Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет математики и информатики
Кафедра информационных и управляющих систем
Направление подготовки 09.03.02 – Информационные системы и технологии
Направленность (профиль) образовательной программы: Безопасность информационных систем

ДОПУСТИТЬ К ЗАЩИТЕ
Зав. кафедрой
_____ А.В. Бушманов
«_____»_____2018 г.

БАКАЛАВРСКАЯ РАБОТА

на тему: Комплексная защита информации для предприятия ЗАО «АНК»

Исполнитель
студент группы 455об _____ А.А. Андреев
(подпись, дата)

Руководитель
доцент, канд.техн.наук _____ С.Г. Самохвалова
(подпись, дата)

Консультант по
безопасности и экологичности
доцент, канд. техн наук _____ А.Б. Булгаков
(подпись, дата)

Нормоконтроль
инженер кафедры _____ В.В. Романико
(подпись, дата)

Благовещенск 2018

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет математики и информатики
Кафедра информационных и управляющих систем

УТВЕРЖДАЮ
Зав.кафедрой
_____А.В.Бушманов
«_____»_____2018 г.

З А Д А Н И Е

К бакалаврской работе студента Андреева Алексея Александровича.

1. Тема бакалаврской работы: Комплексная система защиты информации для предприятия ЗАО «АНК».

(утверждено приказом от 23.04.2018 № 914-уч)

2. Срок сдачи студентом законченной работы 22.06.2018 г.
3. Исходные данные к бакалаврской работе: отчет по преддипломной практике.
4. Содержание бакалаврской работы: анализ деятельности предприятия, описание комплексной системы защиты, этапы построение комплексной системы защиты, модернизация действующей системы защиты, рассмотрение аспектов безопасности жизнедеятельности.
5. Перечень материалов приложения: 2 таблицы, 22 рисунка, 1 приложение.
6. Консультант по безопасности и экологичности Булгаков Андрей Борисович, доцент, канд. техн. наук.
7. Дата выдачи задания 09.05.2018 г.

Руководитель бакалаврской работы Самохвалова Светлана Генадьевна, доцент, канд. техн. наук.

Задание принял к исполнению (дата): _____ Андреев А.А.

РЕФЕРАТ

Бакалаврская работа содержит 80 с., 22 рисунка, 2 таблицы, 17 источников, 1 приложение.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА, АППАРАТНОЕ ОБЕСПЕЧЕНИЕ, СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Для данной бакалаврской работы объектом исследования было выбрано создание комплексной системы защиты информации.

Целью работы является создание комплексной системы защиты информации для подразделения ЗАО «АНК» поликлиника «АНКОР».

Работа выполнялась последовательно в соответствие со следующими этапами: анализ предприятия, описание комплексной системы защиты, этапы построения комплексной системы защиты, модернизация существующей системы защиты, проведения анализа рисков и оценки сохранения конфиденциальности информации, а также исследование аспектов безопасности жизнедеятельности.

Результатом выполнения бакалаврской работы модернизированная комплексной системы защиты информации, которая будет обеспечивать безопасность на предприятии.

НОРМАТИВНЫЕ ССЫЛКИ

В бакалаврской работе использованы следующие стандарты и нормативные документы:

ГОСТ 19.004-80 «ЕСПД. Термины и определения»

ГОСТ 19.105-78 «ЕСПД. Требования к программным документам, выполненным печатным способом»

ГОСТ 19.508-79 «Руководство по техническому обслуживанию. Требования к содержанию и оформлению»

ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»

СТО СМК 4.2.3.05-2011 Стандарт организации. Оформление выпускных квалификационных и курсовых работ (проектов)

ГОСТ Р 51242-98 Конструкции защитные механические и электромеханические для дверных и оконных проемов. Технические требования и методы испытаний на устойчивость к разрушающим воздействиям

ГОСТ 12.1.005-88 Система стандартов безопасности труда (ССБТ). Общие санитарно-гигиенические требования к воздуху рабочей зоны

СанПиН 2.2.2/2.4.1340-03 СанПиН 2.2.2/2.4.1340-03 Гигиенические требования к персональным электронно-вычислительным машинам и организации работы

СанПиН 2.1.7.1322-03 СанПиН 2.1.7.1322-03 Гигиенические требования к размещению и обезвреживанию отходов производства и потребления.

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящей бакалаврской работе использованы следующие сокращения:

АНК – Амурская нефтяная компания;

АРМ – автоматизированное рабочее место;

АС – автоматизированная система;

АТС – автоматическая телефонная станция;

БД – база данных;

БЖД – безопасность жизнедеятельности

ЗАО – закрытое акционерное общество;

ЗИ – защита информации;

ИТЗ – инженерно-техническая защита;

КЗ – контролируемая зона;

КСЗИ – комплексная система защиты информации;

ООО – общество с ограниченной ответственностью;

ОТСС – основные технические средства и система;

ПО – программное обеспечение;

ПЭМИН – побочные электромагнитные излучения и наводки;

ТСПИ – технические средства приема, обработки информации;

СЗИ – средства защиты информации;

СКУД – система контроля управления доступом

ТС – технические средства;

НСД – несанкционированный доступ.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Вступление человечества в XXI век знаменуется бурным развитием информационных технологий во всех сферах общественной жизни. Информация все в большей мере становится стратегическим ресурсом государства, производительной силой и дороги товаром. Это не может не вызывать стремления государств, организаций и отдельных граждан получить преимущества за счет овладения информацией, недоступной оппонентам, а также за счет нанесения ущерба информационным ресурсам противника (конкурента) и защиты своих информационных ресурсов.

Информационный ресурс становится одним из главных источников экономической эффективности предприятия. Фактически наблюдается тенденция, когда все сферы жизнедеятельности предприятия становятся зависимыми от информационного развития, в процессе которого они сами порождают информацию и сами же ее потребляют [1]. На современном этапе развития основными угрозами безопасности предприятия являются угрозы в сфере информационного обеспечения. Последствиями успешного проведения информационных атак могут стать компрометация или искажение конфиденциальной информации, навязывание ложной информации, нарушение установленного регламента сбора, обработки и передачи информации, отказы и сбои в работе технических систем, вызванные преднамеренными и непреднамеренными действиями, как со стороны конкурентов, так и со стороны преступных сообществ, организаций и групп. К одной из наиболее важных задач в области безопасности предприятия следует отнести создание КСЗИ. С каждым годом технические возможности злоумышленников все больше и больше совершенствуются. Соответственно, системы безопасности должны быть готовы дать отпор этим угрозам. Следовательно, необходимо стремиться построить такую систему безопасности, которая не только не устареет, но и могла бы модернизироваться, чтобы стать как можно надежнее и современнее.

Система защиты информации базируется на таких составляющих как, организационная, правовая, инженерно-техническая защита.

Целью бакалаврской работы является создание комплексной системы защиты информации для подразделения ЗАО «АНК» поликлиника ООО «АНКОР», которая будет решать задачи по защите информации. В рамках данной цели необходимо решить следующие задачи:

- провести анализ объекта;
- проанализировать документооборот предприятия;
- проанализировать бизнес-процессы предприятия;
- изучить комплексную защиту информации предприятия;
- модернизировать существующую защиту предприятия;
- провести оценку сохранения конфиденциальности информации.

1 АНАЛИЗ ДЕЯТЕЛЬНОТСТИ ПРЕДПРИЯТИЯ

1.1 Общая характеристика

Объектом исследования, является одно из подразделений ЗАО «АНК», поликлиника ООО «АНКОР», которая оказывает как платные, так и бесплатные медицинские услуги. Организация проводит различные медицинские осмотры при устройстве на работу с оформлением личных медицинских книжек, для ГИБДД (при получении и смене прав), при поступлении в средние и высшие учебные заведения, для получения санаторно-курортных справок и карт. Поликлиника обслуживает не только частных лиц, но и заключает договора с предприятиями по разумным ценам, производится выдача больничных листов, возможен выезд специалистов на дом.

1.2 Организационная структура

В структуру холдинга входят следующие комплексы:

– нефтегазовый комплекс;

– гостиничный комплекс «АНКОР»;

– агрокомплекс;

– строительный холдинг;

– поликлиника ООО «АНКОР».

Нефтегазовый комплекс – ЗАО «АНК» реализует оптом и мелким оптом ГСМ, а так же предлагает транзитные поставки ж/д транспортом всех видов светлых нефтепродуктов по ценам заводов-изготовителей.

Гостиничный комплекс «АНКОР» – предоставление гостиничных услуг для временного проживания граждан.

Агрокомплекс – «Агрохолдинг АНК» это выращивание сельскохозяйственной продукции, которое составляет до 30 тысяч тон сои. Сельское хозяйство для Агрохолдинга это не только обработка земли и получение сельхозпродукции. Это еще и переработка. На новом маслоэкстракционном заводе, построенном в 2014 году, планируется перерабатывать до 200 тонн соевой продукции в день.

Большим направлением в работе «Агрофирмы АНК» является молочное животноводство. В день здесь надаивают до 15 тонн молока. Коровы красно-пестрой породы дают отличную продукцию, жирность молока составляет 4,1 процента на литр.

Строительный холдинг – Холдинг АНК осуществляет практически полный цикл подготовки сырья и материалов для строительства. Помимо сырья, холдинг занимается продажей недвижимости.

Поликлиника «АНКОР» – предоставление качественных медицинских услуг не только персоналу холдинга, но и всем желающим, как частным, так и юридическим лицам.

Организационная структура холдинга представлена на рисунке 1.

Рисунок 1 – Организационная структура ЗАО «АНК»

В структуру поликлиники входят отделы:

– отдел оказания медицинских услуг;

– регистратура;

– бухгалтерия;

– вспомогательный персонал;

– отдел кадров.

Руководство осуществляется главным врачом.

Функции отделов:

– отдел оказания медицинских услуг отвечает за: организацию и проведение комплекса профилактических мероприятий, направленных на снижение заболеваемости, инвалидности и смертности среди населения, проживающего в районе обслуживания, а также среди работающих на прикрепленных предприя-

тиях; проведение профилактических медицинских осмотров населения с целью выявления заболеваний в начальных стадиях и проведения необходимых лечебно-профилактических и оздоровительных мероприятий; оказание квалифицированной специализированной медицинской помощи населению непосредственно в поликлинике;

– регистратура регистрирует новых клиентов, записывает их на приём к врачу (обследования, комиссии и т.д.) в соответствии с расписанием работы учреждения, уведомляет по телефону уже записанных клиентов об изменении в расписании, выдает справочную информацию, связанную с расписанием;

– бухгалтерия производит выплату заработной платы, занимается ведением документооборота организации, формированием и сдачей налоговой отчетности, взаимодействует со всеми отделами службы;

– вспомогательный персонал, поддерживает работоспособность организации;

– главный врач осуществляет общее управление организацией, координирует работу всех отделов, определяет политику развития;

– заместитель главного врача выполняет его функции в момент его отсутствия, а так же докладывает ему о проделанной работе персонала;

– отдел кадров осуществляет документирование трудовой деятельности работников, ведение установленной кадровой документации (прием, увольнение, перевод, отпуска, учеба, аттестация, командировки и др.), организацию ведения и хранения личных дел и трудовых книжек работников, других документов в соответствии с номенклатурой дел отдела кадров, подготовку документов для начисления пенсий медицинским работникам и рабочему персоналу.

Организационная структура поликлиники ООО «АНКОР» представлена на рисунке 2.

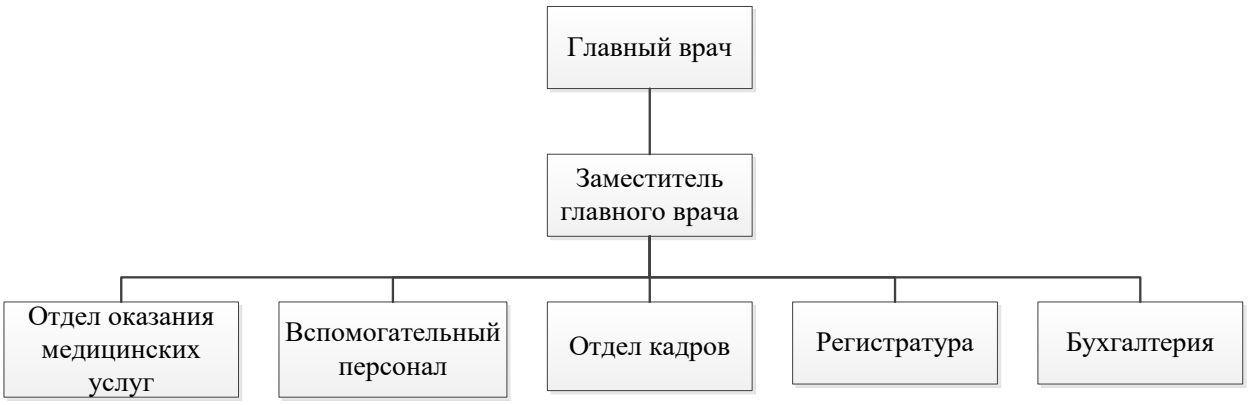

Рисунок 2 – Организационная структура поликлиники ООО «АНКОР»

1.3 Функциональная модель

Функциональная структура управления – это структура, сформированная в соответствии с основными направлениями деятельности организации, где подразделения объединяются в блоки [2,3].

