

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра
«Информационная безопасность
систем и технологий»

Специальность 10.05.02 –

Специализация -

Информационная безопасность
телекоммуникационных систем
Разработка защищенных
телекоммуникационных систем

ДИПЛОМНЫЙ ПРОЕКТ

на тему

ПРОВЕДЕНИЕ РАБОТ ПО ПЕРЕАТТЕСТАЦИИ ЧАСТИ
ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ «АРМ
ДЛО ФЕДЕРАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ «ВОЙСКОВАЯ ЧАСТЬ
45108»»

Студент	_____	<u>Трегулов Ильдар Фяритович</u>
Руководитель	_____	<u>Сидоров А.И.</u>
Нормоконтролёр	_____	<u>Фатеев А.Г.</u>
Рецензент ПФ ФГУП «ЦентрИнформ»	_____	<u>Куликов А.Ю.</u>
Работа допущена к защите (протокол заседания кафедры от _____ № _____)		
Заведующий кафедрой	_____	<u>С.Л. Зефирова</u>

Работа защищена с отметкой _____ (протокол заседания ГЭК от _____ № _____)

Секретарь ГЭК _____ А.Г. Фатеев

Пенза 2017

РЕФЕРАТ

Пояснительная записка содержит 108 с., 12 рис., 36 табл., 19 источников, 10 прил.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ИНФОРМАЦИОННАЯ СИСТЕМА ПЕРСОНАЛЬНЫХ ДАННЫХ, УГРОЗЫ БЕЗОПАСНОСТИ, СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ, АТТЕСТАЦИЯ, ТРЕБОВАНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ.

Объектом исследования в данном дипломном проекте является информационная система персональных данных «АРМ ДЛО Федеральное казенное учреждение «Войсковая часть 45108»».

Цель дипломного проекта – организация обеспечения безопасности персональных данных в информационной системе персональных данных и проведение аттестации по требованиям безопасности информации.

В процессе выполнения дипломного проекта было выполнено ниже перечисленное. Обследование объекта информатизации с формированием документов «Протокола оценки обстановки в части обеспечения безопасности персональных данных» и «Отчета о результатах проведения внутренней проверки обеспечения защиты персональных данных в информационной системе персональных данных». Разработана «Частная модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных». Сформирована организационно-распорядительная документация, включающая перечень персональных данных, акт классификации информационной системы персональных данных, план мероприятий по обеспечению защиты персональных данных, положение о разграничении прав доступа к персональным данным, разработаны инструкции администратора, пользователя, инструкция по антивирусному контролю.

Внедрены выбранные средств защиты информации. Разработана «Программа и методика проведения аттестационных испытаний», определяющая процесс проверки информационной системы персональных данных на соответствие требованиям безопасности информации. Составлен «Протокол испытаний комплексной системы защиты информации информационной системы персональных данных» на соответствие требованиям безопасности информации в части защиты от несанкционированного доступа и компьютерных вирусов», отражающий результаты проведения комплексных испытаний информационной системы персональных данных. Выводы аттестационной комиссии представлены в «Заключении по результатам проведения аттестационных испытаний информационной системы персональных данных на соответствие требованиям безопасности информации». Комиссия принимает решение о выдаче «Аттестата соответствия требованиям безопасности информации», формирование «Аттестата соответствия требованиям безопасности информации».

В результате выполнения дипломного проекта была создана и введена в эксплуатацию система защиты информации ИСПДн госпиталя, обеспечивающая безопасность персональных данных в информационной системе персональных данных, и проведена аттестация информационной системы персональных данных на соответствие требованиям безопасности информации.

СОДЕРЖАНИЕ

Введение.....	17
1 Результаты обследования объекта информатизации.....	21
1.1 Разработка «Протокола оценки обстановки в части обеспечения безопасности ПДн, обрабатываемых в ИСПДн»	21
1.1.1 Анализ информационных ресурсов	21
1.1.2 Анализ уязвимых звеньев и возможных угроз безопасности ПДн	28
1.1.3 Оценка ущерба от реализации УБПДн	29
1.2 Составление «Отчета о результатах проведения внутренней проверки обеспечения защиты ПДн в ИСПДн»	30
1.2.1 Общие положения	30
1.2.2 Структура ИСПДн.....	30
1.2.3 Состав ПДн	30
1.2.4 Объекты защиты в ИСПДн	31
1.2.5 Конфигурация ИСПДн	34
1.2.6 Структура обработки ПДн	36
1.2.7 Режим обработки ПДн.....	36
1.2.8 Угрозы безопасности ПДн	38
1.2.9 Существующие меры защиты.....	38
1.2.10 Необходимые меры защиты.....	39
2 Определение класса защищённости ИСПДн	40
2.1 Определение класса защищённости ИСПДн в соответствии с Приказом ФСТЭК России от 11 февраля 2013 г. №17.....	40
2.2 Определение уровня защищённости ИСПДн в соответствии с Приказом ФСТЭК России от 18 февраля 2013 г. №21.....	41
2.3 Повышение класса защищённости	42

3	Разработка «Частной модели угроз безопасности ПДн при их обработке в ИСПДн».....	43
3.1	Перечень угроз безопасности.....	43
3.1.1	Перечень угроз безопасности персональных согласно документам ФСТЭК и ФСБ.....	43
3.1.2	Угрозы безопасности персональных данных.....	44
3.2	Классификация пользователей ИСПДн	44
3.3	Определение уровня исходной защищенности	44
3.4	Определение вероятности реализации угроз, возможности реализации угроз, оценки опасности угроз и актуальности угроз безопасности.....	45
3.5	Перечень актуальных угроз безопасности ПДн	46
4	Разработка организационно-распорядительной документации	47
4.1	Формирование «Перечня ПДн, подлежащих защите в ИСПДн»	47
4.2	Составление «Плана мероприятий по обеспечению защиты ПДн в ИСПДн».....	47
4.3	Формирование «Положения о разграничении прав доступа к ПДн в ИСПДн».....	48
4.4	Разработка инструкций	48
5	Внедрение СЗИ.....	49
6	Разработка «Программы и методик проведения аттестационных испытаний на соответствие требованиям безопасности информации»	50
6.1	Общие положения.....	50
6.2	Анализ технологического процесса обработки информации ...	51
6.3	Анализ ИСПДн на соответствие различным требованиям по защите информации.....	52

6.3.1 Анализ внутренней и распорядительной документации по защите информации в ИСПДн	52
6.3.2 Анализ информационных потоков	54
6.3.3 Анализ уровня подготовки кадров и распределения ответственности за выполнением требований по защите информации	54
6.4 Испытания ИСПДн на соответствие требованиям по защите информации	55
6.4.1 Испытания подсистемы управления доступом	55
6.4.2 Испытания подсистемы регистрации и учета	55
6.4.3 Испытания подсистемы обеспечения целостности	55
6.4.4 Испытания криптографической подсистемы	56
6.4.5 Испытания подсистемы антивирусной защиты	56
6.5 Оформление отчетной документации по результатам аттестации ИСПДн	56
7 Формирование «Протокола испытаний комплексной системы защиты информации ИСПДн на соответствие требованиям безопасности информации в части защиты от НСД и компьютерных вирусов»	59
7.1 Состав средств контроля защищенности, использованных при аттестационных испытаниях ИСПДн	59
7.2 Проверка технологического процесса обработки информации	59
7.2.1 Общие положения	59
7.2.2 Особенности технологического процесса обработки информации	60
7.2.3 Перечень объектов доступа	61
7.2.4 Перечень субъектов доступа	62
7.2.5 Перечень штатных средств доступа к информации	62
7.2.6 Описание реализованных правил разграничения доступа	64

7.2.7 Перечень угроз НСД в ИСПДн и реализованных мер по их устранению.....	65
7.3 Проверка ИСПДн на соответствие организационно-техническим требованиям по защите информации	66
7.3.1 Проверка внутренней и распорядительной документации по защите информации в ИСПДн.....	66
7.3.2 Проверка информационных потоков	67
7.3.3 Проверка уровня подготовки кадров и распределения ответственности за выполнением требований по защите информации.....	67
7.4 Проверка ИСПДн на соответствие требованиям по защите информации.....	68
7.4.1 Проверка подсистемы управления доступом.....	68
7.4.2 Проверка подсистемы регистрации и учета.....	71
7.4.3 Проверка подсистемы обеспечения целостности.....	72
7.4.4 Проверка криптографической подсистемы.....	73
7.4.5 Проверка подсистемы антивирусной защиты.....	74
7.5 Вывод по «Протоколу испытаний комплексной системы защиты информации ИСПДн на соответствие требованиям безопасности информации в части защиты от НСД и компьютерных вирусов»	74
8 Формирование «Заключения по результатам проведения аттестационных испытаний ИСПДн на соответствие требованиям безопасности информации»	75
8.1 Условия и порядок проведения аттестационных испытаний ...	75
8.2 Результаты проверки состояния технологического процесса обработки информации на ИСПДн.....	75
8.3 Результаты проверки ИСПДн на соответствие организационно-техническим требованиям по защите информации	76

8.4 Результаты испытаний ИСПДн на соответствие требованиям по защите информации от НСД.....	76
8.5 Выводы по результатам проведения аттестационных испытания ИСПДн	77
9 Выдача «Аттестата соответствия ИСПДн требованиям безопасности информации»	78
Заключение.....	80
Список использованных источников.....	82
Приложение А Определение вероятности реализации УБПДн и оценки опасности УБПДн на основе опроса экспертов.....	85
Приложение Б Перечень ПДн, подлежащих защите в ИСПДн.....	88
Приложение В План мероприятия по обеспечению защиты ПДн в ИСПДн	93
Приложение Г Положение о разграничении прав доступа к обрабатываемым ПДн	97
Приложение Д Протокол проверки ВКР на оригинальность	100

ОПРЕДЕЛЕНИЯ

Безопасность персональных данных – состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационной системе персональных данных [7].

Доступ к информации – возможность получения информации и ее использования [7].

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации [7].

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных [7].

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств [1].

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов [7].

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия

решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц [1].

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств [7].

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания [1].

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы [7].

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационной системе персональных данных [7].

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации [7].

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационной системой персональных данных [7].

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных [1].

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных [1].

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности [1].

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных [1].

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-

цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средств защиты информации, применяемые в информационных системах [7].

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация [1].

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования [7].

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа [7].

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства [7].

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ [7].

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных

данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом [1].

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем [7].

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа [7].

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация [7].

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных [7].

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных [1].

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации [7].

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации [7].

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения) [7].

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ – автоматизированное рабочее место;

БД – база данных;

БДЗ – база данных застрахованных лиц Пензенской области;

ГУЗ «МИАЦ» – государственное учреждение здравоохранения «Медицинский информационно аналитический центр»;

ДДР – регистр дополнительной диспансеризации работающих граждан;

ЖМД – жесткий магнитный диск;

ИСПДн – информационная система персональных данных;

КЗ – контролируемая зона;

Минздрав – Министерство здравоохранения и социального развития;

Мининформсвязь – Министерство связи и массовых коммуникаций;

МНИ – магнитный носитель информации;

МУЗ – муниципальное учреждение здравоохранения;

МЭ – межсетевой экран;

НСД – несанкционированный доступ;

ОВД – отдел внутренних дел;

ОМС – обязательное медицинское страхование;

ОС – операционная система;

ПДн – персональные данные;

ПМВ – программно-математическое воздействие;

ПО – программное обеспечение;

ПОУ – перечень оказанных услуг;

ПЭВМ – персональная электронно-вычислительная машина;

ПЭМИН – побочные электромагнитные излучения и наводки;

РДД – реестр диспансеризации детей декретированных возрастов;

РДС – реестр детей сирот и детей, находящихся в тяжелой жизненной ситуации;

РДИ – регистр детей-инвалидов;

РВМ – регистр высокотехнологичной медицинской помощи;

РРВ – реестр медицинского персонала;

СК – страховая компания;

СКЗИ – средство криптографической защиты информации;

СЗИ – средство защиты информации;

СЗПДн – система (подсистема) защиты персональных данных;

СНИЛС – страховой номер индивидуального лицевого счета;

ТФОМС – территориальный фонд обязательного медицинского страхования;

УБПДн – угрозы безопасности персональных данных;

ФЗ – Федеральный закон;

ФСБ – Федеральная служба безопасности;

ФСТЭК – Федеральная служба по техническому и экспортному контролю;

ДЛО – дополнительное лекарственное обеспечение.

ВВЕДЕНИЕ

Необходимость разработки систем защиты информации обусловлена стремительным расширением сферы применения новейших информационных технологий и процессов в учреждениях здравоохранения, при обработке информации вообще, и персональных данных в частности.

В целях защиты прав и свобод человека при обработке его личной (персональной) информации, вступил в силу Федеральный закон РФ № 152 «О персональных данных» от 27.07.2006 г. Федеральный закон направлен на защиту совокупности прав и свобод человека при обработке его личной (персональной) информации, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Закон определяет понятие оператора персональных данных – это организация, которой доверил свои персональные данные человек или другая организация, обрабатывающая персональные данные. Для оператора закон ставит требования, которым должен следовать оператор персональных данных. Эти требования сформулированы в «Положении об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» (Постановление Правительства РФ 2007 г. N 781), совместном Приказе ФСТЭК России, ФСБ России, Мининформсвязи России 2008 г. N 55/86/20, а также в методических документах ФСТЭК России и ФСБ России [4].

Федеральный закон определил временные рамки, в которые все действующие информационные системы должны быть модернизированы в соответствии с новыми требованиями к 1 января 2011 года.

Построение системы защиты информационной системы должно осуществляться с применением системного подхода. Системный подход предполагает проведение комплекса мероприятий, включающих

исследование угроз информационной безопасности и разработку систему защиты персональных данных.

Система защита персональных данных представляют собой совокупность организационных и технических мероприятий для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также иных неправомерных действий с ними.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий с ними.

В дипломном проекте Оператором обработки персональных данных является Федеральное казенное учреждение «Войсковая часть 45108». Информационная система персональных данных представляет собой отдельно стоящую персональную электронно-вычислительную машину, имеющую подключение к интернету.

