтение должно отдаваться использованию готовых, проверенных на практике решений.

4.2 Требования к функциям, выполняемым СЗПДн

4.2.1 Подсистема идентификации и аутентификации субъектов доступа и объектов доступа (ИАФ)

В подсистеме должны обеспечиваться:

1) идентификация и аутентификация пользователей, являющихся работниками оператора (ИАФ.1);

2) управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов (ИАФ.3);

3) управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации (ИАФ.4);

4) защита обратной связи при вводе аутентификационной информации (ИАФ.5);

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации;

– средства защиты информации от несанкционированного доступа, имеющие действующий сертификат соответствия требованиям, предъявляемым к средствам вычислительной техники не ниже 5 класса.

4.2.2 Подсистема управления доступом субъектов доступа к объектам доступа (УПД)

В подсистеме должны обеспечиваться:

5) управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей (УПД.1);

6) реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа (УПД.2);

7) управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами (УПД.3);

8) разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы (УПД.4);

9) назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы (УПД.5);

10) ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) (УПД.6);

11) блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу (УПД.10);

12) разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации (УПД.11);

13) реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети (УПД.13);

14) Регламентация и контроль использования в информационной системе технологий беспроводного доступа (УПД.14);

15) регламентация и контроль использования в информационной системе мобильных технических средств (УПД.15);

16) управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) (УПД.16).

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации;

– средства защиты информации от несанкционированного доступа, имеющие действующий сертификат соответствия требованиям ФСТЭК, предъявляемым к средствам вычислительной техники не ниже 5 класса;

– средства межсетевого экранирования, имеющие действующий сертификат соответствия требованиям ФСТЭК (ФСБ), предъявляемым к межсетевым экранам не ниже 6 класса;

– средства защиты каналов передачи данных, имеющие действующий сертификат соответствия требованиям ФСБ, предъявляемым к средствам криптографической защиты информации.

4.2.3 Подсистема защиты машинных носителей информации (ЗНИ)

В подсистеме должны обеспечиваться:

17) учет машинных носителей информации (ЗНИ.1);

18) управление доступом к машинным носителям информации (ЗНИ.2);

19) уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) (ЗНИ.8).

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации;

– средства защиты информации от несанкционированного доступа, имеющие действующий сертификат соответствия требованиям ФСТЭК, предъявляемым к средствам вычислительной техники не ниже 5 класса.

4.2.4 Регистрация событий безопасности (РСБ)

В подсистеме должны обеспечиваться:

20) определение событий безопасности, подлежащих регистрации, и сроков их хранения (РСБ.1);

21) определение состава и содержания информации о событиях безопасности, подлежащих регистрации (РСБ.2);

22) сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения (РСБ.3);

23) защита информации о событиях безопасности (РСБ.7).

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации;

– средства защиты информации от несанкционированного доступа, имеющие действующий сертификат соответствия требованиям ФСТЭК, предъявляемым к средствам вычислительной техники не ниже 5 класса;

– средства межсетевого экранирования, имеющие действующий сертификат соответствия требованиям ФСТЭК (ФСБ), предъявляемым к межсетевым экранам не ниже 6 класса.

4.2.5 Подсистема антивирусной защиты (АВЗ)

В подсистеме должны обеспечиваться:

24) реализация антивирусной защиты (АВЗ.1);

25) обновление базы данных признаков вредоносных компьютерных программ (вирусов) (АВЗ.2).

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации;

– средства антивирусной защиты информации, имеющие действующий сертификат соответствия требованиям ФСТЭК, предъявляемым к средствам антивирусной защиты не ниже 6 класса.

4.2.6 Подсистема анализа защищенности информации (АНЗ)

В подсистеме должны обеспечиваться:

26) выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей (АНЗ.1);

27) контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации (АНЗ.2);

28) контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации (АНЗ.3);

29) контроль состава технических средств, программного обеспечения и средств защиты информации (АНЗ.4);

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации;

– средства анализа защищенности, имеющие действующий сертификат соответствия требованиям ФСТЭК, предъявляемым к сканерам уязвимостей.

4.2.7 Подсистема защиты технических средств (ЗТС)

В подсистеме должны обеспечиваться:

30) организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования (ЗТС.2);

31) контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены (ЗТС.3);

32) размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр (ЗТС.4).

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации.

4.2.8 Подсистема защиты информационной системы, ее средств, систем связи и передачи данных (ЗИС)

В подсистеме должны обеспечиваться:

33) обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи (ЗИС.3);

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации;

– средства межсетевого экранирования, имеющие действующий сертификат соответствия требованиям ФСТЭК, предъявляемым к межсетевым экранам не ниже 6 класса;

– средства защиты каналов передачи данных, имеющие действующий сертификат соответствия требованиям ФСБ, предъявляемым к средствам криптографической защиты информации.

4.2.9 Подсистема управление конфигурацией информационной системы и системы защиты (УКФ)

В подсистеме должны обеспечиваться:

34) определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных (УКФ.1);

35) управление изменениями конфигурации информационной системы и системы защиты персональных данных (УКФ.2);

36) анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных (УКФ.3);

37) документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных (УКФ.4).

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации.

4.3 Требования к видам обеспечения

4.3.1 Требования к программному обеспечению

4.3.1.1 Выбор программных средств защиты должен проводиться с учетом средств защиты, эксплуатируемых у заказчика.

4.3.1.2 Средства защиты информации, входящие в состав СЗПДн, должны быть сертифицированы на соответствие требованиям руководящих документов ФСТЭК и ФСБ России.

4.3.1.3 При создании СЗПДн должно использоваться только лицензионное общее и специальное программное обеспечение и операционные системы.

4.3.1.4 Требования к программному обеспечению, используемому для защиты информации в ИСПДн «Медицина» (средств защиты информации, в том числе и встроенных в общесистемное и прикладное ПО) в части необходимости обеспечения контроля отсутствия в нем недекларированных возможностей (НДВ) должны быть определены в ТЗ.

4.3.2 Требования к техническому обеспечению

Выбор аппаратных (программно-аппаратных) средств защиты должен проводиться с учетом средств защиты, эксплуатируемых у заказчика.

4.3.3 Требования к организационному обеспечению

4.3.3.1 Мониторы АРМ должны располагаться таким образом, чтобы препятствовать возможности несанкционированного визуального съема информации с них.

4.3.3.2 Должна осуществляться физическая охрана устройств и носителей информации ИСПДн «Медицина», предусматривающая:

4.3.3.3 контроль доступа в помещения ИСПДн «Медицина» посторонних лиц;

4.3.3.4 наличие надежных препятствий для несанкционированного проникновения в помещение ИСПДн «ОПТД 8» и хранилище носителей информации, особенно в нерабочее время.

4.3.3.5 Должны быть проведены работы по подготовке проектов и введению в действие следующих организационно-распорядительных документов, направленных на обеспечение информационной безопасности:

– приказов о назначении ответственных лиц;

– документа, определяющего политику в отношении обработки персональных данных;

– локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;

– уведомления уполномоченного органа по защите прав субъектов персональных данных о намерении осуществлять обработку персональных данных;

– документов, определяющих круг лиц, имеющих доступ к ИСПДн, ее компонентам;

– форм согласия субъекта персональных данных на обработку его персональных данных;

– документа, содержащего перечень обрабатываемых персональных данных;

– документа, содержащего перечень нормативных правовых актов, в соответствии с которыми производится обработка персональных данных.

4.3.3.6 Для соблюдения требований Приказа ФСБ России от 10 июля 2014 г. №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» Заказчику необходимо провести:

– оснащение помещений входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода, а также опечатывания помещений по окончании рабочего дня или оборудование помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений (ФСБ-1);

– утверждение правил доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях. (ФСБ-2);

– утверждение перечня лиц, имеющих право доступа в помещения. (ФСБ-3);

– осуществление хранения съемных машинных носителей персональных данных в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. (ФСБ-4);

– осуществление поэкземплярного учета машинных носителей персональных данных, который достигается путем ведения журнала учета носителей персональных данных с использованием регистрационных (заводских) номеров. (ФСБ-5);

– разработка и утверждение документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей. (ФСБ-6);

– поддержание в актуальном состоянии документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей. (ФСБ-7);

– использование для обеспечения требуемого уровня защищенности персональных данных при их обработке в информационной системе СКЗИ класса КС1 и выше (ФСБ-8);

– назначение обладающего достаточными навыками должностного лица (работника) оператора ответственным за обеспечение безопасности персональных данных в информационной системе (ФСБ-9).

5 СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СЗПДН

5.1 Разработка СЗПДн, поставка оборудования, монтаж оборудования

5.1.1 Разработка СЗПДн

Проводится обследование ИСПДн:

а) уточняется перечень ПДн, подлежащих защите;

б) уточняется информация о категориях и составе ПДн, обрабатываемых автоматизированными и неавтоматизированными способами;

в) проводится анализ состава ПДн в ИСПДн, собирается информация о защищенности ПДн;

г) уточняются условия расположения объекта защиты относительно границ контролируемой зоны;

д) уточняются конфигурация и топология ИСПДн и систем связи в целом и их компонентов, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;

е) уточняются состав технических средств и систем, предполагаемых к использованию в СЗПДн, условия их расположения, общесистемные и прикладные программные средства;

ж) уточняются режимы обработки информации в ИСПДн в целом и в отдельных ее компонентах;

з) для ИСПДн производится анализ собранной информации об угрозах и их показателях для разработки Модели угроз;

и) уточняется уровень защищенности ПДн, обрабатываемых в ИСПДн;

к) разрабатывается Модель угроз для ИСПДн на основе методических рекомендаций ФСТЭК России;

л) уточняется степень участия сотрудников в обработке информации, характер их взаимодействия между собой и со службой ИБ.

Также на данном этапе разрабатывается пакет организационно-распорядительной документации на ИСПДн.