Функция – самая существенная характеристика любой системы, отражает её предназначение, то, для чего она нужна. Подобные модели оперируют, прежде всего, с функциональными параметрами. Графическим представлением этих моделей служат блок-схемы. Они отображают порядок действий, направленных на достижение заданных целей. Функциональной моделью является абстрактная модель.

На функциональной модели можно увидеть информацию о взаимодействии организации с внешней средой, взаимодействии отделов внутри организации, о потоках информации, как вне организации, так и внутри.

Как и на любой функциональной модели, на функциональной модели поликлиники существуют управляющая информация, механизмы, входы и выходы.

Управляющей информацией является Конституция РФ и правила приема пациента. На вход в систему идет пациент, его паспорт, полис ОМС и СНИЛС. На выход идет пациент с рецептом и рекомендациями врача[4].

При поиске амбулаторной карты на вход идут СНИСЛ пациента, его полис ОМС и паспорт. Если амбулаторная карта найдена, то она идет на оформ-

ление записи пациента на прием и выдачи пациенту талона на прием. Если амбулаторная карта не найдена, то на основании паспорта, полиса и СНИЛС создается новая амбулаторная карта, а потом она так же идет на оформление записи на прием. На оформление записи на прием так же идет информация о пациенте, удобное время для его записи на прием, какой врач ему необходим и т.д. После оформления записи на прием пациенту выдается талон на прием. С этим талоном пациент отправляется на прием к врачу. Амбулаторную карту пациента врачу приносит санитарка. После постановки диагноза, врач выписывает пациенту рецепт, дает рекомендации по дальнейшему лечению и, если нужно, выписывает направление на сдачу анализов. Результаты анализов санитарка приносит врачу, который их вклеивает в амбулаторную карту пациента. На основе данных построим функциональную модели и декомпозицию этой функциональной модели, изображенные на рисунках 3 – 4.

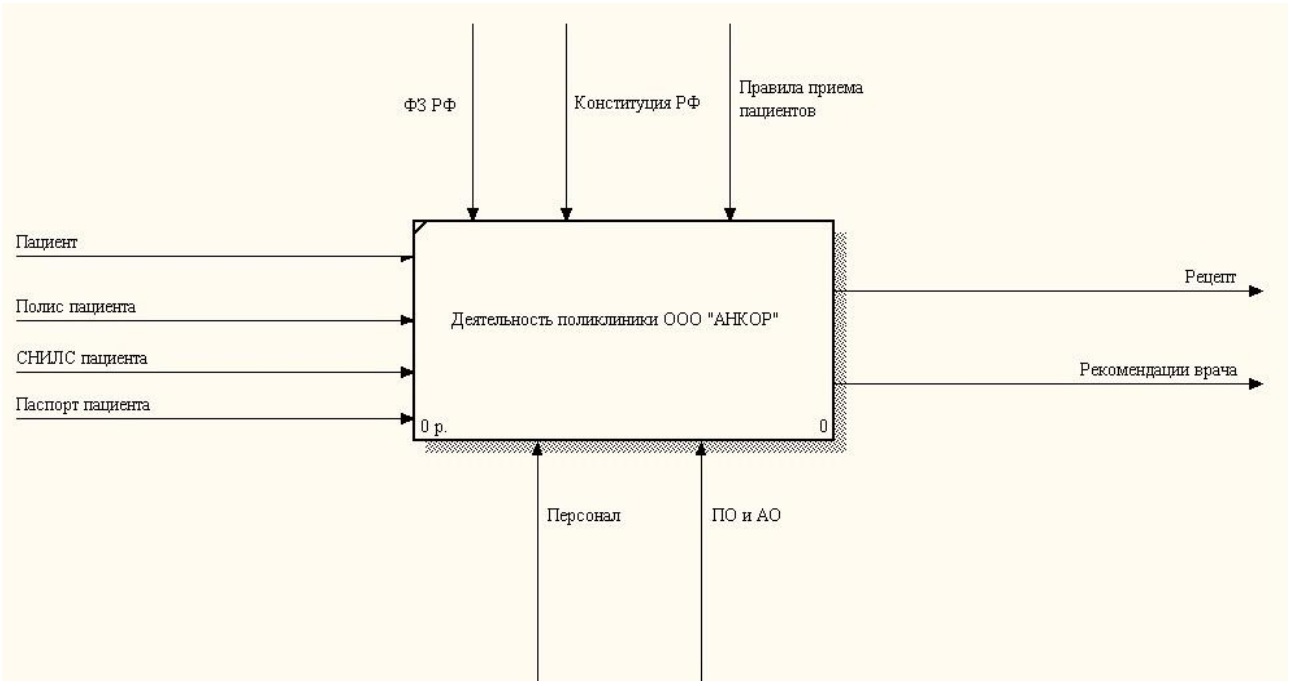

Рисунок 3 – Функциональная модель поликлиники ООО «АНКОР»

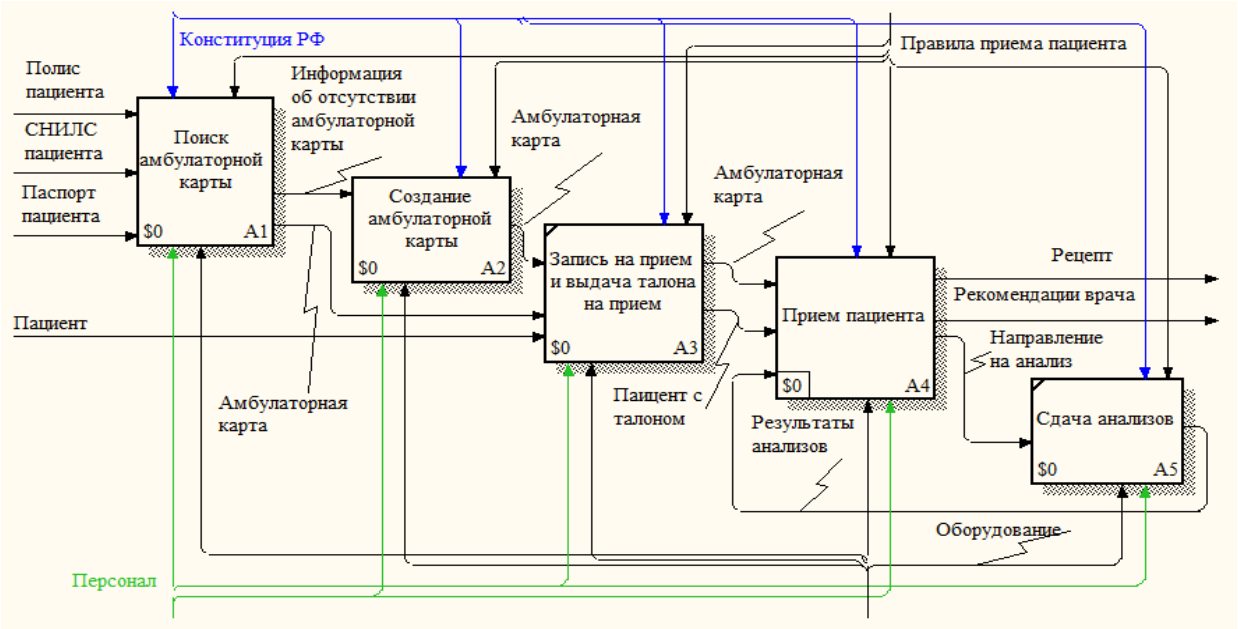

Рисунок 4 – Декомпозиция функциональной модели поликлиники ООО «АНКОР»

1.4 Документооборот

«Документооборот», или «организация движения документов» между пользователями системы, имеет большое значение для безбумажной технологии. Для обеспечения своевременной обработки текущей документации применяется система документооборота, которая позволяет отражать все операции, производимые внутри предприятия.

Документооборот – это движение документов с момента их получения или создания до завершения исполнения, отправки адресату или сдачи их на хранение.

Организация документооборота на предприятии должна обеспечить: строгий учет поступившей и отправляемой документации; ежедневный контроль по каждому документу за своевременным исполнением; надлежащее хранение входящей и исходящей документации.

1.4.1 Внешний документооборот

Внешний документооборот показывает взаимодействие поликлиники ООО «АНКОР» с внешними объектами.

Внешними объектами являются:

– управление Пенсионного фонда РФ (УПФР) по Амурской области;

– управление Федеральной налоговой службы (УФНС) РФ по Амурской области;

– министерство здравоохранения Амурской области;

– ФГУП «Почта России»;

– холдинг ЗАО «АНК».

Схема документооборота данного предприятия с внешними объектами представлена на рисунке 5.

Рисунок 5 – Внешний документооборот поликлиники ООО «АНКОР»

Контроль над деятельностью предприятия со стороны выше стоящих организаций и государственных органов происходит посредством нормативных документов (инструкций, положений), приказов, распоряжений и указаний. В вышестоящие организации предприятие отправляет отчеты о проделанной работе.

В государственные органы предприятие представляет отчеты, связанные с деятельностью организации (финансовая отчетность, налоговая отчетность, ведомости об уплате единого социального налога, отчеты страховых тарифов, об отчислении денежных средств в Пенсионный фонд РФ).

Бухгалтерия является ответственным за своевременное предоставление ежеквартальных и годовых отчетов в налоговую инспекцию и пенсионный фонд. УФНС РФ по Амурской области обеспечивает отчисление организацией всех налогов, контролирует ее деятельность, предоставляет форму подачи декларации о доходах.

УПФР в г. Благовещенске регулирует взаимоотношения работодателя и работника, обеспечивая отчисления единого социального налога на заработную плату трудящегося, пополняющего денежные средства пенсионного фонда, из которого производятся пенсионные выплаты.

Отдел кадров передает в УПФР и в фонд социального страхования соответствующие сведения о сотрудниках. В свою очередь, Пенсионный фонд изготавливает и передает пенсионные удостоверения.

Для хранения денежных средств, осуществления безналичных расчетов и клиентами организация взаимодействует с банками, в числе которых числится «Сбербанк», «ВТБ 24». Банки предоставляют компании кредитные линии, расчетные счета. Через банки осуществляется оплата коммунальных услуг, расчет с поставщиками, строительными и транспортными компаниями, выплата заработной платы сотрудникам предприятия. Ежедневно бухгалтер отправляет в банк платежные поручения, банковские выписки.

1.4.2 Внутренний документооборот

Все документы внутри предприятия распределяются в соответствии с функциями подразделений и исполнителей, которые закреплены в положениях о структурных подразделениях и в должностных инструкциях исполнителей.

Внутренний документооборот объединяет информацию, циркулирующую внутри самого предприятия.

Основными этапами обработки внутренних документов являются:

– подготовка проекта внутреннего документа;

– согласования документа;

– утверждение документа;

– регистрация документа;

– рассылка документов по подразделениям;

– контроль исполнения документа.

Большинство исходящих документов являются ответом организации на соответствующие входящие документы.

К внутренним документам относятся следующие виды документов:

– организационные (устав организации, должностные инструкции, положения о структурных подразделениях);

– распорядительные (постановления, распоряжения, приказы);

– справочно-информационные (акты, анкеты, справки);

– личные (автобиографии, заявления, доверенности).

Главный врач контролирует и координирует всю деятельность предприятия. Сюда поступают оперативные отчеты по деятельности, на основе которых главный врач принимает решения и координирует деятельность подразделений различными приказами и распоряжениями. Заместитель главного врача выполняет обязанности главного в моменты его отсутствия, а так же составляет отчеты о проделанной работе.

Отдел кадров взаимодействует со структурными подразделениями предприятия. В данный отдел поступает вся информация о сотрудниках. Здесь есть хранилище данных – база данных сотрудников и подразделений, в которую вносятся: штатное расписание, табели рабочего времени, больничные листы. Также в отделе кадров осуществляется подбор кадров.

Бухгалтерия получает от руководства приказы на распоряжение денежными средствами в конкретных целях (закупка оборудования, ремонт помещений и т.д.) далее занимается проведением множества платежей предприятия. Также работники бухгалтерии наряду с руководством занимаются планированием и распределением финансовых ресурсов. Сотрудники бухгалтерии подготавливают ежеквартальные и ежегодные налоговые отчеты (НДС, налог на прибыль), бухгалтерские и прочие отчеты.

Регистратура занимается вопросами оформления и информирования клиентов для прохождения медицинских осмотров и получением различной ква-

лифицированной медицинской помощи и передает заявки в отдел оказания медицинских услуг.

Отдел оказания медицинских услуг предоставляет график работы врачей, и получает от регистратуры заявки на прием клиентов.

В случае если есть необходимость оказания выездной медицинской помощи клиентам или организациям, вспомогательный персонал принимает непосредственное участие в этом.

Внутренний документооборот изображен на рисунке 6.

