АННОТАЦИЯ

Выпускная квалификационная работа содержит 85 стр., 16 таблиц, 3 рисунка, 27 источников и 5 приложений.

Объектами разработки и исследования является ИСПДн «Медицинская информационная система».

Целью работы является построение системы защиты персональных данных в ИСПДн «Медицинская информационная система».

Для достижения поставленной целью были проанализированы нормативно-правовые акты в области защиты персональных данных, обследована ИСПДн «Медицинская информационная система».

Результатами работы является проект системы защиты персональных данных в ИСПДн «Медицинская информационная система».

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....5
1 НОРМАТИВНО-ПРАВОВАЯ ОСНОВА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ.....6
1.1 Федеральный закон № 152от 27.07.2006.....6
1.2 Постановление Правительства РФ № 1119 от 01.11.2012.....7
1.3 Приказ ФСБ России № 378 от 10 июля 2014 г.....8
1.4 Приказ ФСТЭК России № 17 от 11.02.2013.....9
2 ОПИСАНИЕ И АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ.....11
ВЫДЕЛЕНИЕ ПРОБЛЕМЫ.....11
2.1 Общие сведения об объекте исследования.....11
2.1.1 Направление деятельности.....11
2.1.2Организационная структура.....12
2.1.3 Техническое оснащение.....14
2.1.4 Программное обеспечение.....17
2.2 Проблемы информационной безопасности учреждения.....18
2.3 Обзор сертифицированных средств защиты информации.....20
2.3.1 Исследование рынка предлагаемых программных и программно-аппаратных средств защиты информации по классам СЗИ.....20
3 ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИСПДн «МЕДИЦИНСКАЯ ИНФОРМАЦИОННАЯ СИСТЕМА».....37
3.1 Обследование информационной системы.....37
3.2 Построение модели угроз.....37
3.2.1Определение типа актуальных угроз.....37
3.2.2 Определение класса защищенности информационной системы.....38
персональных данных.....38
3.2.3 Определение перечня ИСПДн и перечня сведений, содержащих персональные данные.....38
3.2.4 Определение нарушителя безопасности.....39
3.2.5 Определение уровня исходной защищенности.....40
3.2.6 Определение вероятности реализации угроз персональным данным.41
3.2.7 Определение реализуемости угроз персональным данным.....41
3.2.8 Определение опасности угроз персональным данным.....41
3.2.9 Определение актуальности угроз персональным данным.....42

3.2.10 Оценка уязвимости ИСПДн «Медицинская информационная система»....42
3.2.11 Частная модель угроз ИСПДн «Медицинская информационная система»....43
3.3 Технологический процесс ИСПДн «Медицинская информационная система»....43
3.3.1 Общие положения....43
3.3.2 Обработка информации....44
3.3.3 Ввод информации....44
3.3.4 Хранение и обработка персональных данных....45
3.3.5 Вывод информации....45
3.3.6 Обновление программного обеспечения....45
3.3.7 Устранение сбоев....46
3.3.9 Антивирусная защита....46
3.3.10 Резервное копирование и восстановление....47
3.4 Техническое задание на построение системы защиты персональных данных в ИСПДн «Медицинская информационная система»....47
3.4.1 Состав системы зашиты персональных данных....47
3.4.2 Требования к средствам межсетевого экранирования....48
3.4.3 Требования к средствам защиты от несанкционированного доступа.48
3.4.4 Требования к средствам антивирусной защиты....49
3.4.5 Требования к средствам обнаружения вторжений....49
3.4.5 Требования к средствам резервного копирования....49
3.5 Технический проект на построение системы защиты персональных данных....50
3.5.1. Определение средств защиты информации....50
3.6 Разработка организационно – распорядительных документов по защите персональных данных....54
3.7 Аттестация информационной системы защиты персональных данных….55
4 РАСЧЕТ ТЕХНИКО-ЭКОНОМИЧЕСКИХ ПОКАЗАТЕЛЕЙ....58
4.1 Затраты на построение системы зашиты....58
4.2 Затраты на эксплуатацию и техническое обслуживание....59
4.3 Оценка потенциальных финансовых потерь в случае приостановки деятельности по оказанию платных услуг....59
4.4 Оценка экономической эффективности....60
ЗАКЛЮЧЕНИЕ....62

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ.....63
СПИСОК УСЛОВНЫХ СОКРАЩЕНИЙ.....66
Сравнительная таблица КСЗИ.....67
Отчет о результатах проведенной внутренней проверки ИСПДн «МИС».....68
Перечень ПДнв ИСПДн «МИС».....73
Модель УБПДн в ИСПДн «МИС».....77

ВВЕДЕНИЕ

Тема: Построение системы защиты персональных данных в ИСПДн «Медицинская информационная система» (на примере ГБУЗ «Областной Центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями»)

Объект исследования –ИСПДн «Медицинская информационная система»

Предмет исследования – построение системы защиты персональных данных в ИСПДн «Медицинская информационная система»

Цель исследования – провести обследование объекта и построить систему защиты персональных данных в ИСПДн «Медицинская информационная система»

Задачи исследования. Достижение цели подразумевает решение следующих поставленных задач:

1. Провести анализ существующих решений в области защиты ПДн.
2. Обследовать существующую информационную систему учреждения, проанализировать исходные данные, составить отчет об обследовании.
3. Классифицировать информационную систему персональных данных и определить актуальные угрозы.
4. Разработать необходимую организационно - распорядительную и техническую документацию в соответствии с действующим законодательством.

5. Построить системы защиты персональных данных.
6. Подготовить систему к аттестации.
7. Рассчитать экономическую эффективность проекта.

1 НОРМАТИВНО-ПРАВОВАЯ ОСНОВА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.1 Федеральный закон № 152от 27.07.2006

Федеральный закон № 152 от 27.07.2006 «О персональных данных» является основополагающим нормативным актом, регламентирующим деятельность операторов персональных данных по обработке персональных данных. Закон непосредственно определяет термин персональные данные, как любую информацию, относящуюся к определенному физическому лицу (субъекту).

Цель закона - защита прав и свобод гражданина при обработке его персональных данных.

При обработке ПДн должны соблюдаться следующие принципы: обработка осуществляется только с согласия субъекта ПДн (за исключением некоторых случаев), все действия по обработке ПДн должны быть ограничены конкретными целями, по достижению которых информация должна быть либо уничтожена, либо обезличена.

Оператор обязан принимать организационные и технические меры по обеспечению безопасности ПДн субъектов при их обработке, согласно требованиям регуляторов.

Закон устанавливает 4 типа ПДн: общедоступные, специальные, биометрические, иные.

Органы, осуществляющие проверки операторов по соблюдению законодательства в сфере защиты ПДн: РОСКОМНАДЗОР, ФСБ, ФСТЭК,
Ответственность за несоблюдение закона предусматривает гражданско-правовое, административное и уголовное наказание в зависимости от размера нанесенного ущерба.

1.2 Постановление Правительства РФ № 1119 от 01.11.2012

Постановление Правительства РФ № 1119 от 01.11.2012 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" определяет классификацию ИСПДн по категории ПДн, в ней обрабатываемой:

- ИСПДн, обрабатывающая специальные категории ПДн (данные о здоровье, расовой, национальной принадлежности, политических и религиозных взглядов);
- ИСПДн, обрабатывающая биометрические данные (биологические и физиологические данные человека, однозначно идентифицирующие его);
- ИСПДн, обрабатывающие общедоступные данные (данные полученные из общедоступных источников);
- ИСПДН, обрабатывающие иные категории (данные не подпадающие первые три категории).

Определена классификация актуальных угроз, включающая три типа:

- угрозы 1 типа (актуальны недокументированные возможности в системном программном обеспечении ИСПДн);
- угрозы 2 типа (актуальны недокументированные возможности в прикладном программном обеспечении ИСПДн);
- угрозы 3 типа (при неактуальности угроз НДВ в прикладном и системном программном обеспечении ИСПДН).

Установлены 4 уровня защищенности в зависимости от категории ПДн количества субъектов ПДн, формы отношений между оператором и субъектами ПДн:

- 1 уровень защищенности;
- 2 уровень защищенности;
- 3 уровень защищенности;
- 4 уровень защищенности.

Для каждого из 4 уровней защищенности определен минимальный набор мер, по обеспечению безопасности ПДн при их обработке оператором

1.3 Приказ ФСБ России № 378 от 10 июля 2014 г.

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

- оснащение помещений, где эксплуатируются и хранятся СКЗИ металлическими решетками на окнах, железными дверьми, сигнализацией;

- назначение ответвленных лиц за эксплуатацию СКЗИ;
- оформление необходимой документации по учету СКЗИ;
- утверждение перечня лиц, допущенных к эксплуатации СКЗИ;
- определение контролируемой зоны помещений.

СКЗИ разделены по возможности реализации атак (модели нарушителя) на 6 классов:

- Класс КС 1 (нарушитель имеет возможность проведения атак на этапе эксплуатации и разработки СКЗИ);

- Класс КС 2(нарушитель имеет возможность проведения атак на этапе эксплуатации и разработки СКЗИ, находясь в пределах контролируемой зоны);

- Класс КС 3(нарушитель имеет доступ к СВТ, на которых реализованы СКЗИ и среда функционирования, находясь в пределах контролируемой зоны, возможность физического доступа к СВТ, на которых реализованы СКЗИ, возможность располагать аппаратными компонентами СКЗИ и средой функционирования);

- Класс КВ 1 (нарушитель имеет доступ к СВТ, на которых реализованы СКЗИ и среда функционирования, находясь в пределах контролируемой зоны, возможность физического доступа к СВТ, на которых реализованы СКЗИ, возможность располагать аппаратными компонентами СКЗИ и средой функционирования, проведение лабораторных исследований СКЗИ);

-Класс КВ 2 (нарушитель может располагать исходными текстами входящего в среду функционирования прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ);

- Класс КА 1 (злоумышленники имеют возможность располагать всеми аппаратными компонентами СКЗИ и средой функционирования).

1.4 Приказ ФСТЭК России № 17 от 11.02.2013

Приказ ФСТЭК России от 11.02.2013 № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся

в государственных информационных системах" - один из основный нормативных документов, регламентирующий требования при проектировании защиты персональных данных в государственных информационных защитах от формирования требований к защите до проведения процедуры аттестации.

- проводится анализ входящей информации, определяются актуальные угрозы, устанавливается класс защиты, строится модель угроз, определяются требования к средствам защиты информации в ИСПДН;

- проводится проектирование системы защиты ИСПДн, составляется необходимая документация;

- осуществляется внедрение системы защиты ИСПДн, тестирование и опытная эксплуатация, разработка организационно - распорядительных документов;

- проводится аттестационные мероприятия либо оператором, после получения лицензии на осуществление деятельности по ТЗКИ, либо организацией-лицензиатом;

- обеспечение защиты в ходе эксплуатации.

2 ОПИСАНИЕ И АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ. ВЫДЕЛЕНИЕ ПРОБЛЕМЫ

2.1 Общие сведения об объекте исследования

2.1.1 Направление деятельности

Государственное бюджетное учреждение здравоохранения «Областной Центр по профилактике и борьбе сот СПИДом и инфекционными заболеваниями» было образовано в целях противодействия распространению ВИЧ-инфекции в Челябинске в декабре 1990 года в соответствии с приказом Комитета по делам медицины г. Челябинска от 05.12.1990 № 283 «Об открытии городского центра по профилактике и борьбе со СПИДом». На сегодняшний день является основным учреждением по профилактике ВИЧ-инфекции в Челябинской области. Учреждение располагает собственной клинико-диагностической лабораторией и необходимым оборудованием для проведения исследований по обнаружению инфекционных заболеваний.

Направление деятельности:

1.Профилактика и лечение ВИЧ-инфекции и других инфекционных заболеваний.

2.Платные медицинские услуги.