5.1.2 Поставка оборудования

Осуществляются работы по закупке необходимого оборудования.

Все поставляемое оборудование должно пройти процедуру оценки соответствия требованиям по безопасности информации и иметь сертификат ФСТЭК России и ФСБ России (в соответствии с требованиями нормативно-методических документов).

5.1.3 Монтаж оборудования

Если в процессе выполнения работ по монтажу оборудования возникают какие-либо нештатные ситуации, а также ситуации, которые могут повлечь приостановление вышеуказанных работ, то принимаются все необходимые меры по устранению и ликвидации причин, которые привели к таким ситуациям.

5.2 Передача прав на использование программного обеспечения, входящего в состав СЗПДн

Все программное обеспечение должно пройти процедуру оценки соответствия требованиям по безопасности информации и иметь сертификат ФСТЭК России или ФСБ России (в соответствии с требованиями нормативно-методических документов).

5.3 Пусконаладочные работы, опытная эксплуатация СЗПДн, оценка эффективности реализованных мер

5.3.1 Пусконаладочные работы

Проводятся пусконаладочные работы СЗПДн, обеспечивающие интеграцию с локальной вычислительной сетью.

Проводится анализ защищенности сетевых сегментов ИСПДн (в пределах ЛВС) с использованием средств анализа защищенности.

Если в процессе выполнения пусконаладочных работ СЗПДн возникают какие-либо нештатные ситуации, а также ситуации, которые могут повлечь приостановление вышеуказанных работ, принимаются все возможные меры по устранению и ликвидации причин, которые привели к таким ситуациям.

5.3.2 Опытная эксплуатация

Опытная эксплуатация включает в себя комплексную проверку готовности СЗПДн. Опытная эксплуатация имеет своей целью проверку алгоритмов, отладку работы СЗПДн и технологического процесса обработки данных при использовании СЗПДн.

По окончании опытной эксплуатации возможна доработка СЗПДн.

В случае необходимости проводится обучение персонала использованию СЗИ, применяемых в СЗПДн.

5.3.3 Оценка эффективности

Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится учреждением самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже одного раза в 3 года.

6 ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ

6.1. Исполнитель должен быть заранее проинформирован о порядке и сроках согласования отчетных материалов, перечне вопросов, которые подлежат согласованию.

6.2 В случае необходимости может быть проведена защита предлагаемых решений в процессе технического совещания.

6.3 Настоящее ТЗ может быть уточнено или изменено в процессе работы. Уточнения и изменения ТЗ производятся по согласованию сторон. Оформление изменений осуществляется выпуском дополнений, которые являются неотъемлемой частью настоящего ТЗ.

6.4 Согласование и утверждение изменений производится в том же порядке и теми же должностными лицами, что и согласование и утверждение ТЗ.

6.5 Замечания по отчетным материалам должны быть представлены исполнителю с техническим обоснованием в письменной форме.

6.6 Сроки приемки работ определяются календарным планом, согласованным с заказчиком.

7. ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ ОБЪЕКТА АВТОМАТИЗАЦИИ К ВВОДУ СЗПДН В ДЕЙСТВИЕ

В перечень основных мероприятий включают:

а) Приведение поступающей в систему информации к виду, пригодному для обработки с помощью ЭВМ;

б) Изменения, которые необходимо осуществить в информационной системе;

в) Создание условий функционирования информационной системы, при которых гарантируется соответствие создаваемой системы требованиям, содержащимся в ТЗ;

г) Создание необходимых для функционирования системы подразделений и служб;

д) Сроки и порядок комплектования штатов и обучения персонала.

8. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

Комплект проектных материалов предоставляется заказчику по предварительной договоренности в электронном виде и (или) на твердой копии. Вся разрабатываемая проектная документация должна быть выполнена на русском языке.

9. ИСТОЧНИКИ РАЗРАБОТКИ

9.1. При разработке проектных решений необходимо руководствоваться официальными документами фирм-производителей применяемых аппаратных средств и программного обеспечения, документами третьих сторон, осуществляющих тестирование и эксплуатацию решений, материалами, предоставляемыми Пользователем.

9.2. Проектные решения должны обеспечивать соблюдение федеральных законов, постановлений Правительства Российской Федерации и иных нормативных актов.

ПРИЛОЖЕНИЕ 3

УТВЕРЖДАЮ

Главный врач
ГБУЗ «ОПТД № 8»

_____А.С. Куликова
___ _____ _____г.

СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ДЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ
«БУХГАЛТЕРИЯ И КАДРЫ»
Государственного бюджетного учреждения здравоохранения «Областной противотуберкулезный диспансер № 8»

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

На ___ листах
Действует с _____

г. Южноуральск
2018

1 ОБЩИЕ СВЕДЕНИЯ

1.1. Настоящее техническое задание разработано для информационной системы персональных данных «Бухгалтерия и кадры» Государственного бюджетного учреждения здравоохранения «Областной противотуберкулезный диспансер № 8» и описывает требования, предъявляемые к построению, внедрению системы защиты персональных данных.

1.2. Полное наименование и обозначение системы: Система защиты информации, обрабатываемой в информационной системе персональных данных «Бухгалтерия и кадры».

1.3. Сокращенное наименование системы: СЗПДн

1.4. Заказчик:

Заказчик	Государственное бюджетное учреждение здравоохранения «Областной противотуберкулезный диспансер № 8»
Юридический адрес	457040, Челябинская область, г. Южноуральск, ул. Мира, д. 4

1.5. Исполнитель: специалист по защите информации

1.6. Работы по созданию СЗПДн проводятся на основании настоящего технического задания

1.7. При разработке технического задания (далее - ТЗ) использовались следующие нормативно-технические документы и методические материалы:

а) Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

б) Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

в) Постановление Правительства РФ от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

г) Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

д) Приказ Гостехкомиссии России от 30 августа 2002 г. № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»;

е) Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

ж) Приказ ФСБ России от 10 июля 2014 г. №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

з) «Методических рекомендациях по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» №149/7/2/6-432 от 31.03.2015 г.

и) Руководящий документ ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

2 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1 **Назначение системы защиты персональных данных (далее - СЗПДн):**

2.1.1. Назначением СЗПДн является обеспечение информационной безопасности (далее - ИБ) персональных данных (далее - ПДн), обрабатываемых в информационной системе персональных данных (далее - ИСПДн).

2.1.2. СЗПДн призвана обеспечить конфиденциальность, целостность, доступность ПДн при их обработке в ИСПДн.

2.1.3. Объектом защиты СЗПДн является ИСПДн, описание которой приведено в частной модели угроз и модели нарушителя безопасности персональных данных информационной системы персональных данных (далее – Модель угроз).

2.2 **Цели создания СЗПДн:**

2.2.1 Целями создания СЗПДн являются:

в) обеспечение защищенности ИСПДн в процессе обработки и хранения ПДн, а также обеспечение конфиденциальности ПДн при их обработке, а также других необходимых характеристик защищенности информации;

г) соответствие требованиям обеспечения ИБ при обработке ПДн в ИСПДн, регламентируемых РД ФСТЭК России и ФСБ России.

2.2.2 В результате создания СЗПДн должно быть обеспечено:

в) нейтрализация актуальных угроз информационной безопасности ПДн;

г) определение подлинности субъекта доступа, отслеживание действий субъектов доступа.

2.3 **Критериями оценки достижения поставленных целей по созданию СЗПДн являются:**

г) соответствие требованиям по обеспечению безопасности ПДн в ИСПДн, согласно приказу ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», для которых определен уровень защищенности, согласно Постановлению Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

д) соответствие требованиям приказа ФСБ России от 10 июля 2014 г. №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

е) выполнение функциональных требований настоящего ТЗ.

3 ХАРАКТЕРИСТИКА ОБЪЕКТА ЗАЩИТЫ

3.1. Объектом защиты являются ПДн, обрабатываемые в ИСПДн «Бухгалтерия и кадры».

3.2. Категория обрабатываемых персональных данных – иные;

3.3. Принадлежность обрабатываемых персональных данных – не сотрудники;

3.4. Объем обрабатываемых персональных данных в ИСПДн «Бухгалтерия и кадры» – менее 100 000 субъектов;

3.5. Тип актуальных угроз – 3;

3.6. Актуальные угрозы ИБ, которым подвержена ИСПДн «Бухгалтерия и кадры», определяются и обосновываются в Модели угроз, разрабатываемой Исполнителем на этапе проектирования ИСПДн на основе Руководящего документа ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

3.7. Для ПДн при их обработке в ИСПДн «Бухгалтерия и кадры» определен 4 уровень защищенности в соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3.8. Рабочие станции пользователей функционируют под управлением операционных систем Windows 7 Professional.

4 ТРЕБОВАНИЯ К СЗПДН

4.1 Требования к СЗПДн в целом

4.1.1 Требования к структуре и функционированию

4.1.1.1 В состав СЗПДн должны входить следующие подсистемы:

а) идентификации и аутентификации субъектов доступа и объектов доступа;

б) управления доступом субъектов доступа к объектам доступа;

в) защиты машинных носителей информации,

г) регистрации событий безопасности;

д) антивирусной защиты;

е) анализа защищенности;

ж) защиты технических средств;

з) защиты информационной системы, ее средств, систем связи и передачи данных.

4.1.1.2 Структура СЗПДн может изменяться и уточняться по результатам разработки Модели угроз на предпроектной стадии с учетом обоснования необходимых изменений в ТЗ.

4.1.1.3 *Подсистема идентификации и аутентификации субъектов доступа и объектов доступа.* Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

4.1.1.4 *Подсистема управления доступом*. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

4.1.1.5 *Подсистема защиты машинных носителей информации*. Меры по защите машинных носителей информации (средства обработки (хранения) информации, съемные машинные носители информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных носителей информации.