Стадии создания системы защиты информации информационной системы персональных данных госпиталя включают:

- предпроектная стадия, включающая предпроектное обследование информационной системы персональных данных (см. раздел 1) с составлением «Протокола оценки обстановки в части обеспечения безопасности персональных данных, обрабатываемых в информационной системе персональных данных» (см. подраздел 1.1) и «Отчета о результатах проведения внутренней проверки обеспечения защиты персональных данных в информационной системе персональных данных» (см. подраздел 1.2);

– определение уровня защищённости информационной системы персональных данных в соответствии с Приказом ФСТЭК России от 18 февраля 2013 г. № 21, определение класс защищённости информационной системы персональных данных в соответствии с Приказом ФСТЭК России от 11 февраля 2013 г. № 17, повышение класса защищённости до значения, обеспечивающего выполнение пункта 27 Требований, утверждённых приказом ФСТЭК России от 11 февраля 2013 г. № 17, в случае, если определённый в установленном порядке уровень защищённости персональных данных выше, чем установленный класс защищённости государственной информационной системы (см. раздел 2) [14];

– разработку «Частой модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных» (см. раздел 3);

– разработку организационно-распорядительной документации (см. раздел 4);

– внедрение средств защиты информации (см. раздел 5);

– разработку «Программы и методик проведения аттестационных испытаний на соответствие требованиям безопасности информации» (см. раздел 6);

– разработку «Протокола испытаний комплексной системы защиты информации информационной системы персональных данных на соответствие требованиям безопасности информации в части защиты от несанкционированного доступа и компьютерных вирусов» (см. раздел 7);

– формирование «Заключения по результатам проведения аттестационных испытаний информационной системы персональных данных на соответствие требованиям безопасности информации» (см. раздел 8);

– составление и выдачу «Аттестата соответствия информационной системы персональных данных требованиям безопасности информации» (см. раздел 9).

1 Результаты обследования объекта информатизации

1.1 Разработка «Протокола оценки обстановки в части обеспечения безопасности ПДн, обрабатываемых в ИСПДн»

1.1.1 Анализ информационных ресурсов

В процессе обеспечения своей деятельности осуществляет обмен информацией со сторонними организациями.

В целях выполнения требований ФЗ «О персональных данных», а также исходя из возможных финансовых затрат на защиту ПДн, госпиталей выделяется отдельная рабочая станция, с помощью которой будет обеспечиваться защищенный обмен информацией со сторонними организациями. Рабочая станция не включается во внутреннюю локальную сеть госпиталя и имеет подключение к интернету. Перенос защищаемых данных с выделенной рабочей станцией и локальной сетью госпиталя должен осуществляться с использованием учтенных носителей информации.

Таким образом, информационная система персональных данных (ИСПДн), обеспечение безопасности которой посвящен дипломный проект, представляет собой отдельно стоящую рабочую станцию (инв. № 20402005302), подключенную к сети интернет.

Все оборудование ИСПДн территориально размещено на первом этаже в кабинете «Регистратура» госпиталя по адресу: 442542, Пензенская обл., г. Кузнецк-12, ул. Свердловская, 2.

На персональной электронно-вычислительной машине (ПЭВМ) ИСПДн установлено следующее программное обеспечение (ПО):

- ОС Microsoft Windows XP Professional SP3;
- Backup Manager 1.5;
- Microsoft Office профессиональный выпуск версии 2003;
- Microsoft Office Visio Professional 2003;

- Microsoft OLE DB Provider for Visual FoxPro;
- Microsoft SQL Server 2000;
- Open AL;
- Oracle Data Provider for .NET Help;
- Oracle Database 10g Express Edition;
- Order Reminder HP LaserJet 1020;
- Power Quest Partition Magic 8.0;
- Remote Administrator v2.1;
- Total Commander 6.03a XP;
- Visual FoxPro ODBC Driver;
- Windows XP Service Pack 3;
- Архиватор WinRAR;
- Атлас ДЛО ЛПУ v2.1.1.1421;
- Атлас ДЛО ЛПУ v4.9.2.128;
- Библиотеки MS VISUAL FOX PRO 9;
- БИОТЭК ДЛО.

ИСПДн имеет связь с Территориальным фондом обязательного медицинского страхования Пензенской области (ТФОМС), Министерством здравоохранения и социального развития Российской Федерации (Минздрав), с государственное учреждение здравоохранения «Пензенский областной медицинский информационно аналитический центр» (ГУЗ «МИАЦ») и со страховыми компаниями (СК), аккредитованными в области обязательного медицинского страхования по шифрованному каналу связи.

Схема связи госпиталя с этими организациями приведена на рисунке 1.1.

В ИСПДн обрабатываются персональные данные.

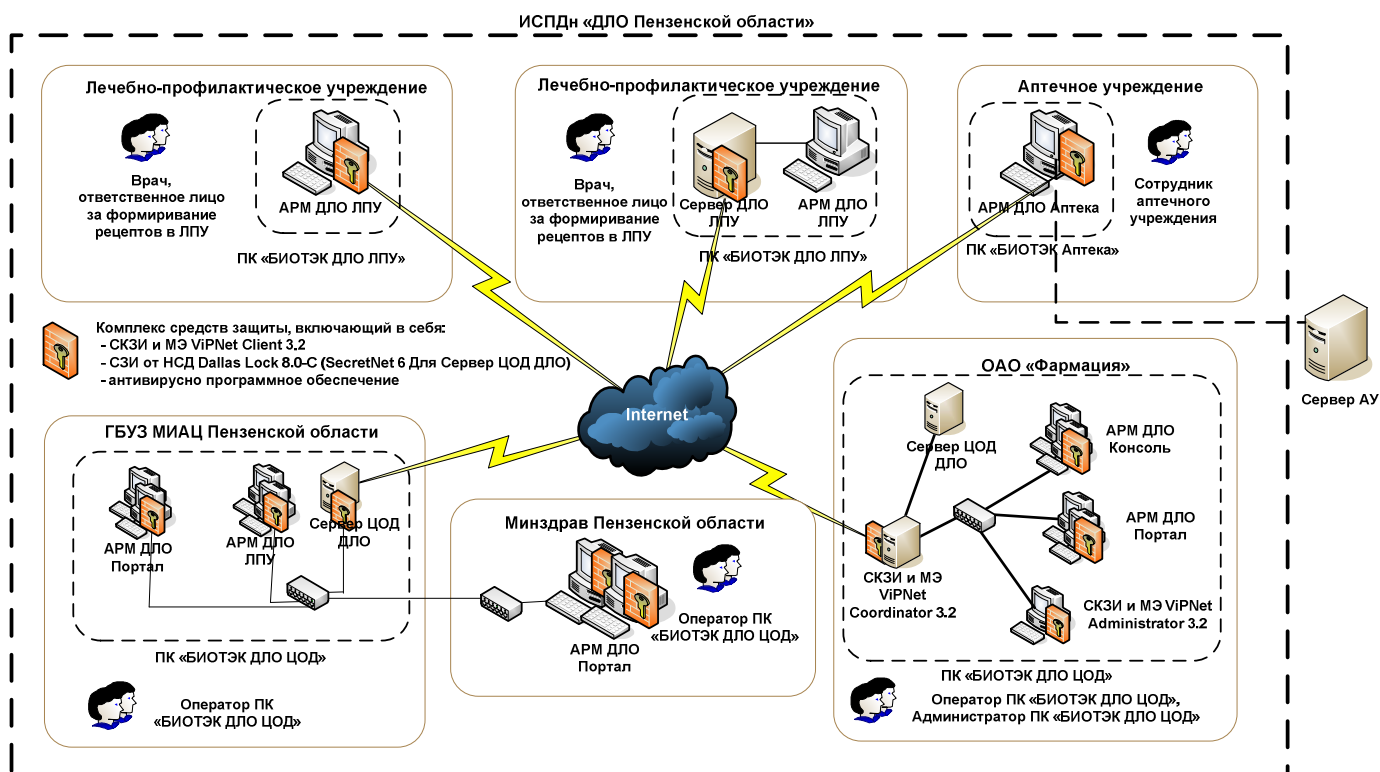


Рисунок 1.1 - Схема связи госпиталя с ЛПУ, аптечным учреждением, ГБУЗ «МИАЦ», Минздравом

Региональный сегмент Федерального регистра граждан, имеющих право на получение лекарственных средств (далее-ЛС), в котором содержатся следующие ПДн граждан:

- фамилия, имя, отчество;
- номер СНИЛС (свидетельства пенсионного обеспечения);
- сведения о полисе ОМС (серия, номер, дата получения полиса);
- пол (М/Ж);
- дата рождения;
- паспортные данные (серия и номер);
- адрес по месту регистрации;
- признак получения набора социальных услуг (НСУ);
- дата начала действия права на получение НСУ;

- дата окончания действия права на получение НСУ;
- код категории, по которой гражданину установлена ГСП;
- дата включения в региональный сегмент Регистра;
- дата исключения из регионального сегмента Регистра.

Регистр лиц страдающих высоко-затратными заболеваниями «7 нозологий», в котором содержатся следующие ПДн граждан:

- фамилия, имя, отчество;
- пол (М/Ж);
- дата рождения;
- сведения о полисе ОМС (серия, номер, дата получения полиса);
- адрес места жительства;
- паспортные данные (серия и номер);
- код заболевания (в кодах МЗ);
- наименование заболевания по МКБ-10;
- код учреждения здравоохранения;
- номер СНИЛС (свидетельства пенсионного обеспечения);
- сведения о том, что больной учтен в Федеральном регистре лиц, имеющих право на получение государственной социальной помощи;
- сведения, о том, что больной имеет право на льготное и бесплатное обеспечение лекарственными средствами;
- информация о включении больного в принятую заявку субъекта Российской Федерации для централизованной закупки лекарственных средств.

Реестр врачей, в котором содержатся следующие ПДн граждан:

- фамилия, имя, отчество;
- дата рождения;
- индивидуальный код врача;
- код врачебной должности;

- место жительства;
- семейное положение;
- дата приема на работу;
- номер приказа о приеме на работу;
- квалификационная категория;
- дата выдачи сертификата;
- ставка.

База данных ЦОД ДЛО, в которой содержатся следующие ПДн граждан:

- номер СНИЛС (свидетельства пенсионного обеспечения);
- ФИО;
- пол (М/Ж);
- серия и номер документа, удостоверяющего личность;
- тип документа, удостоверяющего личность;
- дата рождения;
- сведения о полисе ОМС (серия, номер, дата получения полиса);
- адрес места жительства;
- признак получения набора социальных услуг (НСУ);
- дата начала действия права на получение НСУ;
- дата окончания действия права на получение НСУ;
- код заболевания (в кодах МКБ10);
- наименование заболевания по МКБ-10;
- код учреждения здравоохранения;
- код категории, по которой гражданину установлена ГСП;
- наименование категории, по которой гражданину установлена

ГСП;

- дата включения в региональный сегмент Регистра;
- дата исключения из регионального сегмента Регистра;

- номер документа, подтверждающего право на льготу;
- период действия льготы;
- серия и номер рецепта;
- состояние рецепта;
- дата выписки рецепта;
- код и ФИО врача;
- код и наименование ЛС;
- дозировка;
- выписано единиц ЛС.

Базы данных ДЛО ПК «БИОТЭК ДЛО ЛПУ», ПК «БИОТЭК ДЛО Аптека», в которых содержатся следующие ПДн граждан:

- номер СНИЛС (свидетельства пенсионного обеспечения);
- ФИО;
- пол (М/Ж);
- серия и номер документа, удостоверяющего личность;
- тип документа, удостоверяющего личность;
- дата рождения;
- сведения о полисе ОМС (серия, номер, дата получения полиса);
- адрес места жительства;
- признак получения набора социальных услуг (НСУ);
- дата начала действия права на получение НСУ;
- дата окончания действия права на получение НСУ;
- код заболевания (в кодах МКБ10);
- наименование заболевания по МКБ-10;
- код учреждения здравоохранения;
- код категории, по которой гражданину установлена ГСП;
- наименование категории, по которой гражданину установлена

ГСП;

- дата включения в региональный сегмент Регистра;
- дата исключения из регионального сегмента Регистра;
- номер документа, подтверждающего право на льготу;
- период действия льготы;
- серия и номер рецепта;
- состояние рецепта;
- дата выписки рецепта;
- код и ФИО врача;
- код и наименование ЛС;
- дозировка;
- выписано единиц ЛС.

ИСПДн имеет подключение к сети Интернет, которое используется в качестве среды обмена информацией между госпиталем и ЛПУ, аптечным учреждением, ГБУЗ «МИАЦ», Минздравом. Подключение осуществляется по телефонной линии общего пользования через ADSL-модем.

ИСПДн по заданным характеристикам безопасности ПДн относится к специальным ИСПДн.

Режим обработки ПДн – многопользовательский режимом обработки персональных данных с равными правами доступа к ним.

Понижающая трансформаторная подстанция госпиталя расположена в пределах контролируемой зоны (КЗ).

В работе ИСПДн используются следующие средства защиты информации (СЗИ):

- антивирусная программа Kaspersky Internet Security 6.0;
- средство криптографической защиты информации (СКЗИ) и межсетевой экран (МЭ) «ViPNet Client 3.2».

Все технические средства из состава ИСПДн размещены на территории Российской Федерации.

Проведенный анализ исходных данных по ИСПДн показал, что:

- в качестве защиты информации от несанкционированного доступа (НСД) должны применяться сертифицированные СЗИ;
- в качестве антивирусной защиты применяется антивирус Kaspersky Internet Security 6.0;
- подключение ПЭВМ ИСПДн к каналам связи общего пользования и сетям международного информационного обмена, в том числе сети Интернет, осуществляется при помощи сертифицированного СКЗИ и средства межсетевого экранирования «ViPNet Client 4»;
- помещение, где расположена ИСПДн, имеет одно окно, оборудованные решеткой, дверь, обитую железом и запирающуюся на замок.

1.1.2 Анализ уязвимых звеньев и возможных угроз безопасности ПДн

Уязвимыми звеньями и возможными угрозами безопасности ПДн (УБПДн) являются физический доступ к ИСПДн, который возможен за счет несанкционированного входа в систему лицами, не допущенными к работе на ПЭВМ ИСПДн.

Кроме того, к уязвимым звеньям ИСПДн следует отнести возможность утечки информации за счет НСД, по каналам побочных электромагнитных излучения и наводок (ПЭМИН), а также возможность просмотра текстовой и графической видовой информации, выводимой на экраны видеомониторов (видовой канал).

К возможным УБПДн следует отнести программно-математические воздействия (внедрение вредоносных программ, вирусные атаки, сетевые атаки) и воздействия на аппаратные средства ИСПДн (отключение электропитания, перебои в функционировании каналов связи (для подключения ИСПДн к сети Интернет) и т.д.).

Возможность перехвата информации по акустическому, виброакустическому и электроакустическому каналам с использованием технических средств отсутствует в связи с тем, что голосовой ввод ПДн в ИСПДн пользователями и воспроизведение ПДн акустическими средствами отсутствует.