2.1.2Организационная структура

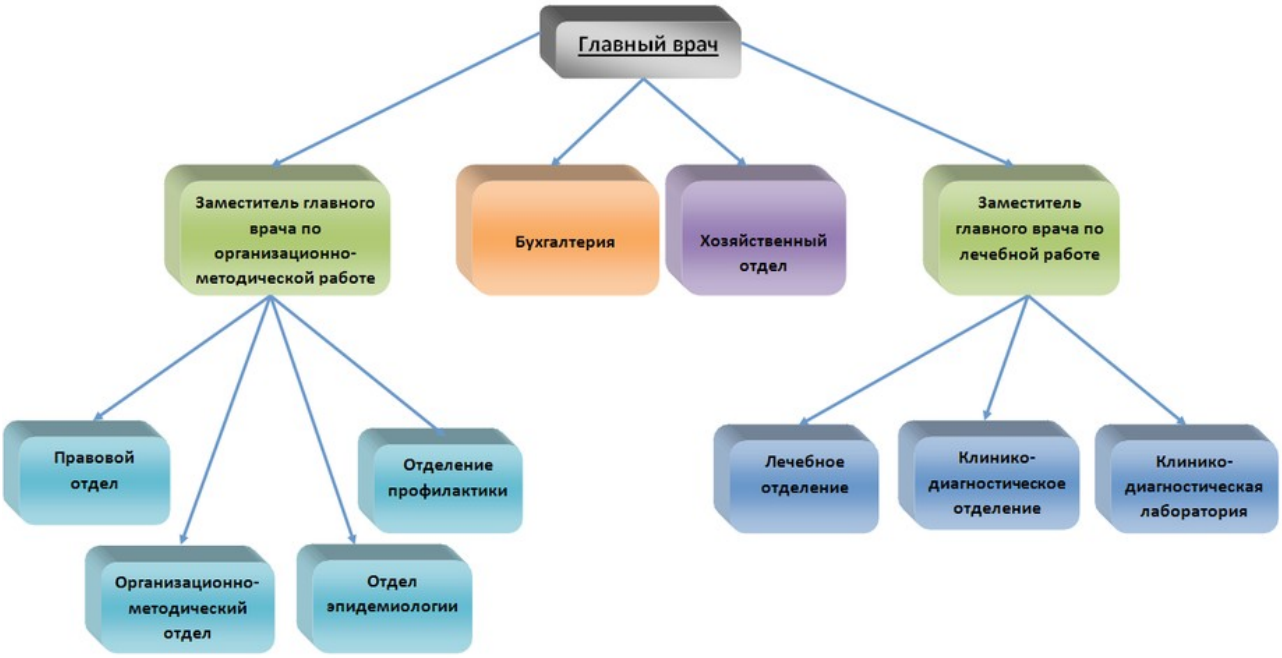

Рисунок 1 - Организационная структура учреждения

Учреждение включает в себя 8 отделов и клинико-диагностическую лабораторию:

1. Организационно – методический отдел. Руководитель отдела – заместитель главного врача по организационно-методической работе. Задачами

отдела является статистическая отчетность, поддержка ИТ-инфраструктуры учреждения, разработка нормативной документации по формам отчетности Министерства здравоохранения Челябинской области.В состав отдела входят: заместитель главного врача по организационно-методической работе, медицинский статистик, инженер-программист, врач-методист.

2. Бухгалтерия. Руководитель отдела – главный бухгалтер. Задачами отдела являются ведение бухгалтерского учета и отчетности, осуществление закупок и экономического планирования.В состав отдела входят: главный бухгалтер, экономист, бухгалтер.

3. Правовой отдел. Руководитель отдела - начальник правового отдела. Задачами отдела является кадровое делопроизводство, решение юридических вопросов, оформление документации.В состав отдела входят: начальник правого отдела, юрисконсульт, секретарь, инспектор отдела кадров.

4. Хозяйственный отдел. Руководитель отдела – начальник хозяйственного отдела. Задачами отдела является поддержание здания и коммуникаций в исправном состоянии, осуществлении ремонтных работ, обеспечение работы автотранспорта учреждения.В состав отдела входят: начальник хозяйственного отдела, водитель, сестра-хозяйка, сантехник, электрик.

5. Отделение профилактики. Руководитель отделения – заведующая отделением профилактики и социальной реабилитации. Задачами отделения является ведение профилактической работы среди населения, оказание консультаций по ВИЧ-инфекции, информационное просвещение.В состав отдела входят: заведующая отделением профилактики, специалист по социальной работе, медицинский психолог.

6. Отдел эпидемиологии. Руководитель отдела – заведующий отделом профилактики. Задачами отдела является отслеживание эпидемиологической ситуации и учет контактный лиц.В состав отдела входят: заведующий отделом эпидемиологии, врач-эпидемиолог, помощник врача-эпидемиолога.

7. Клинико-диагностическое отделение. Руководитель отделения – заведующая клинико - диагностическим отделением. Задачами отделения

является первичная регистрация пациентов, осуществление работы регистратуры.В состав отдела входят: заведующая клинико-диагностическим отделением, медицинский регистратор.

8. Лечебное отделение. Руководитель отделения - заведующая лечебным отделением. Задачами отделения является прием пациентов специалистами, назначение лечения, организация выдачи препаратов.В состав отдела входят: заведующая лечебным отделением, врач-инфекционист, врач-нарколог-психиатр, врач-терапевт, врач-педиатр, врач-дерматовенеролог, врач-невролог, врач-фтизиатр, медицинская сестра.

9. Клинико-диагностическая лаборатория. Руководитель лаборатории – заведующая КДЛ. Задачами КДЛ является клинические исследования крови на обнаружение инфекционных заболеваний.В состав отдела входят: заведующая клинико-диагностической лабораторией, биолог, врач клинико-лабораторной диагностики, фельдшер-лаборант.

2.1.3 Техническое оснащение

Парк вычислительной техники учреждения распределен следующим образом:

Таблица 1 - Количество единиц техники

В штуках

Количество серверов	Количество рабочих станций	Количество единиц оргтехники
1	54	40

Таблица 2 - Технические характеристики серверов и рабочих станций

Наименование	Характеристики

Продолжение таблицы 2

Наименование	Характеристики
Рабочая станция	Процессор компьютера - Intel® PentiumG3250 Кол-во процессоров - 1 Интерфейс накопителя (накопителей) SATA 6Gb/s Тип накопителя RAID – 500Гб Видео компьютера - интегрированное Оперативная память - 2 Гб Сетевая карта компьютера - 10/100/1000 Мбит/сек
Рабочая станция	Процессор компьютера - Intel® Celeron 2400 (S478, L2 128Kb, 400MHz) Кол-во процессоров - 1 Интерфейс накопителя (накопителей) SATA 3Gb/s Тип накопителя RAID – 80Гб Видео компьютера - интегрированное Оперативная память – 512Мб Сетевая карта компьютера - 10/100/1000 Мбит/сек
Сервер	Процессор компьютера - Intel® Core™ i7 Количество процессоров - 1 Интерфейс накопителя (накопителей) SATA 6Gb/s Тип накопителя RAID – 2000Гб Видео компьютера - интегрированное Оперативная память - 16 Гб Сетевая карта компьютера - 10/100/1000 Мбит/сек

Таблица 3 - Сетевая инфраструктура

Наименование	Характеристика

Тип подключения к интернету	оптоволоконная сеть (FTTH)
Маршрутизатор	MikrotikRouterBOARD 951Ui-2HnD
Коммутатор 16 портов	D-LinkDGS-1016D
Коммутатор 8 портов	D-Link DGS-1008D
Количество портов локальной сети	43
Логическая организации компьютеров сети	Рабочая группа

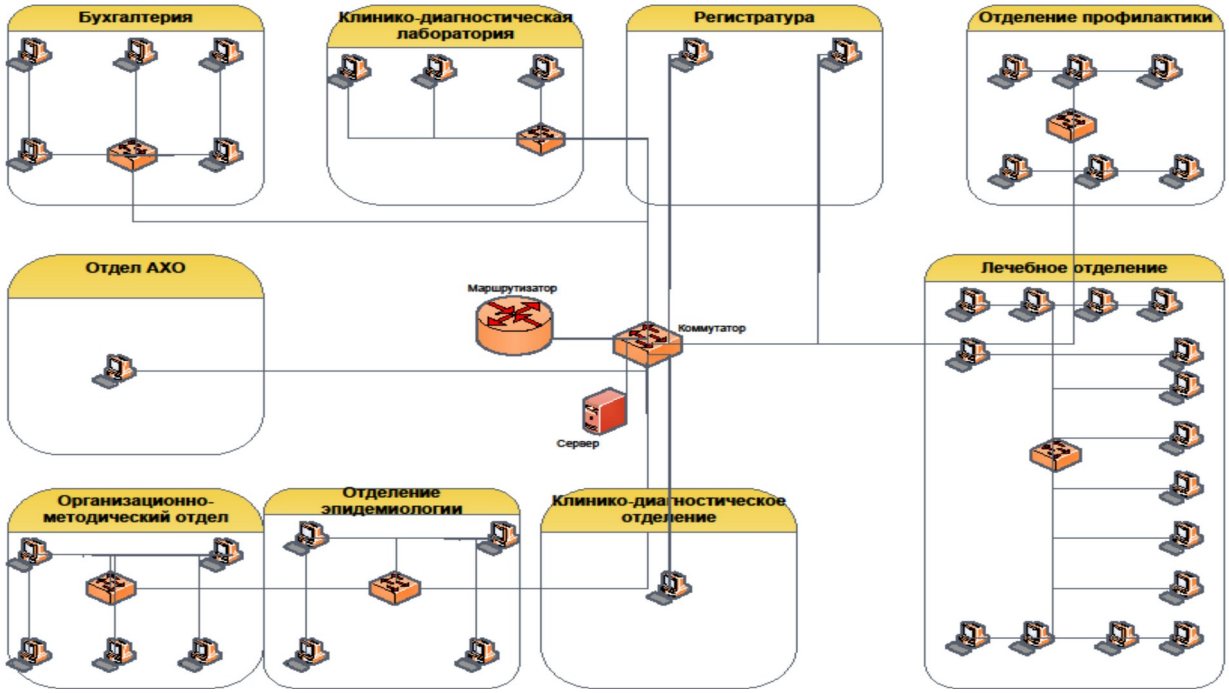

Рисунок 2- Схема локальной сети учреждения

2.1.4 Программное обеспечение

В учреждении используются следующие виды программного обеспечения:

- Операционныесистемы Windows Server 2008R2, Windows 7 Pro, Windows XP SP3, Windows 98, MS-DOS;
- Офисные приложения MicrosoftOffice 2007 Профессиональный;
- АнтивирусныерешениMicrosoft Security Essentials;
- Информационно - справочная система Консультант +;
- Базы данных MS Access 2007;
- Автоматизированная информационная система «Бюджет. Барс-бухгалтерия»;
- Комплексная бухгалтерская система ПП «СТЭК-КБС-Бюджет»;
- Система электронного документооборота «Мотив»;
- Система видеоконференций «TrueConf».
- Автоматизированная информационная система «Веб-мониторинг здравоохранения»;
- Система бухгалтерского учета и отчетности «Барс. Бюджет-отчетность»;
- Система «Сбербанк-онлайн»;
- Система сдачи отчетности «СТЭК-Траст»;
- Система «АЦК-Финансы»;
- Система «РТС-тендер»;
- СКЗИ «Крипто-Про»;
- СКЗИ «VipNet Client»;
- СКЗИ «Верба-OW».

2.2 Проблемы информационной безопасности учреждения

Основной проблемой в информационной безопасности учреждения является отсутствие необходимых мер защиты как организационного, так и технического характера, недостаточная осведомленность работников о мерах безопасности при работе с персональными данными.

Выявлены следующие проблемы в информационной безопасности учреждения:

1) Существующая нормативная документация требует доработки в соответствии с действующим законодательством по защите персональных данных.

2) Отсутствует необходимая документация учреждения как оператора персональных данных в соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных», Приказом ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности".

3) Применяются несертифицированные средства антивирусной защиты

4) Отсутствуют средства межсетевого экранирования.

5) Отсутствуют средства от несанкционированного доступа

6) Отсутствуют средства аутентификации пользователей и разграничение доступа к ПДН.

7) Метод логической организации сети, а именно рабочая группа не позволяет разграничить доступ пользователей к ресурсам информационных систем персональных данных, проводить регистрацию и отслеживание действий пользователей.

8) Отсутствуют технические, а также организационные меры противодействия использованию съемных носителей на АРМ работников учреждения.

9) Применяемая парольная политика не соответствует уровню стойкости паролей ко взлому

10) Сотрудники недостаточно осведомлены о мерах безопасности при работе с персональными данными.

11) В связи с вышеперечисленными проблемами, высок риск неправомерного доступа к информации, ее хищению, искажению или удалению. Поэтому необходимо принять комплекс мер для обеспечения защиты персональных данных, обрабатываемых в информационных системах ГБУЗ «Областной Центр по профилактике и борьбе ос СПИДом и инфекционными заболеваниями».

2.3 Обзор сертифицированных средств защиты информации

2.3.1 Исследование рынка предлагаемых программных и программно-аппаратных средств защиты информации по классам СЗИ

Данный обзор посвящен исследованию рынка средств защиты информации. В настоящее время выбор средств защиты информации достаточно большой. Решения в этой сфере выпускаются широким кругом производителей, как отечественных, так и зарубежных, в их числе наиболее известные: ООО "КРИПТО-ПРО", ООО «Код Безопасности», ЗАО «Лаборатория Касперского », Компания ESET, ООО «Доктор Веб», ОАО «ИнфоТеКС», ООО «АльтЭль», ООО «КОНФИДЕНТ», Компания Check Point Software Technologies Ltd, Компания Fortinet, Компания WatchGuard Technologies, Inc.В государственных информационных системах персональных данных, согласно Постановлению Правительства РФ № 1119 от 1 ноября 2012 г. "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» для устранения актуальных угроз безопасности ПДн необходимо использовать только средства, прошедшие процедуру сертификации во ФСТЭК и ФСБ. Из них можно выделить наиболее хорошо себя зарекомендовавшие, по классам СЗИ:

1) Средства защиты информации от НСД

а) Secret Net (Сетевая и автономная версии)

Представляет собой систему защиты информации на серверах и рабочих станциях от несанкционированного доступа. Сочетает функции защиты информации, средства централизованного управления, инструменты оперативного принятия решений и возможность мониторинга. Существует две версии, сетевая и автономная. Автономная версия применяется в небольших сетях 20-25 ПК, если больше целесообразней использовать сетевую версию, которая обладает функциями централизованного управления и возможность встраивания в доменную структуру.