4.1.1.6 *Подсистема регистрации и учета*. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

4.1.1.7 *Подсистема антивирусной защиты*. Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

4.1.1.8 *Подсистема контроля (анализа) защищенности информации*. Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

4.1.1.9 *Подсистема защиты технических средств*. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее – средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

4.1.1.10 *Подсистема защиты информационной системы, ее средств, систем связи и передачи данных*. Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных

сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

4.1.2 Требования к численности и квалификации персонала ИСПДн, режиму его функционирования

4.1.2.3 Квалификация персонала должна быть достаточной для осуществления им настройки общесистемных и сетевых сервисов СЗПДн и настройки СЗИ СЗПДн.

4.1.2.4 Персонал СЗПДн должен осуществлять обслуживание и эксплуатацию СЗПДн по рабочим дням в рабочее время, с возможностью выхода в нерабочее время для проведения сервисного обслуживания или восстановления работоспособности СЗПДн.

4.1.3 Показатели назначения

4.1.3.3 Системно-технические решения СЗПДн должны обеспечить минимизацию вероятности реализации угроз, описанных в Модели угроз для данной ИСПДн.

4.1.3.4 Экономический эффект от создания СЗПДн должен проявляться в снижении вероятной величины материального и морального ущерба по отношению к субъектам и оператору ПДн.

4.1.4 Требования к надежности

4.1.4.3 Должна быть обеспечена возможность резервного копирования конфигураций и журналов регистрации событий компонентов СЗПДн.

4.1.4.4 Аппаратно-программные компоненты СЗПДн должны функционировать в круглосуточном режиме и позволять осуществлять выполнение процедур резервирования и восстановления системы после сбоев.

4.1.5 Требования безопасности

4.1.5.3 Конструкция используемого оборудования должна обеспечивать защиту эксплуатирующего персонала от поражения электрическим током.

4.1.5.4 Размещение оборудования на штатных местах должно обеспечивать его безопасное обслуживание и эксплуатацию.

4.1.6 Требования к эргономике и технической эстетике

Автоматизированные рабочие места СЗПДн должны обеспечивать возможность непрерывной работы операторов в течение смены в соответствии с требованиями Постановления Главного государственного санитарного врача РФ от 3 июня 2003 г. № 118 «О введении в действие санитарно-эпидемиологических правил и нормативов СанПиН 2.2.2/2.4.1340-03» с изменениями от 25 апреля 2007 г.

4.1.7 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов СЗПДн

4.1.7.1 Эксплуатация программно-технических средств должна предусматривать следующие виды технического обслуживания:

в) оперативное обслуживание;

г) профилактические работы.

4.1.7.2 Оперативное обслуживание должно предусматривать ежедневный контроль функционирования аппаратно-технических средств. Оперативное обслуживание не должно нарушать выполнения функций СЗПДн в целом.

4.1.7.3 Профилактическое обслуживание должно предусматривать периодическую проверку и обслуживание составных частей СЗПДн, для которых такое обслуживание предусмотрено эксплуатационной документацией.

4.1.7.4 Объем и порядок выполнения технического обслуживания технических и программных средств СЗПДн должны определяться эксплуатационной документацией.

4.1.7.5 Физический доступ неуполномоченных лиц к сетевому и серверному оборудованию должен быть запрещен.

4.1.7.6 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению могут уточняться на этапе проектирования СЗПДн.

4.1.8 Требования по сохранности информации при авариях

Сохранность информации при авариях в СЗПДн должна обеспечиваться методом резервного копирования.

4.1.9 Требования к защите от влияния внешних воздействий

Защита ИСПДн от влияния внешних воздействий должна осуществляться в рамках общих организационно-технических мероприятий по обеспечению безопасности и физической защите на объектах заказчика.

4.1.10 Требования к патентной чистоте

4.1.10.3 При создании СЗПДн должны соблюдаться положения законодательных актов Российской Федерации по соблюдению авторских прав и защите специальных знаков.

4.1.10.4 При поставке программного обеспечения должны быть выполнены требования части IV Гражданского Кодекса Российской Федерации, а также международные патентные соглашения.

4.1.11 Требования к стандартизации и унификации

4.1.11.4 Решения по использованию технических средств и ПО в СЗПДн должны использовать однотипные компоненты в целях обеспечения снижения расходов на обслуживание и ремонт, взаимозаменяемости используемых компонентов, удобства эксплуатации.

4.1.11.5 Должна обеспечиваться совместимость технических средств и ПО СЗПДн с техническими средствами и ПО, используемыми в ИСПДн «ОПТД 8».

4.1.11.6 При применении технических средств и ПО особое внимание должно быть уделено унификации программных и аппаратных решений. Предпочтение должно отдаваться использованию готовых, проверенных на практике решений.

4.2 Требования к функциям, выполняемым СЗПДн

4.2.1 Подсистема идентификации и аутентификации субъектов доступа и объектов доступа (ИАФ)

В подсистеме должны обеспечиваться:

1) идентификация и аутентификация пользователей, являющихся работниками оператора (ИАФ.1);

2) управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов (ИАФ.3);

3) управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации (ИАФ.4);

4) защита обратной связи при вводе аутентификационной информации (ИАФ.5);

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации;

– средства защиты информации от несанкционированного доступа, имеющие действующий сертификат соответствия требованиям, предъявляемым к средствам вычислительной техники не ниже 6 класса.

4.2.2 Подсистема управления доступом субъектов доступа к объектам доступа (УПД)

В подсистеме должны обеспечиваться:

5) управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей (УПД.1);

6) реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа (УПД.2);

7) управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами (УПД.3);

8) разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы (УПД.4);

9) назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы (УПД.5);

10) ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) (УПД.6);

11) реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети (УПД.13);

12) Регламентация и контроль использования в информационной системе технологий беспроводного доступа (УПД.14);

13) регламентация и контроль использования в информационной системе мобильных технических средств (УПД.15);

14) управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) (УПД.16).

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации;

– средства защиты информации от несанкционированного доступа, имеющие действующий сертификат соответствия требованиям ФСТЭК, предъявляемым к средствам вычислительной техники не ниже 6 класса;

– средства межсетевого экранирования, имеющие действующий сертификат соответствия требованиям ФСТЭК (ФСБ), предъявляемым к межсетевым экранам не ниже 6 класса;

– средства защиты каналов передачи данных, имеющие действующий сертификат соответствия требованиям ФСБ, предъявляемым к средствам криптографической защиты информации.

4.2.3 Подсистема защиты машинных носителей информации (ЗНИ)

В подсистеме должны обеспечиваться:

15) учет машинных носителей информации (ЗНИ.1);

16) управление доступом к машинным носителям информации (ЗНИ.2);

17) уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) (ЗНИ.8).

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации;

– средства защиты информации от несанкционированного доступа, имеющие действующий сертификат соответствия требованиям ФСТЭК, предъявляемым к средствам вычислительной техники не ниже 6 класса.

4.2.4 Регистрация событий безопасности (РСБ)

В подсистеме должны обеспечиваться:

18) определение событий безопасности, подлежащих регистрации, и сроков их хранения (РСБ.1);

19) определение состава и содержания информации о событиях безопасности, подлежащих регистрации (РСБ.2);

20) сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения (РСБ.3);

21) защита информации о событиях безопасности (РСБ.7).

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации;

– средства защиты информации от несанкционированного доступа, имеющие действующий сертификат соответствия требованиям ФСТЭК, предъявляемым к средствам вычислительной техники не ниже 6 класса;

– средства межсетевого экранирования, имеющие действующий сертификат соответствия требованиям ФСТЭК (ФСБ), предъявляемым к межсетевым экранам не ниже 6 класса.

4.2.5 Подсистема антивирусной защиты (АВЗ)

В подсистеме должны обеспечиваться:

22) реализация антивирусной защиты (АВЗ.1);

23) обновление базы данных признаков вредоносных компьютерных программ (вирусов) (АВЗ.2).

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации;

– средства антивирусной защиты информации, имеющие действующий сертификат соответствия требованиям ФСТЭК, предъявляемым к средствам антивирусной защиты не ниже 6 класса.

4.2.6 Подсистема анализа защищенности информации (АНЗ)

В подсистеме должны обеспечиваться:

24) контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации (АНЗ.2).

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации;

– средства анализа защищенности, имеющие действующий сертификат соответствия требованиям ФСТЭК, предъявляемым к сканерам уязвимостей.

4.2.7 Подсистема защиты технических средств (ЗТС)

В подсистеме должны обеспечиваться:

25) организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования (ЗТС.2);

26) контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены (ЗТС.3);

27) размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр (ЗТС.4).

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации.

4.2.8 Подсистема защиты информационной системы, ее средств, систем связи и передачи данных (ЗИС)

В подсистеме должны обеспечиваться:

28) обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи (ЗИС.3);

Для реализации подсистемы должны использоваться:

– организационные меры защиты информации;

– средства межсетевого экранирования, имеющие действующий сертификат соответствия требованиям ФСТЭК, предъявляемым к межсетевым экранам не ниже 6 класса;

– средства защиты каналов передачи данных, имеющие действующий сертификат соответствия требованиям ФСБ, предъявляемым к средствам криптографической защиты информации.

4.3 Требования к видам обеспечения

4.3.1 Требования к программному обеспечению

4.3.1.1 Выбор программных средств защиты должен проводиться с учетом средств защиты, эксплуатируемых у заказчика.

4.3.1.2 Средства защиты информации, входящие в состав СЗПДн, должны быть сертифицированы на соответствие требованиям руководящих документов ФСТЭК и ФСБ России.

4.3.1.3 При создании СЗПДн должно использоваться только лицензионное общее и специальное программное обеспечение и операционные системы.

4.3.1.4 Требования к программному обеспечению, используемому для защиты информации в ИСПДн «Бухгалтерия и кадры» (средств защиты информации, в том числе и встроенных в общесистемное и прикладное ПО) в части необходимости обеспечения контроля отсутствия в нем недекларированных возможностей (НДВ) должны быть определены в ТЗ.

4.3.2 Требования к техническому обеспечению

Выбор аппаратных (программно-аппаратных) средств защиты должен проводиться с учетом средств защиты, эксплуатируемых у заказчика.