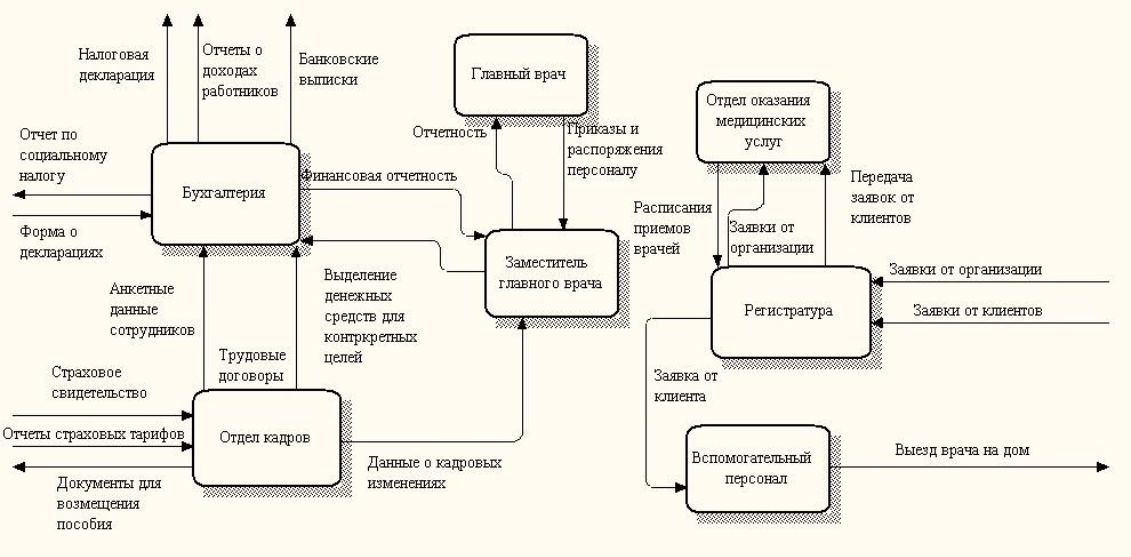

Рисунок 6 – Внутренний документооборот поликлиники ООО «АНКОР»

1.5 Объект и предмет защиты

Основными объектами защиты в организации являются:

– сотрудники учреждения (так как эти лица допущены к работе с охраняемой законом информацией (медицинская тайна, персональные данные) либо имеют доступ в помещения, где эта информация обрабатывается);

– информационные ресурсы, содержащие конфиденциальную информацию, персональные данные, сведения ограниченного распространения;

– системы и средства, обрабатывающие конфиденциальную информацию (технические средства приема, обработки, хранения и передачи информации ТСПИ);

– ТСПИ размещенные в помещениях обработки секретной конфиденциальной информации.

Конфиденциальная_информация – это документированная информация, владельцами которой являются государственные, коммерческие и другие организации и учреждения [5]. Эта информация содержит:

– сведения, содержащие информацию о паспортных данных пациентов;

– данные страхового полиса ОМС;

– данные амбулаторной карты (состояние здоровья, результаты исследований пациента);

– предметом защиты информации в организации являются носители информации, на которых зафиксированы, отображены защищаемые сведения:

a) личные дела пациентов в бумажном и электронном (база данных пациентов) виде;

b) личные дела сотрудников в бумажном и электронном виде;

c) реестр ОМС;

d) другие медицинские сведения, классифицируемые как специальные медицинские данные;

e) приказы, положения, постановления, соглашения, инструкции и обязательства о неразглашении, распоряжения, планы, договоры, отчеты, ведомость ознакомления с положением о конфиденциальной информации и другие документы, в бумажном и электронном виде.

Документы, которые имеют конфиденциальный характер и требующие защиты:

– результаты анализов;

– документы о направлении на исследования;

– амбулаторные карты пациентов;

– квитанции об уплате стоимости услуг;

– выписки рецептов;

– материалы кадрового делопроизводства;

– внутренние приказы и распоряжения;

– персональные данные сотрудников;

– схемы информационных потоков и коммуникаций;

– должностные инструкции по отдельным подразделениям;

– активационные коды на лицензионное по;

– архитектура информационной системы;

– приказ о вводе в эксплуатацию пэвм;

– приказ о категорировании и классификации объектов вычислительной техники;

– положение об отделе администрирования и технического сопровождения информационных систем;

– приказ о введении режима коммерческой тайны на предприятии;

– положение о группе инженерно-технической защиты информации;

– положение о структуре службы безопасности;

– положение о компьютерной сети поликлиники;

– положение об охранно-пропускном режиме предприятия;

– положение об отделе защиты информации;

– положение о системном администрировании компьютерной сети поликлиники;

– должностные инструкции сотрудников предприятия;

– список постоянных пользователей определенного ПЭВМ, допущенных в помещение, и установленные им права доступа к информации и техническим ресурсам ПЭВМ;

– перечень сотрудников учреждения, имеющих доступ к средствам автоматизированной системы (АС) и к обрабатываемой на них информации;

– трудовые договоры сотрудников, работающих с конфиденциальной информацией;

– договоры предоставления услуг;

– бюджет поликлиники;

– договоры, заключенные с пациентами и организациями;

– договоры, заключенные с поставщиками оборудования.

1.6 Угрозы защищаемой информации

Угроза информационной безопасности – совокупность условий и факторов, создающих опасность нарушения информационной безопасности.

Под угрозой (в общем) понимается потенциально возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам [6].

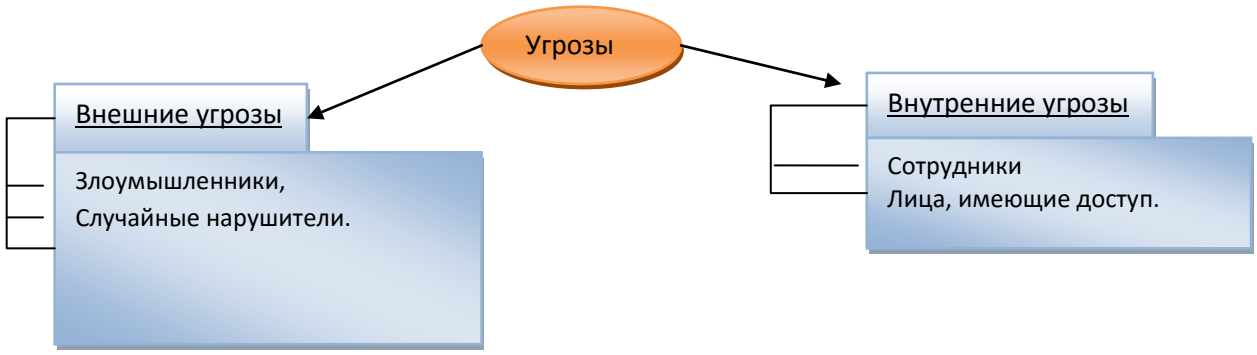

Рисунок 7 – Угрозы защищаемой информации в поликлинике.

Под угрозами защищаемой информации понимаются потенциально возможные негативные воздействия на защищаемую информацию, к числу которых относятся:

– утрата сведений, составляющих медицинскую тайну, коммерческую тайну лечебного – диагностического учреждения и иную, защищаемую информацию, а также искажение такой информации;

– утечка – неконтролируемое распространение информации за пределы организации, помещения, здания, по каналам связи и за счет побочных электромагнитных излучений (ПЭМИН);

– недоступность информации в результате ее блокирования, сбоя оборудования или программ, поликлиники функционирования операционных систем рабочих станций, серверов, маршрутизаторов, систем управления баз данных, распределенных вычислительных сетей, воздействия вирусов и т.д.

1.7. Защищенность поликлиники на данный момент

На данный момент в поликлинике реализованы следующие мероприятия:

Организационные мероприятия:

– доступ в кабинет главного врача в его отсутствие осуществляется только в присутствии заместителя главного врача и охранника;

– пациенты имеют доступ в некоторые помещения, персонал имеет доступ абсолютно во все помещения. Посетители, ожидающие приема, находятся в коридоре;

– вход людей в здание осуществляется через главный вход. Пост охраны на главном входе отсутствует, ни каких СКУД не установлено;

– вход людей в помещение поликлиники осуществляется через двустворчатую пластиковую дверь;

– вся конфиденциальная информация пересылается посредством электронной почты, доступ к которой имеется у большого количества сотрудников.

Правовые мероприятия:

– инструкции сотрудников учреждения, которые несут ответственность за защиту информации;

– утверждены должностные обязанности руководителей, медицинских работников и служащих предприятия;

– плановые проверки.

Инженерно-технические меры:

– монтаж пожарных извещателей (датчики пожарной сигнализации) во всех помещениях поликлиники;

– электропитание здания осуществляется от линий электропередач, которая расположена на неконтролируемой территории и обслуживается сторонней организацией;

Программно-аппаратные меры:

– на автоматизированном рабочем месте (АРМ) сотрудников установлены операционная система – MS Windows 7, офисное приложение – MS Office 2007, антивирусное программное обеспечение – ESET NOD 32;

– на АРМ установлена программа регистрации входа/выхода, а также всех произведенных действий с учетом времени;

– пакет Microsoft Office 2007; Интернет-шлюз UserGate;

– в поликлинике установлено 30 персональных компьютеров, 4 принтера, 2 ксерокса, 3 сканера;

– установлен сервер на основе MS Server 2012;

– для безопасного доступа пользователей локальной сети в Интернет, для защиты компьютеров от вторжений хакеров, вирусов, спама, точного подсчета трафика используется Интернет-шлюз UserGate Proxy & Firewall на платформе Windows;

Инженерно-техническая укрепленность объекта защиты

В соответствии с руководящим документом (РД) 78. 36. 003-2002 объект защиты относится к подгруппе Б II по инженерно-технической укрепленности, хищения на которых в соответствии с уголовным законодательством Российской Федерации могут привести к ущербу в размере до 500 минимальных размеров оплаты труда и свыше 500 соответственно.

Двери, установленные в выделенном помещении, соответствуют категории и классу устойчивости О-II по ГОСТ Р 51242-98, что соответствует второму классу защищенности дверных конструкций. Двери этого класса обязательны для класса Б II.

Оконные конструкции так же удовлетворяют требованиям класса Б II.

1.8. Недостатки в защите медицинского учреждения

Внешние недостатки:

– часть ЛВС выходит за пределы КЗ;

– информация не защищена от утечки по каналу ПЭМИН.

Внутренние недостатки:

– недостаточное внимание к обеспечению защиты информации со стороны руководства;

– довольно равнодушное отношение к обеспечению защиты информации со стороны сотрудников учреждения;

– одинаковые и простые пароли для всех АРМ, а так же ПО;

– сервер, на котором хранится база данных, имеет прямой доступ в интернет, что порождает лишнюю угрозу;

– недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности в поликлинике;

– отсутствуют датчики виброакустического зашумления на стояках отопления, выходящих за пределы контролируемые зоны (КЗ);

– генераторы электромагнитного шума в помещении не установлены;

– отсутствует защита телефонных, а так же UTP-8 линий.

Правовое поле сформировано и существует СКЗИ. Но ей не уделяется достаточного внимания. Сотрудники ведут себя халатно по отношению к мерам защиты информации. Плановые и внеочередные проверки не проводятся, а значит, нет никакого стимулирования для соблюдения элементарных правил для обеспечения мер защиты информации. Нет никакой работающей системы аутентификации и идентификации. Все пароли одинаковые, двери кабинетов оставляются открытыми. В случае съема информации посредством АРМ, невозможно вовремя детектировать и устранить канал.

Полное отсутствие разграничения доступа, а так же отсутствие привязки по физическому адресу для любого ПК, дают возможность подключения к сети в любом удобном месте, без особых проблем.

2 ОПИСАНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

2.1 Этапы построения КСЗИ для поликлиники

Для того чтобы организовать эффективную защиту конфиденциальной информации необходимо разработать программу которая должна осуществлять следующие цели:

– предотвращение утечки, хищения, утраты, искажения, подделки конфиденциальной информации (коммерческой и врачебной тайны);

– предотвращение угроз безопасности личности и медицинского учреждения;

– предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию конфиденциальной информации;

– предотвращение других форм незаконного вмешательства в информационные ресурсы и системы, обеспечение правового режима документированной информации как объекта собственности;

– защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

– сохранение, конфиденциальности документированной информации в соответствии с законодательством.

Планируемые мероприятия должны:

– способствовать достижению определенных задач

– являться оптимальными.

Не должны:

– противоречить законам, ГОСТам, требованиям руководителя организации;

– повторять другие действия.

2.2 Комплексная система защиты

Комплексная система защиты информации (КСЗИ) предприятия есть совокупность методов и средств, объединенных единым целевым назначением и обеспечивающих необходимую эффективность ЗИ предприятия.

Главной целью КСЗИ является обеспечение непрерывности бизнеса, устойчивого функционирования коммерческого предприятия и предотвращения угроз его безопасности.