Электромагнитное воздействие (электромагнитное навязывание) на ИСПДн исключается ввиду сложности реализации и нецелесообразности его реализации для противника.

Угрозы утечки информации по каналу ПЭМИН маловероятны, т.к. размер КЗ большой, элементы ИСПДн находятся в центре здания и экранируются несколькими несущими стенами, паразитный сигнал маскируется со множеством других паразитных сигналов элементов, не входящих в ИСПДн.

1.1.3 Оценка ущерба от реализации УБПДн

Ущерб от реализации УБПДн может быть непосредственным и опосредованным.

К непосредственному ущербу следует отнести разглашение информации о субъектах ПДн, злоумышленные действия в отношении субъектов ПДн и т.д.

К опосредованному ущербу относятся: приостановка или замедление работы госпиталя, ТФОМС Пензенской области, Минздрава, ГУЗ «МИАЦ», СК, штрафные санкции в случае утечки информации, неполучение Госпиталей оплаты медицинских услуг, предоставленных по системе ОМС.

Данные виды ущерба при нарушении характеристик безопасности персональных данных, хранящихся в ИСПДн, могут привести к значительным негативным последствиям для субъектов ПДн, госпиталя и ТФОМС, ГУЗ «МИАЦ», СК.

1.2 Составление «Отчета о результатах проведения внутренней проверки обеспечения защиты ПДн в ИСПДн»

1.2.1 Общие положения

В ходе проверки была выявлена следующая ИСПДн: «АРМ ДЛО Федеральное казенное учреждение «Войсковая часть 45108»».

Данные проверки представляют из себя основу для организационно-распорядительных документов.

Данные о составе и структуре объектов защиты описаны в «Перечне персональных данных, подлежащих защите».

Данные о составе и структуре обрабатываемых ПДн, конфигурация ИСПДн и режиме обработке используются для составления «Акта классификации ИСПДн».

Данные о лицах, допущенных к обработке ПДн, и степени их осведомлённости информацией отражаются в «Положении о разграничении прав доступа к обрабатываемым персональным данным».

Данные об угрозах безопасности ПДн служат основной для составления «Частной модели угроз безопасности персональных данных при их обработке в ИСПДн».

Данные о существующих и необходимых мерах защиты ПДн служат основной для составления «Плана мероприятий по обеспечению защиты ПДн».

1.2.2 Структура ИСПДн

Структура ИСПДн представлена в таблице 1.1.

1.2.3 Состав ПДн

Обрабатываемые ПДн в ИСПДн представлены в пункте 1.1.1.

В БДЗ содержатся ПДн, отнесенные ко 2 категории (позволяют идентифицировать субъекта ПДн и получить о нем дополнительную информацию, за исключением данных, касающихся расовой,

национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни). В БДЗ содержатся данные субъектов всей Пензенской области, что составляет более 100000 субъектов ПДн (Хнпд равно 1).

Таблица 1.1 – Параметры ИСПДн

Заданные характеристики безопасности персональных данных	Специальная информационная система
Структура информационной системы	Автоматизированное рабочее место
Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена	Имеется подключение к сети Интернет через ADSL-модем
Режим обработки персональных данных	Многопользовательская система
Режим разграничения прав доступа пользователей	Система без разграничения прав доступа к защищаемым ПДн
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации
Дополнительная информация	К ПДн предъявляется требование целостности и конфиденциальности

В базе уволенных содержатся ПДн, отнесенные ко 2 категории (позволяют идентифицировать субъекта ПДн и получить о нем дополнительную информацию, за исключением данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни). Объем данных в базе уволенных периодически увеличивается и может составлять более 100000 субъектов ПДн (Хнпд равно 1).

В ПОУ, ДДР, РВМ, РДС, РДИ, РДД, запросах из ОВД содержатся ПДн, отнесенные к 1 категории, что определяется данными о состоянии здоровья субъектов ПДн.

В РРВ содержатся ПДн, отнесенные ко 2 категории (Хнпд равно 3).

1.2.4 Объекты защиты в ИСПДн

В ИСПДн существуют объекты защиты.

Технологическая информация:

- информация, служащая для управления системами (конфигурации, различные таблицы маршрутизации, настройки всех систем защиты и пр.);
- технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);
- информация, представленная на разнообразных носителях информации, которые содержат защищаемую информацию системы управления ресурсами или различных средств доступа к этим системам;
- информация о средствах защиты ПДн (СЗПДн), их составе и структуре, принципах и технических решениях защиты;
- различные информационные ресурсы, которые включают в себя техническую информацию о системах, о трафике, о событиях, планы обеспечения бесперебойной работы и управления в аварийных режимах;
- служебные данные (метаданные) появляющиеся при работе ПО, сообщений и протоколов межсетевого взаимодействия, в результате обработки обрабатываемой информации.

Программно-технические средства обработки:

- общесистемное и специальное ПО (см. таблицу 1.2);
- резервные копии общесистемного ПО;
- аппаратные средства обработки ПДн (см. таблицу 1.3).

Средства защиты ПДн:

- средства управления и разграничения доступа пользователей:
MS Windows XP Pro;
- средства обеспечения регистрации и учета действий с информацией: MS Windows XP Pro;
- средства антивирусной защиты: Kaspersky Internet Security 6.0;

- средства межсетевого экранирования: ViPNet Client 4;
- средства криптографической защиты ПДн, при их передаче по каналам связи сетей общего и (или) международного обмена: ViPNet Client 4.

Каналы информационного обмена и телекоммуникации. В качестве канала информационного обмена, по которому передаются обрабатываемая и технологическая информация, используется общедоступная сеть Интернет, подключение к которой осуществляется через ADSL-модем.

Объекты и помещения, в которых размещены компоненты ИСПДн.

ИСПДн располагается в комнате «Помещение приема и передачи электронной почты» на первом этаже двухэтажного здания госпиталя, дверь обита железом и оборудована замком. Помещение имеет одно окно, оборудованное решеткой, которое выходит на внутреннюю территорию госпиталя.

Таблица 1.2 - Общесистемное и специальное ПО

№ п/п	Наименование программного средства
1	ОС Microsoft Windows XP Professional SP3, лиц. № 76456-OEM-0013082-43768
2	Backup Manager 1.5
3	DallasLock8.0C
4	Kaspersky Internet Security 2016
5	Microsoft Office - профессиональный выпуск версии 2003
6	Microsoft Office Visio Professional 2003
7	Microsoft OLE DB Provider for Visual FoxPro

Продолжение таблицы 1.2

№ п/п	Наименование программного средства
8	Microsoft SQL Server 2000
9	Oracle Data Provider for .NET Help
10	Oracle Database 10g Express Edition
11	OrderReminder HP LaserJet 1020
12	PowerQuest PartitionMagic 8.0
13	Remote Administrator v2.1
14	Total Commander 6.03a XP
15	ViPNet Client
16	Visual FoxPro ODBC Driver
17	Windows XP Service Pack 3
18	ZET
19	Архиватор WinRAR
20	Атлас ДЛО ЛПУ v2.1.1.1421
21	Атлас ДЛО ЛПУ v4.9.2.128
22	Библиотеки MS VISUAL FOX PRO 9
23	БИОТЭК ДЛО

Таблица 1.3 - Аппаратные средства обработки ПДн

№ п/п	Наименование	Тип (модель)	Серийный (заводской) номер
1	Системный блок	Kraftway	20402005302
2	Монитор	Acer AL1716F	ETL460C26073000B53404B
3	Клавиатура	Kraftway KB-9810	ZCE793902924
4	Манипулятор типа «мышь»	Kraftway MSO-0502	0706017871
5	Принтер	HP LaserJet 1020	CNC2393348

1.2.5 Конфигурация ИСПДн

На рисунке 1.2 представлено территориальное расположение ИСПДн относительно границ КЗ.

На рисунке 1.3 представлено размещение ИСПДн в кабинете «Бухгалтерия».

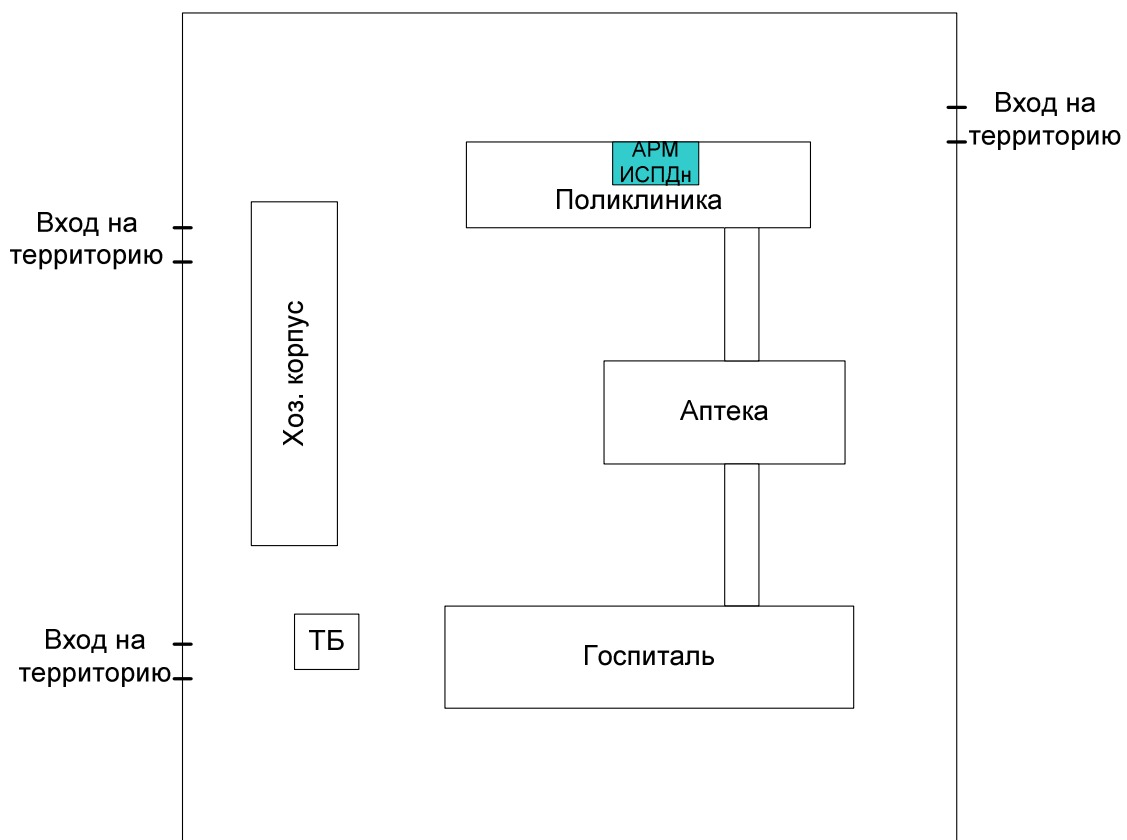


Рисунок 1.2 – Расположение АРМ ИСПДн относительно границ контролируемой зоны

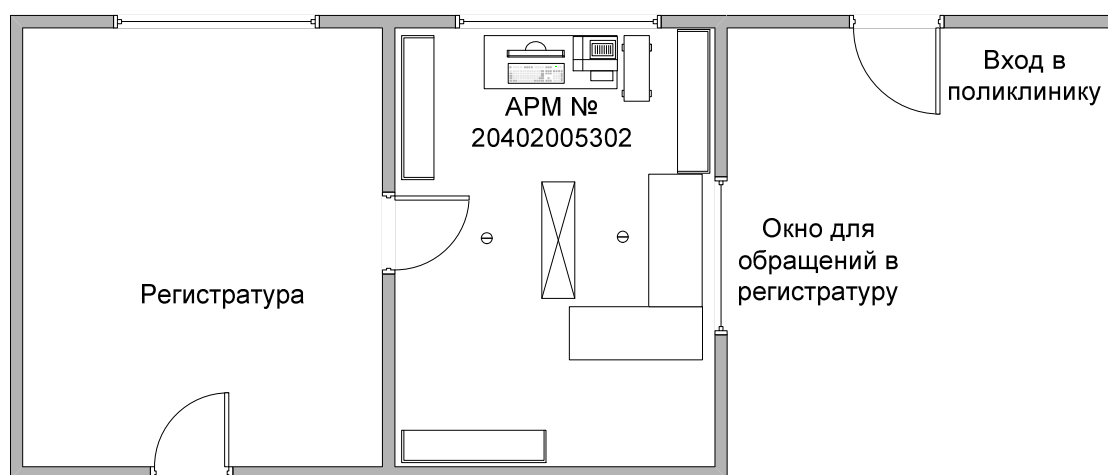


Рисунок 1.3 – Расположение АРМ ИСПДн в помещении «Регистратура» госпиталя

1.2.6 Структура обработки ПДн

В ИСПДн обработка ПДн происходит следующим образом:

- пользователь ИСПДн авторизуется на своем рабочем месте в операционные системы (ОС) Windows XP;
- пользователь ИСПДн авторизуется в программе «ViPNet Client 4»;
- пользователь ИСПДн производит обмен ПДн по защищенному каналу связи при помощи СКЗИ «ViPNet Client 4» с организациями, указанными на рисунке 1.1, с необходимой периодичностью;
- пользователь ИСПДн производит копирование полученных по защищенному каналу связи ПДн от организаций, указанных на рисунке 1.1, на учетный внешний носитель или в папку d:/ПДн;
- пользователь ИСПДн производит копирование ПДн с учетного внешнего носителя в папку d:/ПДн для последующей передачи по защищенному каналу связи в организации, указанные на рисунке 1.1, с необходимой периодичностью;
- пользователь ИСПДн обрабатывает ПДн с помощью программных средств, установленных на автоматизированном рабочем месте (АРМ) ИСПДн;
- пользователь ИСПДн при служебной необходимости может разрабатывать, хранить, удалять и выводить на печать документы, содержащие ПДн.

1.2.7 Режим обработки ПДн

В ИСПДн обработка ПДн осуществляется в многопользовательском режиме обработки ПДн и равных правах доступа к ним.

ИСПДн предназначена для обмена ПДн по защищенному каналу связи с организациями, указанными на рисунке 1.1, а также для разработки, хранения, и печати документов, содержащих ПДн.

Режим обработки предусматривает следующие действия с ПДн: получение из канала связи, сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, печать и передачу по каналу связи, блокирование, уничтожение ПДн.

Все пользователи ИСПДн имеют собственные роли. Список типовых ролей представлен в виде матрицы доступа в таблице 1.4.