4.3.3 Требования к организационному обеспечению

4.3.3.7 Мониторы АРМ должны располагаться таким образом, чтобы препятствовать возможности несанкционированного визуального съема информации с них.

4.3.3.8 Должна осуществляться физическая охрана устройств и носителей информации ИСПДн «Бухгалтерия и кадры», предусматривающая:

4.3.3.9 контроль доступа в помещения ИСПДн « Бухгалтерия и кадры» посторонних лиц;

4.3.3.10 наличие надежных препятствий для несанкционированного проникновения в помещение ИСПДн « Бухгалтерия и кадры» и хранилище носителей информации, особенно в нерабочее время.

4.3.3.11 Должны быть проведены работы по подготовке проектов и введению в действие следующих организационно-распорядительных документов, направленных на обеспечение информационной безопасности:

– приказов о назначении ответственных лиц;

– документа, определяющего политику в отношении обработки персональных данных;

– локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;

– уведомления уполномоченного органа по защите прав субъектов персональных данных о намерении осуществлять обработку персональных данных;

– документов, определяющих круг лиц, имеющих доступ к ИСПДн, ее компонентам;

– форм согласия субъекта персональных данных на обработку его персональных данных;

– документа, содержащего перечень обрабатываемых персональных данных;

– документа, содержащего перечень нормативных правовых актов, в соответствии с которыми производится обработка персональных данных.

4.3.3.12 Для соблюдения требований Приказа ФСБ России от 10 июля 2014 г. №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» Заказчику необходимо провести:

– оснащение помещений входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода, а также опечатывания помещений по окончании рабочего дня или оборудование помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений (ФСБ-1);

– утверждение правил доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях. (ФСБ-2);

– утверждение перечня лиц, имеющих право доступа в помещения. (ФСБ-3);

– осуществление хранения съемных машинных носителей персональных данных в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. (ФСБ-4);

– осуществление поэкземплярного учета машинных носителей персональных данных, который достигается путем ведения журнала учета носителей персональных данных с использованием регистрационных (заводских) номеров. (ФСБ-5);

– разработка и утверждение документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей. (ФСБ-6);

– поддержание в актуальном состоянии документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей. (ФСБ-7);

– использование для обеспечения требуемого уровня защищенности персональных данных при их обработке в информационной системе СКЗИ класса КС1 и выше (ФСБ-8);

– назначение обладающего достаточными навыками должностного лица (работника) оператора ответственным за обеспечение безопасности персональных данных в информационной системе (ФСБ-9).

5 СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СЗПДН

5.1 Разработка СЗПДн, поставка оборудования, монтаж оборудования

5.1.1 Разработка СЗПДн

Проводится обследование ИСПДн:

а) уточняется перечень ПДн, подлежащих защите;

б) уточняется информация о категориях и составе ПДн, обрабатываемых автоматизированными и неавтоматизированными способами;

в) проводится анализ состава ПДн в ИСПДн, собирается информация о защищенности ПДн;

г) уточняются условия расположения объекта защиты относительно границ контролируемой зоны;

д) уточняются конфигурация и топология ИСПДн и систем связи в целом и их компонентов, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;

е) уточняются состав технических средств и систем, предполагаемых к использованию в СЗПДн, условия их расположения, общесистемные и прикладные программные средства;

ж) уточняются режимы обработки информации в ИСПДн в целом и в отдельных ее компонентах;

з) для ИСПДн производится анализ собранной информации об угрозах и их показателях для разработки Модели угроз;

и) уточняется уровень защищенности ПДн, обрабатываемых в ИСПДн;

к) разрабатывается Модель угроз для ИСПДн на основе методических рекомендаций ФСТЭК России;

л) уточняется степень участия сотрудников в обработке информации, характер их взаимодействия между собой и со службой ИБ.

Также на данном этапе разрабатывается пакет организационно-распорядительной документации на ИСПДн.

5.1.2 Поставка оборудования

Осуществляются работы по закупке необходимого оборудования.

Все поставляемое оборудование должно пройти процедуру оценки соответствия требованиям по безопасности информации и иметь сертификат ФСТЭК России и ФСБ России (в соответствии с требованиями нормативно-методических документов).

5.1.3 Монтаж оборудования

Если в процессе выполнения работ по монтажу оборудования возникают какие-либо нештатные ситуации, а также ситуации, которые могут повлечь приостановление вышеуказанных работ, то принимаются все необходимые меры по устранению и ликвидации причин, которые привели к таким ситуациям.

5.2 Передача прав на использование программного обеспечения, входящего в состав СЗПДн

Все программное обеспечение должно пройти процедуру оценки соответствия требованиям по безопасности информации и иметь сертификат ФСТЭК России или ФСБ России (в соответствии с требованиями нормативно-методических документов).

5.3 Пусконаладочные работы, опытная эксплуатация СЗПДн, оценка эффективности реализованных мер

5.3.1 Пусконаладочные работы

Проводятся пусконаладочные работы СЗПДн, обеспечивающие интеграцию с локальной вычислительной сетью.

Проводится анализ защищенности сетевых сегментов ИСПДн (в пределах ЛВС) с использованием средств анализа защищенности.

Если в процессе выполнения пусконаладочных работ СЗПДн возникают какие-либо нештатные ситуации, а также ситуации, которые могут повлечь приостановление вышеуказанных работ, принимаются все возможные меры по устранению и ликвидации причин, которые привели к таким ситуациям.

5.3.2 Опытная эксплуатация

Опытная эксплуатация включает в себя комплексную проверку готовности СЗПДн. Опытная эксплуатация имеет своей целью проверку алгоритмов, отладку работы СЗПДн и технологического процесса обработки данных при использовании СЗПДн.

По окончании опытной эксплуатации возможна доработка СЗПДн.

В случае необходимости проводится обучение персонала использованию СЗИ, применяемых в СЗПДн.

5.3.3 Оценка эффективности

Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится учреждением самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже одного раза в 3 года.

6 ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ

6.1 Исполнитель должен быть заранее проинформирован о порядке и сроках согласования отчетных материалов, перечне вопросов, которые подлежат согласованию.

6.2 В случае необходимости может быть проведена защита предлагаемых решений в процессе технического совещания.

6.3 Настоящее ТЗ может быть уточнено или изменено в процессе работы. Уточнения и изменения ТЗ производятся по согласованию сторон. Оформление изменений осуществляется выпуском дополнений, которые являются неотъемлемой частью настоящего ТЗ.

6.4 Согласование и утверждение изменений производится в том же порядке и теми же должностными лицами, что и согласование и утверждение ТЗ.

6.5 Замечания по отчетным материалам должны быть представлены исполнителю с техническим обоснованием в письменной форме.

6.6 Сроки приемки работ определяются календарным планом, согласованным с заказчиком.

7 ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ ОБЪЕКТА АВТОМАТИЗАЦИИ К ВВОДУ СЗПДН В ДЕЙСТВИЕ

В перечень основных мероприятий включают:

а) Приведение поступающей в систему информации к виду, пригодному для обработки с помощью ЭВМ;

б) Изменения, которые необходимо осуществить в информационной системе;

в) Создание условий функционирования информационной системы, при которых гарантируется соответствие создаваемой системы требованиям, содержащимся в ТЗ;

г) Создание необходимых для функционирования системы подразделений и служб;

д) Сроки и порядок комплектования штатов и обучения персонала.

8 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

Комплект проектных материалов предоставляется заказчику по предварительной договоренности в электронном виде и (или) на твердой копии. Вся разрабатываемая проектная документация должна быть выполнена на русском языке.

9 ИСТОЧНИКИ РАЗРАБОТКИ

9.1 При разработке проектных решений необходимо руководствоваться официальными документами фирм-производителей применяемых аппаратных средств и программного обеспечения, документами третьих сторон, осуществляющих тестирование и эксплуатацию решений, материалами, предоставляемыми Пользователем.

9.2 Проектные решения должны обеспечивать соблюдение федеральных законов, постановлений Правительства Российской Федерации и иных нормативных актов.

ПРИЛОЖЕНИЕ И

Перечень
требований к функционалу системы защиты персональных данных в ГБУЗ «ОПТД № 8»

В таблице представлен список требований по защите информации и мер по их выполнению с учетом актуальных угроз безопасности персональных данных и особенности функционирования информационной системы согласно приказу ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Условные обозначения мер:

ОРГ – используются организационные меры по защите информации

НСД – используются средства защиты информации от несанкционированного доступа совместно с организационными мерами

МЭ – используются средства межсетевого экранирования совместно с организационными мерами

САВЗ – используются средства антивирусной защиты информации совместно с организационными мерами

САНЗ – используются средства анализа защищенности совместно с организационными мерами

СКЗИ – используются средства криптографической защиты информации совместно с организационными мерами

№	Требование		«Бухгалтерия и кадры»	«Медицина»
Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)				
1	ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	НСД	НСД
2	ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	НСД	НСД
3	ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	НСД	НСД
4	ИАФ.5	Защита обратной связи при вводе аутентификационной информации	НСД	НСД
Управление доступом субъектов доступа к объектам доступа (УПД)				
5	УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	НСД	НСД
6	УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	НСД	НСД
7	УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	НСД, МЭ	НСД, МЭ
8	УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	НСД	НСД

№	Требование		«Бухгалтерия и кадры»	«Медицина»
9	УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	ОРГ	ОРГ
10	УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	НСД	НСД
11	УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		НСД
12	УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации		НСД
13	УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	СКЗИ	СКЗИ
Защита машинных носителей персональных данных (ЗНИ)				
14	ЗНИ.1	Учет машинных носителей персональных данных	ОРГ	ОРГ
15	ЗНИ.2	Управление доступом к машинным носителям персональных данных	ОРГ (НСД)	ОРГ (НСД)
16	ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания	ОРГ	ОРГ
Регистрация событий безопасности (РСБ)				
17	РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	ОРГ	ОРГ
18	РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	ОРГ	ОРГ
19	РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	НСД, МЭ	НСД, МЭ
20	РСБ.7	Защита информации о событиях безопасности	НСД, МЭ	НСД, МЭ
Антивирусная защита (АВЗ)				
21	АВЗ.1	Реализация антивирусной защиты	САВЗ	САВЗ
22	АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	САВЗ	САВЗ
Контроль (анализ) защищенности персональных данных (АНЗ)				
23	АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		САНЗ
24	АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	ОРГ	САНЗ
25	АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		САНЗ
26	АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		САНЗ
Защита технических средств (ЗТС)				
27	ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования	ОРГ	ОРГ