Возможности:

- идентификация и аутентификация пользователей;
- разграничение доступа к защищаемой информации и устройствам;
- централизованное управление политиками безопасности (сетевая версия);
- ведение журналов событий, аудит;
- гарантированное уничтожение данных при их удалении пользователем;
- поддержка терминальных сессий пользователей для платформ Microsoft;
- управление доступом пользователей к конфиденциальным данным;
- защита от загрузки с внешних носителей;
- контроль аппаратной конфигурации компьютера;
- защита информации в процессе хранения: шифрование файлов, контроль печати конфиденциальной информации и регистрация событий;
- интеграция с ActiveDirectory (сетевая версия).

Примечание:

- проблемы совместимости с KasperskyEndpointSecurity

- невозможность постраничной печати документа при включенной опции «Защита печати».
- невозможность сохранения документа из приложения офисного пакета MSOffice в папку в режиме работы «Секретно»
- Сертификаты ФСТЭК и Минобороны России.

б) Dallas Lock 8.0-K

Представляет собой программный комплекс средств защиты информации в ОС семейства Windows с возможностью подключения аппаратных идентификаторов.

Возможности:

- защиту информации от несанкционированного доступа на персональных компьютерах, портативных и мобильных компьютерах (ноутбуках и планшетных ПК), серверах (файловых, контроллерах домена и терминального доступа), работающих как автономно, так и в составе ЛВС. Поддерживает виртуальные среды;
- дискреционный и мандатный принципы разграничения доступа к информационным ресурсам и подключаемым устройствам;
- аудит действий пользователей – санкционированных и без соответствующих прав; ведение журналов регистрации событий;
- контроль целостности файловой системы, программно-аппаратной среды и реестра;
- объединение защищенных ПК для централизованного управления механизмами безопасности;
- приведение АС, ГИС и обработки ПДн в соответствие законодательству РФ по защите информации.

Примечание:

- конфликт с системой самозащиты в антивирусе Касперского;
- проблемы с отправкой почты из MSOutlook 2013;
- проблемы при сохранении документа MSWord;

- дублирование папки Temp;
- сертификат ФСТЭК России № 2720 от 25.09.2012.

в) Secure Pack Rus 3.0

Средство защиты информации Secure Pack Rus версия 3.0 (СЗИ SPR 3.0) является сервисным пакетом для операционных систем семейства Microsoft Windows и позволяет обеспечить выполнение требований ФСБ России по защите конфиденциальной информации по классу АК2 и АК3.

Возможности:

- возможность доменной аутентификации пользователей на основе метода двухфакторной аутентификации с использованием сертификатов стандарта X.509;
- возможность дискреционного разграничения доступа именованных субъектов системы (пользователей) к именованным объектам системы (файлы, процессы и т. д.);
- возможность дискреционного разграничения доступа именованных субъектов системы (пользователей) к устройствам (отчуждаемые хранилища данных, мобильные устройства, принтеры, порты ввода/вывода и т. д.);
- обнуление освобожденной оперативной памяти системы;
- возможность аудита входа/выхода субъектов доступа (пользователей) в систему/из системы;
- возможность аудита;
- возможность периодического контроля целостности объектов файловой системы;
- возможность задания администратором списка разрешенных на выполнение программных модулей;
- возможность задания администратором списка разрешенных для установки в систему инсталляционных пакетов;
- возможность задания администратором списка разрешенных на выполнение сценариев;

- возможность криптографической защиты информации, передаваемой по канал связи, с посредством создания аутентичного защищенного соединения с использованием протокола КриптоПро TLS и/или посредством защиты IP-соединений с использованием протоколу КриптоПро IPSec. Криптографическая защита информации осуществляется по классу КС2;
- возможность криптографической защиты информации, записываемой на съемные хранилища данных посредством шифрующей файловой системы КриптоПро EFS. Криптографическая защита информации осуществляется по классу КС2;
- возможность криптографической защиты информации, записываемой на жестких дисках АРМ и серверов посредством шифрующей файловой системы КриптоПро EFS. Криптографическая защита информации осуществляется по классу КС2;
- возможность централизованного удаленного управления через механизм групповых политик ОС Microsoft Windows.

Примечание:

- Программный пакет "Secure Pack Rus" версии 3.0 сертифицирован ФСБ России

2) Средства межсетевого экранирования

а) Персональный МЭ ViPNetOfficeFirewall 4.1

Программный межсетевой экран, предназначенный для контроля и управления трафиком и преобразования трафика (NAT) между сегментов локальных сетей при их взаимодействии, а также при взаимодействии узлов локальных сетей с ресурсами сетей общего пользования.

Возможности:

- использование технологии MSI для установки ПО ViPNet;
- динамическая и статическая трансляция сетевых адресов (NAT);
- автоматическая настройка фильтров антиспуфинга;

- возможность использования экранной клавиатуры для аутентификации;
- экранная клавиатура;
- специальные правила обработки IP-трафика от приложений, использующих протоколы FTP, DNS, H.323, SCCP, SIP;
- использование групп объектов;
- фильтрация широковещательных IP-пакетов по адресам отправителя
- работа сетевых фильтров по расписанию;
- журнал регистрации IP-пакетов и преобразования сетевых адресов (NAT);
- создание нескольких конфигураций и быстрое переключение;
- поддержка нескольких сетевых карт, возможность использования на шлюзе шлюзе для сегментирования ИСПДн.

Примечание:

- проблема с совместимостью ViPNet Office Firewall и ViPNet CSP;
- Сертификат соответствия ФСБ России № СФ/515-2428.

б) ПерсональныйМЭ Security Studio Endpoint Protection

Средство защиты компьютера от сетевых вторжений, вредоносных программ и спама, которое обеспечивает защиту компьютера с применением межсетевого экрана, антивируса и средства обнаружения вторжений.

Возможности:

- межсетевой экран;
- антивирус и антишпион;
- средство обнаружения вторжений;
- веб-контроль;
- антиспам;
- журнал событий.

Примечание:

- конфликты с ViPNet Client;
- сертификаты ФСТЭК России.

в) Персональный МЭ KasperskyEndpointSecurity 10 (расширенный)

Комплексная защита от всех видов угроз обеспечивается многоуровневой системой, включающей контроль запуска и активности программ, контроль внешних устройств, веб-контроль доступа к ресурсам сети Интернет и защиту от вредоносных программ, онлайн и сетевых угроз.

Возможности:

- защита от вредоносного ПО;
- сетевой экран;
- контроль программ, устройств и веб-контроль ;
- шифрование данных;
- защита;
- управление (MDM);
- системное администрирование;
- развертывание ОС и приложений;
- управление лицензиями ;
- мониторинг уязвимостей;
- управление установкой исправлений;
- контроль доступа в сеть (NAC).

Примечание:

- проблема совместимости с продуктами Secret Net 7
- частичная несовместимость с CheckPointVPNclientR75
- потеря работоспособности java-аплетов после удаления KasperskyEndpointSecurity10
- проблемы с USB-клавиатурой и мышью после удаления KasperskyEndpointSecurity10
- сертификат №3025 ФСТЭК России

г) ПерсональныйМЭESET NOD32 Secure Enterprise

Комплексное кроссплатформенное решение, которое надежно защищает каждый узел корпоративной сети и позволяет централизованно подойти к вопросу обеспечения безопасности на всех уровнях системы в организациях любого масштаба.

Возможности:

- защита рабочих станций;
- защита мобильных устройств;
- защита файловых серверов;
- расширенная защита рабочих станций;
- защита почтовых серверов;
- защита интернет-шлюзов;
- централизованное управление.

Примечание:

- Сертификат соответствия ФСТЭК России № 3243 от 13 октября 2014 года сроком действия до 13 октября 2017 г.

д)Программный МЭ (интернет-шлюз) TrustAccess

Представляет собой распределенный межсетевой экран с централизованным управлением и аудитом событий информационной безопасности, предназначенный для защиты серверов и рабочих станций локальной сети от несанкционированного доступа, разграничения сетевого доступа к информационным системам предприятия.

Возможности:

- рабочих станций, клиентов терминальных серверов и клиентов встроенных систем;
- файловых серверов и серверов приложений (включая терминальные серверы);
- почтовых серверов;
- интернет-шлюзов;

- мобильных устройств.

Примечание:

- сертификаты ФСТЭК России (МЭ2/НДВ4 для защиты конфиденциальной информации до 1Г включительно, ИСПДн до У31 и ГИС до 1 класса включительно).

е)Программно-аппаратный МЭ WatchGuardXTM 505;

ж) Программно-аппаратный МЭ ALTELLNEO (FW);

з) Программно-аппаратный МЭ FortiGate-60C;

к)Программно-аппаратный МЭ StoneGateFirewall/VPN;

3) Средства обнаружения вторжений;

а) ПрограммноеСОВSecurityStudioEndpointProtection;

б)ПрограммноеСОВ Kaspersky Endpoint Security;

в)ПрограммноеСОВESET NOD32 Secure Enterprise;

г)Аппаратное СОВ WatchGuardXTM 505;

д)Аппаратное СОВ ALTELLNEO (UTM);

ж)Аппаратное СОВ StoneGate IPS-1030.

Представляет собой систему обнаружения и предотвращения вторжений.

Возможности:

- обнаружение и предотвращение попыток НСД в режиме реального времени в прозрачном для пользователей сети режиме;
- применение фирменной технологии AET (Advanced Evasion Techniques) - технологии защиты от динамических техник обхода;
- обширный список сигнатур атак (по содержанию, контексту сетевых пакетов и другим параметрам);
- возможность обработки фрагментированного сетевого трафика;
- возможность контроля нескольких сетей с разными скоростями;
- декодирование протоколов для точного определения специфических атак, в том числе и внутри SSL соединений;

- возможность обновления базы данных сигнатур атак из различных источников (возможен импорт сигнатур из Open Source баз);
- блокировка или завершение нежелательных сетевых соединений;
- анализ «историй» событий безопасности;
- анализ протоколов на соответствие RFC;
- встроенный анализатор событий, позволяющий эффективно снижать поток ложных срабатываний;
- создание собственных сигнатур атак, шаблонов анализа атак, аномалий и др.; дополнительная функциональность прозрачного межсетевого экрана Transparent Access Control, что позволяет в отдельных случаях отказаться от использования МЭ без какого-либо снижения эффективности защиты;
- анализ GRE туннелей, любых комбинаций инкапсуляции IP v6, IPv4;
- централизованное управление и мониторинг, простая в использовании и одновременно гибкая в настройке система генерации отчетов.

Примечание:

- Сертификат ФСТЭК №2163 от 31.08.10 (до 31.08.16)

4)Средства антивирусной защиты;

а) Kaspersky Endpoint Security;

б) ESET NOD32 Secure Enterprise;

в)Dr.Web Enterprise Security Suite;

г)SecurityStudioEndpointProtection.

5. Обеспечение доверенной загрузки

а)Электронный замок "Соболь"

Представляет собой сертифицированный аппаратно-программный модуль доверенной загрузки.

Возможности:

- аутентификация пользователей;
- блокировка загрузки ОС со съемных носителей;
- контроль целостности программной среды;

- контроль целостности системного реестра Windows;
- сторожевой таймер;
- регистрация попыток доступа к ПЭВМ;
- контроль конфигурации.

Примечание:

- Сертификат ФСТЭК России;
- Сертификат ФСБ России.

6)Комплексные средства защиты информации (UTM)

а)ALTELLNEO 120 UTM

Представляет собой программно-аппаратный комплекс, включающий маршрутизатор, межсетевой экран, веб-фильтр, систему обнаружения вторжений, VPN, почтовый фильтр.

Возможности:

- Статическая маршрутизация;
- Межсетевое экранирование с поддержкой NAT, PAT;
- Web-Proxy;
- VPN: PPTP Client;
- VPN: PPTP Server;
- VPN: IPSec
- VPN: OpenVPN;
- Антиспам Kaspersky;
- Антивирус Kaspersky;
- Фильтрация электронной почты;
- Защита от шпионского ПО;
- DNS-прокси & DHCP сервер
- Управление доступом к веб-ресурсам;
- QoS;
- Сетевая статистика;
- Динамическая маршрутизация;

- Функционирование в режиме моста (bridging);
- Фильтрация сетевого трафика на основе;
- данных протоколов прикладного уровня (L7 фильтрация);
- SIP-прокси;
- IDS/IPS;
- Система обновления Altell NEO.