В комплексную систему защиты информации входит:

– правовая защита:

a) наличие в организационных документах, правилах внутреннего трудового распорядка, трудовых договорах, контрактах, заключаемых с персоналом, в должностных инструкциях (регламентах) положений и обязательств по защите информации;

b) формулирование и доведение до сведения всего персонала медицинского учреждения (в том числе не связанного с защищаемой и охраняемой информацией) положения о правовой ответственности за разглашение информации, несанкционированное уничтожение или фальсификацию документов;

c) разъяснение лицам, принимаемым на работу, положения о добровольности принимаемых ими на себя ограничений, связанных с выполнением обязанностей по защите документированной информации.

– организационная защита:

a) организацию охраны, режима, работу с кадрами, с документами;

b) использование ТС безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз предпринимательской деятельности.

– инженерно-техническая защита использует такие средства как:

a) физические – устройства, инженерные сооружения, организационные меры, исключающие или затрудняющие проникновение к источни-

кам конфиденциальной информации (системы ограждения, системы контроля доступа, запирающие устройства и хранилища);

b) аппаратные – устройства, защищающие от утечки, разглашения и от ТС промышленного шпионажа;

c) программные средства – средства, охватывающие специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных.

2.3 Правовая защита

Правовая защита – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

Правовая защита информации как ресурса признана на международном, государственном уровне и определяется межгосударственными договорами, конвенциями, декларациями и реализуется патентами, авторским правом и лицензиями на их защиту. На государственном уровне правовая защита регулируется государственными и ведомственными актами.

В нашей стране такими правилами (актами, нормами) являются Конституция, законы Российской Федерации, гражданское, административное, уголовное право, изложенные в соответствующих кодексах. Что касается ведомственных нормативных актов, то они определяются приказами, руководствами, положениями и инструкциями, издаваемыми ведомствами, организациями и предприятиями, действующими в рамках определенных структур.

Персональные данные, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в т.ч. его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Законом об информации установлено, что не допускаются сбор, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную тайну, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения.

Список необходимых организационно-распорядительных документов в сфере защиты персональных данных и во исполнение Федерального закона РФ от 27 июня 2006 года № 152-ФЗ.

К документам, регламентирующим деятельность в области защиты информации относятся:

1)приказ:

– о назначении ответственного за организацию обработки персональных данных (далее ПДн);

– назначении сотрудников имеющих доступ к ПДн;

– о создании комиссии (Классификация каждой информационной системы персональных данных (далее ИСПДн), установка класса защищенности АС, уничтожение документов ограниченного распространения);

– о назначении ответственных лиц по работе с шифровальными (криптографическими средствами);

– о утверждении перечня информационных систем ПДн;

– об утверждении перечня конфиденциальной информации;

– об установлении границ контролируемой зоны ИСПДн;

– об утверждении инструкции о порядке работы с документвсм ограниченного распространения, не содержащих государственную тайну;

– об утверждении инструкции по опечатыванию кабинетов;

– об утверждении инструкции о внутреобъектовом порядке режимных помещений;

– об утверждении инструкции о внутреобъектовом порядке режимных помещений;

– об утверждении инструкции по резервному копированию (восстановлению) информации;

– об утверждении инструкции о средствах антивирусной защиты ИСПДн;

– об утверждении инструкции ответственного за организацию обработки ПДн;

– об утверждении Положения об осуществлении внутреннего контроля соответствия обработки ПДн Федеральному закону Российской Федерации от 27 июня 2006 года №152-ФЗ и принятыми в соответствии с ними нормативными правовыми актами, требованиям к защите персональных данных, политике оператора в отношении обработки ПДн, локальным актам оператора;

– об утверждении Положения о комиссии по вопросам информационной безопасности;

– об утверждении политики обработки ПДн;

– об утверждении инструкции пользователя при обработке ПДн без средств автоматизации;

– об утверждении Положения об обработке ПДн;

– об утверждении Положения об оценке вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона от 27 июня 2006 года №152-ФЗ «О персональных данных»;

– об утверждении перечня мест хранения материальных носителей ПДн;

– об утверждении инструкции работника Учреждения по эксплуатации автоматизированного рабочего места и пользования ведомственной сетью передачи данных;

– об утверждении схемы передачи ПДн по каналам связи Учреждения;

– об утверждении инструкции по эксплуатации машинных носителей информации;

– о создании комиссии по вопросам информационной безопасности;

– об утверждении модели угроз безопасности ПДн при обработке в информационных системах ПДн;

– о назначении пользователей и правил работы со средствами криптографической защиты информации.

2)журнал:

– журнал учета обращении субъектов ПДн или их представителей;

– журнал учета лиц о факте обработки ими ПДн, обработка которых осуществляется оператором без использования средств автоматизации;

– журнал ознакомления работников, непосредственно ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику «Учреждения» в отношении обработки ПДн, локальными актами по вопросам обработки ПДн;

– журнал учета фактов несанкционированного доступа к ПДн и принятых мер;

– журнал по экземплярного учета крипто средств;

– журнал учета

3)для организации Службы защиты информации (СлЗИ) такие документы:

– положение о СлЗИ;

– должностные инструкция начальник службы безопасности;

– должностные инструкция инженер по защите информации;

– должностные инструкция начальник отдела конфиденциального делопроизводства;

– инструкция по защите конфиденциальной информации.

К уже существующему уставу медицинского учреждения необходимо внести в устав следующие дополнения:

– медицинское учреждение имеет право определять состав, объем и порядок защиты сведений, составляющих коммерческую тайну; требовать от своих сотрудников обеспечения ее сохранности;

– обязано обеспечить сохранность коммерческой тайны;

– состав и объем информации, являющейся конфиденциальной и составляющей коммерческую тайну, а также порядок защиты определяются руководителем медицинского учреждения;

– имеет право не предоставлять информацию, содержащую коммерческую тайну;

– руководителю предоставляется право возлагать обязанности, связанные с защитой информации, на сотрудников.

Внесение этих дополнений дает право администрации:

– создавать организационные структуры по защите коммерческой тайны;

– издавать нормативные и распорядительные документы, определяющие порядок выделения сведений, составляющих коммерческую тайну, и механизмы их защиты;

– включать требования по защите коммерческой тайны в договора по всем видам деятельности;

– требовать защиты интересов учреждения перед государственными и судебными органами;

– распоряжаться информацией, являющейся собственностью, в целях извлечения выгоды и недопущении экономического ущерба коллективу учреждения и собственнику средств производства.

Общество организует защиту своей конфиденциальной информации. Состав и объем сведений конфиденциального характера, и порядок их защиты определяются генеральным директором.

Внесение этих дополнений дает право администрации:

– создавать организационные структуры по защите коммерческой тайны или возлагать эти функции на соответствующих должностных лиц;

– издавать нормативные и распорядительные документы, определяющие порядок выделения сведений, составляющих коммерческую тайну, и механизмы их защиты;

– включать требования по защите коммерческой тайны в договоры по всем видам хозяйственной деятельности (коллективный и совместные со смежниками);

– требовать защиты интересов учреждения перед государственными и судебными органами;

– распоряжаться информацией, являющейся собственностью фирмы, в целях извлечения выгоды и недопущения экономического ущерба коллективу и собственнику средств производства.

А также необходимо проставить грифы конфиденциальности:

– самый низкий гриф конфиденциальности для служебного пользования (ДСП) проставить на телефонные справочники, в которых указываются отдельные данные о кадровом составе или партнерах; журналы регистрации, документы, регламентирующие деятельность, служебную переписку (заявления, распоряжения, приказы, докладные и т.д.);

– гриф «КОНФИДЕНЦИАЛЬНО» проставить на информации об отдельных аспектах сделок за короткий промежуток времени; развернутые сведения о персонале компании (персональные данные работников); текущие документы, отражающие финансовую деятельность; документы, содержащие данные о пациентах, не предоставляемые третьим лицам, неопубликованная информация, обладающая экономической ценностью для учреждения и его персонала;

– гриф «СТРОГО КОНФИДЕНЦИАЛЬНО» присвоить документам, содержащим данные о сделках с партнерами или пациентами фирмы, об итогах деятельности за продолжительный период времени; документам, содержащим важнейшие аспекты коммерческой деятельности, документам, содержащих медицинскую тайну.

Рассмотрим требования, которые должен содержать коллективный договор:

Раздел «Предмет договора»: администрация обязуется в целях недопущения нанесения экономического ущерба коллективу обеспечить разработку и осуществление мероприятий по экономической безопасности и защите конфиденциальной информации.

Трудовой коллектив принимает на себя обязательства по соблюдению установленных на фирме требований по экономической безопасности и защите конфиденциальной информации.

Администрации учесть требования экономической безопасности и защиты конфиденциальной информации в правилах внутреннего трудового распорядка, в функциональных обязанностях сотрудников и положениях о структурных подразделениях.

Раздел «Кадры. Обеспечение дисциплины труда: администрация обязуется нарушителей требований по информационной безопасности и защите конфиденциальной информации привлекать к ответственности в соответствии с законодательством РФ.

Раздел «Порядок приема и увольнения рабочих и служащих»: при приеме сотрудника на работу или при переводе его в установленном порядке на другую работу, связанную с конфиденциальной информацией, а также при увольнении администрация обязана:

– проинструктировать сотрудника о правилах экономической безопасности и сохранения конфиденциальной информации;

– оформить письменное обязательство о неразглашении конфиденциальной информации. Администрация вправе;

– принимать решения об отстранении от работы лиц, нарушающих требования по защите конфиденциальной информации;

– осуществлять контроль за соблюдением мер по защите и неразглашении конфиденциальной информации в пределах предприятия.

– при решении об увольнении или отстранении от обязанностей заранее ограничить его доступ к системе.

Раздел «Основные обязанности медицинских работников и служащих»: медицинские работники и служащие обязаны:

– знать и строго соблюдать требования экономической безопасности и защиты конфиденциальной информации;

– дать добровольное письменное обязательство о неразглашении сведений конфиденциального характера;

– бережно относиться к хранению личных и служебных документов и продукции, содержащих сведения конфиденциального характера. В случае их утраты немедленно сообщить об этом администрации.

Раздел «Основные обязанности администрации»: администрация и руководители подразделений обязаны:

– обеспечить строгое соблюдение требований экономической безопасности и защиты конфиденциальной информации;

– последовательно вести организаторскую, воспитательную работу, направленную на защиту интересов и конфиденциальной информации;

– включать в положения о подразделениях и должностные инструкции конкретные требования по экономической безопасности и защите конфиденциальной информации;

– неуклонно выполнять требования устава, коллективного договора, трудовых договоров, правил внутреннего трудового распорядка и других хозяйственных и организационных документов в части обеспечения экономической безопасности и защиты конфиденциальной информации.

Администрация и руководители подразделений несут прямую ответственность за организацию и соблюдение мер по информационной безопасности и защите конфиденциальной информации.

2.4 Организационная защита

Организационная защита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба исполнителям.

Организационные мероприятия играют существенную роль в создании надежного механизма защиты информации, так как возможности несанкционированного использования конфиденциальных сведений в значительной мере обусловливаются не техническими аспектами, а злоумышленными действиями, нерадивостью, небрежностью и халатностью пользователей или персонала защиты. Влияния этих аспектов практически невозможно избежать с помощью технических средств. Для этого необходима совокупность организационно-правовых и организационно-технических мероприятий, которые исключали бы (или, по крайней мере, сводили бы к минимуму) возможность возникновения опасности конфиденциальной информации. К основным организационным мероприятиям можно отнести:

– организацию режима и охраны, которая исключает возможности тайного проникновения на территорию и в помещения посторонних лиц; обеспечение удобства контроля прохода и перемещения сотрудников и посетителей; создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа; контроль и соблюдение временного режима труда и пребывания на территории персонала фирмы; организация и поддержание надежного пропускного режима и контроля сотрудников и посетителей и др.;

– организацию работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;

– организацию работы с документами и документированной информацией, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение;

– организацию использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации;

– организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты;

– организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

2.4.1 Организационные меры по системе допуска сотрудников к конфиденциальной информации

Защита информации в компьютерах должна осуществляться в соответствии с требования РД ГостехКомиссии, и СТР-к.

Сотрудники поликлиники, допускаемые по роду своей работы или функциональным обязанностям к сведениям, составляющим конфиденциальную информацию, должны под расписку ознакомится с этим приказом и приложением к нему.

Перечень дифференцированно должен доводиться не реже 1 раза в год до всех сотрудников организации, которые используют в своей работе частично или в полном объёме сведения, информацию, данные или работают с документами ДСП и их носителями. Все лица принимаемы на работу в поликлинику, должны пройти инструктаж и ознакомиться с памяткой о сохранении конфиденциальной информации и врачебной тайны.

Сотрудник, получивший доступ к конфиденциальной информации и документам, должен подписать индивидуальное письменное договорное обязательство об их неразглашении. Обязательство составляется в одном экземпляре и хранится в личном деле сотрудника не менее 5 лет после его увольнения. При его увольнении из организации ему даётся подписка о неразглашении конфиденциальной информации организации.