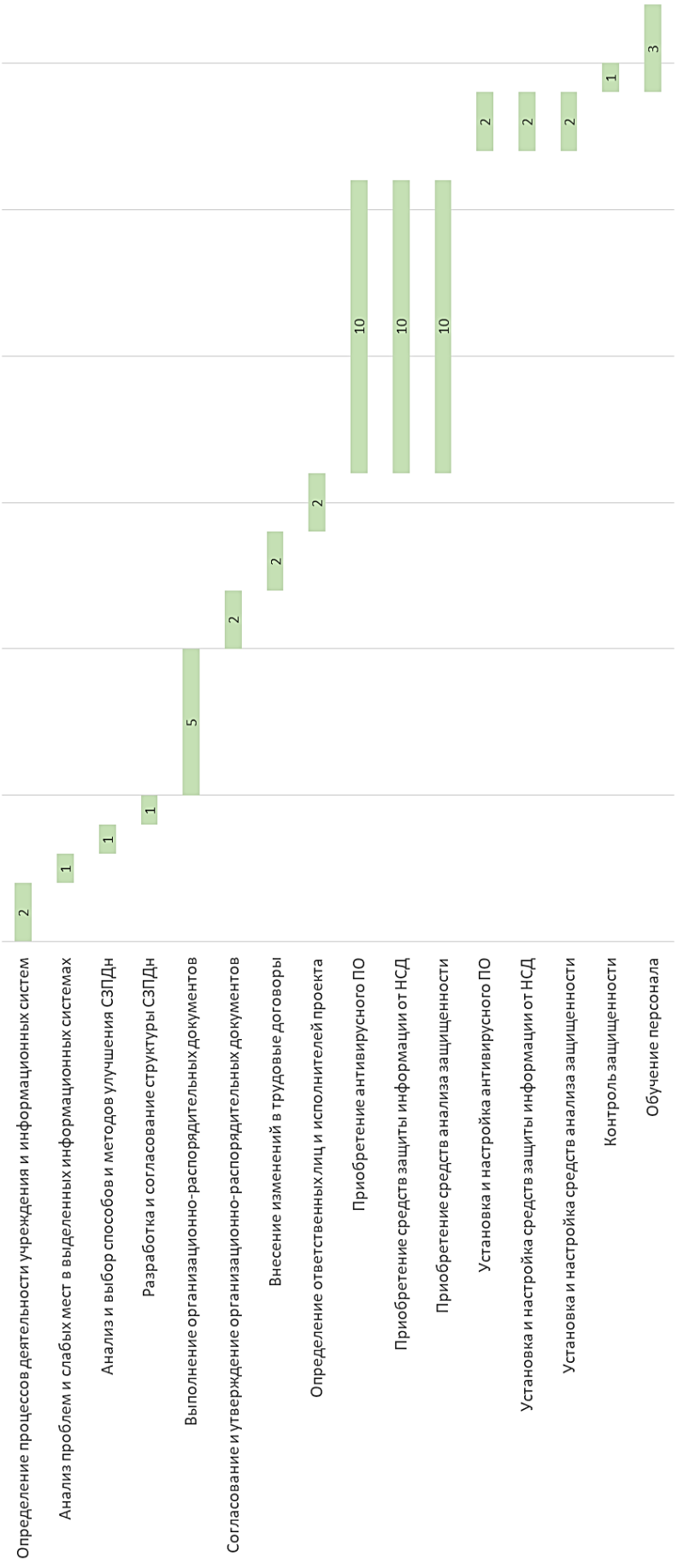
№	Требование		«Бухгалтерия и кадры»	«Медицина»
28	ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	ОРГ	ОРГ
29	ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	ОРГ	ОРГ
Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)				
30	ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	МЭ	МЭ
Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)				
31	УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных		ОРГ
32	УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных		САНЗ
33	УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных		ОРГ
34	УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		САНЗ

ПРИЛОЖЕНИЕ К

Для построения диаграммы Ганта определим перечень поставленных задач и их сроки:

Название работы	Длительность	Начало	Окончание
1. Проектирование			
Определение процессов деятельности учреждения и информационных систем	2	12.03.2018	13.03.2018
Анализ проблем и слабых мест в выделенных информационных системах	1	14.03.2018	14.03.2018
Анализ и выбор способов и методов улучшения СЗПДн	1	15.03.2018	15.03.2018
Разработка и согласование структуры СЗПДн	1	16.03.2018	16.03.2018
2. Разработка организационно-распорядительной документации			
Выполнение организационно-распорядительных документов	5	17.03.2018	21.03.2018
Согласование и утверждение организационно-распорядительных документов	2	22.03.2018	23.03.2018
Внесение изменений в трудовые договоры	2	24.03.2018	25.03.2018
3. Подготовка реализации проекта			
Определение ответственных лиц и исполнителей проекта	2	26.03.2018	27.03.2018
Приобретение антивирусного ПО	10	28.03.2018	07.04.2018
Приобретение средств защиты информации от НСД	10	28.03.2018	07.04.2018
Приобретение средств анализа защищенности	10	28.03.2018	07.04.2018
4. Внедрение			
Установка и настройка антивирусного ПО	2	08.04.2018	09.04.2018
Установка и настройка средств защиты информации от НСД	2	08.04.2018	09.04.2018
Установка и настройка средств анализа защищенности	2	08.04.2018	09.04.2018
Контроль защищенности	1	10.04.2018	10.04.2018
Обучение персонала	3	10.04.2018	12.04.2018

На основе этих данных построим диаграмму Ганта:


12.03.2018
17.03.2018
22.03.2018
27.03.2018
01.04.2018
06.04.2018
11.04.2018
Определение процессов деятельности учреждения и информационных систем
2
Анализ проблем и слабых мест в выделенных информационных системах
1
Анализ и выбор способов и методов улучшения СЗПДн
1
Разработка и согласование структуры СЗПДн
1
Выполнение организационно-распорядительных документов
5
Согласование и утверждение организационно-распорядительных документов
2
Внесение изменений в трудовые договоры
2
Определение ответственных лиц и исполнителей проекта
2
Приобретение антивирусного ПО
10
Приобретение средств защиты информации от НСД
10
Приобретение средств анализа защищенности
10
Установка и настройка антивирусного ПО
2
Установка и настройка средств защиты информации от НСД
2
Установка и настройка средств анализа защищенности
2
Контроль защищенности
1
Обучение персонала
3

ПРИЛОЖЕНИЕ Л

Для своевременного выполнения работ необходимо определить сроки их выполнения.

i-j – код работы
T – длительность работы, дней
$T_{рн}$ – ранний срок начала работы
$T_{пн}$ – поздний срок начала работы
$T_{ро}$ – ранний срок окончания работы
$T_{по}$ – поздний срок окончания работы

i-j	Название работы	T	$T_{рн}$	$T_{пн}$	$T_{ро}$	$T_{по}$
	Проектирование	5	0	0	5	5
1-2	Определение процессов деятельности учреждения и информационных систем	2	0	0	2	2
2-3	Анализ проблем и слабых мест в выделенных информационных системах	1	2	2	3	3
3-4	Анализ и выбор способов и методов улучшения СЗПДн	1	3	3	4	4
4-5	Разработка и согласование структуры СЗПДн	1	4	4	5	5
	Разработка организационно-распорядительной документации	9	5	5	14	14
5-6	Выполнение организационно-распорядительных документов	5	5	5	10	10
6-7	Согласование и утверждение организационно-распорядительных документов	2	10	10	12	12
7-8	Внесение изменений в трудовые договоры	2	12	12	14	14
	Подготовка реализации проекта	12	14	14	26	26
8-9	Определение ответственных лиц и исполнителей проекта	2	14	14	16	16
9-10	Приобретение антивирусного ПО	10	16	16	26	26
10-11	Приобретение средств защиты информации от НСД	10	16	16	26	26
11-12	Приобретение средств анализа защищенности	10	16	16	26	26
	Внедрение	5	26	26	31	31
12-13	Установка и настройка антивирусного ПО	2	26	26	28	28
13-14	Установка и настройка средств защиты информации от НСД	2	26	26	28	28
14-15	Установка и настройка средств анализа защищенности	2	26	26	28	28
15-16	Контроль защищенности	1	28	28	29	29
15-17	Обучение персонала	3	28	28	31	31

ПРИЛОЖЕНИЕ М

УТВЕРЖДЕНА
приказом
главного врача
ГБУЗ «ОПТД № 8»
от _____ № _____

ПОЛИТИКА
обработки и защиты персональных данных
Государственного бюджетного учреждения здравоохранения «Областной противотуберкулезный диспансер № 8»

ОБЩИЕ ПОЛОЖЕНИЯ

1.1. В целях соблюдения законодательства Российской Федерации, регулирующего отношения, связанные с обработкой и обеспечением безопасности персональных данных, а также поддержания деловой репутации Государственного бюджетного учреждения здравоохранения «Областной противотуберкулезный диспансер № 8» (далее – ГБУЗ «ОПТД № 8») считает своими задачами соблюдение принципов законности, справедливости и конфиденциальности при обработке персональных данных, а также обеспечение безопасности процессов их обработки.

1.2. Настоящая Политика в отношении обработки и защиты персональных данных в ГБУЗ «ОПТД № 8» (далее – Политика):

1.2.1. Раскрывает основные категории персональных данных, обрабатываемых ГБУЗ «ОПТД № 8», цели, способы и принципы обработки персональных данных, права и обязанности ГБУЗ «ОПТД № 8» при обработке персональных данных, права субъектов персональных данных.