Таблица 1.4 – Матрица доступа

Группа	Уровень доступа к ПДн	Разрешенные действия	Сотрудники
Администратор ИСПДн	Обладает информацией о ПО ИСПДн. Обладает информацией о ТС и конфигурации ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Обладает правами настройки ТС ИСПДн.	- получение из канала связи - сбор - систематизация - накопление - хранение - уточнение - использование - печать - передача по каналу связи - уничтожение	Иванов А.А. - программист В/ч 45108
Администратор безопасности	Права администратора ИСПДн. Имеет доступ к СЗИ и к части элементов ИСПДн. Не обладает правами конфигурирования и настройки ТС ИСПДн	-получение из канала связи - сбор - систематизация - накопление - хранение - уточнение - использование - печать - передача по каналу связи - уничтожение	Иванов А.А. - программист В/ч 45108
Операторы ИСПДн	Имеет доступ ко всем ПДн.	- получение из канала связи - сбор - систематизация - накопление - хранение - уточнение	Операторы ИСПДн госпиталя в/ч 45108

1.2.8 Угрозы безопасности ПДн

При обработке ПДн в ИСПДн были выделены некоторые угрозы, актуальные для данной ИСПДн, которые будут рассмотрены.

1.2.9 Существующие меры защиты

Существующие в ИСПДн технические меры защиты представлены в таблице 1.5.

В ИСПДн введены следующие организационные меры защиты:

- принятие мер по недопущению в помещении бесконтрольного пребывания посторонних лиц;
- использование лицензионного ПО;
- применение источников гарантированного и бесперебойного питания;
- применение сертифицированного СКЗИ «ViPNet Client 4» со встроенным сертифицированным межсетевым экраном 3 класса защищенности (по требованиям ФСТЭК (Гостехкомиссии) России);
- применение антивирусных средств (Антивирус Kaspersky Internet Security 6.0) и периодическое обновление их баз.

Таблица 1.5 – Меры защиты

Элемент ИСПДн	ПС обработки ПДн	Установленные СЗИ
АРМ ИСПДн	ОС «Windows XP»	Средства ОС: <ul style="list-style-type: none">- управление доступом пользователей;- регистрация действий пользователя с информацией.
	Антивирус «Kaspersky Internet Security 6.0»	Антивирус «Kaspersky Internet Security 6.0»: <ul style="list-style-type: none">- обнаружение вирусов;- обезвреживание вирусов;- обнаружение вторжений.

Продолжение таблицы 1.5

Элемент ИСПДн	ПС обработки ПДн	Установленные СЗИ
Каналы передачи	СКЗИ и МЭ «ViPNet Client 4»	СКЗИ и МЭ «ViPNet Client 4»: - шифрование ПДн при передаче по каналу связи; - регистрация и учет действий с передаваемой (принимаемой) информацией; - обеспечение целостности защищаемой информации при передаче (приеме) по каналу связи; - обеспечение безопасного межсетевого взаимодействия

1.2.10 Необходимые меры защиты

На основании анализа выявленных УБПДн для достижения требуемого уровня защиты рекомендуется осуществить следующие мероприятия:

- использование сертифицированного СЗИ от НСД, а также соответствующая настройка и эксплуатация данного средства;
- ведение учета носителей защищаемой информации;
- обеспечение надежного хранения защищаемых носителей информации (металлический шкаф, сейф);
- проведение внутренних проверок режима безопасности ПДн на постоянной, периодической основе;
- осуществление резервного копирования защищаемой информации и средств защиты.

Состав и перечень необходимых мер и СЗИ может уточняться на этапе проектирования ИСПДн.

2 Определение класса защищённости ИСПДн

2.1 Определение класса защищённости ИСПДн в соответствии с Приказом ФСТЭК России от 11 февраля 2013 г. №17

Класс защищенности информационной системы определен исходя от уровня значимости информации, обрабатываемой в этой информационной системе, и масштаба информационной системы.

Уровень значимости информации определён исходя из степени возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации.

Для свойств безопасности информации были определены степени ущерба, которые приведены в таблице 2.1.

Таблица 2.1 – Соответствие степени ущерба свойствам безопасности информации

Свойство информации	Степень ущерба
Конфиденциальность	Средняя
Целостность	Средняя
Доступность	Средняя

Исходя из таблицы 2.1 информация имеет средний уровень значимости (УЗ 2), так как для каждого из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба.

Класс защищенности информационной системы определён в соответствии с таблицей 2.2.

Таблица 2.2 – Определение класса защищённости информационной системы

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ 1	K1	K1	K1
УЗ 2	K1	K2	K2
УЗ 3	K2	K3	K3
УЗ 4	K3	K3	K4

В соответствии с таблицей 2.2 определён 2 класс защищённости для информационной системы.

2.2 Определение уровня защищённости ИСПДн в соответствии с Приказом ФСТЭК России от 18 февраля 2013 г. №21

По результатам проведенного анализа исходных данных информационной системы персональных данных «АРМ ДЛО Федеральное казенное учреждение «Войсковая часть 45108»» выявлены следующие характеристики, представленные в таблице 2.3.

Таблица 2.3 – Характеристики информационной системы персональных данных «АРМ ДЛО Федеральное казенное учреждение «Войсковая часть 45108»»

Тип угроз, связанных с наличием недокументированных (недекларированных) возможностей (на основании частной модели угроз)	Угрозы 3-го типа
Объем обрабатываемых персональных данных	Более 100000
Тип информационной системы персональных данных	Специальная

На основании полученных данных и в соответствии с Постановлением Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» в информационной

системе персональных данных «АРМ ДЛО Федеральное казенное учреждение «Войсковая часть 45108»» необходимо обеспечить 2-й уровень защищенности персональных данных.

2.3 Повышение класса защищённости

Повышение класса защищённости до значения, обеспечивающего выполнения пункта 27 Требований, утверждённых приказом ФСТЭК России от 11 февраля 2013 г. №17, не было осуществлено, так как определённый в установленном порядке уровень защищённости персональных данных не выше, чем установленный класс защищённости государственной информационной системы.

3 Разработка «Частной модели угроз безопасности ПДн при их обработке в ИСПДн»

3.1 Перечень угроз безопасности

3.1.1 Перечень угроз безопасности персональных согласно документам ФСТЭК и ФСБ

Разработка «Частной модели угроз безопасности ПДн при их обработке в ИСПДн» производится на основе «Базовой модели угроз безопасности...» ФСТЭК [7].

Обработка ПДн в ИСПДн осуществляется с использованием СКЗИ, поэтому при составлении «Частной модели угроз безопасности...» кроме «Базовой модели угроз безопасности...» ФСТЭК необходимо руководствоваться документом Федеральной службы безопасности (ФСБ) «Методические рекомендации по обеспечению с помощью криптосредств безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации» [8].

Таблица 3.1 – Исходный уровень защищенности

Позиция	Технические и эксплуатационные характеристики	Уровень защищенности
1	По территориальному размещению	высокий
2	По наличию соединения с сетями общего пользования	средний
3	По встроенным (легальным) операциям с записями баз ПДн	низкий
4	По разграничению доступа к ПДн	средний
5	По наличию соединений с другими базами ПДн иных ИСПДн	высокий
6	По уровню обобщения (обезличивания) ПДн	низкий
7	По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	средний

3.1.2 Угрозы безопасности персональных данных

Существует большое количество угроз безопасности персональных данных, которые зависят как от топологической структуры сети и расположения ИСПДн в помещении, как и от объемов обрабатываемой информации, квалификации пользователей и администраторов ИСПДн, квалификации возможного злоумышленника.

3.2 Классификация пользователей ИСПДн

Пользователи ИСПДн делятся на пять основных категорий:

- администратор ИСПДн;
- сотрудник госпиталя, который занимается настройкой, внедрением и сопровождением системы;
- администратор безопасности;
- сотрудник госпиталя, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент;
- оператор ИСПДн.

3.3 Определение уровня исходной защищенности

Под исходным уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y_I).

Оценка степени исходной защищенности (Y_I) ИСПДн делается на основе технических и эксплуатационных характеристик ИСПДн и таблицы соответствия этих характеристик уровням защищенности ИСПДн, по совокупности которых делается вывод об исходной защищенности ИСПДн и коэффициенту Y_I ставится соответствующее числовое значение:

- 0 - высокая;
- 5 - средняя;
- 10 - низкая.

В таблице 3.1 представлены характеристики уровня исходной защищенности для ИСПДн.

Таким образом, ИСПДн имеет среднюю степень исходной защищенности (Y_1 равно 5), так как более 70% характеристик соответствуют уровню не ниже «средний».

3.4 Определение вероятности реализации угроз, возможности реализации угроз, оценки опасности угроз и актуальности угроз безопасности

После реализуемость угроз оценивалась по величине исходной защищенности (Y_1) и вероятности реализации угрозы (Y_2).

Вероятность реализации угрозы (Y_2) характеризует насколько для данной информационной системы возможна реализация конкретной угрозы безопасности.

Числовой коэффициент (Y_2) имеет четыре степени:

- маловероятно (Y_2 равно 0);
- низкая вероятность (Y_2 равно 2);
- средняя вероятность (Y_2 равно 5);
- высокая вероятность (Y_2 равно 10).

Коэффициент реализуемости высчитывается (Y_2) и выражает возможность реализации угрозы.

Определение вероятности реализации и оценка опасности производится на основе экспертной оценки специалистов и определяется показателем, который имеет три значения:

- низкая опасность;
- средняя опасность;
- высокая опасность.

Определение оценки вероятности реализации УБПДн и оценки опасности УБПДн на основе опроса экспертов представлено в приложении

А. Количество экспертов равно трем. Итоговые оценки вероятности реализации УБПДн и оценки опасности находились усреднением значений опроса экспертов.

Для ИСПДн определяется степень актуальности угрозы (см. таблицу 3.2).

Таблица 3.2 – Правило отнесения угрозы безопасности к актуальной

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

3.5 Перечень актуальных угроз безопасности ПДн

Были выявлены следующие актуальные угрозы, в соответствии с особенностями данной ИСПДн. Для снижения опасности реализации актуальных УБПДн рекомендуется осуществить следующие мероприятия:

- для обеспечения требуемых характеристик безопасности базы данных (БДЗ, База уволенных, ПОУ, РРВ, ДДР, РВМ, РДС, РДИ, РДД, запросы из ОВД) при обмене с ТФОМС, Минздравом, СК, ГУЗ «МИАЦ» по открытым каналам связи использовать СКЗИ, обеспечивающую криптографическую защиту по уровню КС1, что должно подтверждаться соответствующим сертификатом ФСБ России.

4 Разработка организационно-распорядительной документации

4.1 Формирование «Перечня ПДн, подлежащих защите в ИСПДн»

Настоящий перечень ПДн, подлежащих защите в ИСПДн разработан на основе методических рекомендаций Министерства здравоохранения и социального развития РФ.

«Перечень ПДн, подлежащих защите в ИСПДн» представлен в приложении Б.

4.2 Составление «Плана мероприятий по обеспечению защиты ПДн в ИСПДн»

План составлен на основании списка мер, методов и средств защиты, необходимых для создания системы защиты информации ИСПДн госпиталя.

Выбор мероприятий произведён на основании «Отчета по результатам внутренней проверки...» и «Частной модели угроз безопасности ПДн ...».

В план включены следующие категории мероприятий:

- организационные мероприятия;
- физические мероприятия;
- технические (аппаратные и программные) мероприятия;
- контролирующие мероприятия.

В «План мероприятий по обеспечению защиты...» включена следующая информация об мероприятии, направленному на обеспечению защиты:

- название;
- периодичность (разовое/периодическое);
- исполнитель/ответственный за исполнение.

«План мероприятий по обеспечению защиты ПДн в ИСПДн» представлен в приложении Г.

4.3 Формирование «Положения о разграничении прав доступа к ПДн в ИСПДн»

Целью данного Положения является защита ПДн работников от НСД, неправомерного их использования или утраты.

Настоящее Положение разработано на основании статей Конституции РФ, Трудового Кодекса РФ, Кодекса об административных правонарушениях РФ, Гражданского Кодекса РФ, Уголовного Кодекса РФ, а также Федерального закона «Об информации, информатизации и защите информации».

ПДн являются конфиденциальной информацией.

Настоящее Положение является обязательным для исполнения всеми работниками, имеющими доступ к ПДн сотрудников.

«Положение о разграничении прав доступа к ПДн в ИСПДн» приведено в приложении Д.

4.4 Разработка инструкций

Инструкции определяют права, возможности и ограничения в действии администраторов и пользователей.

На ИСПДн разрабатывается пять инструкций. Данные инструкции предназначены различным категориям работников. Для администратора ИСПДн, для администратора безопасности ИСПДн, для пользователя ИСПДн, для пользователя ИСПДн на случай экстренных или внештатных ситуаций. Также разработана инструкция по антивирусной защите.

5 Внедрение СЗИ

На ИСПДн выполняется:

- установка СЗИ НСД «Secret Net 7.6» (установка платы Secret Net Touch Memory Card, установка ПО «Secret Net 7.6»);
- настройка СЗИ НСД «Secret Net 7.6», антивируса Касперского 6.0;
- контроль настройки СКЗИ «ViPNet Client 4».

Система защиты информации от НСД «Secret Net 7.6» (автономный вариант), производимая ЗАО «НИП «Информзащита» (г. Москва).

Существующая система защиты информации от НСД к информации и ресурсам в сетях с IP-протоколом «ViPNet CUSTOM 3.1» (в состав которой входит СКЗИ «ViPNet Client 4»), производимая ОАО «Инфотекс» (г. Москва).

Программное изделие «Антивирус Касперского 6.0», производимое ЗАО «Лаборатория Касперского», является антивирусным средством защиты, функционирующим под управлением операционной системы семейства Microsoft Windows.

6 Разработка «Программы и методик проведения аттестационных испытаний на соответствие требованиям безопасности информации»

6.1 Общие положения

Настоящая программа определяет условия и порядок проведения аттестационных испытаний ИСПДн на соответствие требованиям по безопасности ПДн.

Целью аттестационных испытаний является оценка защищенности ИСПДн в соответствии с действующими специальными требованиями и нормами ФСТЭК России по защите информации, обрабатываемой ИСПДн, от несанкционированных действий к информации.