2.5.Инженерно-техническая защита

Инженерно-техническая защита (ИТЗ) по определению – это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации.

2.5.1Структура существующей системы

На данный момент в поликлинике существует ИСПДн, отвечающая за его работу и содержащая всю информацию о пациентах, а так же информацию страховых реестров, подразделений, штата, работников, расписания и т.д. Система реализована через программу ТМ МИС, полностью отсутствует система разграничения доступа, что неприемлемо. Халатное отношение к ЗИ со стороны персонала и руководства, ставит учреждение в положение, когда система есть и она работает, но польза от нее уменьшается до нуля. Следует предпринять организационные, а так же инженерно-технические меры по устранению недостатков и понижению уровней риска.

2.5.2 Серверная

В серверной находится шкаф сетевого оборудования, который включает в себя несколько программируемых маршрутизаторов в т.ч. для связи с другими поликлиниками и органами управления. Свитчи, концентратор VipNet, необходимый для передачи информации по зашифрованному каналу связи, мини – АТС отвечающую за работу всех IP-телефонов, для данной организации, USP для гарантии сохранности оборудования, подключенным посредством него оборудования в т.ч. сам сервер.

Сервер работает на базе ОС Windows Server 2012, оборудован антивирусной защитой ESET NOD 32 Системой резервного копирования Cobian Backup 10, настроенной таким образом, что каждый день в нерабочее время, создается резервная копия БД. Жесткий диск на 500Gb, имеет зеркало, так что в случае краха оборудования, базу данных можно будет восстановить с небольшим откатом. Серверный ПК несет в себе обязанности:

– сервера БД (ТМ МИС);

– интернет сервера, сервера почты;

– сервера терминалов;

– сервера печати;

– ISS сервера (связь с сайтом поликлиники);

– зеркалирования информации.

При такой нагрузке и количестве выполняемых задач создаются огромные проблемы. Не смотря на архитектуру процессора (intel core i5), и 4Gb RAM, сервер плохо загружает, а иногда и вовсе зависает, не выдерживая нагрузки выполняемых задач. Ко всему прочему ПО, используемое в поликлинике, не очень хорошо оптимизировано, но постоянно дорабатывается, выпускаются обновления, заплатки, улучшения.

Ко всему прочему очень сложно администрировать сервер, выполняющий такое количество функций очень проблематично.

2.5.3 Автоматизированное рабочее место

В медицинском учреждении вся работа с БД осуществляется посредством использования терминального доступа, через встроенную утилиту RemoteDesktop. То есть наличие пароля, дает возможность доступа к БД с абсолютно любого АРМ, подключенного к сети. Все АРМ распределены по поликлинике в зависимости от надобности и потребности, получить к ним доступ не составляет труда, некоторые кабинеты находятся на “отшибе” и вероятность обнаружения поимки злоумышленника остается ничтожной. К тому же, нет никакого разграничения доступа для всех пользователей АРМ, вне зависимости от выполняемых обязанностей, что приводит нас к ситуации, когда любые пользователи обладают равными правами.

Так же на АРМ функционируют все USB порты, что дает возможность использования любых доступных накопителей с интерфейсом USB 2.0.

АРМ организованы на базе тонких пациентов, все изменения операционной системы хранятся в оперативной памяти и устраняются после перезагрузки. Функция отключается программно, посредством ввода пароля Возможность установки стороннего ПО, требующих права Администратора отсутствует. Так же все АРМ оборудованы Антивирусной защитой ESET NOD 32. Все АРМ имеют статический IP-адрес, отсутствует привязка по MAC.

Из огромных брешей в системе можно выделить одинаковые пароли для терминала, для всех пользователей АРМ, за исключением пароля администратора.

Все АРМ типовые, закуплены и установлены в большинстве поликлиник, комплектация дополняется лишь периферийными устройствами.

Комплектация АРМ:

- тонкие клиенты TONK;
- монитор Viewsonic 22;
- клавиатура, мышь;
- допускается использование сканера, принтера

2.5.4 ЛВС и внутренняя связь

Локальная сеть раскинута, посредством которой работают АРМ в учреждении, раскинута на все здание, включая стационар, поликлинику. Пролегает через коридор в кабель канале, разветвляется свитчами, находящимися в специальных шкафчиках. Вся ЛВС приходит на центральный свитч в серверную комнату, где посредством программируемого маршрутизатора она соединяется с другими поликлиниками. Диапазон IP адресов ограничен 10.30.131.1-10.30.131.255. Никакой привязки по MAC-адресу, кроме доступа в интернет не существует.

Посредством ЛВС так же работают IP-телефоны, которые находятся в той же подсети что и ПК, т.к. выделенный диапазон для нашей поликлинике, предусматривает адреса типа 10.30.131.

2.5.5 Вывод о существующей системе в медицинском учреждении

Из приведенной выше информации можно сделать следующие заключения. Правовая защита: находится на приемлемом уровне, т.к. все пакеты необходимой документации разработаны специалистами в рамках государственной программы модернизации поликлиники Доработок не требуется.

Аппаратная часть: доступ к сети извне полностью ограничен. Передача конфиденциальных данных осуществляется по закрытому каналу, обеспечиваемому посредством программно-аппаратного комплекса VipNet. Концентратор вмонтирован в шкаф в серверной, вместе с клиентом ПК. Во внутренней сети у любого ПК есть доступ ко всем компьютерам сети, более того, нет никаких препятствий для подключения нового клиента к сети, что открывает возмож-

ность для третьих лиц. На экстренный случай, выделен специальный канал, реализуемый через GSM модем. Так же в поликлинике установлена система охранной сигнализации. Главный пульт находится в регистратуре, системой пожаротушения в соответствии с СП 5.131130.2009.

Программная часть: Все ПК находятся в доменной системе, сервером которой является тот же ПК, который выполняет роль сервера БД. Программная часть практически отсутствует, за исключением интернет-шлюза UserGate на серверной машине и система CobianBackup, выполняющая резервное копирование всей базы в нерабочее время. Никаких средств разграничения доступа на данный момент не существует. База хранится на ПК в открытом доступе. Никаких блокирующих копирование утилит на клиентских ПК не установлено. Доступ клиентов осуществляется через службу терминалов RemoteDesktop.

2.5.6 Дополнительные физически средства защиты информации.

Информация, хранимая в учреждении, находится как на бумажных носителях, так и на электронных носителях. Чтобы обезопасить данные от хищения со стороны злоумышленников на информацию, хранящуюся на бумажных носителях, необходимо хранить в специальных сейфах для документов.

В качестве хранилища для документов содержащих конфиденциальную информацию используем SteelOff US8 12.L22, так остальные сейфы уступают ему по качеству надежности и приемлемой цене . Производитель дает на них 5 лет гарантии. Отличительные особенности.

За частую, двери в поликлинике бывают, открыты из-за невнимательности либо не желании вообще закрывать любую дверь. В результате чего любой посторонний человек может либо подсмотреть или подслушать любую информацию, а так же проникнуть в помещение для непосредственного взаимодействия с АРМ. Для того чтобы это избежать оснастим каждую дверь доводчиком для двери. Необходимо 60 штук.

2.5.7 Выбор средств защиты

В поликлинике уже существует система обработки и передачи информации между всеми ПК. Однако, ее следует улучшить, используя управляемый

маршрутизатор и привязку по MAC адресам. Для этого подойдет сходный по параметрам коммутатор.

Выбор аппаратных средств основан на ряде факторов:

– цена;

– эффективность (относительно других схожих аппаратных средств);

– простота использования.

Для решения поставленной задачи выбраны следующие технические решения.

2.5.7.1 Защита телефонной линии

В поликлинике установлена мини АТС Yeastar PBX U100. Данный вид связи надежно защищен от прослушивания и манипуляции путем шифрования и криптографической аутентификации VoIP. Данный способ обеспечения защиты информации на данный момент является самым надежным, однако, если злоумышленник получит доступ к сети, он сможет добраться и до консоли АТС, тогда все переговоры станут доступными для манипуляции и прослушивания. Для предотвращения такой ситуации выделим отдельную VPN для IP-телефонии, поскольку физически отсоединить ее не представляется возможным. Все это легко реализуется после установки нового программируемого коммутатора DES-1100-24V/A1A.

Рисунок 8 – Мини АТС Yeastar PBX U100

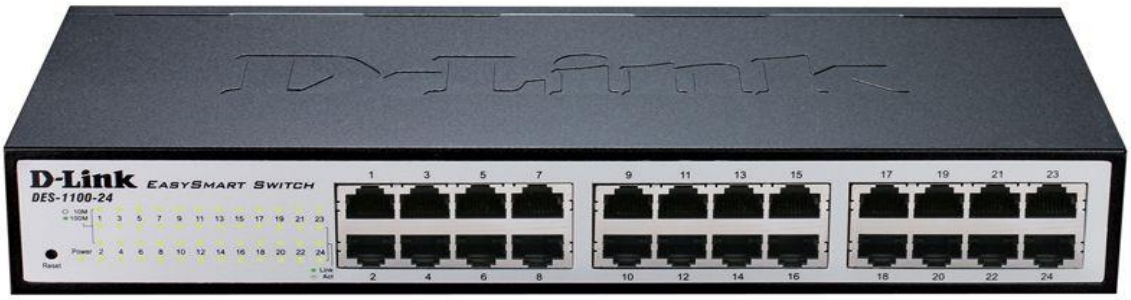

Рисунок 9 – Коммутатор DES-1100-24V/A1A

Так же при установке этого устройства мы полностью физически обезопасим ЛВС от несанкционированного подключения других пользователей, поскольку на коммутаторе установлены программируемые порты, с привязкой по MAC-адресу.

2.5.7.2 Защита от ПЭМиН

По этой проблеме, если не вдаваться в технические тонкости, можно сказать, что в соответствии с существующими методическими документами в ИСПДн 1 класса необходимо применять средства защиты, снижающие вероятность реализации угрозы утечки за счёт ПЭМиН.

Таблица 1 – Технические характеристики устройств

Устройство – Канал обмена.	Тактовая частота	Разрядность, число параллельных линий передачи	Мощность ПЭМИ
1	2	3	4
Блок питания	50 Гц и гармоники 80-150КГц	1 до 30	250-500 Вт 2-50 Вт
Процессор цепи питания	До 3,2 ГГц	4	1 – 20 Вт
Процессор - шина данных	до 400 МГц	16, 32, 64	10-3 - 10-2 Вт
Память	до 667 МГц	16, 32, 64	до 5 Вт/Гбайт
Чипсет	до 533 МГц	16, 32, 64	до 1 Вт
Шина PCI	33-66 МГц	32, 64	10-3 – 10-4 Вт
Шина IDE(ATA)	66, 100, 133 МГц	16	10-2 – 10-3 Вт

Продолжение таблицы 1

1	2	3	4
VGA	до 85 МГц	5 (R, G, B, 2-синхронизация)	10-4 – 10-5 Вт
Шина AGP1, 2, 4, 8	66МГц	32	10-2 – 10-3 Вт
Шина PCI-E	2500МГц	1-32	10-4 – 10-5 Вт
Порт LTP (IEEE 1384)	5- 2000 Кбайт/сек	8	10-3 Вт
SATA-150, -300, -600	1500 МГц 3000 МГц 6000 МГц	1+1	10-3 Вт
Порт USB1.1-2.0 (IEEE1394)	0,18-60	1+1	10-3 Вт
COM	До 920 Кбайт/сек	1+1	до 10-3 Вт

Существуют две основные методики оценки защищенности ТС от утечки по каналу ПЭМИН. Это методика специальных исследований, результатом измерения которой является расчет радиусов R2, r1 и r1', и методика оценки защищенности, результатом которой является измеренное и рассчитанное соотношение сигнал/шум на границе контролируемой зоны (реальное затухание).

Пространство вокруг ОТСС, в пределах которого напряженность ЭМ-поля превышает допустимое (нормированное) значение, называется **зоной 2 (R2)**. Фактически зона R2 – это зона, в пределах которой возможен перехват средством разведки ПЭМИН с требуемым качеством.

Пространство вокруг ОТСС, в пределах которого уровень наведенного от ОТСС информативного сигнала в сосредоточенных антеннах превышает допустимое (нормированное), значение называется **зоной 1 (r1)**, а в распределенных антеннах – **зоной 1' (r1')**. Рассчитаем радиус зоны r1(ближняя зона) и зоны r2(дальняя зона) для основных устройств и каналов связи на основании формул.

Ближняя зона:

$$r_1 = \frac{150}{\pi * f} \quad (\text{м}) \qquad (1)$$

Дальняя зона:

$$R_2 = \frac{1800}{f} \text{ (м)}, \quad (2)$$

где f – тактовая частота (МГц)

Возьмем упрощённую модель ПК для расчёта. В нее будут входить USB порты, процессор, ОЗУ, VGA карта и дисковые накопители.