1.2.2. Является общедоступным документом, декларирующим концептуальные основы деятельности ГБУЗ «ОПТД № 8» при обработке персональных данных.

1.3. Термины и определения, используемые в Политике:

1.3.1. Биометрические персональные данные - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

1.3.2. Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

1.3.3. Доступ к информации (доступ) - ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

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

1.3.5. Несанкционированный доступ (НСД) – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

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

1.3.7. Персональные данные (далее – ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.3.8. Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. Оператором является ГБУЗ «ОПТД № 8».

1.3.9. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

1.3.10. Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

1.3.11. Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

1.3.12. Специальные категории персональных данных - категории персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

1.3.13. Субъект персональных данных (субъект) - физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

1.3.14. Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.3.15. Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

1.4. Основные права Субъектов персональных данных:

1.4.1. Субъект персональных данных имеет право на получение сведений об обработке его персональных данных в ГБУЗ «ОПТД № 8»;

1.4.2. Субъект персональных данных вправе требовать от ГБУЗ «ОПТД № 8», который их обрабатывает, уточнения этих персональных данных, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не могут быть признаны необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

1.4.3. Право Субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами;

1.4.4. Для реализации своих прав и защиты законных интересов Субъект персональных данных имеет право обратиться к ГБУЗ «ОПТД № 8». Тот рассматривает любые обращения и жалобы со стороны субъектов персональных данных, тщательно расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, наказания виновных лиц и урегулирования спорных и конфликтных ситуаций в досудебном порядке;

1.4.5. Субъект персональных данных вправе обжаловать действия или бездействие ГБУЗ «ОПТД № 8» путем обращения в уполномоченный орган по защите прав субъектов персональных данных (территориальный орган Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций);

1.4.6. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и/или компенсацию морального вреда в судебном порядке.

1.5. Основные обязанности ГБУЗ «ОПТД № 8»:

1.5.1. Соблюдать требования законодательства РФ в области обработки и защиты персональных данных;

1.5.2. При сборе персональных данных предоставить субъекту персональных данных по его просьбе информацию, касающуюся обработки персональных данных;

1.5.3. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, работники ГБУЗ «ОПТД № 8» обязаны разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные;

1.5.4. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации;

1.5.5. Опубликовать или иным образом обеспечить неограниченный доступ к актуальному документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных (настоящую Политику);

1.5.6. Принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним;

1.5.7. Сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя;

1.5.8. Уточнять персональные данные Субъектов, блокировать или уничтожать их в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не могут быть признаны необходимыми для заявленной цели обработки;

1.5.9. Прекратить обработку персональных данных в случае отзыва субъектом персональных данных согласия на обработку его персональных данных. ГБУЗ «ОПТД № 8» вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

II. ЦЕЛИ СБОРА ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. ГБУЗ «ОПТД № 8» обрабатывает следующие категории субъектов персональных данных (далее – Субъекты):

2.1.1. Персональные данные работников.

2.1.2. Персональные данные родственников работников.

2.1.3. Персональные данные бывших работников.

2.1.4. Персональные данные кандидатов на замещение вакантных должностей.

2.1.5. Персональные данные пациентов и их законных представителей.

2.1.6. Персональные данные контрагентов, представителей юридических лиц.

2.2. ГБУЗ «ОПТД № 8» обрабатывает персональные данные работников исключительно в следующих целях:

2.2.1. Выполнение требований законодательства Российской Федерации;

2.2.2. Осуществление трудовых отношений;

2.2.3. Ведение бухгалтерского, налогового и кадрового учета;

2.2.4. Организация выдачи заработной платы по банковским картам;

2.2.5. Совершенствование профессиональных знаний работников и продвижение по службе;

2.2.6. Обеспечение личной безопасности и сохранности имущества.

2.3. ГБУЗ «ОПТД № 8» обрабатывает персональные данные родственников работников исключительно в целях ведения бухгалтерского, налогового и кадрового учета.

2.4. ГБУЗ «ОПТД № 8» обрабатывает персональные данные бывших работников исключительно в целях ведения бухгалтерского, налогового и кадрового учета.

2.5. ГБУЗ «ОПТД № 8» обрабатывает персональные данные кандидатов на замещение вакантных должностей исключительно в целях принятия решения о трудоустройстве кандидата в ГБУЗ «ОПТД № 8».

2.6. ГБУЗ «ОПТД № 8» обрабатывает персональные данные контрагентов, представителей юридических лиц исключительно в целях заключения и выполнения обязательств по договорам с контрагентами.

2.7. ГБУЗ «ОПТД № 8» обрабатывает персональные данные пациентов исключительно в целях оказания специализированной туберкулезной (противотуберкулезной) медицинской помощи населению Челябинской области.

III. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Правовым основанием обработки персональных данных является совокупность правовых актов, во исполнение которых и в соответствии с которыми ГБУЗ «ОПТД № 8» осуществляет обработку персональных данных.

3.2. Обработка персональных данных в ГБУЗ «ОПТД № 8» осуществляется в соответствии со следующими правовыми основаниями:

3.2.1. Конституция Российской Федерации от 25.12.1993;

3.2.2. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ;

3.2.3. Гражданский кодекс Российской Федерации от 30.11.1994 № 51-ФЗ;

3.2.4. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ;

3.2.5. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ;

3.2.6. Налоговый Кодекс Российской Федерации часть первая от 31.07.1998 № 146-ФЗ и часть вторая от 05.08.2000 № 117-ФЗ (с изменениями и дополнениями);

3.2.7. Федеральный закон от 19.12.2005 №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;

3.2.8. Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

3.2.9. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»;

3.2.10. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

3.2.11. Постановление правления пенсионного фонда Российской Федерации от 31.07.2006 г. № 192п «О формах документов индивидуального (персонифицированного) учета в системе обязательного пенсионного страхования и инструкции по их заполнению»;

3.2.12. Федеральный закон от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

3.2.13. Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;

3.2.14. Федеральный закон РФ от 09.11.2011 № 323 «Об основах охраны здоровья граждан в Российской Федерации»;

3.2.15. Закон РФ от 07.02.1992 г. № 2300-1 «О защите прав потребителей»;

3.2.16. Федеральный закон от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;

3.2.17. Федеральный закон от 18.06.2001 № 77-ФЗ «О предупреждении распространения туберкулеза в Российской Федерации»;

3.2.18. Постановление Правительства РФ от 25.12.2001 №892 «О реализации Федерального закона "О предупреждении распространения туберкулеза в Российской Федерации»;

3.2.19. Приказ Минздрава РФ от 21.03.2003 № 109 «О совершенствовании противотуберкулезных мероприятий в Российской Федерации»;

3.2.20. Приказ Министерства здравоохранения Российской Федерации от 29.12.2014 № 951 «Об утверждении методических рекомендации по совершенствованию диагностики и лечения туберкулеза органов дыхания»;

3.2.21. Приказ Министерства здравоохранения Челябинской области от 21.12.2009 № 1470 «О ведении Федерального регистра медицинских работников»;

3.2.22. Приказ Министерства здравоохранения Челябинской области от 19.04.2007 № 161 «О порядке ведения регионального сегмента Федерального регистра медицинских и фармацевтических работников муниципальных и государственных учреждений здравоохранения Челябинской области»;

3.2.23. Приказ Минздравмедпрома РФ от 14.03.1996 № 90 «О порядке проведения предварительных и периодических медицинских осмотров работников и медицинских регламентах допуска к профессии»;

3.2.24. Лицензия на осуществление медицинской деятельности от 16.01.2012 № 74-01-001692;

3.2.25. Устав ГБУЗ «ОПТД № 8»;

3.2.26. Трудовые договоры с работниками;

3.2.27. Договоры, заключаемые между ГБУЗ «ОПТД № 8» и субъектами персональных данных;

3.2.28. Согласия субъектов на обработку персональных данных.

IV. ОБЪЕМ И КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ, КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Содержание и объем обрабатываемых персональных данных Субъектов соответствует целям обработки.

4.2. Содержание и объем обрабатываемых персональных данных Субъектов соответствует Перечню обрабатываемых персональных данных:

4.3. ГБУЗ «ОПТД № 8» не осуществляет обработку биометрических персональных данных (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются для установления личности субъекта персональных данных).

4.4. ГБУЗ «ОПТД № 8» выполняет обработку специальных категорий персональных данных, касающихся состояния здоровья.

4.5. ГБУЗ «ОПТД № 8» не осуществляет трансграничную (на территории иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу) передачу персональных данных.

4.6. В ГБУЗ «ОПТД № 8» созданы общедоступные источники персональных данных (информационный стенд). Персональные данные (фамилия, имя, отчество, должность) включаются в такие источники только с письменного согласия работников.

V. ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. В ГБУЗ «ОПТД № 8» обработка персональных данных субъектов осуществляется в целях, указанных в разделе II настоящей Политики.

5.2. В ГБУЗ «ОПТД № 8» обрабатываются категории персональных данных, указанные в разделе IV настоящей Политики.

5.3. Обработка персональных данных в ГБУЗ «ОПТД № 8» осуществляется только при условии получения согласия субъектов персональных данных. Согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом "О персональных данных".

5.4. Обработка персональных данных субъектов включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение персональных данных.

5.5. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от субъектов персональных данных (их законных представителей).

5.6. ГБУЗ «ОПТД № 8» и работники ГБУЗ «ОПТД № 8», получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

5.7. ГБУЗ «ОПТД № 8» вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

5.8. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, работник ГБУЗ «ОПТД № 8», осуществляющий сбор (получение) персональных данных непосредственно от субъектов персональных данных, обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

5.9. ГБУЗ «ОПТД № 8» в своей деятельности обеспечивает соблюдение принципов обработки персональных данных, указанных в ст.5 Федерального закона 152-ФЗ «О персональных данных».