Объем аттестационных испытаний ИСПДн определен следующим перечнем работ:

а) анализ технологического процесса обработки информации (см. подраздел 6.2);

б) анализ ИСПДн на соответствие организационно-техническим требованиям по ЗИ (см. подраздел 6.3):

1) анализ внутренней и распорядительной документации по защите информации в ИСПДн (см. пункт 6.3.1);

2) анализ информационных потоков (см. пункт 6.3.2);

в) анализ уровня подготовки кадров и распределения ответственности за выполнением требований по защите информации (см. пункт 6.3.4);

г) испытания ИСПДн на соответствие требованиям по защите информации (см. подраздел 6.4):

1) испытания подсистемы обеспечения целостности (см. пункт 6.4.1);

2) испытания подсистемы регистрации и учета (см. пункт 6.4.2);

- 3) испытания подсистемы управления доступом (см. пункт 6.4.3);
- 4) испытания криптографической подсистемы (см. пункт 6.4.4);
- 5) испытания подсистемы антивирусной защиты (см. пункт 6.4.5);

д) подготовка отчетной документации – «Протокола испытаний комплексной системы защиты информации ИСПДн на соответствие требованиям безопасности информации в части защиты от НСД и компьютерных вирусов» и «Заключения по результатам аттестационных испытаний ИСПДн на соответствие требованиям безопасности информации», «Аттестата соответствия ИСПДн требованиям безопасности информации» (см. подраздел 6.5).

6.2 Анализ технологического процесса обработки информации

При изучении технологического процесса автоматизированной обработки и хранения информации анализу подвергаются:

- особенности процесса обработки информации в ИСПДн;
- полный список объектов, к которым осуществляется доступ;
- перечень лиц, которые осуществляют доступ;
- список штатных, постоянно используемых средств для получения или модификации информации;
- список используемых СЗИ;
- описание всех используемых правил для обеспечения разделения доступа;
- угрозы НСД.

Проверяется соответствие описания процесса реальной практике.

Проверяются исходные данные на ИСПДн и устанавливаются опасные факторы и угрозы, критические места, снижающие уровень защиты, комплектность и характеристики средств защиты.

Проверяются наличие оформленных разрешений на допуск персонала к информации, содержащей ПДн, метки на информационных носителях, соответствие инструкций пользователей и администратора безопасности информации установленным требованиям.

По результатам изучения уточняется схема технологического процесса.

По результатам анализа технологического процесса обработки и хранения информации в ИСПДн проверяется выполнение требований по физической охране средств ИСПДн и носителей информации в ИСПДн, пропускному режиму и оборудованию помещений необходимыми защитными средствами. Проверяется наличие в системе администратора безопасности ИСПДн, оценивается его уровень подготовленности и степень оснащения его рабочего места необходимыми средствами оперативного контроля и сопровождения СЗИ.

6.3 Анализ ИСПДн на соответствие различным требованиям по защите информации

6.3.1 Анализ внутренней и распорядительной документации по защите информации в ИСПДн

На момент проведения аттестации ИСПДн аттестационной комиссии должны быть представлены, а аттестационной комиссией проанализированы следующие исходные данные и документация:

- протокол оценки обстановки в части безопасности ПДн, обрабатываемых в ИСПДн «АРМ ДЛО Федеральное казенное учреждение «Войсковая часть 45108»» с ТФОМС по Пензенской области»;
- отчет о результатах проведения внутренней проверки обеспечения защиты ПДн в ИСПДн «АРМ ДЛО Федеральное казенное учреждение «Войсковая часть 45108»» с ТФОМС по Пензенской области»;

- частная модель угроз безопасности ПДн при их обработке в ИСПДн «АРМ ДЛО Федеральное казенное учреждение «Войсковая часть 45108»» с ТФОМС по Пензенской области»;
- перечень ПДн, подлежащих защите в ИСПДн «АРМ ДЛО Федеральное казенное учреждение «Войсковая часть 45108»» с ТФОМС по Пензенской области»;
- план мероприятий по обеспечению защиты ПДн в ИСПДн «АРМ ДЛО Федеральное казенное учреждение «Войсковая часть 45108»» с ТФОМС по Пензенской области»;
- положение о разграничении прав доступа к обрабатываемым ПДн в ИСПДн «АРМ ДЛО Федеральное казенное учреждение «Войсковая часть 45108»» с ТФОМС по Пензенской области»;
- инструкция администратора ИСПДн «Обмен Федеральное казенное учреждение «Войсковая часть 45108»» с ТФОМС по Пензенской области»;
- инструкция пользователя ИСПДн «Обмен Федеральное казенное учреждение «Войсковая часть 45108»» с ТФОМС по Пензенской области»;
- инструкция администратора безопасности ИСПДн «Обмен Федеральное казенное учреждение «Войсковая часть 45108»» с ТФОМС по Пензенской области»;
- инструкция пользователя ИСПДн «Обмен Федеральное казенное учреждение «Войсковая часть 45108»» с ТФОМС по Пензенской области» по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций;
- инструкция по антивирусной защите в ИСПДн Федеральное казенное учреждение «Войсковая часть 45108»».

По результатам проверки комиссия должна сделать выводы о соответствии (или несоответствии) предъявленных документов и исходных данных установленным требованиям по безопасности информации.

6.3.2 Анализ информационных потоков

Используя исходные данные по технологии обработки и передачи информации, матрицу доступа персонала к защищаемым ресурсам, анализируется обобщенная технологическая схема ИСПДн с существующими и возможными информационными потоками, возможностями доступа к обрабатываемой и передаваемой информации.

6.3.3 Анализ уровня подготовки кадров и распределения ответственности за выполнением требований по защите информации

Проверка уровня подготовки кадров и распределения ответственности производится на основе следующих показателей:

- оценки знания пользователями и администраторами ИСПДн инструкций;
- наличия матрицы доступа персонала к защищаемым ресурсам, определяющей полномочия по доступу к ПДн, и процедуры их оформления, системы распределения ответственности персонала за выполнение требований по ИБ;
- оценки проведения учебы и повышения квалификации в сфере ИБ персонала и пользователей ИСПДн.

Путем проведения бесед с работниками проверяется осведомленность работников и степень знания ими руководящих документов, приказов, актов, инструкций и уровень знания основ безопасной обработки информации, описанных в инструкция, приведённых выше.

6.4 Испытания ИСПДн на соответствие требованиям по защите информации

6.4.1 Испытания подсистемы управления доступом

Проверка подсистемы управления доступом осуществляется с применением средства создания модели системы разграничения доступа «Ревизор 1 ХР» и программы контроля полномочий доступа к информационным ресурсам «Ревизор 2 ХР», системы анализа программного и аппаратного обеспечения ТСР/IP сетей «Ревизор Сети» версии 2.0.

6.4.2 Испытания подсистемы регистрации и учета

Для проверки регистрации изменения полномочий субъектов доступа необходимо произвести эти изменения при помощи средств СЗИ и просмотреть результаты регистрации.

Для проверки процедуры автоматического учета создаваемых защищаемых информационных ресурсов необходимо смоделировать создание защищаемого носителя информации. При помощи средств СЗИ просматриваются результаты учета. Должны быть автоматически учтены все созданные защищаемые информационные ресурсы с требуемыми параметрами учета.

Проверяется ведение учета всех защищаемых носителей информации, осуществляемого вручную персоналом, в соответствии с инструкциями, проверки правильности ведения журналов.

6.4.3 Испытания подсистемы обеспечения целостности

Надежность функций контроля целостности программных средств проверяется следующим способом: вносятся изменения в отдельные программы или они заменяются полностью. При этом отслеживаются последствия данных действий и их влияние на систему. При помощи программы «ФИКС 2.0.2» осуществляется расчет контрольных сумм

файлов из состава системы защиты для их сравнения с эталонными контрольными суммами на момент аттестации и при дальнейших проверках.

6.4.4 Испытания криптографической подсистемы

Проверка криптографической подсистемы проводится по перечню функций, определенных требованиями положения о «Методах и способах защиты информации в ИСПДн».

6.4.5 Испытания подсистемы антивирусной защиты

Проводится оценка защищенности информационных ресурсов ИСПДн от компьютерных вирусов по методике ПФ ФГУП «ЦентрИнформ».

6.5 Оформление отчетной документации по результатам аттестации ИСПДн

Результаты аттестационных испытаний ИСПДн по всем рассмотренным выше направлениям обеспечения безопасности информации оформляются Протоколом испытаний комплексной системы защиты информации ИСПДн на соответствие требованиям безопасности информации в части защиты от НСД и компьютерных вирусов, содержащим:

- состав комиссии, дату испытаний, наименование ИСПДн;
- цель испытаний;
- перечень используемых в работе документов и применяемых методик испытаний;
- результаты испытаний на момент их окончания.

На основании полученных результатов испытаний принимается заключение по аттестации ИСПДн, которое должно включать:

- оценку соответствия ИСПДн требованиям безопасности информации;

- перечень выявленных недостатков и нарушений;
- рекомендации по устранению выявленных недостатков и нарушений;
- вывод о возможности выдачи «Аттестата соответствия ИСПДн требованиям безопасности информации».

Оценка соответствия ИСПДн требованиям безопасности информации производится путём анализа полученных полностью результатов произведённых испытаний и найденных в процессе этого конкретных недостатков и нарушений.

Если ИСПДн соответствует установленным требованиям по защите информации комиссия выполняет работу по определению предложения заявителя по способу устранить найденные недостатки и нарушения. Можно использовать следующие меры:

- более полная проработка существующей организационно-распорядительной документации;
- исключение отдельных технических средств из состава ИСПДн;
- исключение отдельных программных средств из состава ИСПДн;
- определение и использование новых, более удовлетворяющих данным условиям, организационно-технических мер защиты;
- использование СЗИ, которые будут использоваться с основными и обеспечивать более высокий уровень защиты.

Если в процессе аттестационных испытаний выявлены недостатки, не приводящие к нарушению установленных требований и норм защищенности информации, то комиссия может рекомендовать следующие меры:

- оперативное устранение выявленных недостатков в процессе аттестационных испытаний;
- устранение установленных недостатков и нарушений в согласованные с комиссией сроки с представлением необходимых документов в ПФ ФГУП «ЦентрИнформ»;
- проведение дополнительных частичных испытаний в согласованные сроки.

7 Формирование «Протокола испытаний комплексной системы защиты информации ИСПДн на соответствие требованиям безопасности информации в части защиты от НСД и компьютерных вирусов»

7.1 Состав средств контроля защищенности, использованных при аттестационных испытаниях ИСПДн

При проведении контроля защищенности ИСПДн от НСД в процессе аттестационных испытаний использовались сертифицированные Гостехкомиссией России программные средства контроля эффективности применения СЗИ:

- программа «ФИКС 2.0.2»;
- программа поиска и гарантированного уничтожения информации на дисках «Terrier 3.0», произведенная ЗАО «ЦБИ – Сервис»;
- средство создания модели системы разграничения доступа «Ревизор 1 ХР»;
- программа контроля полномочий доступа к информационным ресурсам «Ревизор 2 ХР»;
- система анализа программного и аппаратного обеспечения ТСР/IP сетей (сетевой сканер) «Ревизор Сети» версии 2.0.

7.2 Проверка технологического процесса обработки информации

7.2.1 Общие положения

Проверка заключалась в определении качества реального технологического процесса обработки информации в ИСПДн и написании заключения о его соответствии или несоответствии предоставленной документации при испытаниях.

В ходе проверки были определены:

- основы данного процесса обработки информации (см. пункт 7.2.2);

- список объектов, к которым предоставляется доступ (см. пункт 7.2.3);
- список субъектов, которые имеют доступ (см. пункт 7.2.4);
- перечень используемых постоянно средств получения доступа к используемой информации (см. пункт 7.2.5);
- перечень СЗИ (см. пункт 7.2.6);
- описание реализованных правил разграничения доступа (см. пункт 7.2.7);
- перечень угроз НСД (см. пункт 7.2.8).

7.2.2 Особенности технологического процесса обработки информации

Согласно описанию технологического процесса, представленному в вышеуказанной документации, ИСПДн предназначена для подготовки ПДн и обмена файлами, содержащими ПДн, в зашифрованном виде с ТФОМС, Минздрав, ГУЗ «МИАЦ» и СК.

ИСПДн предназначена для работы в многопользовательском режиме, доступ пользователей к работе на ПЭВМ организуется по матрице доступа, пользователи имеют равные права доступа к ПДн, обрабатываемым в ИСПДн.

Каждый пользователь имеет право постоянного хранения файлов с защищаемыми ПДн в специально выделенных каталогах. Ключи шифрования хранятся на жестком магнитном диске (ЖМД) ПЭВМ. Порядок хранения информации на ЖМД и сменных магнитных носителях информации (МНИ), а также права доступа к ним определены в вышеперечисленных внутренних документах.

Доступ к работе на ПЭВМ ИСПДн осуществляется по предъявлению персонального идентификатора (имени пользователя) и пароля конкретного пользователя, после чего тот получает установленные

администратором безопасности права доступа к различным объектам, необходимым для полноценной работы и выполнения своих обязанностей персоналом ИСПДн.

Для защиты информации от НСД в ИСПДн используется СЗИ от НСД «Secret Net 7.6» (автономный вариант).

Средствами СЗИ НСД «Secret Net 7.6» (автономный вариант) на ПЭВМ организуются права доступа пользователей к ресурсам ПЭВМ.

Настройка СЗИ от НСД для определённых правилами пользователей и регулирование и настройка её работы осуществляется администратором безопасности.

Для защиты ресурсов ПЭВМ от доступа со стороны локальный вычислительных сетей и открытых каналов связи применяется межсетевой экран в составе «ViPNet Client 4».

На ПЭВМ установлена операционная система Microsoft Windows XP.

Для шифрования документов (сообщений, файлов) перед отправкой их абоненту используется СКЗИ в составе «ViPNet Client 4».

Для антивирусной защиты системы применяется ПС Антивирус Касперского 6.0 в соответствии с «Инструкцией по антивирусной защите».

В помещении обеспечено отсутствие бесконтрольного пребывания посторонних лиц.

7.2.3 Перечень объектов доступа

Объектами доступа являются:

- ПЭВМ в целом;
- устройство ввода-вывода на сменные МНИ;
- ЖМД;
- монитор с отображаемой на нем конфиденциальной информацией;

- персональные сменные МНИ с расположенными на них ключами;

- каталоги всех файлов, хранимых на магнитных носителях;
- оперативная память ПЭВМ;
- операционная система;
- программа, предназначенная для шифрования документов.

7.2.4 Перечень субъектов доступа

Субъектами доступа к защищаемой информации в ИСПДн являются:

- администратор безопасности ИСПДн;
- администратор ИСПДн;
- пользователи системы, выполняющие свои обязанности, связанные с ПДн;

- процессы, выполняемые на ПЭВМ от имени администратора и пользователей при обработке информации и настройке ИСПДн.

7.2.5 Перечень штатных средств доступа к информации

Для пользователей в качестве штатных средств доступа в ИСПДн предусмотрены:

- стандартные средства операционной системы Microsoft Windows XP;

- программы из списка, установленного ПО, разрешенного для запуска пользователями.