Таблица 2 – технические характеристика ПК для расчета

Устройство, Канал связи, Интерфейс	Тактовая частота, МГц	Ближняя зона, м	Дальняя зона, м
CPU Intel Core i5	3200	0,014	0,5625
VGA GMA 4500	400	0,119	4,5
USB 2.0	480	0,099	3,75
PCI-E	2 500	0,019	0,72
RAM DDR3	1333	0,035	1,350
Fast Ethernet	100	0,47	9

На основании расчётов можем сделать вывод, что радиус ближней зоны r1 = 0,47м. Дальняя зона R2 имеет границы в радиусе 9м.

Из расчётов видно, что канал актуален, т.к. зона распространения сигнала выходит за границу контролируемой зоны. Для этого рекомендуется использовать генератор шума по цепям электропитания, заземления и ПЭМИ «ЛГШ-503» Имеет сертификат Сертификат ФСТЭК России № 3521 и применяется для ИСПДн.

Рисунок 10 – Генератор шума «ЛГШ-503»

В поликлинике уже есть программные средства защиты, которые защищают доступность и целостность.

Утилита Cobian Backup сохраняет целостность информации, путем ежедневного резервного копирования БД. Так же целостность обеспечивается зеркалированным жестким диском. На жестком диске сервера содержатся БД за последние 7 дней, так что в любой момент существует возможность отката на любую БД по выбору. Другими словами возможен контролируемый откат.

2.5.7.3 Разграничение доступа

Для этих целей воспользуемся СЗИ SecretNet 8.1 сетевая версия. Всем АРМ будут назначены привилегии в соответствии с выполняемыми задачами. Будут ограничены использование флеш накопителей и доступ к сетевым ресурсам, а так же прочие возможности, необходимые для работы системы.

По причине большого количества компьютеров (более 35 машин), администрирует по сети. Устанавливается на Сервер Домена, что очень удобно вследствие его существования.

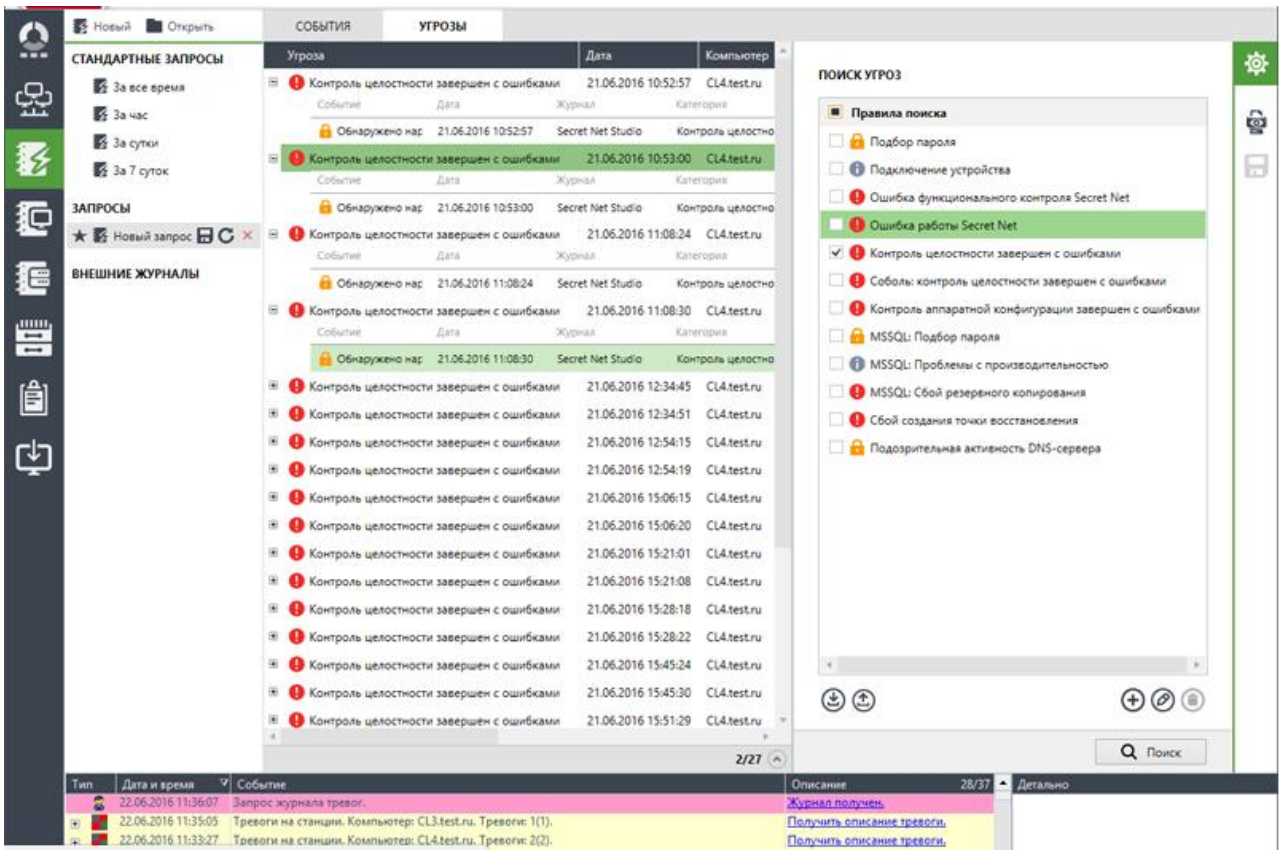

Рисунок 11 – Интерфейс программы SecretNet 8.1

Возможности СЗИ:

– идентификация и аутентификация пользователей;

– защита терминальной инфраструктуры и поддержка технологий виртуализации рабочих столов(vdi);

– система генерации отчетов;

– централизованное управление системой защиты, оперативный мониторинг и аудит безопасности;

– масштабируемая система защиты, возможность применения secret net(сетевой вариант)в организации с большим количеством филиалов;

– шифрование информации;

– гарантированное затирание удалённой информации;

– контроль аппаратной конфигурации;

– регистрация событий;

– контроль целостности программ и данных;

– избирательное и полномочное управление доступом;

– разграничение доступа к устройствам;

– замкнутая программная среда;

– защита от загрузки с внешних носителей.

Так же Secret Net позволяет оперативно среагировать на НСД и устранить канал утечки и ведет аудит всех событий.

2.5.7.4 Система контроля управления доступом

Объекты, подлежащие оснащению системой контроля и управления доступа:

– КПП;

– бухгалтерия;

– отдел безопасности;

– регистратура;

– техническое помещения;

– кабинет главного врача.

Системой контроля и управлением доступа решаются следующие задачи:

– контроля и управления доступом сотрудников и посетителей на территорию объекта;

– контроля и управления доступом сотрудников и посетителей в ряд помещений;

– автоматического ведения баз данных доступа в пределах защищаемого объекта.

Общее количество пользователей системы. В организации на постоянной основе работает 40 сотрудников. Среднее количество прибывающих в организацию клиентов - 10 человек в час.

Тип идентификаторов пользователей: бесконтактные карты MIFARE Classic 4k. На картах постоянных пользователей (сотрудников организации) размещается фотография, логотип компании и иная информация о сотруднике. На временных картах клиентов не размещается никакой информации о посетителе.

Территория предприятия оборудована одним КПП для персонала и клиентов. Максимальная нагрузка на проходную - 120 чел/час.

Для управления СКУД используется одно автоматизированное рабочее место, расположенное на посте охраны. АРМ поста охраны защищено от НСД и вредоносного программного обеспечения с помощью DeviceLock и антивирус ESET NOD 32 Соединение с другими АРМ по ЛВС отсутствует.

Структура приоритетности защищаемых зон. Высший приоритет – кабинет главного врача. Средний приоритет – бухгалтерия, отдел безопасности, серверная. Низший приоритет – КПП.

Описание работы системы:

1) сотрудники предприятия проходят КПП, поднося постоянный пропуск к считывателю карт на турникете. Факт идентификации личности записывается на АРМ СКУД (регистрируется время идентификации и Ф.И.О. сотрудника);

2) посетители предприятия обращаются в регистратуру, где им выдается талон содержащий информацию о времени посещения врача, далее на посту охраны они предъявляют талон и удостоверение личности, после чего их пропускают. Доступ в бухгалтерию имеют только бухгалтер, старший бухгалтер, главный врач и заместитель главного врача. Их постоянный пропуск запрограммирован соответственным образом, чтобы они могли получить доступ к кабинету бухгалтерии;

Доступ в отдел безопасности и серверную имеют главный администратор, начальник отдела безопасности, главный врач и его заместитель.

Их постоянный пропуск запрограммирован соответствующим образом, для получения доступа к кабинету отдела безопасности и серверной.

Система поддерживает возможность дальнейшего расширения, путем установки дополнительных считывателей.

Функциональные возможности системы контроля и управления доступом:

– регистрацию и протоколирование тревожных и текущих событий;

– приоритетное отображение тревожных событий;

– управление работой преграждающими устройствами в точках доступ по командам оператора;

– задание временных режимов действия идентификаторов;

– защиту технических и программных средств от НСД;

– автоматический контроль исправности средств, входящих в систему, и линий передачи информации;

– установку режима свободного доступа с пункта управления при аварийных ситуациях и чрезвычайных происшествиях;

– блокировку прохода по точкам доступа командой с пункта управления.

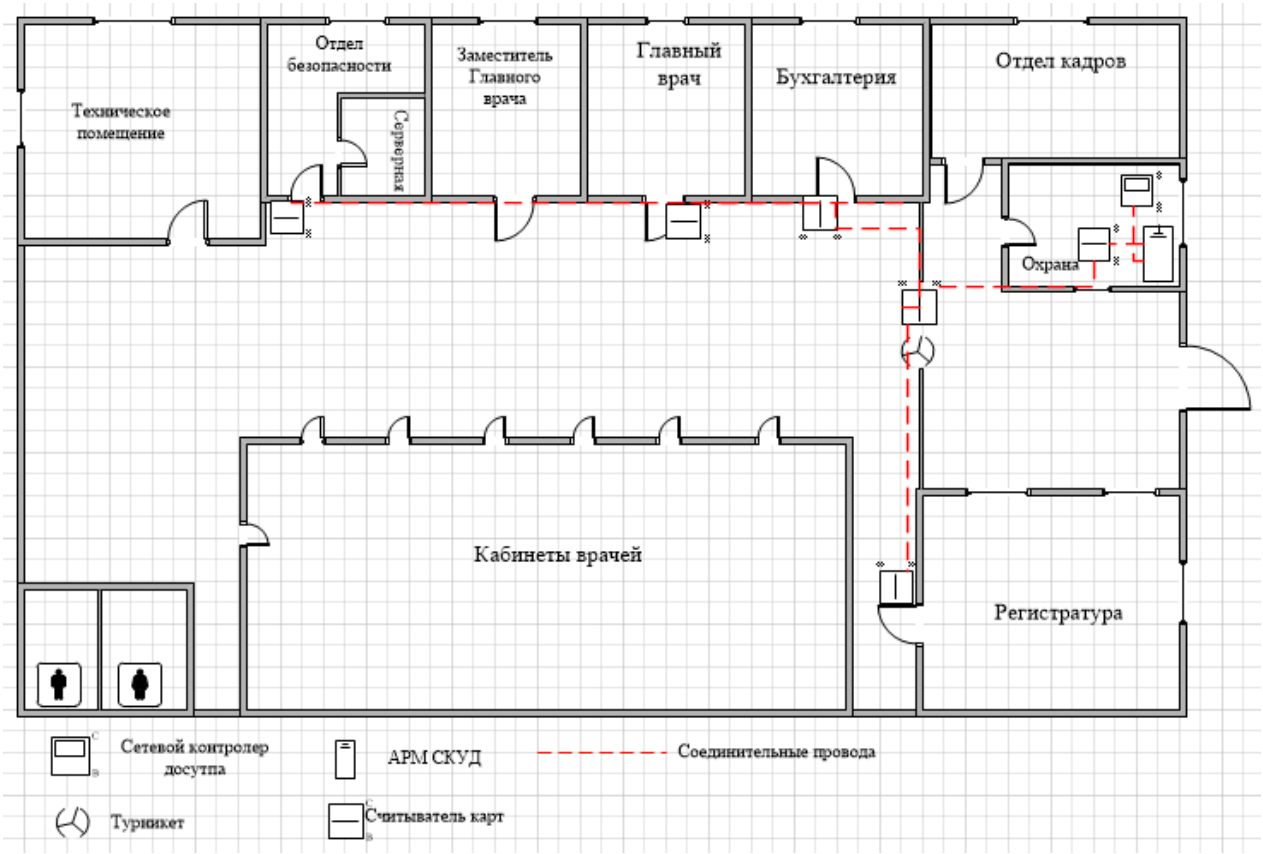

Рисунок 12 – Схема системы контроля и управления доступом

2.5.7.6 Система видеонаблюдения

Зоны обзора:

– КПП. Цель наблюдения в дневном и ночном режиме: идентификация личности. Дневное освещение: светодиодные лампы мощностью 9Вт. Ночное освещение: светодиодные лампы меньшей интенсивности;

– главный коридор. Цель в наблюдении в дневном и ночном режиме: опознавание личности. Дневное освещение: Светодиодные лампы. Ночное освещение: Светодиодные лампы меньшей интенсивности;

– улица. Цели наблюдения в дневном и ночном режиме: опознание личности и транспортного средства, ночь - опознание личности и транспортного средства. Дневное освещение: естественное. Ночное освещение: встроенный ИК прожектор камеры наблюдения, искусственное освещение от близлежащих зданий.