5.10. ГБУЗ «ОПТД № 8» в своей деятельности принимает меры, предусмотренные ч. 2 ст. 18.1, ч.1 ст.19 Федерального закона 152-ФЗ «О персональных данных».

5.11. В ГБУЗ «ОПТД № 8» не используются для обработки персональных данных базы данных, находящиеся за пределами границ Российской Федерации.

5.12. Условия прекращения обработки персональных данных ГБУЗ «ОПТД № 8»:

5.12.1. достижение целей обработки персональных данных;

5.12.2. истечение срока действия согласия или отзыв согласия субъекта персональных данных на обработку его персональных данных;

5.12.3. выявление неправомерной обработки персональных данных;

5.12.4. утрата правовых оснований обработки персональных данных.

5.13. Назначенными лицами ГБУЗ «ОПТД № 8» осуществляется контроль за хранением и использованием материальных носителей персональных данных, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях.

5.14. Срок хранения персональных данных в форме, позволяющей определить субъекта персональных данных, осуществляется не дольше, чем этого требуют цели обработки персональных данных, кроме случаев, когда срок хранения персональных данных не установлен федеральным законом, договором, стороной которого является субъект персональных данных.

5.15. В целях соблюдения законодательства РФ, для достижения целей обработки, а также в интересах и с согласия субъектов персональных данных ГБУЗ «ОПТД № 8» в ходе своей деятельности предоставляет персональные данные следующим организациям:

5.15.1. Федеральной налоговой службе;

5.15.2. Пенсионному фонду России;

5.15.3. Фонду социального страхования;

5.15.4. Кредитным организациям;

5.15.5. ГБУЗ «Городская больница г. Южноуральск»;

5.15.6. ГБУЗ «Челябинский областной клинический противотуберкулезный диспансер»;

5.15.7. ГБУЗ «Челябинский областной медицинский информационно-аналитический центр»;

5.15.8. ГОУ ДПО «Челябинский областной центр дополнительного профессионального образования специалистов здравоохранения»;

5.15.9. Министерство здравоохранения Челябинской области.

VI. АКТУАЛИЗАЦИЯ, ИСПРАВЛЕНИЕ, УДАЛЕНИЕ И УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОТВЕТЫ НА ЗАПРОСЫ СУБЪЕКТОВ НА ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

6.1. В случае выявления неправомерной обработки персональных данных ГБУЗ «ОПТД № 8» осуществляет блокирование неправомерно обрабатываемых персональных данных.

6.2. В случае выявления неточных персональных данных ГБУЗ «ОПТД № 8» осуществляет блокирование соответствующих персональных данных на период проверки. В случае подтверждения факта неточности персональных данных ГБУЗ «ОПТД № 8» на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов уточняет персональные данные и снимает блокирование персональных данных.

6.3. ГБУЗ «ОПТД № 8» обязан сообщить субъекту персональных данных или его представителю информацию об осуществляемой им обработке персональных данных такого субъекта по запросу последнего.

6.4. Сведения, касающиеся обработки персональных данных, предоставляются субъекту персональных данных или его представителю при получении запроса субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

6.5. Рассмотрение запросов субъектов персональных данных или их представителей, а также уполномоченного органа по защите прав субъектов персональных данных:

6.5.1. Субъекты персональных данных имеют право на получение информации, касающейся обработки их персональных данных, в том числе содержащей:

6.5.1.1. Подтверждение факта обработки персональных данных в ГБУЗ «ОПТД № 8»;

6.5.1.2. Правовые основания и цели обработки персональных данных;

6.5.1.3. Применяемые в ГБУЗ «ОПТД № 8» способы обработки персональных данных;

6.5.1.4. Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6.5.1.5. Сроки обработки персональных данных, в том числе сроки их хранения в ГБУЗ «ОПТД № 8»;

6.5.1.6. Порядок осуществления субъектом персональных данных прав, предусмотренных законодательством Российской Федерации в области персональных данных;

6.5.1.7. Иные сведения, предусмотренные законодательством Российской Федерации в области персональных данных.

6.5.2. При получении запроса Субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных, ГБУЗ «ОПТД № 8» предоставляет сведения в сроки в соответствии требований статьи 20 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

6.6. Субъекты персональных данных вправе требовать от ГБУЗ «ОПТД № 8» уточнения их персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав

6.7. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

6.8. Для получения необходимой информации, касающейся обработки персональных данных, описанной в пункте 6.5.1. настоящей Политики, Субъекту (либо законному представителю) необходимо заполнить соответствующую форму запроса субъекта персональных данных информации, касающейся обработки персональных данных (приложение 1 или 5) и передать лично работникам ГБУЗ «ОПТД № 8», принимающим обращения граждан, либо по почте.

6.9. Для уточнения определенных персональных данных Субъекту (либо законному представителю) необходимо заполнить соответствующую форму запроса субъекта персональных данных на уточнение персональных данных (приложение 2 или 6) и передать лично работникам ГБУЗ «ОПТД № 8», принимающим обращения граждан, либо по почте.

6.10. Для исключения неправомерности обработки персональных данных Субъекту (либо законному представителю) необходимо заполнить соответствующую форму запроса субъекта персональных данных на уничтожение персональных данных (приложение 3 или 7) и передать лично работникам ГБУЗ «ОПТД № 8», принимающим обращения граждан, либо по почте.

6.11. Для отзыва согласия Субъекта персональных данных на обработку его персональных данных субъекту (либо законному представителю) необходимо заполнить соответствующую форму отзыва согласия субъекта персональных данных на обработку его персональных данных (приложение 4 или 8) и передать лично работникам ГБУЗ «ОПТД № 8», принимающим обращения граждан, либо по почте. В случае отзыва согласия на обработку персональных данных ГБУЗ «ОПТД № 8» вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных».

6.12. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если:

6.12.1. Иное не предусмотрено договором, стороной которого является субъект персональных данных;

6.12.2. Иное не предусмотрено иным соглашением между ГБУЗ «ОПТД № 8» и субъектом персональных данных.

6.13. При получении запроса Субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных, по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных, ГБУЗ «ОПТД № 8» осуществляет соответствующие меры и уведомляет о выполненных мерах в сроки согласно требованиям статьи 21 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных».

VII. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1. Настоящая политика является внутренним документом ГБУЗ «ОПТД № 8», общедоступной и подлежит размещению на стенде ГБУЗ «ОПТД № 8».

7.2. Настоящая политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года.

7.3. Контроль исполнения требований настоящей политики осуществляется ответственным за организацию обработки персональных данных в ГБУЗ «ОПТД № 8».

7.4. Ответственность должностных лиц ГБУЗ «ОПТД № 8», имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами ГБУЗ «ОПТД № 8».

ПРИЛОЖЕНИЕ Н

УТВЕРЖДЕНА
приказом
главного врача
ГБУЗ «ОПТД № 8»
от _____ № _____

ИНСТРУКЦИЯ
пользователя информационной системы

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция регламентирует обязанности сотрудников, участвующих в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющих доступ к аппаратным средствам, программному обеспечению и данным информационной системы (далее ИС) Государственного бюджетного учреждения здравоохранения «Областной противотуберкулезный диспансер № 8» (далее - ГБУЗ «ОПТД № 8»).

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

2.2. **База данных** – это информация, упорядоченная в виде набора элементов, записей одинаковой структуры

2.3. **Информация** – сведения (сообщения, данные) независимо от формы их представления (ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.4. **Информационная система (ИС)** – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

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

2.6. **Обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.7. **Пароль** – секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.

2.8. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.9. **Программное обеспечение** – все или часть программ, процедур, правил и соответствующей документации системы обработки информации (ISO/IEC 2382-1:1993)

2.10. **Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.11. **Средство защиты информации (СЗИ)** – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

III. ОБЩИЕ ОБЯЗАННОСТИ СОТРУДНИКОВ

Каждый сотрудник ГБУЗ «ОПТД № 8», являющийся пользователем ИС, обязан:

3.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИС.

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

3.3. Соблюдать правила работы с паролем своей учётной записи.

3.4. Немедленно вызывать ответственного за обеспечение безопасности информации и поставить в известность руководителя структурного подразделения при обнаружении:

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

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

3.4.3. 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;

3.4.4. некорректного функционирования установленных на АРМ технических средств защиты;

3.4.5. непредусмотренных отводов кабелей и подключенных к АРМ дополнительных устройств.

3.5. Всем сотрудникам ГБУЗ «ОПТД № 8», являющимся пользователями ИС, запрещается:

3.5.1. использовать компоненты программного и аппаратного обеспечения ИС ГБУЗ «ОПТД № 8» в неслужебных целях;

3.5.2. самовольно вносить какие-либо изменения в конфигурацию АРМ или устанавливать в АРМ любые программные и аппаратные средства, кроме выданных или разрешённых к использованию ответственным за обеспечение безопасности персональных данных;

3.5.3. оставлять без присмотра своё АРМ, не активизировав блокировки доступа, или оставлять своё АРМ включенным по окончании работы;

3.5.4. умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению безопасности персональных данных.

IV. ОБЕСПЕЧЕНИЕ СОХРАННОСТИ ИНФОРМАЦИИ

4.1. Для обеспечения сохранности электронных информационных ресурсов ГБУЗ «ОПТД № 8» необходимо соблюдать следующие требования:

4.1.1. Для копирования информации не должны использоваться непроверенные на наличие компьютерных вирусов и других вредоносных программ носители информации.

4.2. Субъектам доступа запрещается:

4.2.1. Установка и использование при работе в АРМ вредоносных программ, ведущих к блокированию работы сети.

4.2.2. Самовольное изменение сетевых адресов.

4.2.3. Самовольное вскрытие блоков АРМ, модернизация или модификация АРМ и программного обеспечения.

4.2.4. Несанкционированная передача АРМ с прописанными сетевыми настройками. Передача АРМ из одного подразделения в другое производится только ответственным за обеспечение безопасности информации с предварительно удаленными сетевыми настройками.