- перечень СЗИ

- общесистемное ПО не позволяет обеспечить защиту информации, поэтому на ПЭВМ используются следующие сертифицированные СЗИ:

- СЗИ НСД «Secret Net 7.6» в составе: ПО «Secret Net 7.6» (автономный вариант), плата Secret Net Touch Memory Card;

- МЭ и СКЗИ «ViPNet Client 4».

Лицензионные продукты были приобретены у производителя данного продукта. Средства защиты были установлены в соответствии с руководствами по установке и администрированию и функционируют в среде Microsoft Windows XP в соответствии с руководствами по эксплуатации.

СКЗИ и МЭ «ViPNet Client 4» выполняет следующие функции:

- фильтрация защищенного и открытого трафиков по множеству параметров («белый» и «черный» списки IP-адресов, порты, протоколы, типы сервисов и приложений);
- реализация режима «stealth» (режим инициативных соединений), позволяющий сделать невидимым компьютер защищенной сети из открытой сети;
- обнаружение вторжений (IDS), позволяющая обнаруживать следующие виды атак:
 - основанные на особенностях протокола IP (атака Land, IP-опции нулевой длины, пустой IP-фрагмент, атака JoIt2);
 - основанные на особенностях протокола ICMP (возможная атака Smurf, ICMP-запрос маски подсети, фрагментация ICMP-заголовка);
 - основанные на особенностях протокола UDP (урезанный UDP-заголовок, возможная атака Fraggle, зацикливание портов UDP, атака Snork);
 - основанные на особенностях протокола TCP (фрагментация TCP-заголовка, урезанный TCP-заголовок, неправильное смещение Urgent в TCP-заголовке, атака WinNuke, TCP-опции нулевой длины, сканирование TCP XMAS, сканирование TCP null);
- мониторинг сетевой активности приложений, позволяющий обнаружить и блокировать несанкционированную активность программ-«троянцев»;

- авторизация и обеспечение юридической значимости электронных документов при обмене ими посредством использования процедур формирования и проверки ЭЦП в соответствии со стандартами ГОСТ Р 34.10-94 («Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма») [16]. ГОСТ Р 34.10-2001. («Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи») [17], ГОСТ Р 34.11-94 («Информационная технология. Криптографическая защита информации. Функция хэширования») [18];

- обеспечение конфиденциальности и контроль целостности информации посредством ее шифрования и имитозащиты, в соответствии с ГОСТ 28147-89 («Системы обработки информации. Защита криптографическая») [19];

- реализация стандартного интерфейса Microsoft Crypto API 2.0.

Реальные условия эксплуатации вышеперечисленных СЗИ обеспечивают условия эксплуатации, рекомендованные разработчиками данных СЗИ.

7.2.6 Описание реализованных правил разграничения доступа

С помощью применяемых в ИСПДн СЗИ субъектам доступа присвоены официальные полномочия для допуска к информации в соответствии с принятой матрицей доступа.

В соответствии с представленной на ИСПДн документацией реализованы правила доступа, при которых каждый пользователь имеет право доступа:

- к средствам ОС Microsoft Windows XP, обеспечивающим запуск и функционирование ИСПДн;

- к средствам антивирусной защиты (Антивирус Касперского 6.0);
- к программам из списка программ, разрешенных для выполнения;
- к сменным МНИ, предназначенным для хранения ключевой информации;
- к каталогам на ЖМД;
- к определенным абонентам при отправке им сообщений в зашифрованном виде.

Всем пользователям, кроме администратора безопасности, запрещен доступ к средствам настройки и изменения полномочий доступа СЗИ.

Операции доступа к объектам доступа документируются средствами регистрации и учета СЗИ.

7.2.7 Перечень угроз НСД в ИСПДн и реализованных мер по их устранению

Типовыми угрозами могут являться:

- копирование защищаемых ресурсов на неучтенные МНИ;
- хищение, вывод из строя ПЭВМ в целом, либо носителей информации;
- доступ к ресурсам ПЭВМ за счет обхода СЗИ с использованием загрузки с МНИ, а также путем исключения загрузки модулей и драйверов СЗИ;
- нарушение целостности файлов операционной системы, СЗИ, в том числе компьютерными вирусами;
- разрушение защищаемой информации компьютерными вирусами;

- доступ во время отсутствия пользователя на рабочем месте при выполненном санкционированном входе в ОС, в том числе к загруженной ключевой информации;
- несанкционированное ознакомление с защищаемой информацией, отображаемой на видеомониторе;
- несанкционированное ознакомление с защищаемой информацией при ее выводе на печатающее устройство;
- запуск пользователем вредоносной программы с МНИ или ЖМД;
- отправка сообщений в канал связи в незашифрованном виде;
- отправка сообщений посторонним абонентам;
- доступ к ПЭВМ со стороны открытых каналов связи.

Согласно представленной документации перечисленные угрозы устраняются применением в ИСПДн СЗИ НСД «Secret Net 7.6» (автономный вариант), МЭ и СКЗИ в составе «ViPNet Client 4» и их специальной настройкой, а также реализацией ряда организационных мер.

7.3 Проверка ИСПДн на соответствие организационно-техническим требованиям по защите информации

7.3.1 Проверка внутренней и распорядительной документации по защите информации в ИСПДн

Аттестационной комиссии в ходе подготовки и проведения испытаний ИСПДн были представлены имеющиеся на ИСПДн исходные данные и документы согласно списку пункта 6.3.1.

Проверка представленных документов показала их достаточность для проведения аттестационных испытаний заявленной ИСПДн.

Проверка состава технических средств, места их расположения, а также перечня установленных на ПЭВМ программных средств показала

соответствие представленных исходных данных реальным условиям размещения и эксплуатации ИСПДн.

7.3.2 Проверка информационных потоков

Обобщенная технологическая схема ИСПДн с существующими информационными потоками представлена на рисунке 7.1.

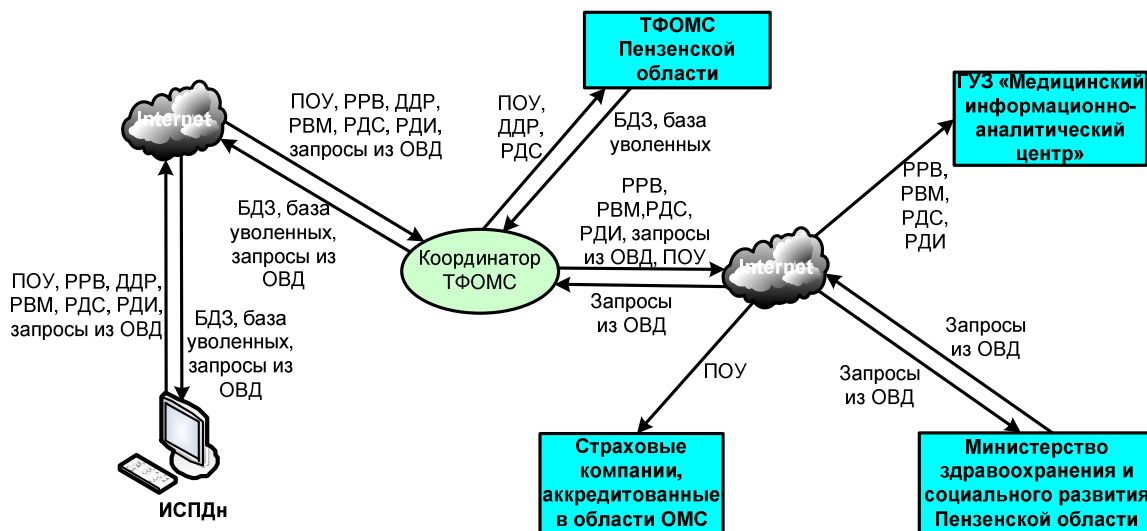


Рисунок 7.1 – Схема информационных потоков между ИСПДн и ТФОМС, ГУЗ «МИАЦ», Минздравом, СК

7.3.3 Проверка уровня подготовки кадров и распределения ответственности за выполнением требований по защите информации

Результат проверки уровня подготовки кадров:

- до персонала доведены соответствующие инструкции по безопасности информации в ИСПДн;
- проведен опрос персонала на выполнение требований инструкций по безопасности информации, опрос показал достаточность знаний для работы в ИСПДн;
- в ИСПДн составлена матрица доступа персонала к ресурсам, необходимым для выполнения возложенных на них обязанностей.

7.4 Проверка ИСПДн на соответствие требованиям по защите информации

7.4.1 Проверка подсистемы управления доступом

В рамках испытаний подсистемы управления доступом проверке был подвержен механизм идентификации и проверки подлинности субъектов доступа при входе в систему.

Идентификация и проверка подлинности субъектов доступа осуществляется средствами СЗИ «Secret Net 7.6» (автономный вариант) при входе в систему по персональному идентификатору (имени пользователя) и паролю условно-постоянного действия, состоящим не менее, чем из шести буквенно-цифровых символов.

Настройки СЗИ выполнены таким образом, что при задании или смене пароля невозможно ввести пароль длиной менее шести символов. Смена паролей осуществляется каждым пользователем самостоятельно, не реже одного раза в квартал.

Надежность аутентификации оценивалась возможностью подбора или несанкционированного получения пароля посторонним субъектом доступа в период действия этого пароля с учетом временной блокировки ПЭВМ после превышения, заданного в СЗИ «Secret Net 7.6» (автономный вариант) предела (пять раз) попыток неправильного ввода пароля или предъявления незарегистрированного электронного идентификатора. Данные события фиксируются в журнале СЗИ НСД «Secret Net 7.6» (автономный вариант), находящемся в энергонезависимой памяти контроллера СЗИ НСД. Доступ к журналу разрешен только администратору безопасности.

Устройства ПЭВМ, программы, каталоги, файлы идентифицируются по именам и логическим адресам при обращении к ним при помощи

средств ОС Microsoft Windows XP и установленной на ПЭВМ СЗИ НСД «Secret Net 7.6».

Для хранения файлов различной степени конфиденциальности используются различные каталоги на ЖМД (для информации, содержащей ПДн – каталоги с метками «ПДн»).

При временном оставлении рабочего места пользователем принудительно (либо по истечении интервала неактивности) включается блокировка монитора и клавиатуры ПЭВМ. Снятие блокировки возможно только путем предъявления электронного идентификатора и ввода пароля пользователя, инициировавшего блокировку, или администратора безопасности.

Средствами МЭ из состава «ViPNet Client 4» разрешены соединения только с абонентами госпиталя. Таким образом, доступ к ПЭВМ со стороны открытых каналов связи разрешен только для абонентов защищенной сети. В случае выявления нарушений политики безопасности или попыток нарушения администратор безопасности в зависимости от произошедшего события принимает решение о дальнейших действиях (внеочередное тестирование работоспособности МЭ, добавление новых правил фильтрации и т.д.).

Конфиденциальность информации при ее передаче по открытым каналам связи обеспечивается шифрованием всех сообщений посредством СКЗИ «ViPNet Client 4».

Пользователи не имеют доступа к настройкам СЗИ НСД. Таким образом, возможность изменения настроек доступна только для администратора безопасности.

Система разграничения доступа, реализованная на объекте средствами СЗИ «Secret Net 7.6», была испытана с помощью программы «Ревизор 1 XP» (средства автоматизации процесса создания избирательной

модели системы разграничения доступа к файловым ресурсам (логическим дискам, каталогам, файлам) и сетевым ресурсам ЛВС в соответствии с установленными в организации требованиями матрицы доступа) и программы «Ревизор 2 ХР» (средства автоматизированной проверки соответствия прав пользователей по доступу к защищаемым информационным ресурсам АРМ, описанных в модели системы разграничения доступа, реальным правам доступа, предоставляемым установленной на АРМ системой защиты информации, либо соответствующей операционной системой).

Анализ результатов работы программ «Ревизор 1 ХР» и «Ревизор 2 ХР», а также имитации несанкционированных действий показал, что реальные права пользователей по доступу к защищаемым ресурсам соответствуют установленной разрешительной системе доступа, а примененные способы и средства контроля защищенности не позволяют получить НСД к защищаемым ресурсам ПЭВМ.

Система фильтрации, реализованная на ПЭВМ средствами МЭ из состава «ViPNet Client 4», была проверена с помощью системы анализа программного и аппаратного обеспечения ТСР/ІР сетей (сетевой сканер) «Ревизор Сети» версии 2.0, разработанной ЗАО «ЦБИ-Сервис», г. Юбилейный Московской области. Для этого к ПЭВМ ИСПДн был подключен тестовый компьютер (ноутбук).

Анализ результатов работы программы «Ревизор Сети» версии 2.0 показал, что ПЭВМ ИСПДн недоступна извне (со стороны открытых каналов связи или ЛВС организации в случае включения ПЭВМ ИСПДн в такую).

Для защиты от программно-математических воздействия (ПМВ) используется Антивирус Касперского 6.0 и СЗИ НСД «Secret Net 7.6» (автономный вариант).

7.4.2 Проверка подсистемы регистрации и учета

В ходе проверки моделировались процессы, которые затрагивают обработку информации, после чего просматривались результаты учета в журнале регистрации событий.

СЗИ НСД «Secret Net 7.6» (автономный вариант) регистрирует вход и выход пользователей в систему, факты печати документов, запуска и завершения программ (процессов) для обработки ПДн, изменения полномочий пользователей, создание защищаемых файлов, сигнализация попыток нарушения средств защиты, запуск Антивируса Касперского 6.0, МЭ и СКЗИ «ViPNet Client 4», запуск и завершение модулей средства защиты от ПМВ.

МЭ «ViPNet Client 4» осуществляет регистрацию IP-трафика. Факты несанкционированных соединений также отмечаются в журнале МЭ. В журнале регистрируются блокированные пакеты, причины их блокировки (блокирование фильтром, неподдерживаемый тип сообщения, недопустимый размер пакета, длина заголовка, неверная контрольная сумма пакета, недопустимые флаги TCP-пакета и др.).

Также система обнаружения атак, входящая в состав МЭ «ViPNet Client 4», регистрирует в журнале обнаруженные сетевые атаки.

Установленные на ПЭВМ СЗИ не осуществляют автоматическую регистрацию, учет и маркировку защищаемых носителей информации. Однако выполнение соответствующих требований РД обеспечивается организационными мерами.

Очистка областей оперативной памяти осуществляется при окончании работы на ПЭВМ, путем перезагрузки ПЭВМ. Очистка памяти на магнитных носителях информации автоматически осуществляется программными средствами, встроенными в СЗИ. Эффективность очистки была проверена с помощью программы поиска и гарантированного

уничтожения информации на дисках «Terrier 3.0», произведенной ЗАО «ЦБИ-Сервис». Проверка показала, что после удаления файла участок на магнитном носителе, где располагался этот файл, заполнен случайной последовательностью.