Примечание:

- Сертификаты ФСТЭК по классам МЭ2/МЭ3/МЭ4 и НДВ2/3, ФСБ по классу МЭ4.

б)WatchGuardXTM 505

Представляет собой аппаратный межсетевой экран WatchGuardXTM 505 и полный пакет дополнительных сервисов SecurityBundle (LiveSecurity, WebBlocker, SpamBlocker, GatewayAntivirus, IntrusionPreventionService, ReputationEnabledDefense, ApplicationControl).

Возможности:

- Сетевойэкран: Stateful packet inspection, deep packet inspection, proxy firewall;
- Проксиуровняприложений: HTTP, HTTPS, SMTP, FTP, DNS, TCP/UDP, POP3;
- Защитаотугроз: блокировка spyware, атак DoS/DDoS, fragmented packets, malformed packets, blended threats имногоедругое;
- VoIP: H.323, SIP прокси-фильтры;
- Подпискибезопасности: WebBlocker, spamBlocker, Gateway AntiVirus, Intrusion Prevention Service, RED, Application Control;
- Шифрование: DES (в аппаратных реализациях этот алгоритм оказывается достаточно быстрым, правда, его скорость недостаточна при программной реализации. Поэтому этот алгоритм может быть применён в троекратном исполнении (3DES) для повышения уровня безопасности в сети), 3DES, AES 128-, 192-, 256-bit;

- IPSec: SHA-1, MD5, IKE pre-shared key, 3rd party cert;
- VPN failover;
- SSL: Thin client, Web exchange;
- PPTP: Server and Passthrough;
- Single sign-on: Transparent Active Directory Authentication;
- Внешняяаутентификация: Radius, LDAP, Windows Active Directory;
- Другиевидыаутентификации: VASCO, RSA SecurID, web-based, local;
- Платформауправления: WatchGuard System Manager (WSM);
- 4 включённых лицензии WSM;
- Уведомления: SNMP v2/v3, Email, Management System Alert;
- Server support: Logging and Reporting with Server Health status, Quarantine, WebBlocker, Management;
- Командная строка: поддержка прямого доступа и скриптов;
- Назначение IP-адресов: Static, DynDNS, PPPoE, DHCP (server, client, relay)

Примечание:

- Сертификат ФСТЭК по 3 классу защищенности для устройства WatchGuard XTM 505.

в) FortiGate-60C

Представляет собой комплексное устройство сетевой безопасности, включающее межсетевой экран, систему обнаружения вторжений, антивирус, веб-фильтр, систему контроля приложений.

Возможности:

- Межсетевое экранирование;
- Обнаружение и предотвращение вторжений (IPS) ;
- IPSec и SSL VPN; Защита от вредоносных программ (Антивирус);
- Антиспам;
- Web-фильтрация;
- Контроль приложений;

- WAN-оптимизация;
- Балансировка нагрузки;
- Маршрутизация/коммутация;
- Сканер уязвимостей.

Примечание:

- Сертификат ФСТЭК России.

г) Checkpoint UTM-1 Edge N

Программно-аппаратный комплекс UTM-1 Edge N,реализующий полный набор функций от межсетевого экрана и механизма защиты соединения между сайтами и удаленного доступа (VPN-шлюз) до механизма блокирования систем мгновенных сообщений (IM), шлюзового антивируса и антиспама.

Возможности:

- Межсетевой экран;
- Защищенная связь между сайтами и удаленный доступ Checkpoint UTM-1 Edge N;
- Защита от вирусов на рубеже шлюза Checkpoint UTM-1 Edge N;
- Защита электронных сообщений и анти-спам Checkpoint UTM-1 Edge N;
- Web-фильтрация Checkpoint UTM-1 Edge N;
- Контроль доступа к сети Checkpoint UTM-1 Edge N;
- Централизованное управление Checkpoint UTM-1 Edge N.

Примечание:

- Сертификат ФСТЭК №2578 от 21.02.12 (до 21.02.15)

2.3.2 Сравнение программных и программно-аппаратных средств защиты информации. Выбор решения

По данным приведенного обзора средства защиты информации можно разделить на два типа: программные и программно-аппаратные решения. Каждый из этих типов имеет свои положительные и отрицательные стороны.

Таблица 4 - Сравнение программных и программно-аппаратных СЗИ

Программные СЗИ	Программно-аппаратные СЗИ
ПЛЮСЫ	
Простота установки и настройки	Не требуют обслуживания
Регулярное обновление	Низкое энергопотребление
Низкая цена	Закрытость архитектуры
	Предсказуемая производительность при пиковой нагрузке
	компактность
МИНУСЫ	
Несанкционированный доступ пользователя	Высокая начальная стоимость
Непредсказуемая производительность	Сложность или невозможность обновления
	Невозможность адаптации под конкретные нужды

Характеристики программно - аппаратных решений представлены в Приложении 2[1].

Комплексную защиту невозможно обеспечить каким-то одним решением, будь оно программным или аппаратно-программным, необходим комплекс из

[1]Сравнительная таблица КСЗИ. (См. Приложение 2)

нескольких средств, которые бы дополняли друг друга. Отдельно стоит отметить UTM (Unified Threat Management) – решения, которые подразумевают объединение функций различных типов устройств в одном: маршрутизатор, межсетевой экран, антивирус, средство обнаружения вторжений. Тенденция комплексного подхода характерна и для программных средств, например, практически все антивирусные решения для корпоративного сектора являются центрами безопасности, обладающими всеми функциями других типов средств защиты информации. Положительными сторонами такого подхода является хорошая совместимость компонентов между собой, отсутствие конфликтов, полноценная защита. К минусам же можно отнести не всегда достаточную эффективность встроенных компонентов в сравнении с узкоспециализированными средствами.

Исследование рынка UTM - устройств, показывает, что потребность в комплексных средствах увеличивается, производители все чаще стали включать в свою линейку моделей UTM- решения, которые в свою очередь становятся все более эффективными.

UTM - устройства представлены как зарубежными, так и отечественными производителями. Из сертифицированных средств отечественного производства можно выделить модель ALTELLNEO 120 UTM от ООО «АльтЭль», данное UTM – устройство обладает оптимальным соотношение цена/качество/ функциональность, поддержкой шифрования по ГОСТу, что в первую очередь отличает эту модель от зарубежных. Из моделей иностранного производства наиболее производительной является модель FortiGate-100D от Компании Fortinet, Inc, основной ее недостаток это отсутствие шифрования по ГОСТу и высокая стоимость подписки на обновления.

Но при всех достоинствах UTM-решений, у них есть и недостаток, который заключается в снижающейся производительности при включении защитных функций, особенно это касается потокового антивируса, который снижает пропускную способность в среднем в два раза. В данном случае есть два пути решения, либо не активировать антивирус, либо выбирать модели с учетом

падения пропускной способности, то есть более старшие модели. Поэтому антивирус в UTM-устройстве это не замена антивирусу на конечном оборудовании, а лишь дополнительная защитная функция, тем более что он рассчитан на защиту о вирусов из внешней среды, и не защитит от вирусов на съемных носителях, уже имеющихся в системе.

В качестве антивируса для рабочих станций и сервера целесообразно использоватьсертифицированный ESET NOD32 Secure Enterprise Pack 5.0, в который входит ESET Endpoint Antivirus для Microsoft Windows и ESET File Security для Microsoft Windows Server. Преимуществом данного решения является невысокая нагрузка на систему, хорошая скорость сканирования, достаточный уровень детектирования вирусов, невысокая нагрузка на канал, вследствие использования локального зеркала обновлений, возможность гибкой настройки.

Для устранения угроз недекларированные возможностей и несанкционированного доступа целесообразно использовать встроенные механизмы аутентификации и разграничения доступа Microsoft Windows, такие как доменные службы Active Directory, для этого необходимо провести сертификацию операционной системы Microsoft Windows и установитьсредство защиты информации от НСД Secure Pack Rus версия 3.0.

Выбор набора средств защиты зависит от угроз безопасности, целесообразность того или иного подхода определяется исходя из ценности информации, исходных затрат на ее защиту, дальнейшей поддержки защиты в актуальном состоянии; объем средств направленных на защиту информации не должен превышать ценность этой информации.

3 ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИСПДн «МЕДИЦИНСКАЯ ИНФОРМАЦИОННАЯ СИСТЕМА»

3.1 Обследование информационной системы

- Сбор и анализ исходных данных по обработке ПДн;
- Определение способа и вида обработки ПДн;
- Определение категории и состава обрабатываемых ПДн;
- Анализ сведений о конфигурации сети, аппаратном и программном обеспечении используемым при обработке ПДн;
- Анализ целей обработки ПДн, определение порядка передачи третьим лицам;
- Исследование существующих локальных документов на соответствие требованиям законодательства и создания дополнительных нормативных документов или внесения изменений в существующие при их несоответствии.

По результатам проведенного обследования составлен отчет[2] в котором отражен исходный уровень защищенности персональных данных в учреждении. Данный отчет необходим для составления плана реализации по защите персональных данных в ИСПДн «Медицинская информационная система».

3.2 Построение модели угроз

3.2.1Определение типа актуальных угроз

В ходе проведенного анализа было выявлено следующее:

Таблица 5 - Определение типа актуальных угроз

Тип ИСПДн	обрабатывающие специальные категории персональных данных
Объем	менее 100 000
Тип актуальных угроз	угрозы 3 типа

[2]Отчет о результатах проведенной внутренней проверки ИСПДн «МИС» (См. Приложение 3)

3.2.2 Определение класса защищенности информационной системы персональных данных

Классификация информационной системы персональных данных произведена в соответствии с Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». В ходе проведенного анализа было выявлено следующее:

Таблица 6 - Определение уровня значимости и масштаба информационной системы

Уровень значимости	УЗ 3
Масштаб информационной системы	Объектовый

На основании информации, содержащейся в пунктах 1, 2 для информационной системы персональных данных присвоен следующий уровень защищенности персональных данных**:** 3 уровень.

Класс защищенности ИСПДн «Медицинская информационная система» - 3 класс.

В результате проведенной работы составлен Акт классификации ИСПДн «Медицинская информационная система» № 1 от 05.06.2015.

3.2.3 Определение перечня ИСПДн и перечня сведений, содержащих персональные данные

Перечень ИСПДн и перечень персональных данных обрабатываемых в ИСПДн «Медицинская информации оная система» приведены в Приложении 4[3].

[3] Перечень ПДн в ИСПДн «МИС» (См.Приложение 4)

3.2.4 Определение нарушителя безопасности

Модель угроз безопасности персональным данным в ИСПДн «Медицинская информационная система» (далее – Модель угроз) Государственного бюджетного учреждения здравоохранения «Областной Центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями» (далее – ГБУЗ «Областной Центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями») разработана в соответствии с требованиями следующих документов:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 15.02.2008;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 14.02.2008;
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Утверждены Руководством 8 Центра ФСБ России 21.02.2008 №149/54-144.

Модель угроз персональным данным в ИСПДн «Медицинская и информационная система» приведена в Приложении 5[4].

Таблица 7 - Определение типа нарушителя

[4] Модель УБПДн в ИСПДн «МИС» (См. Приложение 5)

Предполагаемые возможности нарушителя	Нарушитель
Располагает только доступными в свободной продаже аппаратными компонентами криптосредств и СФК (H_1, H_2)	+
Может использовать штатные средства в пределах КЗ (H_2)	+

В данном случае нарушитель относится к H_2, т.к. нет предположений о принадлежности нарушителя к другим типам и есть предположение относящееся к типам нарушителя H_2.

3.2.5 Определение уровня исходной защищенности

Таблица 8 - Определение уровня исходной защищенности

Технические и эксплуатационные характеристики	Уровень защищенности
По территориальному размещению: локальная ИСПДн, развернутая в пределах одного здания	Высокий
По наличию соединения с сетями общего пользования: имеет одноточечный выход в сеть общего пользования	Средний
По встроенным (легальным) операциям с записями баз ПДн: модификация, передача	Низкий
По разграничению доступа к ПДн: к ИСПДн имеют доступ определенные перечнем сотрудники	Средний
По наличию соединений с другими базами ПДн иных ИСПДн: база ПДн принадлежит ГБУЗ «Областной Центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями»	Высокий
По уровню (обезличивания) ПДн: предоставляемые пользователю данные не являются обезличенными	Низкий
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:	Средний

предоставляется часть ПДн	

Не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний», а остальные – низкому уровню защищенности. Следовательно, ИСПДн имеет средний уровень исходной защищенности ($Y_1 = 5$).

3.2.6 Определение вероятности реализации угроз персональным данным

Средняя вероятность ($Y_2 = 5$) – объективные предпосылки для реализации угрозы существуют и принятые меры обеспечения безопасности ПДн недостаточны;

3.2.7 Определение реализуемости угроз персональным данным

Коэффициент реализуемости угрозы Y определяется соотношением:

$$Y = \frac{Y_1 + Y_2}{20} = \frac{(5 + 5)}{20} = 0{,}5, \qquad (1)$$

где Y – коэффициент реализуемости угрозы.