Решаемые задачи:

– контроль несанкционированного доступа сотрудников и (или) нарушителей на территорию объекта;

– контроль несанкционированного доступа сотрудников или нарушителей на территорию (или с территории) объекта через ограждения или запретные зоны;

– защита людей и материальных ценностей в пределах контролируемой зоны;

– идентификация личности посетителя или сотрудника при прохождении кпп, или при посещении кабинета директора;

– обнаружение автомобилей, въезжающих на территорию контролируемой зоны;

– автоматическая фиксация и хранение в течение определенного времени записи противоправных или иных событий по тревожному извещению с защищаемого объекта;

– обнаружение и фиксирование иных противоправных действий.

Посты наблюдения и управления комплексом

Присутствует один пост наблюдения, пост Охраны. Расположен на КПП, при входе на охраняемую территорию.

Система видеонаблюдения согласована с интегрированной системой безопасности ИСБ-1. Одна АРМ видеонаблюдения расположена на посту охраны.

Возможность видео регистрации: непрерывная, по сигналу оператора, по таймеру, детектор движения.

Возможен просмотр одновременно всех видеокамер комплекса.

Камеры могут выполнять охранные функции в качестве детектора движения.

Система видеонаблюдения согласована с интегрированной системой безопасности. Одно АРМ видеонаблюдения расположено в комнате охраны.

Общие требования к системе видеонаблюдения:

– цветная, черно-белая, комбинированная;

– срок хранения видеозаписей в архиве;

– необходимость в дополнении системы видеонаблюдения системой автоматизированного управления доступом в помещения и на объекты;

– необходимость фиксации аудиоинформации с охраняемых объектов,

– возможность расширения системы;

– наличие и расположение щитов электропитания вблизи мест установки оборудования и на постах наблюдения;

– наличие резервного или дублирующего питания;

– возможность дальнейшего расширения путем добавление новых телекамер и постов наблюдения (охраны).

Срок хранения видеозаписей в архиве 5 дней.

Возможность расширения: система может быть расширена путем добавления новых постов наблюдений, телекамер, видеорегистраторов и интерфейсов синхронизации с ПК.

Система видеонаблюдения: Присутствует комбинированная система видеонаблюдения. Внутри помещения применяются цветные камеры, для уличного наблюдения применяются черно-белые камеры, с встроенным инфракрасным прожектором.

Видеонаблюдение ведется с 3 камер внутри помещения, и с 2 – х уличных камер. Камеры могут выполнять охранные функции в качестве детектора движения. Информация с камер выводится на экран монитора оператора.

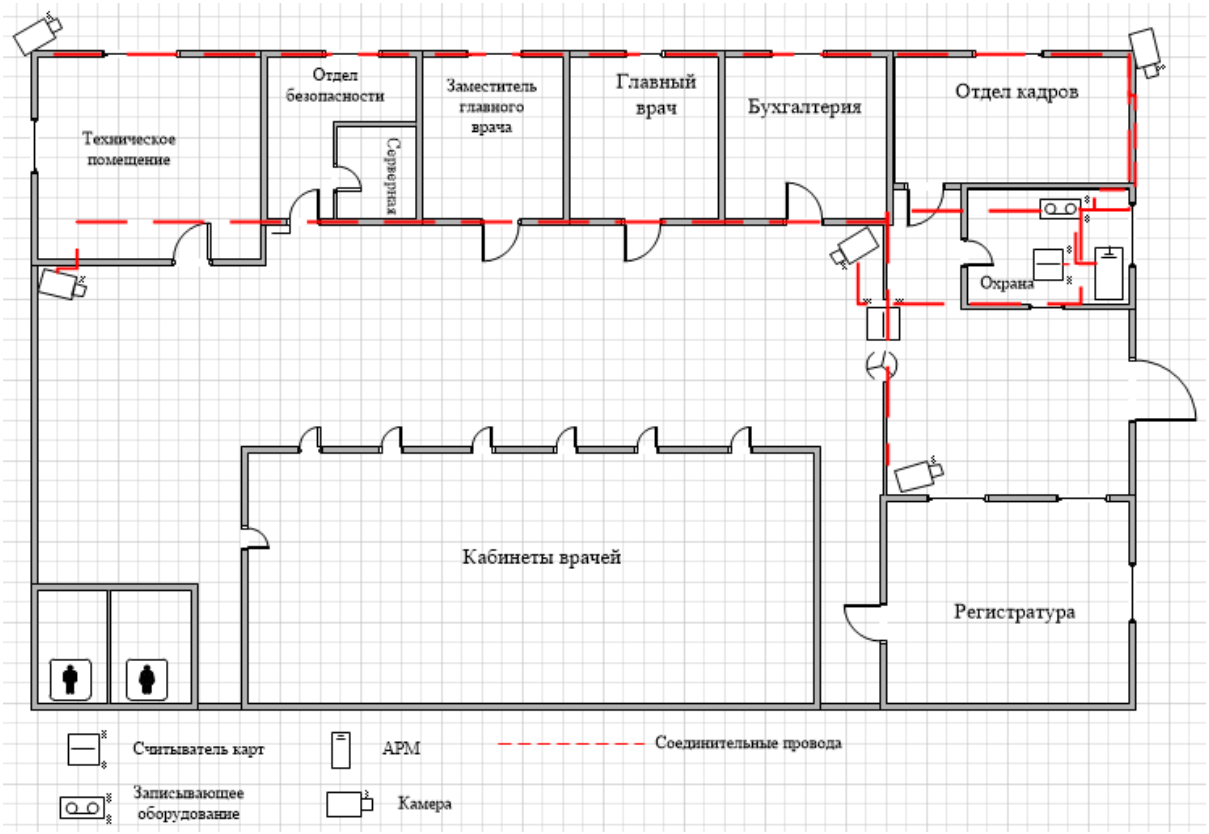

Рисунок 13 – Схема расположения камер

2.5.7.6 Система охранно – пожарной сигнализации

Системой охранной сигнализации оборудуются:

– коридор (общедоступная зона);

– отдел безопасности;

– серверная;

– пункт охраны;

– отдел кадров;

– бухгалтерия;

– кабинет заместителя главного врача;

– кабинет главного врача;

– техническое помещение.

К категории особо важных помещений относятся:

– кабинет главного врача. Оборудован хранилищем ценностей (огнеупорный сейф);

– бухгалтерия;

– отдел безопасности;

– серверная.

Наиболее уязвимыми местами для несанкционированного доступа на объект из-за пределов защищаемой зоны, являются: Окна и оконные проемы.

Основные ценности (материальные, ценные бумаги, денежные) хранятся в огнеупорном сейфе в кабинете руководителя. Доступ к сейфу имеет только руководитель предприятия. В отделе безопасности установлен сейф, в котором хранятся устройства резервного копирования информации. Доступ к сейфу имеет главный администратор и начальник службы безопасности. Наиболее уязвимые места для проникновения нарушителя на эти объекты являются окна и двери.

Зонами охраны являются помещения, содержащие материальные ценности, кроме мест общего пользования (коридоры, туалеты).

Зоны охраны:

– коридор;

– регистратура;

– отдел безопасности;

– серверная;

– пункт охраны;

– отдел кадров;

– бухгалтерия;

– кабинет главного врача;

– кабинет заместителя главного врача;

– техническое помещение.

Приоритетными зонами защиты являются кабинет руководителя, и помещение службы безопасности, серверная, бухгалтерия.

Описание системы пожарной сигнализации:

Пожарной сигнализацией оборудованы все помещения, за исключением туалетов. Ручные извещатели установлены на путях эвакуации. Дымовые извещатели установлены в коридоре, и других помещениях. В случае получение на

пульт сигнала «Пожар», автоматически подается сигнал тревоги, при помощи системы оповещения о пожаре, которая включает в себя 4 комбинированные сирены. На стенах коридора указаны пути эвакуации при пожаре. Дополнительно, раз в три месяца, проводятся учебные тревоги.

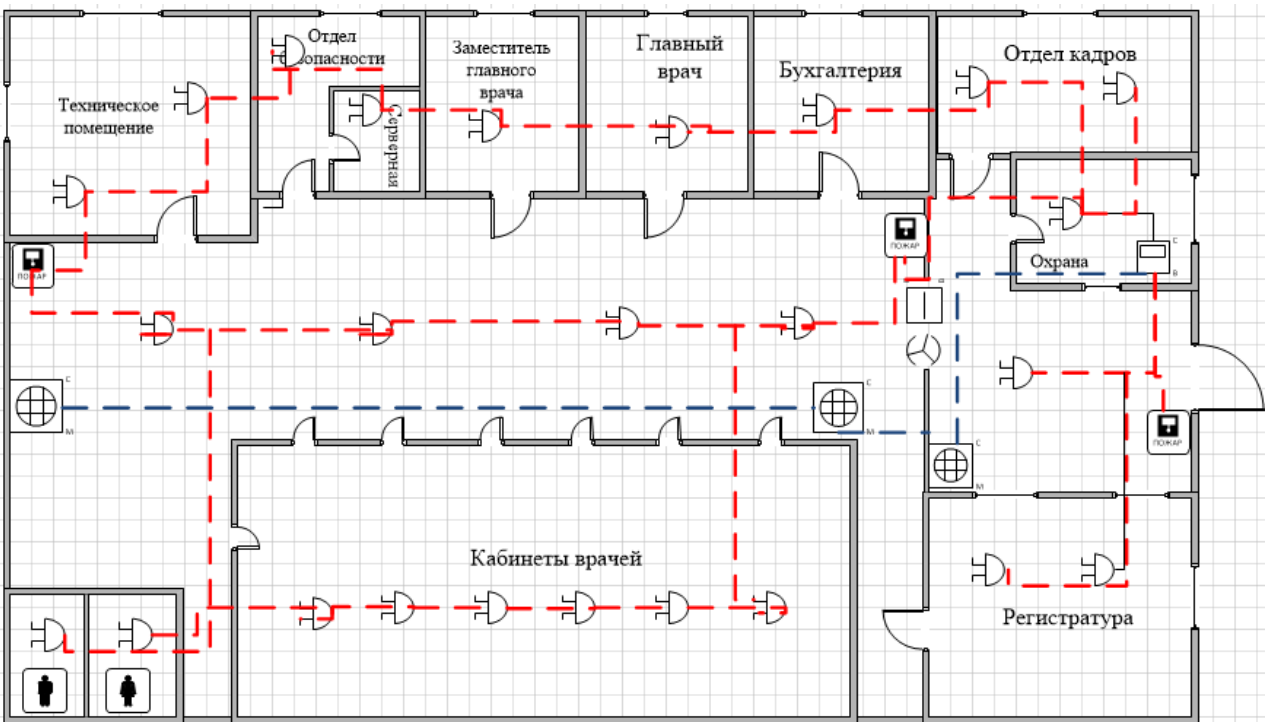

Рисунок 14 – Схема пожарной охраны

Опишем систему охранной сигнализации:

Регистратура, отдел кадров, бухгалтерия, кабинет главного врача и кабинет заместителя главного врача, отдел безопасности, техническое помещение оборудованы датчиками движения, предназначенными для обнаружения проникновения в помещения через окна. Контролируется возможность несанкционированного проникновения через дверь, так как коридорное пространство просматривается камерами наблюдения, что дает возможность оператору среагировать на возможное проявление угрозы. Так же, немаловажным является факт, что злоумышленнику, чтобы покинуть охраняемую территорию, необходимо пройти либо через пункт КПП, либо вылезти через окно, которые контролируются датчиками движения. В случае обнаружения подается сигнал на пульт оператора, который принимает решение о дальнейших действиях (задержание нарушителя силами личного состава охраны).

Отдел безопасности, бухгалтерия, оборудованы магнитоконтактным датчиками. Акустические датчики реагируют на разбитие стекла, что позволяет обнаружить попытку проникновения до того, как злоумышленник проникнет в помещение, и быстрее среагировать. Магнитоконтактные датчики реагируют при попытке открытия двери, что так же дает возможность обнаружить попытку проникновения до попадания нарушителя в охраняемое помещение. В случае обнаружения попытки проникновения подается сигнал на пульт оператора, который принимает решение о дальнейших действиях.