4.2.5. Использование технологии беспроводного доступа без разрешения Ответственнного за обеспечение безопасности в информационных системах.

4.3. Сведения, содержащиеся в электронных документах и базах данных ГБУЗ «ОПТД № 8», должны использоваться только в служебных целях в рамках полномочий сотрудника, работающего с соответствующими материалами.

V. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПРАВИЛ РАБОТЫ

5.1. Каждый пользователь ИС несёт персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учётной записи в ИС, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

5.2. За разглашение персональных данных и нарушение порядка работы со средствами ИС, содержащими персональные данные, сотрудники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

5.3. Распространение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) ГБУЗ «ОПТД № 8», влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Сотрудник ГБУЗ «ОПТД № 8», имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба ГБУЗ «ОПТД № 8» (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

5.3.1. В отдельных случаях, при разглашении персональных данных, сотрудник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

5.4. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

ПРИЛОЖЕНИЕ О

УТВЕРЖДЕНА
приказом
главного врача
ГБУЗ «ОПТД № 8»
от _____ № _____

ИНСТРУКЦИЯ
по организации парольной защиты

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная инструкция регламентирует процессы генерации, смены и прекращения действия паролей (удаления учётных записей пользователей) в информационных системах (далее – ИС) Государственного бюджетного учреждения здравоохранения «Областной противотуберкулезный диспансер № 8» (далее – ГБУЗ «ОПТД № 8»), а также контроль над действиями пользователей при работе с паролями.

1.2. Осуществление процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИС и контроль за действиями пользователей при работе с паролями возлагается на ответственного за обеспечение безопасности информации.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.2. **Информационная система (ИС)** – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

2.3. **Пароль** – секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.

2.4. **Пользователь** – сотрудник, участвующий в рамках своих функциональных обязанностей в процессах обработки персональных данных.

2.5. **Компрометация пароля** – раскрытие, обнаружение или утеря пароля.

III. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

3.1. Правила формирования паролей:

3.1.1. Личные пароли должны генерироваться и распределяться централизованно, либо выбираться пользователями информационной системы самостоятельно с учетом следующих требований:

3.1.1.1. длина пароля должна быть не менее 6 символов;

3.1.1.2. в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

3.1.1.3. пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе.

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

3.1.2. Пользователям допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например, Кожзгсф7!).

3.1.3. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на ответственного за обеспечение безопасности информации.

3.2. Порядок смены личных паролей:

3.2.1. Смена паролей должна проводиться регулярно, не реже одного раза в 3 месяца.

3.2.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учётной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

3.2.3. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственных за обеспечение безопасности информации, администраторов информационной системы и других сотрудников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

3.2.4. Ответственный за обеспечение безопасности информации ведёт «Журнал учёта работ в информационных системах», в котором он отмечает факт смены паролей пользователей.

3.2.4.1. Временный пароль, заданный ответственным за обеспечение безопасности информации при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

3.3. Действия в случае утери и компрометации пароля:

3.3.1. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

IV. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ ИС

4.1. Правила формирования паролей:

4.1.1. Личные пароли должны генерироваться и распределяться централизованно, либо выбираться пользователями информационной системы самостоятельно с учетом следующих требований:

4.1.1.1. длина пароля должна быть не менее 8 символов;

4.1.1.2. в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

4.1.1.3. пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и

т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;

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

4.1.2. Сотрудникам допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например, Кожзгсф7!).

4.1.3. Для обеспечения возможности использования имён и паролей некоторых сотрудников в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), сотрудники обязаны сразу же после установки своих паролей передавать их на хранение вместе с именами своих учетных записей ответственному за обеспечение безопасности информации в запечатанном конверте или опечатанном пенале.

4.2. Порядок Ввод пароля:

4.2.1. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

4.3. Порядок смены личных паролей:

4.3.1. Смена паролей должна проводиться регулярно, не реже одного раза в 3 месяца, самостоятельно каждым пользователем.

4.3.2. Временный пароль, заданный ответственным за обеспечение безопасности информации при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

4.4. Хранение пароля:

4.4.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других предметах и носителях информации.

4.4.2. Запрещается сообщать свой пароль полностью или частично другим пользователям, запрещается спрашивать или подсматривать пароль других пользователей.

4.4.3. Запрещается регистрировать других пользователей в ИС со своим личным паролем, запрещается входить в ИС под учётной записью и паролем другого пользователя.

4.5. Действия в случае утери и компрометации пароля:

4.5.1. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователь должен немедленно обратиться к ответственному за обеспечение безопасности информации с целью смены личного пароля.

V. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЯ ИС И ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ

5.1. Администратор и пользователи ИС несут персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых ими работ по обеспечению безопасности информации и за все действия, совершенные от имени их учётных записей в ИС, если с их стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

5.2. Администратор и пользователи ИС при нарушении норм, регулирующих получение, обработку и защиту информации, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

5.3. Разглашение информации (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) ГБУЗ «ОПТД № 8», влечет наложение на сотрудника, имеющего доступ к защищаемой информации, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Сотрудник ГБУЗ «ОПТД № 8», имеющий доступ к информации и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба ГБУЗ «ОПТД № 8» (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

5.3.1. В отдельных случаях, при разглашении персональных данных, сотрудник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

5.4. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

ПРИЛОЖЕНИЕ П

УТВЕРЖДЕНА
приказом
главного врача
ГБУЗ «ОПТД № 8»
от _____ № _____

ИНСТРУКЦИЯ
по организации антивирусной защиты

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная инструкция определяет требования к организации защиты информационной системы (далее – ИС) Государственного бюджетного учреждения здравоохранения «Областной противотуберкулезный диспансер № 8» (далее – ГБУЗ «ОПТД № 8») от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (далее – вредоносное ПО), устанавливает ответственность пользователей ИС, ответственного за обеспечение безопасности информации и других должностных лиц, за выполнение указанных требований.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Антивирусная база** – это база, которая содержит уникальные данные о каждом конкретном вирусе

2.2. **Антивирусная защита** – комплекс мер, направленных на предотвращение, обнаружение и обезвреживание действий вредоносного ПО при помощи антивирусных программных продуктов.

2.3. **Средство антивирусной защиты** – программный пакет, предназначенный для эффективной защиты, перехвата и удаления из операционной системы компьютера максимального количества вредоносных (или потенциально вредоносных) программ.

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

2.5. **Информация** – сведения (сообщения, данные) независимо от формы их представления (Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»)

2.6. **Информационная система (ИС)** – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

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

2.8. **Программное обеспечение** – все или часть программ, процедур, правил и соответствующей документации системы обработки информации (ISO/IEC 2382-1:1993)

2.9. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

III. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

3.1. К использованию в ГБУЗ «ОПТД № 8» допускаются только сертифицированные и лицензионные средства антивирусной защиты, закупленные у разработчиков или поставщиков данных средств.

3.2. Установка средств антивирусного контроля на автоматизированных рабочих местах (далее – АРМ) и серверах ИС ГБУЗ «ОПТД № 8» осуществляется ответственным за обеспечение безопасности информации или под его контролем, настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств и требованиями нормативных документов ФСТЭК РФ в области защиты информации.

3.3. Антивирусный контроль должен быть настроен в режиме постоянной антивирусной защиты.

3.4. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), хранящаяся на АРМ, передающаяся по сети, а также информация на съемных носителях. Контроль входящей информации должен осуществляться автоматически, непосредственно после её приёма. При передаче файлов, запакованных в архивы, без их распаковки, должна вручную инициироваться антивирусная проверка этих архивов.

3.5. Процедура обновления баз средства антивирусной защиты должна проводиться в автоматическом режиме не реже 1 (одного) раза в день на всех АРМ ИС, работающих в сети, не реже 1 (одного) раза в неделю для всех АРМ ИС, работающих автономно.

3.6. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено ответственным за обеспечение безопасности информации на предмет отсутствия вредоносного программного обеспечения (далее – ПО).

3.7. Подключаемые к компьютеру внешние устройства и носители информации должны проверяться антивирусным ПО непосредственно после подключения.

3.8. Периодический контроль за состоянием антивирусной защиты (обновление антивирусной программы и антивирусных баз, а также проверка работоспособности средств антивирусной защиты) в ИС ГБУЗ «ОПТД № 8», осуществляется ответственным за обеспечение безопасности информации, пользователями ИС и всеми должностными лицами, настраивающими и сопровождающими средства антивирусной защиты в ИС ГБУЗ «ОПТД № 8».

IV. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ ИС

4.1. При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) самостоятельно или вместе с ответственным за обеспечение безопасности информации провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля - уведомить о результатах ответственного за обеспечение безопасности информации для определения им факта наличия или отсутствия вредоносного программного обеспечения.

4.2. В случае появления информационного окна средства антивирусной защиты, сигнализирующем об обнаружении вредоносного программного обеспечения:

4.2.1. приостановить обработку данных;

4.2.2. немедленно поставить в известность о факте обнаружения вредоносного программного обеспечения ответственного за обеспечение безопасности информации, владельца заражённых файлов, а также смежные структурные подразделения, использующие эти файлы в работе;

4.2.3. совместно с владельцем файлов, заражённых вредоносным программным обеспечением, провести анализ необходимости дальнейшего их использования;

4.2.4. произвести лечение или уничтожение заражённых файлов (при необходимости для выполнения требований данного пункта привлечь ответственного за обеспечение безопасности информации).

V. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЯ ИС И ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ

5.1. Администратор и пользователи ИС несут персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых им работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени их учётных записей в ИС, если с их стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

5.2. Администратор и пользователи ИС при нарушении норм, регулирующих получение, обработку и защиту информации, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

5.3. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) ГБУЗ «ОПТД № 8», влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Сотрудник ГБУЗ «ОПТД № 8», имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба ГБУЗ «ОПТД № 8» (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

5.3.1. В отдельных случаях, при разглашении персональных данных, сотрудник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

5.4. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.