Таким образом имеем среднююреализуемость угроз $(0{,}3 \le Y \le 0{,}6)$

3.2.8 Определение опасности угроз персональным данным

- низкая опасность (реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных);
- средняя опасность (реализация угрозы может привести к негативным последствиям для субъектов персональных данных);
- высокая опасность (реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных).

Опасность угроз персональным данным определена в Приложении 5[5].

3.2.9 Определение актуальности угроз персональным данным

Таблица 9 - Актуальность угроз персональным данным

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

Актуальность угроз персональным данным определена в Приложении 5[6].

3.2.10 Оценка уязвимости ИСПДн «Медицинская информационная система»

Технические и программные средства ИСПДн «Медицинская информационная система» приобретены у доверенных поставщиков. На АРМ пользователей ИСПДн установлены лицензионные копии операционных систем и прикладного программного обеспечения.

Учитывая вышесказанное, наличие преднамеренно скрытых недокументированных (недекларированных) возможностей в микропрограммах, прошивках, драйверах оборудования, утилитах, а также в средствах операционной системы и прикладном программном обеспечении исключено.

---

[5] Модель УБПДн в ИСПДн «МИС» (См. Приложение 5)

[6] Модель УБПДн в ИСПДн «МИС» (См.Приложение 5)

3.2.11 Частная модель угроз ИСПДн «Медицинская информационная система»

На основании настоящей Модели УБПДн в ИСПДн «Медицинская информационная система»[7] были определены следующие актуальные угрозы:

1. Угрозы НСД с применением стандартных средств ОС и специализированных программных средств
2. Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия

Для устранения вышеперечисленных угроз необходимо принять следующие технические меры противодействия:

- Установка сертифицированного средства антивирусной защиты;
- Установка СЗИ от НСД и пакета сертификации операционной системы MSWindows и пакета сертификации приложений MSOffice 2007 Professional;
- Установка сертифицированного средства межсетевого экранирования.

3.3 Технологический процесс ИСПДн «Медицинская информационная система»

3.3.1 Общие положения

В ИСПДн «Медицинская информационная система» обрабатываются данные в электронном и бумажном виде. ИСПДн «Медицинская информационная система» представляет собой автоматизированную систему, состоящую из комплекса автоматизированных рабочих мест (далее – АРМ), объединенных между собой локальной сетью с выходом к сетям международного информационного обмена.

Оператор – сотрудник, осуществляющий работу с персональными данными, в связи с выполнением служебных обязанностей.

---

[7] Модель УБПДн в ИСПДн «МИС» (См. Приложение 5)

Системный администратор – сотрудник, должностные обязанности которого подразумевают обеспечение штатной работы компьютерной техники, сети и программного обеспечения.

3.3.2 Обработка информации

- к основным операциям обработки данных относятся:
- ввод данных;
- хранение и обработка данных;
- вывод данных.
- к служебным операциям персональных данных относятся:
- обновление программного обеспечения
- устранение сбоев;
- антивирусная защита;
- резервное копирование и восстановление.
- служебные операции персональных данных выполняются только системным администратором.

3.3.3 Ввод информации

Под вводом информации понимается перенос информации в АРМ при помощи клавиатуры и компьютерной мыши на внутренние носители автоматизированной системы с использованием приложения MicrosoftOfficeAccess 2007.

Оператору АРМ предоставляются документы, затем он производит ввод информации в АРМ. Для осуществления ввода, оператор включает АРМ, заходит в систему под своим логином и паролем, открывает программу, вводит предоставленную информацию. После ввода информации оператор АРМ возвращает документы, переходит к следующей операции или завершает работу.

3.3.4 Хранение и обработка персональных данных

Под обработкой информации понимается преобразование входной информации к формату, необходимому для ее хранения, преобразование хранимой информации к формату, соответствующему требованиям вывода документа на экран монитора для анализа, либо вывода документа на принтер, с использованием приложения MicrosoftOfficeAccess 2007.

Введенные данные отправляются на сервер, где осуществляется их хранение и обработка. Для получения информации, для ее дальнейшего редактирования или вывода, оператор АРМ отправляет запрос на сервер, в котором указываются необходимые, для поиска нужной информации, реквизиты. Реквизиты вводятся с помощью клавиатуры и мыши в АРМ. Далее оператор переходит к следующей операции или завершает работу.

3.3.5 Вывод информации

Под выводом информации понимается перенос информации с АРМ на бумажные носители, с использованием приложения MicrosoftOfficeAccess 2007. Информация скачивается с сервера на АРМ, выводится на дисплее и распечатывается при помощи принтера. Далее оператор переходит к следующей операции или завершает работу.

3.3.6 Обновление программного обеспечения

Под обновлением понимается замена программного обеспечения устаревшей версии на новую версию этого же программного обеспечения. Обновление программного обеспечения будет допустимо лишь в той мере и в том случае, если это подтверждено производственной необходимостью и имеет непосредственное отношение к технологическому процессу.

3.3.7 Устранение сбоев

Под устранением сбоев понимается восстановление работоспособности, как отдельных элементов автоматизированной системы, так и всей автоматизированной системы в целом.

При возникновении неполадок в АРМ, в случае необходимости, заменяется на рабочий или ремонтируется, если это возможно.

При возникновении неполадок в периферийных устройствах, таких как клавиатура, компьютерная мышь, монитор, принтер, в случае необходимости, заменяются на рабочие или ремонтируются, если это возможно.

При прекращении работы сети, обратиться к системному администратору, заблокировать АРМ и ждать восстановления работы сети.

3.3.9 Антивирусная защита

Под Антивирусной защитой понимается – обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

В качестве средства антивирусной защиты используется Microsoft Security Essentials.

При включении АРМ происходит автоматическая проверка на наличие компьютерных вирусов.

Один раз в день осуществляется автоматическое обновление вирусных баз.

3.3.10 Резервное копирование и восстановление

Под резервным копированием понимается вывод информации на внешние носители с целью использования ее в случае потери (удаления либо разрушения) файлов из хранилища информации на внутренних носителях автоматизированной системы или при невозможности доступа к ней.

Резервное копирование системы осуществляется при операции обновления программного обеспечения.

Под восстановлением понимается ввод информации с внешнего носителя на внутренние носители автоматизированной системы, где расположено хранилище файлов.

3.4 Техническое задание на построение системы защиты персональных данных в ИСПДн «Медицинская информационная система»

Основанием для разработки данного технического задания является частная модель угроз ИСПДн «Медицинская информационная система» которая послужила основой для определения состава и требований к средствам защиты информации, используемых при построении системы защиты.

3.4.1 Состав системы зашиты персональных данных

- средства межсетевого экранирования;
- средства защиты от несанкционированного доступа;
- средства антивирусной защиты;
- средства обнаружения вторжений;
- средства резервного копирования.

3.4.2 Требования к средствам межсетевого экранирования

Перечень требований к средствам межсетевого экранирования:

- Фильтрация протоколов прикладного уровня;
- Фильтрация трафика с учетом заданного контекста, состояния соединений, даты, времени;
- Противодействие DDoS-атакам;
- Регистрация и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);
- Фильтрация на сетевом уровне для каждого сетевого пакета;
- Восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
- Возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации.

3.4.3 Требования к средствам защиты от несанкционированного доступа

Перечень требований к средствам защиты от несанкционированного доступа:

- Идентификация и проверка подлинности пользователя при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее восьми буквенно-цифровых символов;
- Контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа;
- Обнуление освобожденной оперативной памяти системы;
- Возможность периодического контроля целостности объектов файловой системы;
- Контроль работы пользователей со сменными накопителями;

3.4.4 Требования к средствам антивирусной защиты

Перечень требований к средствам антивирусной защиты:

- механизмы восстановления зараженного объекта в исходное состояние, удаление, блокирование;
- регулярное обновление антивирусных баз в автоматическом режиме;
- централизованные механизмы управления;
- механизмы контроля съемных носителей;
- средства восстановления после заражения.

3.4.5 Требования к средствам обнаружения вторжений

Перечень требований к средствам обнаружения вторжений:

- обнаружение сетевых атак на основе, как сигнатурных методов анализа;
- обнаружение несанкционированной активности;
- регулярного обновления базы сигнатур.

3.4.5 Требования к средствам резервного копирования

Перечень требований к средствам резервного копирования:

- механизм регулярного резервного копирования по расписанию;
- возможность резервного копирования на съемные носители, сетевые ресурсы;
- централизованное управление;
- возможность восстановления отдельных файлов и папок.

3.5 Технический проект на построение системы защиты персональных данных

3.5.1. Определение средств защиты информации

Выбор средств защиты информации осуществляется на основе требований предъявляемых в техническом задании и на опираясь на актуальные угрозы указанные в модели угроз ИСПДн «Медицинская информационная система». Основанием для выбора конкретного продукта являлось наличие действующего сертификата соответствия ФСБ или ФСТЭК.

По результатампроведенного анализа рынка существующих решений в сфере защиты информации, выбор был сделан в пользу производителей, удовлетворяющих требованиям к системе защиты персональных данных.

а) Средства межсетевого экранирования/средства обнаружения вторжений

В качестве межсетевого экрана и средства обнаружения вторжений был выбрано комплексное средство защиты информации ALTELLNEO 120,обеспечивающее защиту от угроз связанных с использованием протоколов межсетевого взаимодействия, регистрацию атак,а также фильтрацию спама.

Наличие сертификатов ФСТЭК по классам МЭ2/МЭ3/МЭ4 и НДВ2/3, ФСБ по классу МЭ4.

Угрозы безопасности, нейтрализуемые данным средством защиты:

- анализ сетевого трафика для изучения логики работы ИСПДн, выявления протоколов, портов, перехвата данных, их подмены;
- применение специальных программ дл выявления пароля (IP-спуфинг, разные виды перебора);
- внедрение специализированных троянов, вредоносных программ;
- удаленный запуск приложений;
- реализация угрозы «отказа в обслуживании»;
- навязывание ложного маршрута путем несанкционированного изменения маршрутно-адресных данных;

- сканирование сети для изучения логики работы ИСПДн, выявления протоколов, портов;
- подмена доверенного объекта в сети с присвоением его прав доступа, внедрение ложного объекта сети.

Таблица 10 - Затраты на приобретение межсетевого экрана/средства обнаружения вторжений

№ п.п.	Наименование	Кол-во, шт.	Цена, Руб.	Сумма поставки, руб
1	ALTELLNEO 120	1	139 600,00	139 600,00
ИТОГО				139 600,00

b) Средства защиты от несанкционированного доступа

В качестве средства защиты от несанкционированного доступа был выбран продукт Secure Pack Rus версия 3.0, который позволит противодействовать следующим угрозам:

- Перехват паролей или идентификаторов в ходе загрузки ОС, модификация BIOS, перехват управления загрузкой;
- Доступ в операционную среду (локальную ОС отдельного ТС ИСПДн) с возможностью выполнения НСД вызовом штатных процедур или запуска специально;

Программный пакет "Secure Pack Rus" версии 3.0 сертифицирован Федеральной службой безопасности Российской Федерации

Таблица 11 - Затраты на приобретение средств защиты от несанкционированного доступа

Наименование	Кол-во, шт.	Цена, Руб.	Сумма поставки, руб
Средство защиты информации SecurePackRus версия 3.0 для сервера	1	10 350,00	10 350,00
Средство защиты информации SecurePackRus версия 3.0 для АРМ	37	4 150,00	153 550,00
Сертифицированная версия Microsoft Windows 7 Профессиональная (Полный пакет)	37	3020,00	111 740,00
Сертифицированная версия Microsoft Windows Server 2008 R2 Standard Edition (Полный пакет)	1	8 900,00	8 900,00
Сертифицированный USB-ключ eToken PRO (Java) для получения сертифицированных обновлений	1	2 000,00	2 000,00
Сертифицированнаяверсия Microsoft Office 2010 Professional Plus	38	3 825,00	145 350,00
ИТОГО			431 890,00

c) Средства антивирусной защиты

В качестве стредства антивирусной защиты был выбран программный продукт • ESET NOD32 Secure Enterprise с пакетом сертификации ESET NOD32 Secure Enterprise Pack 5.0, обеспечивающий нейтрализацию следующих угроз:

- Действия вредоносных программ (компьютерных вирусов);
- Внедрение специализированных троянов, вредоносных программ.

Наличие сертификата соответствия ФСТЭК России № 3243 от 13 октября 2014 года.