Вывод: регистрация и учет различных событий осуществляется средствами установленных СЗИ: СЗИ НСД «Secret Net 7.6» (автономный вариант), МЭ и СКЗИ «ViPNet Client 4», Антивирусом Касперского 6.0.

7.4.3 Проверка подсистемы обеспечения целостности

При загрузке системы средствами СЗИ НСД «Secret Net 7.6» осуществляется автоматический контроль целостности CMOS ПЭВМ, главных загрузочных записей (MBR0...MBR2) ЖМД, файлов СЗИ от НСД, а также основных файлов загрузчика операционной системы. При обнаружении нарушений СЗИ НСД сигнализирует об этом администратору и не позволяет пользователю загрузить ОС.

Кроме того, при загрузке СЗИ НСД «Secret Net 7.6» (автономный вариант) и МЭ и СКЗИ «ViPNet Client 4» данные СЗИ проверяют целостность своих файлов.

Средства разработки и отладки программного обеспечения на ПЭВМ отсутствуют.

Кабинет «Помещение приема и передачи электронной почты» здания госпиталя находится на первом этаже двухэтажного здания и оборудовано дверью с замком, на окне установлена решетка. Все сменные носители конфиденциальной информации хранятся в кабинете «Помещение приема и передачи электронной почты».

Администратором безопасности проводится периодическое обслуживание и тестирование функций, установленных на ПЭВМ СЗИ: СЗИ НСД «Secret Net 7.6» (автономный вариант), МЭ и СКЗИ «ViPNet Client 4», Антивируса Касперского 6.0. Порядок и периодичность

проведения администратором технологических операций по обслуживанию и тестированию СЗИ и системы в целом определены в инструкциях для администратора безопасности.

Все МНИ, используемые в ИСПДн, а также контейнеры с информацией (файлы, архивы, сообщения), получаемая из открытых каналов связи подвергаются обязательному контролю на наличие компьютерных вирусов при помощи антивирусной программы Антивирус Касперского 6.0. ЖМД находится под контролем антивирусной программы постоянно. Кроме того, периодически проводится антивирусный контроль ЖМД по расширенному алгоритму. Обновление баз данных антивирусного средства периодически производится администратором безопасности.

В ходе проверки установлено наличие дистрибутивов используемого общего ПО и сертифицированного ПО СЗИ: «Secret Net 7.6» (автономный вариант), МЭ и СКЗИ «ViPNet Client 4», Антивируса Касперского 6.0.

Для контроля целостности ПО СЗИ НСД «Secret Net 7.6» (автономный вариант), МЭ и СКЗИ «ViPNet Client 4», Антивируса Касперского 6.0 были зафиксированы контрольные суммы файлов, входящих в его состав. Расчет контрольных сумм производился на момент проведения аттестационных испытаний. Контрольные суммы вычислялись по алгоритму Уровень 1 (с постоянным кодом, вшитым в программу) с использованием специального ПО «Программа фиксации и контроля исходного состояния программного комплекса (ФИКС 2.0.2)».

7.4.4 Проверка криптографической подсистемы

В ИСПДн используется сертифицированная СКЗИ «ViPNet Client 4», осуществляющая шифрование информации при передаче по каналу связи и расшифрование информации при приеме. Так как пользователи ИСПДн имеют равные права доступа, шифрование информации при хранении на ПЭВМ не требуется.

7.4.5 Проверка подсистемы антивирусной защиты

В ИСПДн для защиты от компьютерных вирусов, ПМВ используется лицензионная антивирусная программа Антивирус Касперского 6.0.

Обновление вирусных баз осуществляется в соответствии с «Инструкцией по антивирусной защите», что позволяет обеспечить необходимую защиту информационных ресурсов, программных и технических средств объекта информатизации от компьютерных вирусов.

Реализация мероприятий по предотвращению проникновения вирусной инфекции, ПМВ и их проявлений в ИСПДн была проверена в соответствии с методикой ПФ ФГУП «ЦентрИнформ».

7.5 Вывод по «Протоколу испытаний комплексной системы защиты информации ИСПДн на соответствие требованиям безопасности информации в части защиты от НСД и компьютерных вирусов»

Учитывая вышеизложенное, комиссия считает, что при выполнении положений организационно-распорядительных документов на ИСПДн, а также при выполнении должностных обязанностей администратором безопасности и пользователями, обрабатываемые в ИСПДн ПДн защищены от НСД, при этом возможность внесения компьютерных вирусов и осуществления ПМВ в ИСПДн сведена к минимуму.

8 Формирование «Заключения по результатам проведения аттестационных испытаний ИСПДн на соответствие требованиям безопасности информации»

8.1 Условия и порядок проведения аттестационных испытаний

Аттестационные испытания ИСПДн проводились в соответствии с «Программой и методиками проведения аттестационных испытаний на соответствие требованиям безопасности информации».

Аттестационные испытания ИСПДн проведены в сентябре 2016 года. Состав средств контроля, использованных при аттестационных испытаниях ИСПДн в части защиты от НСД.

При проведении контроля защищенности ИСПДн от НСД в процессе аттестационных испытаний использовались сертифицированные Гостехкомиссией России программные средства контроля эффективности применения СЗИ:

- программа фиксации и контроля исходного состояния программного комплекса «ФИКС 2.0.2»;
- программа поиска и гарантированного уничтожения информации на дисках «Terrier 3.0»;
- средство создания модели системы разграничения доступа «Ревизор 1 ХР»;
- программа контроля полномочий доступа к информационным ресурсам «Ревизор 2 ХР»;
- система анализа программного и аппаратного обеспечения ТСР/IP сетей (сетевой сканер) «Ревизор Сети».

8.2 Результаты проверки состояния технологического процесса обработки информации на ИСПДн

Технологический процесс обработки ПДн в ИСПДн, описан внутренними организационно-распорядительными документами,

соответствует реальной практике и требованиям нормативно-методических документов.

8.3 Результаты проверки ИСПДн на соответствие организационно-техническим требованиям по защите информации

Содержание представленных документов и их оформление соответствует установленным требованиям.

Ответственность за организацию работ на ИСПДн, ее эксплуатацию, а также за выполнение требований по защите информации определена внутренней организационно-распорядительной документацией Госпиталя.

Сотрудники Госпиталя, допущенные к обработке ПДн, достаточно подготовлены в вопросах защиты ПДн, и требованиях, предъявляемых к эксплуатации ИСПДн.

Таким образом, аттестуемая ИСПДн соответствует организационно-техническим требованиям, предъявляемым к ИСПДн, обрабатывающей ПДн.

8.4 Результаты испытаний ИСПДн на соответствие требованиям по защите информации от НСД

При испытании СЗИ от НСД:

- проверялось ее соответствие требованиям нормативно-методических документов по защите ПДн в части НСД;
- проводился контроль работоспособности систем управления доступом, регистрации и учета, обеспечения целостности. Проводился анализ, и оценка технологического процесса обработки ПДн в части НСД.
- ИСПДн располагается в кабинете «Помещение приема и передачи электронной почты» на первом этаже двухэтажного здания госпиталя, дверь обита железом и оборудована замком. Помещение имеет одно окно, которое выходит на внутреннюю территорию госпиталя.

Режим обработки ПДн – многопользовательский с равными правами доступа к ПДн, обрабатываемым и хранимым на ИСПДн и носителях информации.

В ИСПДн обрабатываются ПДн категории 1, что определяется данными о состоянии здоровья субъектов ПДн.

Объем ПДн характеризуется коэффициентом $X_{НПД}$ равно 1 (данные субъектов всей Пензенской области, что составляет более 100000 субъектов ПДн).

Хранение ПДн в ИСПДн - на ЖМД и сменных МНИ осуществляется в соответствии с внутренней организационно-распорядительной документацией.

При соблюдении требований организационной документации и установленного технологического процесса обработки информации в ИСПДн защита конфиденциальности и целостности ПДн обеспечивается.

Таким образом, аттестуемая ИСПДн соответствует требованиям нормативно-методических документов по защите ПДн от НСД.

8.5 Выводы по результатам проведения аттестационных испытания ИСПДн

Выводы:

- требования нормативных и методических документов по защите ПДн, выполняются;
- защита в ИСПДн конфиденциальности и целостности ПДн обеспечивается;
- комиссия считает возможным выдать «Аттестат соответствия ИСПДн требованиям безопасности информации» с разрешением обработки ПДн в ИСПДн, сроком на три года.

9 Выдача «Аттестата соответствия ИСПДн требованиям безопасности информации»

Организационная структура, уровень подготовки специалистов, нормативно-методическое обеспечение позволяют осуществлять контроль принятых мер и средств защиты и поддержание уровня защищенности ИСПДн в процессе эксплуатации в соответствии с установленными требованиями.

Аттестация ИСПДн выполнена в соответствии с «Программой и методиками проведения аттестационных испытаний на соответствие требованиям безопасности информации».

С учетом результатов аттестационных испытаний на технических средствах из состава ИСПДн разрешается обработка ПДн.

При эксплуатации ИСПДн запрещается:

- вносить изменения в состав и размещение технических средств и СЗИ без согласования с ПФ ФГУП «ЦентрИнформ»;
- вносить изменения в состав программных средств без согласования с ПФ ФГУП «ЦентрИнформ»;
- обрабатывать ПДн без выполнения требований по защите информации;
- изменять установленный порядок доступа к циркулирующей в ИСПДн защищаемой информации;
- производить копирование защищаемой информации на неучтенные носители информации, в том числе для временного хранения информации;
- осуществлять другие технические и организационные мероприятия, которые могут создать предпосылки для утечки защищаемой информации за счет НСД к информации.

Контроль реализованных мер и средств защиты на ИСПДн возлагается на Администратора безопасности ИСПДн.

Результаты аттестационных испытаний приведены в «Заключении по результатам проведения аттестационных испытаний ИСПДн на соответствие требованиям безопасности информации» и «Протоколе испытаний комплексной системы защиты ИСПДн на соответствие требованиям безопасности информации в части защиты от НСД и компьютерных вирусов».

«Аттестат соответствия ИСПДн требованиям безопасности информации» выдан на 3 года, в течение которых должны быть обеспечены неизменность условий функционирования ИСПДн и технологии обработки защищаемой информации, а также ежегодный контроль соблюдения требований по эксплуатации аттестованной ИСПДн и реализованных мер защиты информации.

ЗАКЛЮЧЕНИЕ

В процессе выполнения дипломного проекта были получены результаты, представленные ниже.

В ходе работы над дипломным проектом производилась разработка системы защиты информации для ИСПДн госпиталя в целях обеспечения безопасности ПДн, проводилась аттестация ИСПДн с целью подтверждения выполнения требований безопасности информации.

Создание системы защиты информации ИСПДн госпиталя осуществлялось в три стадии.

На предпроектной стадии было выполнено обследование объекта информатизации. На этой стадии определялись исходные данные на ИСПДн, такие как: структура ИСПДн, состав ПДн, конфигурация ИСПДн, структура обработки ПДн, режим обработки ПДн, угрозы безопасности ПДн, существующие и необходимые защитные меры.

На стадии проектирования и реализации СЗПДн была разработана «Частная модель угроз безопасности...», в ней определен перечень угроз безопасности, уровень исходной защищенности ИСПДн, вероятности реализации угроз безопасности, возможности реализации угроз безопасности, оценки опасности угроз и составлен перечень актуальных угроз безопасности. На данной стадии разработан комплект организационно-распорядительной документации, включающей: «Перечень ПДн, подлежащих защите в ИСПДн», «План мероприятий по обеспечению защиты ПДн в ИСПДн», «Положение о разграничении прав доступа к ПДн в ИСПДн».

На стадии ввода в действия СЗПДн были установлены и настроены необходимые СЗИ, сформирована системы защиты информации ИСПДн госпиталя. Разработана «Программа и методики проведения аттестационных испытаний на соответствие требованиям безопасности

информации», которая описывает условия и порядок проведения аттестационных испытаний. По разработанной программе и методикам были проведены аттестационные испытания, результаты которых зафиксированы в «Протоколе испытаний комплексной системы защиты информации ИСПДн на соответствие требованиям безопасности информации в части защиты от НСД и компьютерных вирусов». Выводы были представлены в «Заключении по результатам проведения аттестационных испытаний ИСПДн на соответствие требованиям безопасности информации». Комиссией принято решение о выдаче «Аттестата соответствия требованиям безопасности информации».

Таким образом, все пункты технического задания на выпускную квалификационную работу выполнены полностью.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных».
- 2 Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- 3 Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».
- 4 Совместный приказ ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 года N 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».
- 5 Приказ ФСТЭК N 58 от 05.02.2010 г. «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».
- 6 Методические материалы ФСТЭК «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года.
- 7 Методические материалы ФСТЭК «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года.
- 8 Методические материалы ФСБ «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных

данных с использованием средств автоматизации» от 21 февраля 2008 года.

9 Методические материалы ФСБ «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» от 21 февраля 2008 года.

10 Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости.

11 Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости.

12 Рекомендации ИТ-директорам России по защите ПДн [Электронный ресурс] - Режим доступа: <http://www.iemag.ru/analitics/detail.php?IDравно18921#2>.

13 Приказ ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

14 Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

15 Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

16 ГОСТ Р 34.10 94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма».

17 ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

18 ГОСТ Р 34.11 94 «Информационная технология. Криптографическая защита информации. Функция хэширования».

19 ГОСТ 28147 89 «Системы обработки информации. Защита криптографическая».

ПРИЛОЖЕНИЕ А

(обязательное)

Определение вероятности реализации УБПДн и оценки опасности
УБПДн на основе опроса экспертов

Определение вероятности реализации УБПДн и оценки опасности УБПДн на основе опроса экспертов (специалистов в области защиты информации)

Оператор обработки ИСПДн: Федеральное казенное учреждение «Войсковая часть 45108».

Название ИСПДн: «АРМ ДЛЮ Федеральное казенное учреждение «Войсковая часть 45108»».