Таблица 12 - Затраты на приобретение средств антивирусной защиты

№ п.п.	Наименование	Кол-во, шт.	Цена, Руб.	Сумма поставки, руб
1	ESET NOD32 Secure Enterprise	38	2 369,00	90 022,00
2	ESET NOD32 Secure Enterprise Pack 5.0	1	2 500,00	2 500,00
ИТОГО				92 522,00

d) Средства резервного копирования

В качестве средства резервного копирования был выбран Acronis Backup & Recovery 11 Server for Windows, который удовлетворяет требованиям технического задания и обеспечивает:

- Механизм регулярного резервного копирования по расписанию;
- Возможность резервного копирования на съемные носители, сетевые ресурсы;
- Централизованное управление;
- Возможность восстановления отдельных файлов и папок.

Наличие сертификата соответствия ФСТЭК России № 2681

Таблица 13 - Затраты на приобретение средств резервного копирования

Наименование	Кол-во, шт.	Цена, Руб.	Сумма поставки, руб
Acronis Backup & Recovery 11 Server for Windows (сертифицированаверсия)	1	43 750,37	43 750,37
ИТОГО			43 750,37

Стоимость закупки средств защиты информации и средств резервного копирования для реализации технической защиты персональных данных в ИСПДн «Медицинская информационная система» составит: 707 762, 37 рублей.

3.6 Разработка организационно – распорядительных документов по защите персональных данных

В результате разработаны и утверждены следующие локальные нормативные акты:

- Перечень ИСПДн и ПДн;
- Модель угроз безопасности персональных данных и модель нарушителя безопасности в ИСПДн «Медицинская информационная система»;
- Техническое задание системы защиты персональных данных в ИСПДн «Медицинская информационная система»;
- Технологический процесс ИСПДн «Медицинская информационная система»;
- Информационное письмо о внесении изменений в РОСКОМНАДЗОР;
- Положение о ПДЭК;
- Перечень сотрудников имеющих доступ к средствам СКЗИ;
- Перечень сотрудников режимное помещение;
- Перечень сотрудников, допущенных к ПДн;
- План внутренних проверок;
- Приказ о контролируемой зоне;
- Приказ об утверждении матрицы доступа;
- Приказ об утверждении мест хранения носителей ПДн;
- Приказ об утверждении мест хранения СКЗИ;
- Регламент резервного копирования и восстановления данных;
- План мероприятий по обеспечению защиты ПДн;

- Инструкция о действиях сотрудников учреждения при возникновении нештатных ситуаций;
- Инструкция о парольной защите;
- Инструкция о режимных помещениях;
- Инструкция ответственного за обеспечение безопасности персональных данных в информационных системах;
- Инструкция ответственного за организацию обработки ПДн;
- Инструкция по антивирусной защите;
- Инструкция пользователя ИСПДн;
- Инструкция пользователя СКЗИ.

3.7 Аттестация информационной системы защиты персональных данных

Состав работ по проведению аттестации ИСПДн включает следующие этапы:

1. Разработка и согласование «Программы и методики аттестационных испытаний».
2. Проведение аттестационных испытаний ИСПДн на соответствие требованиям по безопасности информации.
3. Выдача заключения по результатам аттестационных испытаний.
4. Выдача аттестата соответствия в случае положительного заключения по результатам аттестационных испытаний.

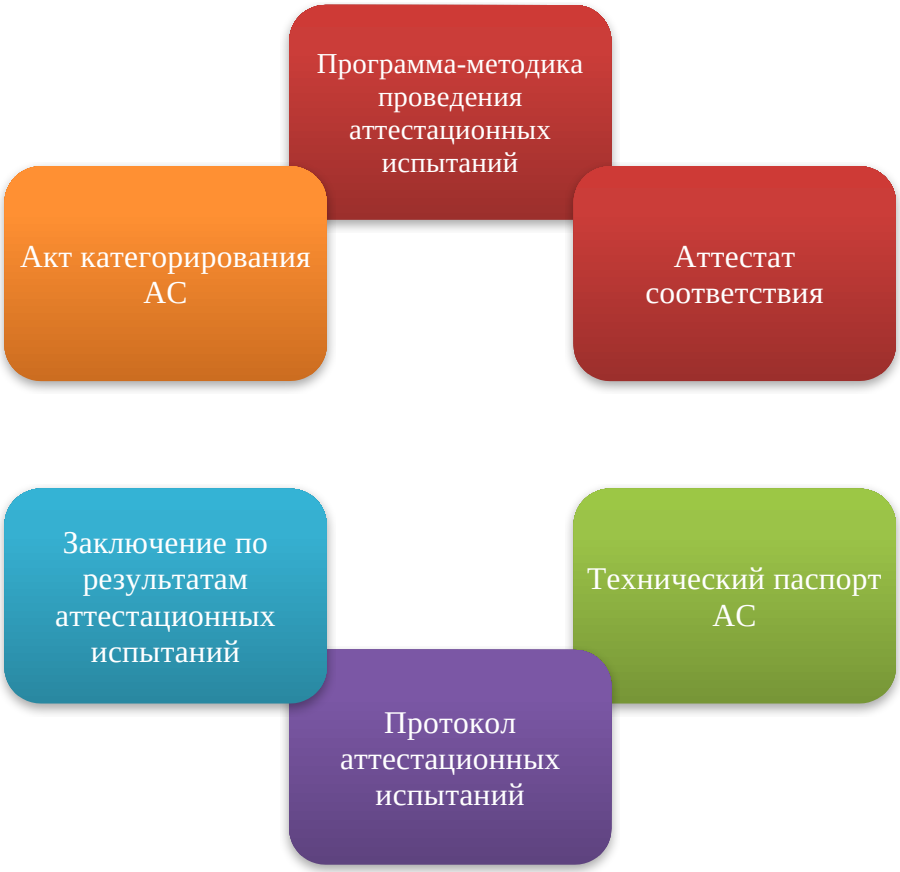

Рисунок 3 - Этапы аттестационных мероприятий

Требования к аттестации информационных систем в государственных учреждениях определены в Приказе ФСТЭК России от 11.02.2013 № 17, в связи с этим необходимо провести комплекс аттестационных испытаний на подтверждение соответствия организационных и технических мер защиты информационной системы персональных данных требуемому уровню защиты, который будет включать в себя:

- Анализ исходных данных по объекту аттестации;
- Анализ разработанных нормативных актов по защите персональных данных;
- Проведение испытаний используемых средств защиты в отдельности;

- Проведение испытаний комплекса всех средств защиты в совокупности;
- Анализ проведенных испытаний и подготовка заключения об итогах испытаний.

Стоимость проведения аттестации ИСПДн «Медицинская информационная система» составит 416 600,00 рублей.

Результатом проведенных мероприятий будут являться оформление следующих отчетных документов:

- Технический паспорт ИСПДн «Медицинская информационная система»;
- Методика и программа проведенных испытаний;
- Протокол испытаний;
- Заключение по результатам испытаний;
- Аттестат соответствия.

Заключительным этапом будет являться получение "Аттестата соответствия" которым подтверждается, что ИСПДн «Медицинская информационная система» ГБУЗ «Областной Центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями» соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России.

4 РАСЧЕТ ТЕХНИКО-ЭКОНОМИЧЕСКИХ ПОКАЗАТЕЛЕЙ

4.1 Затраты на построение системы зашиты

Общие затраты на построение системы защиты персональных данных в первую очередь будут складываться из стоимости средств защиты информации и стоимости услуг по аттестации на соответствие требования защиты персональных данных в государственных информационных системах, а также расходов на эксплуатацию и техническое обслуживание средств защиты.

Согласно проведенным расчетам в разделе 4,стоимость закупки средств защиты составит 707 762, 37 руб.

Таблица 14 - Затраты на построение системы защиты персональных данных

Этапы	Исполнитель	Стоимость, руб
Обследование информационной системы	Учреждение	0
Разработка модели угроз и нарушителей безопасности ПДн, классификация ИСПДн	Учреждение	0
Разработка Технического задания на создание системы защиты ПДн.	Учреждение	0
Разработка технического проекта СЗПДн.	Учреждение	0
Разработка организационно-правовых документов	Учреждение	0
Закупка средств защиты информации	Учреждение	707762,37
Проведение пуско-наладочных работ.	Учреждение	0
Стоимость реализации системы защиты ИСПДн «Медицинская информационная система»		1 124 363,00

4.2 Затраты на эксплуатацию и техническое обслуживание

Таблица 15 - Затраты на эксплуатацию и техническое обслуживание

Наименование	Стоимость, руб.
Обновление версии ПО МЭ AltellNeo 120	41 880,00
Обновление баз сигнатур антивируса	51 000,00
Обновление ESET NOD32 Secure Enterprise (продлениелицензии)	53998,00
Стоимость обслуживания в год	146 878,00

Затраты на создание системы защиты ИСПДН «Медицинская информационная система» и техническое обслуживание в течении 1 года составят:

$$Z = R + T \quad (2)$$

= 1 124 363,00 + 146 878,00 = 1 271 241,00 руб.,

где Z - Затраты на создание системы защиты ПДн и техническое обслуживание в год;

R - Стоимость реализации системы защиты персональных даны в ИСПДн «Медицинская информационная система»;

T - Стоимость технического обслуживания в год.

4.3 Оценка потенциальных финансовых потерь в случае приостановки деятельности по оказанию платных услуг

Таблица 16 - Потенциальные финансовые потери

Деятельность	Доход в месяц
Оказание платных услуг	1 300 000,00

Наиболее критичным риском при проварке регулятором медицинского учреждения является приостановка деятельности по оказанию услуг на возмездной основе на срок 90 суток.

В качестве административного взыскания для данного учреждения наиболее вероятно наложение штрафа по ст. 13.11 и ч. 2 ст. 13.12 в совокупном размере 30 000 рублей.

Учитывая, что плановые проверки регулирующими органами проходят раз в 3 года, то объем единоразовых потенциальных потерь будет составлять:

$$P = U + N = 3\,900\,000 + 30\,000 = 3\,930\,000 \text{ руб.}, \quad (3)$$

где P - потенциальные финансовые потери за счет приостановки и наложения штрафных санкций регуляторами;

U - размер упущенной выгоды в случае приостановки деятельности;

N - потери в случае наложения штрафов.

4.4 Оценка экономической эффективности

Экономическая эффективность построения и техничного обслуживания системы защиты персональных данных в ИСПДН «Медицинская информационная система» будет составлять:

$$E = \frac{P \cdot 100\,\%}{Z} = \frac{3390000,00}{1\,227\,654,00} = 2,76, \quad (4)$$

где E - экономическая эффективность построения и технического обслуживания системы защиты персональных данных;

P - потенциальные финансовые потери за период 1 год за счет риска упущенной выгоды и риска наложения штрафов регуляторами;

Z - затраты на построение и техническое обслуживание системы защиты персональных данных в течении 1 года.

Анализ показал, что каждый рубль, направленный на реализацию системы защиты персональных данных в ИСПДн «Медицинская информационная система» позволит снизить риски на 2,76 руб. в течение года, исходя из чего можно сделать вывод об эффективности и экономической целесообразности построения системы защиты ИСПДн «Медицинская информационная система» в ГБУЗ «Областной Центр по профилактики и борьбе со СПИДом и инфекционными заболеваниями

ЗАКЛЮЧЕНИЕ

В результате проведенной работы в ГБУЗ «Областной Центр по профилактике и борьбе со СПИДом и информационными Были разработаны необходимые нормативные документы, согласно законодательству в области персональных данных, определен класс и уровень защищенности ИСПДН, построена модель угроз и основании перечня выявленных актуальных угроз определены меры защиты. На основании анализа рынка средств защиты информации были отобраны средства, наиболее подходящие для нейтрализации актуальных угроз, произведен расчет необходимого количества СЗИ по среднерыночным ценам поставщиков средств защиты информации, определена конечная стоимость реализации технической защиты персональных данных в ИСПДн «Медицинская информационная система». После установки средств защиты информации и настройки, дальнейшим шагом будет проведение аттестации созданной системы защиты ПДн организацией, лицензированной на осуществление деятельности в области ТЗКИ, согласно Приказу ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".

Проведён расчёт стоимости для построения системы защиты персональных, рассмотрена целесообразность и экономическая эффективность системы защиты.

В совокупности средства защиты информации образуют комплексную систему защиты персональных данных ИСПДн «Медицинская информационная система».

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. О персональных данных: Федеральный закон РФ от 27 июля 2006 г. N 152-ФЗ: принят Государственной Думой 8 июля 2006 г.: одобрен Советом Федерации 14 июля 2006 г. // КонсультантПлюс – 2014. – 21 июля.

2. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства РФ от 1 ноября 2012 г. № 1119 // КонсультантПлюс – 2012. – 6 ноября.

3. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: Приказ ФСТЭК России от 11.02.2013 № 17 //ФСТЭК России – 2013. – 11 февраля.

4. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности: Приказ ФСБ России от 10 июля 2014 г. N 378 // ФСБ России – 2014 – 10 июля.

5. Об утверждении положения о ведении реестра операторов, осуществляющих обработку персональных данных : Приказ Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия от 28.03.2008 г. №154 // Российская газета – 2008. – 26 апреля.

6. Методика определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных, утвержденная 14 февраля 2008 г. заместителем директора ФСТЭК России.

7. Базовая модель угроз безопасности персональным данным при обработке в информационных системах персональных данных, утвержденная 15 февраля 2008 г. заместителем директора ФСТЭК России.

8. ОАО «ИнфоТеКС» (Информационные Технологии и Коммуникационные Системы). – Режим доступа: http://www.infotecs.ru.

9. Код безопасности, ГК «Информзащита». – Режим доступа: http://www.securitycode.ru/.

10. – Режим доступа: ИСПДН.ру http://ispdn.ru.

11. Федеральная служба по техническому и экспортному контролю. – Режим доступа: (ФСТЭК России) http://fstec.ru/ .

12. Федеральная служба безопасности Российской Федерации – Режим доступа: http://www.fsb.ru/ .

13. ГБУЗ «Областной Центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями». – Режим доступа: http://спидцентр.рф/

14. Антивирусные решения ESETNOD32 [Электронный ресурс]. - Режим доступа: https://www.esetnod32.ru/ .- Заглавие с экрана.- (Дата обращения. – 20.07.2015).

15. Антивирус Dr.Web [Электронный ресурс]. - Режим доступа: http://www.drweb.ru/ .- Заглавие с экрана.- (Дата обращения. – 21.07.2015).

16. Лаборатория Касперского [Электронный ресурс]. - Режим доступа: http://www.kaspersky.ru/ .- Заглавие с экрана.- (Дата обращения. – 21.07.2015).

17. АЛТЭКС-СОФТ [Электронный ресурс]. - Режим доступа: http://www.altx-soft.ru/ .- Заглавие с экрана.- (Дата обращения. – 21.07.2015).

18. АльтЭл [Электронный ресурс]. Режим доступа: http://www.altell.ru/ .- Заглавие с экрана.- (Дата обращения. – 21.07.2015)

19. Check Point Software Technologies Ltd. [Электронный ресурс]. - Режим доступа: http://rus.checkpoint.com/ Заглавие с экрана.- (Дата обращения. – 21.07.2015).

20. WatchGuard Technologies, Inc . [Электронныйресурс]. - Режим доступа: https://www.watchguard.com/ Заглавие с экрана.- (Дата обращения. – 21.07.2015).

21. Fortinet,Inc [Электронный ресурс]. - Режим доступа: http://www.fortinet.com/Заглавие с экрана.- (Дата обращения. – 21.07.2015).

22. КРИПТО-ПРО [Электронный ресурс]. - Режим доступа: https://www.cryptopro.ru/ Заглавие с экрана.- (Дата обращения. – 21.07.2015).

23. Бизнес без опасности [Электронный ресурс]. - Режим доступа: http://lukatsky.blogspot.ru/ Заглавие с экрана.- (Дата обращения. – 21.07.2015).

24. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс]. - Режим доступа: http://pd.rkn.gov.ru/ Заглавие с экрана.- (Дата обращения. – 21.07.2015).

25. Блог безопасника [Электронный ресурс]. - Режим доступа:http://www.secsite.ru/ Заглавие с экрана.- (Дата обращения. – 21.07.2015).

26. Ружель [Электронный ресурс]. - Режим доступа: http://www.rujel.net/ Заглавие с экрана.- (Дата обращения. – 21.07.2015).

27. Информационный портал[Электронный ресурс]. - Режим доступа: SecurityLab.ruhttp://www.securitylab.ru/ Заглавие с экрана.- (Дата обращения. – 21.07.2015).

ПРИЛОЖЕНИЕ 1

СПИСОК УСЛОВНЫХ СОКРАЩЕНИЙ

АРМ	автоматизированное рабочее место
ИСПДн	информационная система персональных данных
МИС	медицинская информационная система
КСЗИ	комплексные средства защиты информации
НСД	несанкционированный доступ
НДВ	недокументированные возможности
ПДн	персональные данные
ПДЭК	постоянно действующая экспертная комиссия
СВТ	средства вычислительной техники
СЗИ	средства защиты информации
СКЗИ	средства криптографической защиты информации
СФ	среда функционирования
ТЗКИ	техническая защита конфиденциальной информации
УБПДн	угроза безопасности персональным данным

ПРИЛОЖЕНИЕ 2

Сравнительная таблица КСЗИ

№ п.п.	Название СЗИ	Производитель-ность межсетевого экрана	Производитель-ность антиви-руса	Производитель-ность средств обнаружения вторжения	Производитель-ность IPsecVPN	Шифро-вание по ГО-СТу	Стоимость	Полная стои-мость (с обновления-ми)
1	ALTELLNEO 120 UTM	2700Мбит/с	Нет данных	80 Мбит/с	150 Мбит/с	есть	130 000 руб.	139 600 руб.
2	WatchGuard XTM 515	2048Мбит/с	1536 Мбит/с	1638,4 Мб/с	250 Мб/с	нет	212 124.00 руб.	230 124 руб.
3	FortiGate-100 D	2500 Мбит/с	300 Мбит/с	950 Мбит/с	450 Мбит/с	нет	178897 руб	265 217 руб.
4	Checkpoint UTM-1 Edge N	1000 Мбит/с	Нет данных	180 Мбит/с	200Мбит/с	нет	103 032 руб.	141 192 руб.

Условные обозначения:

т Худший резу Данные отсутствую

ПРИЛОЖЕНИЕ 3

Отчет о результатах проведенной внутренней проверки ИСПДн «МИС»

1. Организационно-распорядительная документация	
Разработаны документы:	- Приказ об организации работы ПДн - Положение о персональных данных - Политика безопасности Подано уведомление в РОСКОМНАДЗОР. Учреждение занесено в реестр операторов персональных данных, регистрационный номер 74-13-000766
Отсутствует локальные нормативные акты:	- Перечень ИСПДн и ПДн - Модель угроз безопасности персональных данных и модель нарушителя безопасности в ИСПДн «Медицинская информационная система» - Техническое задание системы защиты персональных данных в ИСПДн «Медицинская информационная система» - Технологический процесс ИСПДн «Медицинская информационная система» - Информационное письмо о внесении изменений в РОСКОМНАДЗОР - Политика информационной безопасности - Положение об обработке ПДн - Положение о ПДЭК - Перечень сотрудников имеющих доступ к средствам СКЗИ - Перечень сотрудников режимное помещение - Перечень сотрудников, допущенных к ПДн - План внутренних проверок - Приказ о контролируемой зоне - Приказ об утверждении матрицы доступа - Приказ об утверждении мест хранения носителей ПДн - Приказ об утверждении мест хранения СКЗИ - Регламент резервного копирования и восстановления дан-

	ных - План мероприятий по обеспечению защиты ПДн - Инструкция о действиях сотрудников учреждения при возникновении нештатных ситуаций - Инструкция о парольной защите - Инструкция о режимных помещениях - Инструкция ответственного за обеспечение безопасности персональных данных в информационных системах - Инструкция ответственного за организацию обработки ПДн - Инструкция по антивирусной защите - Инструкция пользователя ИСПДн - Инструкция пользователя СКЗИ
2. Физическая защищенность	
Расположение	Г.Челябинск,ул.Пекинская,д.7
Сигнализация	В нерабочее время учреждение ставится на сигнализацию, охрана объекта осуществляемся ООО ОП «Витязь». Кабинеты оснащены тревожной кнопкой вызова охраны.
Помещения	Все кабинеты учреждения оборудованы запираемыми дверьми ,сейфами и запираемыми шкафами для хранения ПДн на бумажных носителях. При отсутствии работников в кабинете, кабинет запирается на ключ. В конце рабочего дня ключи от кабинетов убираются в сейф.
Видеонаблюдение	По периметру здания учреждения и в местах входа ведется круглосуточное видеонаблюдение
Ограждения	Все окна учреждения оборудованы решетками. Территория учреждения ограждена забором.
Пожарная сигнализация	Все помещения оборудованы пожарной сигнализацией.
3. Сведения о сети учреждения и вычислительной технике, используемой для хранения ПДн	
- Тип подключения к интернету – оптоволоконная сеть (FTTB) - Скорость передачи данных – 2 Мбит/с - Маршрутизатор – Mikrotik RouterBOARD 951Ui-2HnD	

- Коммутатор 16 портов – D-Link DGS-1016D -1 шт. - Коммутатор 8 портов – D-Link DGS-1008D - 6 шт. - Метод организации компьютеров в сети – Рабочая группа - Сервер - S5000B (S5367LNi): Core i7-4790 / 16 Гб / 2 x 2 Тб SATA RAID - АРМпользователей - A5000B-ITX (A5328LNi): Pentium G3250 / 2 Гб / 500 Гб / HD Graphics / DVDRW	
4. Программное обеспечении используемое при обработке ПДн	
Прикладное программное обеспечение	Microsoft Office 2007 Professional
4. Сведения о ИСПДн «Медицинская информационная система»	
Характеристики безопасности персональных данных	Специальная информационная система, в которой требуется обеспечить конфиденциальность, целостность и доступность ПДн, использующая реляционную СУБД Microsoft Access 2007
Структура информационной системы	Локальная информационная система, вся обработка ПДн производится в рамках одной локальной вычислительной сети, имеющей автоматизированные рабочие места (АРМ)
Способ обработки ПДн	смешанная обработка персональных данных с передачей полученной информации по внутренней сети юридического лица. Трансграничной передачи нет.
Категория ПДн	специальные
Цели обработки ПДн	1. Обработка персональных данных пациентов осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну. 2. Обработка персональных данных пациентов может осуществляться для статистических или иных научных целей при условии обязательного обезличивания персональных данных
Состав обрабатываемых ПДн	ФИО, пол, дата рождения, данные паспорта, данные миграционной карты, адрес прописки, адрес проживания, место

	работы, телефонный номер, анамнез, сведения о контактных лицах, диагноз, вид оказанной медицинской помощи, сроки оказания медицинской помощи, результаты лабораторных анализов и инструментального обследования, результат обращения за медицинской помощью, сведения об оказанных медицинских услугах
Носители ПДн	<u>В бумажном виде</u>: Талон амбулаторного пациента (форма № 025-12/у), медицинская карта амбулаторного больного (форма № 025/у-04), договор на оказание платных медицинских услуг, карта экстренного извещения об инфекционном заболевании (Ф № 58/у), извещение о новорожденном, рожденным ВИЧ – инфицированной матерью (Ф № 309/у), донесение о снятии с диспансерного наблюдения ребенка рожденного ВИЧ – инфицированной матерью (Ф № 310/у), донесение о подтверждении диагноза у ребенка рожденного ВИЧ – инфицированной матерью (Ф № 311/у), сертификат об обследовании на антитела к вирусу иммунодефицита человека, медицинское заключение по результатам медицинского освидетельствования иностранного гражданина или лица без гражданства на наличие инфекционных заболеваний, представляющих опасность для окружающих, журнал учета инфекционных заболеваний (Ф № 60/у).
	<u>В электронном виде</u>: RAID-массив IntelRaid
Режим обработки персональных данных	однопользовательская
Режим разграничения прав доступа пользователей	Без разграничения прав
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации по месту нахождения ГБУЗ «Областной Центр по профилактике и борьбе со СПИДом и инфекционными

	заболеваниями»
Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена	С АРМ пользователей имеется возможность подключения к сети Интернет
5. Технические средства защиты ПДн	
Антивирусная защита	Microsoft Security Essentials
Межсетевое экранирование	Отсутствует
Система обнаружения вторжений	Отсутствует
Средства от несанкционированного доступа	Отсутствуют
Средства доверенной загрузки	Отсутствует
Сертифицированное системное и прикладное программное обеспечение	Отсутствует
Лицензированное системное и прикладное программное обеспечение	Используется только лицензионное программное обеспечение

ПРИЛОЖЕНИЕ 4

Перечень ПДнв ИСПДн «МИС»

Содержание персональных данных	Субъекты персональных данных	Носители персональных данных		Основания для обработки персональных данных
		Бумажные	Электронные	
ИСПДн «Медицинская информационная система»				
ФИО, пол, дата рождения, данные паспорта, данные миграционной карты, адрес прописки, адрес проживания, место работы, телефонный номер, анамнез, сведения о контактных лицах, диагноз, вид оказанной медицинской помощи, сроки оказания медицинской помощи, результаты лабораторных анализов и инструментального обследования, результат обращения за медицинской помощью, сведения об оказанных медицинских услугах	Пациенты ГБУЗ «Областной Центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями»	Талон амбулаторного пациента (форма № 025-12/у), медицинская карта амбулаторного больного (форма № 025/у-04), договор на оказание платных медицинских услуг, карта экстренного извещения об инфекционном заболевании (Ф № 58/у), извещение о новорожденном, рожденным ВИЧ – инфицированной матерью (Ф № 309/у), донесение о снятии с диспансерного наблюдения ребенка рожденного ВИЧ – инфицированной матерью (Ф №	RAID-массив Intel Raid	Федеральный закон от 30.03.1995 № 38 –ФЗ «О предупреждении распространения в РФ заболевания вызываемого вирусом иммунодефицита человека (ВИЧ – инфекция), Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан Российского