Таблица А.1 - Характеристики ИСПДн

Категория ПДн	К1
Структура ИСПДн	автоматизированное рабочее место
Подключение к сети Интернет	да
Выход в Интернет (при наличии подключения к сети Интернет)	одноточечный
Использование защищенных каналов связи (при наличии подключения к сети Интернет)	да
Режим обработки ПДн	многопользовательский
Разграничение прав доступа (при многопользовательском режиме обработки ПДн)	равные права
Антивирус	да
Межсетевой экран	да
Используется только лицензионное или свободно распространяемое ПО	да
Использование сменных носителей информации	да
Хранение носителей информации с защищаемыми ПДн в сейфе	нет
Учет носителей информации с защищаемыми ПДн	нет
Печать документов на бумажный носитель	да

Таблица А.2 - Характеристики помещения, где располагается ИСПДн

Металлическая дверь	да
Система охранной сигнализации	да
Система пожарной сигнализации	нет
Система видеонаблюдения	нет
Окна помещения выходят на внутреннюю территорию	да
Этаж расположения	первый
Количество этажей здания	два
Решетка на окнах	да
Жалюзи на окнах	да
Ограничение допуска в помещение, где располагается ИСПДн	да
Наличие контролируемой зоны	да

Таблица А.3 - Перечень имеющихся документов

Перечень ПД, подлежащих защите в ИСПДн	нет
Акт классификации ИСПДн	нет
План мероприятий по обеспечению защиты ПДн	нет
Положение о разграничении прав доступа к обрабатываемым ПДн	нет
Инструкция администратора ИСПДн	нет
Инструкция администратора безопасности	нет
Инструкция пользователя ИСПДн	нет
Инструкция пользователя по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций	нет
Инструкция по антивирусной защите	нет

Используемые средства защиты информации:

- МЭ/СКЗИ ViPNet Client 4;
- Антивирус Kaspersky Internet Security 6.0.

Подробное описание ИСПДн представлено в «Протоколе оценки обстановки в части безопасности персональных данных, обрабатываемых в информационной системе персональных данных».

ПРИЛОЖЕНИЕ Б

(обязательное)

Перечень ПДн, подлежащих защите в ИСПДн

УТВЕРЖДАЮ

Главный врач Федеральное
казенное учреждение

«Войсковая часть 45108»»

_____ Т.А. Чернова

«__» _____ 2016 г.

Перечень ПДн, подлежащих защите в ИСПДн «Обмен Федеральное
казенное учреждение «Войсковая часть 45108»» с ТФОМС по Пензенской
области»

1 Перечень ПДн субъектов ПДн

В ИСПДн обрабатываются следующие ПДн:

- база данных застрахованных лиц Пензенской области в системе обязательного медицинского страхования, в которой содержатся следующие ПДн каждого из застрахованных лиц Пензенской области в системе ОМС;
- база уволенных, в которой содержатся следующие ПДн каждого из уволенных застрахованных лиц Пензенской области в системе ОМС;
- перечень услуг, оказанных госпиталями гражданам в системе ОМС за отчетный период, в котором содержатся следующие ПДн по услугам, оказанным гражданам;
- реестр медицинского персонала, работающего в госпитале, в котором содержатся следующие ПДн;

- регистр дополнительной диспансеризации работающих граждан, в котором содержатся следующие ПДн;
- регистр высокотехнологичной медицинской помощи по профилю «Сердечно-сосудистая хирургия», в котором содержатся следующие ПДн;
- реестр детей сирот и детей, находящихся в тяжелой жизненной ситуации, в котором содержатся следующие ПДн;
- федеральный регистр детей-инвалидов, в котором содержатся следующие ПДн;
- реестр диспансеризации детей декретированных возрастов, в котором содержатся следующие ПДн;
- запросы из отдела внутренних дел, в которых содержатся следующие ПДн.

2 Программно-технические средства обработки

Программно-технические средства обработки информации включают в себя:

- общесистемное и специальное программное обеспечение (ПО) (см. таблицу Б.1);
- резервные копии общесистемного ПО;
- аппаратные средства обработки информации (см. таблицу Б.2);
- сетевое оборудование (см. таблицу Б.3).

Таблица Б.1 - Общесистемное и специальное ПО

№ п/п	Наименование программного средства
1	ОС MS Windows XP Pro, лиц. № 76456-OEM-0013262-16151
2	Microsoft Office 2007 лиц. № 89451-417-6467113-66023
3	Антивирус Kaspersky Internet Security 6.0
4	3DMark06
5	7-Zip 4.65
6	Foxit Reader 3.0.1817
7	K-Lite Mega Codec Pack 5.1.0
8	NVIDIA PhysX
9	PCMark05

Продолжение таблицы Б.2

№ п/п	Наименование программного средства
10	СКЗИ «ViPNet Client 4»
11	Winamp
12	XnView 1.96.2
13	Архиватор WinRAR
14	Базовый пакет поставщика службы криптографии смарт-карт

Таблица Б.2 - Аппаратные средства обработки информации

№ п/п	Наименование	Тип (модель)	Серийный (заводской) номер
1	Системный блок ПЭВМ	ATX	Без номера
2	Монитор	Samsung SyncMaster 943	MY19H9FS916315R
3	Клавиатура	Genius K627	XE9803017411
4	Манипулятор типа «мышь»	Oklick 143M	7082521104
5	МФУ	HP LaserJet M1120MFP	Инв. №010.4.0932
6	Фильтр-удлинитель	Power Cube	Без номера

Таблица Б.3 - Сетевое оборудование

№ п/п	Наименование	Тип (модель)	Серийный (заводской) номер
1	ADSL-модем	Интеркросс ICxDSL 5633E	BB50-0325530

4 Средства защиты ПДн

Средства защиты ПДн включают в себя:

- средства управления и разграничения доступом пользователей:

MS Windows XP Pro;

- средства обеспечения регистрации и учета действий с информацией: MS Windows XP Pro;

- средства антивирусной защиты: Kaspersky Internet Security 6.0;

- средства межсетевого экранирования: ViPNet Client 4;

- средства криптографической защиты ПДн, при их передаче по каналам связи сетей общего и (или) международного обмена: ViPNet Client 4.

5 Каналы информационного обмена и телекоммуникации

В качестве канала информационного обмена, по которому передаются обрабатываемая и технологическая информация, используется

общедоступная сеть Интернет, подключение к которой осуществляется через ADSL-модем.

6 Объекты и помещения, в которых размещены компоненты ИСПДн

ИСПДн располагается в комнате «Помещение приема и передачи электронной почты» на первом этаже двухэтажного здания госпиталя, дверь обита железом и оборудована замком. Помещение имеет одно окно, которое выходит на внутреннюю территорию госпиталя.

ПРИЛОЖЕНИЕ В

(обязательное)

План мероприятия по обеспечению защиты ПДн в ИСПДн

УТВЕРЖДАЮ

Главный врач Федеральное
казенное учреждение

«Войсковая часть 45108»»

_____Т.А. Чернова

«__» _____ 2016 г.

План мероприятий по обеспечению защиты персональных данных в
информационных системах персональных данных Федеральное казенное
учреждение «Войсковая часть 45108»»

Таблица Г.1 – План мероприятий по обеспечению защиты ПДн в ИСПДн

Мероприятие	Периодичность	Исполнитель/ Ответственный
Мероприятия для всех ИСПДн		
Организационные мероприятия		
Организация информирования и обучения сотрудников о введенном режиме защиты ПДн	Разовое срок до 01.11.2016 г	Главный врач Т.А. Чернова
Определение перечня ПД ИСПДн	Разовое срок до 01.11.2016 г.	программист Улбутов Н.А.
Введение режима защиты ПДн	Разовое срок до 06.09.2016 г	Главный врач Т.А. Чернова
ИСПДн «Обмен Федеральное казенное учреждение «Войсковая часть 45108»» с ТФОМС по Пензенской области»		
Организационные мероприятия		
Первичная внутренняя проверка	Разовое срок до 06.09.2016 г.	программист Улбутов Н.А.
Определение перечня ПД ИСПДн	Разовое срок до 06.09.2016 г.	программист Улбутов Н.А.
Определение обрабатываемых ПДн и объектов защиты	Разовое срок до 06.09.2016 г.	программист Улбутов Н.А.
Определение круга лиц участвующих в обработке ПДн	Разовое срок до 06.09.2016 г.	программист Улбутов Н.А.
Определение ответственности лиц участвующих в обработке	Разовое срок до 06.09.2016 г.	программист Улбутов Н.А.
Определение прав разграничения доступа пользователей ИСПДн, необходимых для выполнения должностных обязанностей	Разовое срок до 06.09.2016 г.	программист Улбутов Н.А.
Назначение ответственного за безопасность ПДн	Разовое срок до 06.09.2016 г	Главный врач Т.А. Чернова
Собрание комиссии по классификации ИСПДн	Разовое срок до 06.09.2016 г	Главный врач Т.А. Чернова

Продолжение таблицы Г.1

Мероприятие	Периодичность	Исполнитель/ Ответственный
Классификация ИСПДн	Разовое срок до 06.09.2016 г	Главный врач Т.А. Чернова
Первичный анализ актуальности угроз безопасности ПДн	Разовое срок до 06.09.2016 г	программист Улбутов Н.А.
Установление контролируемой зоны вокруг ИСПДн	Разовое срок до 06.09.2016 г	программист Улбутов Н.А.
Выбор помещений для установки аппаратных средств ИСПДн в помещение, с целью исключения НСД лиц, не допущенных к обработке ПДн	Разовое срок до 06.09.2016 г	Главный врач Т.А. Чернова
Организация режима и контроля доступа (охраны) в помещение, в котором установлены аппаратные средства ИСПДн	Разовое срок до 06.09.2016 г	Главный врач Т.А. Чернова
Организация порядка восстановления работоспособности технических средств, ПО, баз данных с подсистем СЗПДн	Разовое срок до 06.09.2016 г	Главный врач Т.А. Чернова
Разработка должностных инструкций о порядке обработки ПДн и обеспечении введенного режима защиты	Разовое срок до 06.09.2016 г	программист Улбутов Н.А.
Разработка инструкций о действии в случае возникновения внештатных ситуаций	Разовое срок до 06.09.2016 г	программист Улбутов Н.А.
Организация перечня по учету технических средств и средств защиты, а так же документации к ним	Разовое срок до 06.09.2016 г	программист Улбутов Н.А.
Физические мероприятия		
Организация постов охраны для пропуска в контролируемую зону	Разовое срок до 06.09.2016 г	Главный врач Т.А. Чернова
Установка жалюзи на окнах	Разовое срок до 01.11.2016 г	Главный врач Т.А. Чернова
Установка системы пожаротушения в помещениях, где расположены элементы ИСПДн	Разовое срок до 01.11.2016 г	Главный врач Т.А. Чернова
Технические (аппаратные и программные) мероприятия		
Внедрение специальной подсистемы управления доступом, регистрации и учета (Secret Net)	Разовое срок до 08.09.2016 г	Главный врач Т.А. Чернова
Внедрение антивирусной защиты (Kaspersky Internet Security 6.0)	Разовое срок до 06.09.2016 г	Главный врач Т.А. Чернова
Внедрение межсетевого экранирования (ViPNet Client 4)	Разовое срок до 06.09.2016 г	Главный врач Т.А. Чернова
Контролирующие мероприятия		
Контроль над соблюдением режима обработки ПДн	Еженедельно	программист Улбутов Н.А.
Контроль над соблюдением режима защиты	Ежедневно	программист Улбутов Н.А.

Продолжение таблицы Г.1

Мероприятие	Периодичность	Исполнитель/ Ответственный
Контроль над выполнением антивирусной защиты	Еженедельно	программист Улбутов Н.А.
Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	программист Улбутов Н.А.
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Ежегодно	программист Улбутов Н.А.
Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	Еженедельно	программист Улбутов Н.А.
Контроль за обеспечением резервного копирования	Ежемесячно	программист Улбутов Н.А.
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз	Ежегодно	программист Улбутов Н.А.
Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно	программист Улбутов Н.А.

ПРИЛОЖЕНИЕ Г

(обязательное)

Положение о разграничении прав доступа к обрабатываемым ПДн

УТВЕРЖДАЮ

Главный врач Федеральное
казенное учреждение

«Войсковая часть 45108»»

_____ Т.А. Чернова

«__» _____ 2016 г.

Положение о разграничении прав доступа к обрабатываемым
персональным данным в ИСПДн Федеральное казенное учреждение
«Войсковая часть 45108»»

Таблица Д.1 - Перечень групп, участвующих в обработке ПДн в ИСПДн

Группа	Уровень доступа к ПДн	Разрешенные действия
Администратор ИСПДн, Администратор безопасности	Обладает полной информацией о системном и прикладном ПО ИСПДн. Обладает полной информацией о ТС и конфигурации ИСПДн. Имеет доступ ко всем ТС обработки информации и данным ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн.	- получение из канала связи - сбор - систематизация - накопление - хранение - уточнение - использование - печать - передача по каналу связи - уничтожение
Операторы ИСПДн	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.	- получение из канала связи - сбор - систематизация - накопление - хранение - уточнение - использование - печать - передача по каналу связи - уничтожение

Таблица Д.2 - Перечень лиц, получивших доступ к ПДн

№	Роль	ФИО сотрудника	Подразделение
1	Администратор ИСПДн	Улбутов Н.А.	программист Федеральное казенное учреждение «Войсковая часть 45108»»
2	Администратор безопасности	Улбутов Н.А.	программист Федеральное казенное учреждение «Войсковая часть 45108»»
3	Оператор	Лычко Н.В.	экономист Федеральное казенное учреждение «Войсковая часть 45108»»
4	Оператор	Никина Н.Н.	бухгалтер Федеральное казенное учреждение «Войсковая часть 45108»»
5	Оператор	Податнова Л.	бухгалтер Федеральное казенное учреждение «Войсковая часть 45108»»

ПРИЛОЖЕНИЕ Д

(обязательное)

Протокол проверки ВКР на оригинальность

Протокол

проверки на оригинальность в системе «Антиплагиат.ВУЗ» выпускной квалификационной работы на тему «Проведение работ по переаттестации части информационной системы персональных данных «АРМ ДЛО Федеральное казенное учреждение «Войсковая часть 45108»» студента шестого курса И.Ф. Трегулова специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

Руководитель ВКР Сидоров Алексей Игоревич.

Информация о документе:

Имя исходного файла: Otchet_po_VKR_Tregulov.docx
Имя компании: Пензенский гос. Университет
Тип документа: Прочее
Имя документа: Группа 11ПТ1 ВКР Трегулов ИФ
Дата проверки: 17.01.2017 16:09
Модули поиска: Интернет (Антиплагиат), Кольцо вузов, Университетская библиотека онлайн, Модуль поиска ЭБС БиблиоРоссика, Модуль поиска ЭБС "Лань", Диссертации и авторефераты РГБ, Научные статьи Elibrary, Цитирования, Пензенский гос. Университет

Текстовые статистики:

Индекс читаемости: очень сложный
Неизвестные слова: в пределах нормы
Макс. длина слова: в пределах нормы
Большие слова: в пределах нормы
Оригинальные блоки: 69,2%
Заимствованные блоки: 29,33%
Заимствование из "белых" источников: 1,47%
Итоговая оценка оригинальности: **70,67%**

18.01.2017 г

_____ А.И. Сидоров