Содержание персональных данных	Субъекты персональных данных	Носители персональных данных		Основания для обработки персональных данных
		Бумажные	Электронные	
		310/у), донесение о подтверждении диагноза у ребенка рожденного ВИЧ – инфицированной матерью (Ф № 311/у), сертификат об обследовании на антитела к вирусу иммунодефицита человека, медицинское заключение по результатам медицинского освидетельствования иностранного гражданина или лица без гражданства на наличие инфекционных заболеваний, представляющих опасность для окружающих, журнал учета инфекционных заболеваний (Ф № 60/у).		Федерации», СП 3.1.5.2826-10 «Профилактика ВИЧ-инфекции», приказ МЗ России от 08.11.2012 № 689Н «об утверждении порядка оказания медицинской помощи взрослому населению при заболевании, вызываемом вирусом иммунодефицита человека (ВИЧ – инфекции)», приказ МЗ России от 16.09.2003г. № 442 «Об утверждении учетных форм для регистрации детей, рожденных ЫИЧ – инфицированными матерями», приказ МЗ

Содержание персональных данных	Субъекты персональных данных	Носители персональных данных		Основания для обработки персональных данных
		Бумажные	Электронные	
				России от 24.12.2012г. № 1511Н, «Об утверждении стандарта оказания первичной медико-санитарной помощи при болезни вызванной вирусом иммунодефицита человека (ВИЧ – инфекцией), Постановление правительства РФ от 25.11.1995г. № 1158 «Об утверждении требований к сертификации об отсутствии ВИЧ – инфекции, предъявляемому иностранным гражданам и лицам без гражданства при их обращении за визой на въезд в Российскую

Содержание персональных данных	Субъекты персональных данных	Носители персональных данных		Основания для обработки персональных данных
		Бумажные	Электронные	
				Федерацию на срок свыше трех месяцев», Постановление Правительства РФ от 04.10.2012 № 1006 «Об утверждении Правил предоставления медицинскими организациями платных медицинских услуг», приказ МЗ Челябинской области от 19.07.2013г. № 1159 «О совершенствовании оказания медицинской помощи больным ВИЧ инфекцией в Челябинской области», приказ МЗ Челябинской области от 31.01.2013г., № 147/18 «О

Содержание персональных данных	Субъекты персональных данных	Носители персональных данных		Основания для обработки персональных данных
		Бумажные	Электронные	
				повышении эффективности работы по медицинскому освидетельствованию иностранных граждан и лиц без гражданства».

ПРИЛОЖЕНИЕ 5

Модель УБПДн в ИСПДн «МИС»

№ п/п	Наименование угрозы	Вероятность реализации (Y_2)	Возможность реализации (Y)	Опасность	Актуальность	Обоснование актуальности (неактуальности)
1. Угрозы утечки информации по техническим каналам						
1.1	Утечка акустической (рече-	Маловероятно (0)	Низкая (0,25)	Низкая	Неактуальна	Реализация данной угрозы маловеро-

№ п/п	Наименование угрозы	Вероятность реализации (Y_2)	Возможность реализации (Y)	Опасность	Актуальность	Обоснование актуальности (неактуальности)
	вой) информации					ятна, так как в ИСПДн отсутствует голосовой ввод ПДн, а также их воспроизведение акустическими средствами
1.2	Утечка видовой информации	Низкая (2)	Средняя (0,35)	Низкая	Неактуальна	Приняты следующие меры: Расположение АРМ, исключающее визуальный доступ к мониторам Жалюзи на окнах
1.3	Утечка информации по каналам ПЭМИН	Маловероятно (0)	Низкая (0,25)	Низкая	Неактуальна	Реализация данной угрозы маловероятна, так как все ТС ИСПДн находятся в пределах КЗ, а паразитный сигнал маскируется множеством других паразитных сигналов элементов, не входящих в ИСПДн. Кроме того, перехват по каналам ПЭМИН требует высоких затрат в связи с применением дорогостоящего оборудования и должен осуществляться специалистом с соответствующим образованием
2. Угрозы НСД						

№ п/п	Наименование угрозы	Вероятность реализации (Y_2)	Возможность реализации (Y)	Опасность	Актуальность	Обоснование актуальности (неактуальности)
2.1. Угрозы несанкционированного физического доступа к элементам ИСПДн						
2.1.1	Хищение носителей информации	Высокая (10)	Высокая (0,75)	Средняя	Неактуальна	Угроза неактуальна вследствие соблюдения требований к хранению носителей и наличия внутриобъектового режима
2.1.2	Хищение ключей, паролей и иных атрибутов доступа	Высокая (10)	Высокая (0,75)	Средняя	Неактуальна	Угроза неактуальна вследствие соблюдения требований к хранению ключей и паролей, наличия внутриобъектового режима
2.1.3	Несанкционированное копирование, модификация, уничтожение информации	Высокая (10)	Высокая (0,75)	Высокая	Неактуальна	Угроза неактуальна вследствие осуществления резервного копирования информации и наличия внутриобъектового режима
2.1.4	НСД к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Высокая (10)	Высокая (0,75)	Высокая	Неактуальна	Угроза неактуальна вследствие соблюдения установленного порядка проведения технических работ в ИСПДн, а также их учета
2.1.5	Хищение ПЭВМ	Высокая (10)	Высокая (0,75)	Высокая	Неактуальна	Угрозы неактуальны вследствие наличия внутриобъектового режима
2.1.6	Вывод из строя узлов ПЭВМ,	Высокая (10)	Высокая (0,75)	Средняя	Неактуальна	

№ п/п	Наименование угрозы	Вероятность реализации (Y_2)	Возможность реализации (Y)	Опасность	Актуальность	Обоснование актуальности (неактуальности)
	каналов связи					
2.1.7	Несанкционированное отключение СЗИ	Высокая (10)	Высокая (0,75)	Средняя	Неактуальна	
2.2. Угрозы НСД с применением стандартных средств ОС и специализированных программных средств						
2.2.1	Действия вредоносных программ (компьютерных вирусов)	Высокая (10)	Высокая (0,75)	Средняя	**Актуальна**	Угроза актуальна вследствие отсутствия сертифицированных средств антивирусной защиты информации
2.2.2	Перехват паролей или идентификаторов в ходе загрузки ОС, модификация BIOS, перехват управления загрузкой	Высокая (10)	Высокая (0,75)	Высокая	**Актуальна**	Угрозы актуальны вследствие отсутствия средств защиты от несанкционированного доступа
2.2.3	Доступ в операционную среду (локальную ОС отдельного ТС ИСПДн) с возможностью выполнения НСД вызовом штатных процедур или запуска специально разработанных	Высокая (10)	Высокая (0,75)	Высокая	**Актуальна**	

№ п/п	Наименование угрозы	Вероятность реализации (Y_2)	Возможность реализации (Y)	Опасность	Актуальность	Обоснование актуальности (неактуальности)
	программ					
2.3. Угрозы, реализуемые посредством уязвимостей ПО						
2.3.1	НДВ системного ПО	Маловероятно (0)	Низкая (0,25)	Средняя	Неактуальна	Приняты следующие меры: ТС ИСПДн приобретены у доверенного поставщика На АРМ установлено лицензионное ПО и ОС
2.3.2	НДВ прикладного ПО (в том числе предназначенного для обработки ПДн)	Маловероятно (0)	Низкая (0,25)	Средняя	Неактуальна	
2.4. Угрозы непреднамеренных действий пользователей ИСПДн и нештатных ситуаций						
2.4.1	Утрата ключей, паролей и иных атрибутов доступа	Высокая (10)	Высокая (0,75)	Средняя	Неактуальна	Угроза неактуальна вследствие хранения паролей на различных носителях и осведомленности сотрудников о мерах, которые необходимо принять при утере ключей и атрибутов доступа
2.4.2	Непреднамеренное разглашение, модификация или уничтожение информации сотрудниками	Высокая (10)	Высокая (0,75)	Высокая	Неактуальна	Угроза неактуальна вследствие осведомленности пользователей о правилах работы с элементами ИСПДн и об ответственности за распространение ПДн без согласия субъекта
2.4.3	Установка стороннего ПО, не	Высокая (10)	Высокая (0,75)	Средняя	Неактуальна	Угроза неактуальна вследствие разгра-

№ п/п	Наименование угрозы	Вероятность реализации (Y_2)	Возможность реализации (Y)	Опасность	Актуальность	Обоснование актуальности (неактуальности)
	связанного с исполнением служебных (трудовых) обязанностей					ничения прав на установку ПО и (или) осведомленности пользователей о правилах работы с элементами ИСПДн
2.4.4	Непреднамеренное отключение СЗИ	Высокая (10)	Высокая (0,75)	Средняя	Неактуальна	Угроза неактуальна вследствие осведомленности пользователей о правилах работы с элементами ИСПДн и СЗИ в ее составе
2.4.5	Выход из строя технических и программных средств ИСПДн	Высокая (10)	Высокая (0,75)	Высокая	Неактуальна	Угроза неактуальна вследствие резервирования ключевых элементов ИСПДн и (или) установленного регламента
2.4.6	Сбой системы электроснабжения	Высокая (10)	Высокая (0,75)	Высокая	Неактуальна	Неактуальны вследствие использования истопников бесперебойного питания для критически важных элементов ИСПДн
2.4.7	Нештатные ситуации	Средняя (2)	Средняя (0,35)	Высокая	Неактуальна	Принятые меры: Установлена система пожарной сигнализации Сотрудники осведомлены о мерах по-

№ п/п	Наименование угрозы	Вероятность реализации (Y_2)	Возможность реализации (Y)	Опасность	Актуальность	Обоснование актуальности (неактуальности)
						жарной безопасности Данные меры достаточны ввиду осведомленности сотрудников о мерах обеспечения безопасности ИСПДн при возникновении различных нештатных ситуаций
2.5. Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия						
2.5.1	Анализ сетевого трафика для изучения логики работы ИСПДн, выявления протоколов, портов, перехвата данных, их подмены	Средняя (5)	Средняя (0,35)	Средняя	**Актуальна**	Угроза актуальна вследствие отсутствия сертифицированного межсетевого экрана
2.5.2	Применение специальных программ дл выявления пароля (IP-спуффинг, разные виды перебора)	Высокая (10)	Высокая (0,75)	Средняя	**Актуальна**	Угроза актуальна вследствие отсутствия сертифицированного межсетевого экрана
2.5.3	Внедрение специализированных троянов, вредоносных программ	Высокая (10)	Высокая (0,75)	Средняя	**Актуальна**	Угроза актуальна вследствие отсутствия сертифицированных средств антивирусной защиты

№ п/п	Наименование угрозы	Вероятность реализации (Y_2)	Возможность реализации (Y)	Опасность	Актуальность	Обоснование актуальности (неактуальности)
2.5.4	Удаленный запуск приложений	Высокая (10)	Высокая (0,75)	Высокая	**Актуальна**	Угроза актуальна вследствие отсутствия сертифицированного межсетевого экрана, средства антивирусной защиты
2.5.5	Реализация угрозы «отказа в обслуживании»	Высокая (10)	Высокая (0,75)	Низкая	**Актуальна**	Угрозы актуальны вследствие отсутствия сертифицированного межсетевого экрана
2.5.6	Навязывание ложного маршрута путем несанкционированного изменения маршрутно-адресных данных	Высокая (10)	Высокая (0,75)	Средняя	**Актуальна**	Угрозы актуальны вследствие отсутствия сертифицированного межсетевого экрана
2.5.7	Сканирование сети для изучения логики работы ИСПДн, выявления протоколов, портов	Высокая (10)	Высокая (0,75)	Средняя	**Актуальна**	
2.5.8	Подмена доверенного объекта в сети с присвоением его прав доступа, внедрение ложного объекта сети	Высокая (10)	Высокая (0,75)	Средняя	**Актуальна**	

№ п/п	Наименование угрозы	Вероятность реализации (Y_2)	Возможность реализации (Y)	Опасность	Актуальность	Обоснование актуальности (неактуальности)
2.6. Угрозы НСД к СКЗИ и документации к ним						
2.6.1	Внесение негативных функциональных возможностей в технические и программные компоненты криптосредства и СФК, в том числе с использованием вредоносных программ	Высокая (10)	Высокая (0,75)	Высокая	Неактуальна	Угрозы неактуальны вследствие соблюдения установленного порядка работы с СКЗИ, а также порядка хранения СКЗИ и документации к ним
2.6.2	Внесение несанкционированных изменений в документацию на криптосредство, технические и программные компоненты СФК	Высокая (10)	Высокая (0,75)	Средняя	Неактуальна	
2.6.3	Хищение компонентов СКЗИ и документации к ним	Высокая (10)	Высокая (0,75)	Высокая	Неактуальна	