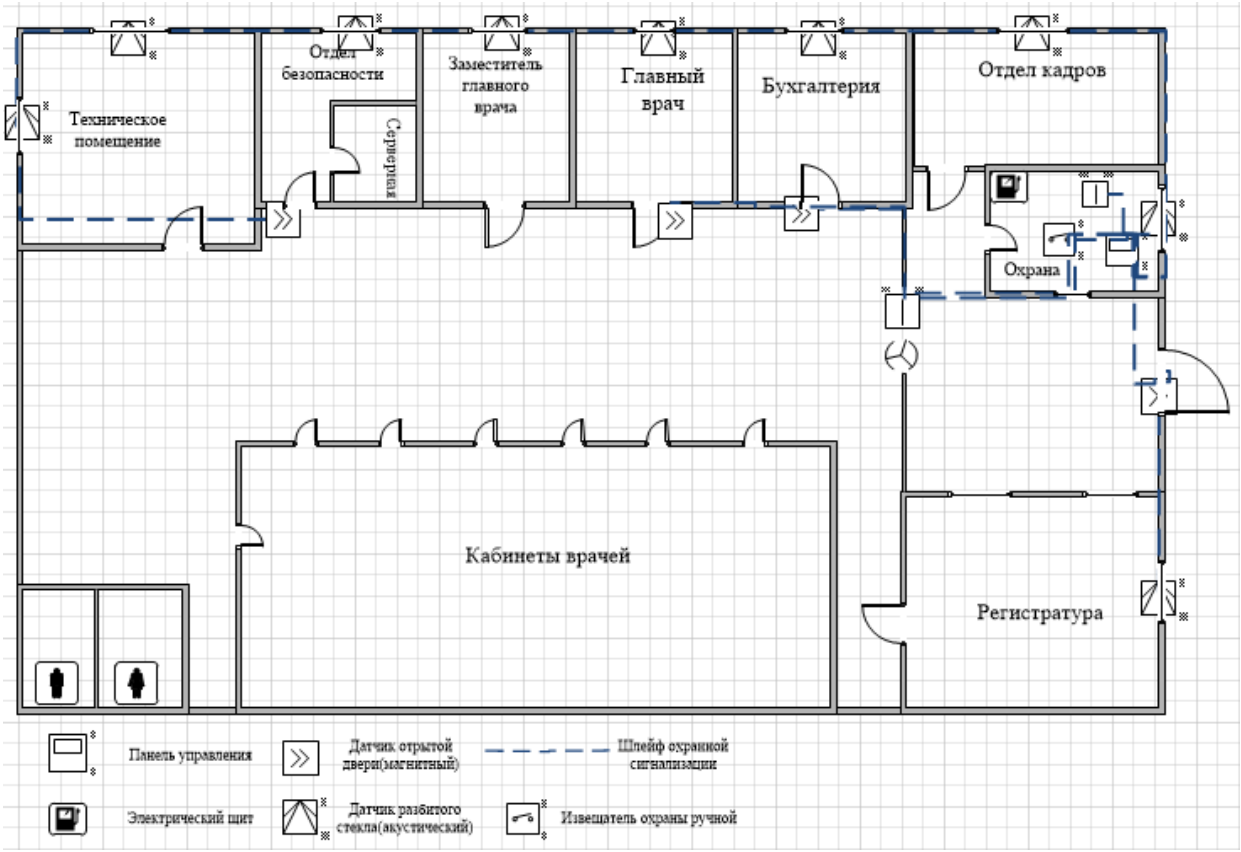

Рисунок 15 – Схема периметра охраняемой территории

3 АНАЛИЗ РИСКОВ ПРЕДПРИЯТИЯ

3.1 Оценка и управление рисками

Анализ рисков – процедуры выявления факторов рисков и оценки их значимости, по сути, анализ вероятности того, что произойдут определенные нежелательные события и отрицательно повлияют на достижение целей проекта. Анализ рисков включает оценку рисков и методы снижения рисков или уменьшения связанных с ним неблагоприятных последствий.

Оценка рисков – это определение количественным или качественным способом величины (степени) рисков.

Американский эксперт Б. Берлимер предложил при анализе использовать некоторые допущения:

– потери от риска независимы друг от друга.

– потеря по одному направлению деятельности не обязательно увеличивает вероятность потери по другому (за исключением форс-мажорных обстоятельств).

– максимально возможный ущерб не должен превышать финансовых возможностей участника.

Анализ рисков является наиболее важной частью комплексной оценки безопасности предприятия. Риск описывает вероятный ущерб, который зависит от защищенности системы, и характеризуется парой значений: вероятность ущерба и величина ущерба в условных единицах. На выходе процедура анализа риска можно получить либо количественную оценку рисков, либо качественную (уровни риска; обычно: высокий, средний, низкий). Существует несколько подходов к анализу рисков: обычно условно выделяется анализ рисков базового и полного уровня. Для анализа рисков базового уровня достаточно проверить риск невыполнения требований общепринятого стандарта безопасности (например ISO 17799) с получением на выходе качественной оценки уровня рисков (высокий, средний, низкий). Основное отличие полного анализа рисков от базового состоит в необходимости построения полной модели анализируе-

мой системы. Модель должна включать: виды ценной информации, объекты ее хранения; группы пользователей и виды доступа к информации; средства защиты (включая политику безопасности), виды угроз. После моделирования необходимо перейти к анализу защищенности построенной полной модели информационной системы.

Управление рисками заключается в снижении вероятности или последствий воздействия событий, которые могут явиться причиной изменений качества, затрат, сроков или технических характеристик производственных процессов предприятия. В ходе управления рисками производится установление, оценка, анализ и контроль рисков, возникающих в течение полного жизненного цикла системы, а также выработка ответных мероприятий по обеспечению безопасности.

3.2 Оценка сохранения конфиденциальности информации

Требуемая конфиденциальность информации обеспечивается на основе реализации мероприятий, гарантирующих защищенность информационных ресурсов системы от несанкционированного доступа до истечения периода объективной конфиденциальности данной информации[7].

Моделируемые случаи соотношения между временем смены значений параметров преград системы защиты и их расшифровки (вскрытия) и периодом объективной конфиденциальности информации для одной преграды приведены на рисунке 15.

Конфиденциальность информации сохранена в случаях 2, 3, 5, нарушена в случаях 1, 4. Вероятность сохранения конфиденциальности информации вычисляют по формуле (3):

$$\mathrm{P}_{\text{конф}} = 1 - \mathrm{P}_{\text{преод конф } m} \quad (3)$$

где $\mathrm{P}_{\text{преод конф } m}$ – вероятность преодоления нарушителем m-ой преграды до истечения периода объективной конфиденциальности информации $\mathrm{T}_{\text{конф}}$.

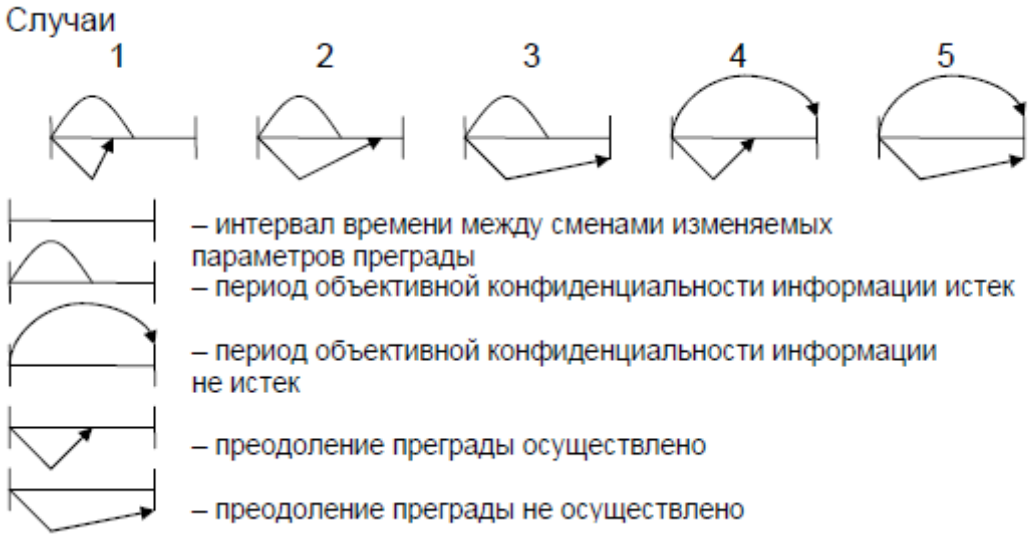

Рисунок 16 – Иллюстрация формальных процессов нарушения конфиденциальности информации (на примере одной преграды).

Для экспоненциальной аппроксимации распределений исходных характеристик при их независимости $P_{\text{преод конф } m}$ равна:

$$P_{\text{преод конф } m} = \frac{T_{\text{конф}} f_m}{T_{\text{конф}} f_m + u_m f_m + T_{\text{конф}} f_m} \quad (4)$$

где f_m – среднее время между соседними изменениями параметров защиты m-ой преграды;

U_m – среднее время преодоления (вскрытия значений параметров защиты) m-ой преграды;

$T_{\text{конф}}$ – средняя длительность периода объективной конфиденциальности информации.

Необходимые для моделирования исходные количество преград и пределы значений *um* определяют в результате дополнительного моделирования, натурных экспериментов, учитывающих специфику системы защиты и возможные сценарии действий нарушителей, или сравнения с аналогами, диапазон возможных значений *Тконф* задают в техническом задании или в постановках функциональных задач. Будем считать, что преграда для доступа, установленная в результате отработки ряда запланированных мероприятий может воспрепятствовать как нарушителю (событие *Ан*), так и добропорядочному сотруднику (событие), для которого эта информация предназначается. Событие преодоления нарушителем m-ой преграды обозначим *Апреод конф* .Таким образом, вероятность того, что пользователь, получающий доступ к информации являет-

ся нарушителем P, а вероятности сохранения охраняемой информации в этом случае можно вычислить по формуле (5):

$$P_{конф} = 1 - P(\frac{A_{преод\ конф}\ m}{A_н}) \quad (5)$$

Для удобства расчета была написана небольшая программа, имеющая довольно простой интерфейс. Работа программы изображена в рисунках.

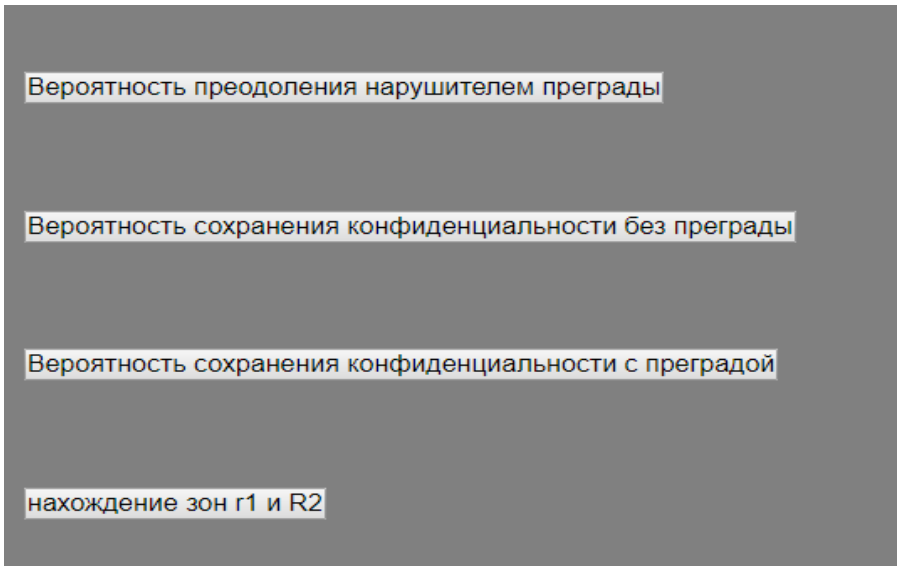

Рисунок 17 – Главное окно программы

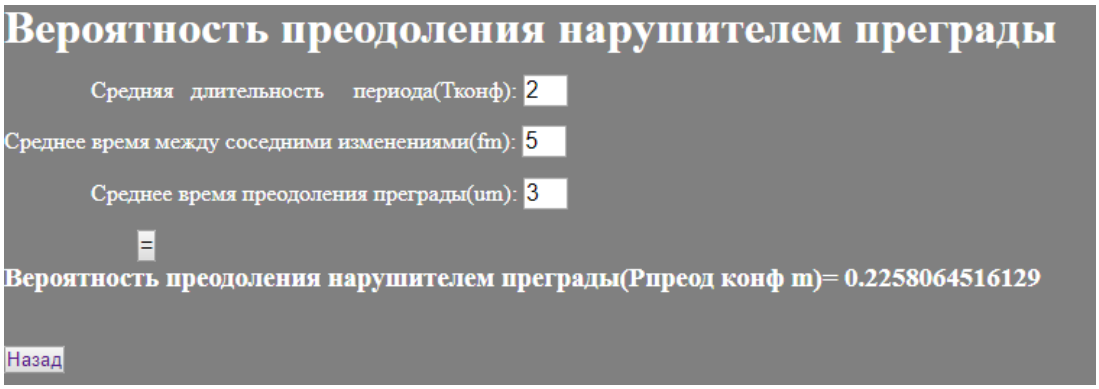

Рисунок 18 – Расчет вероятности преодоления нарушителем преграды

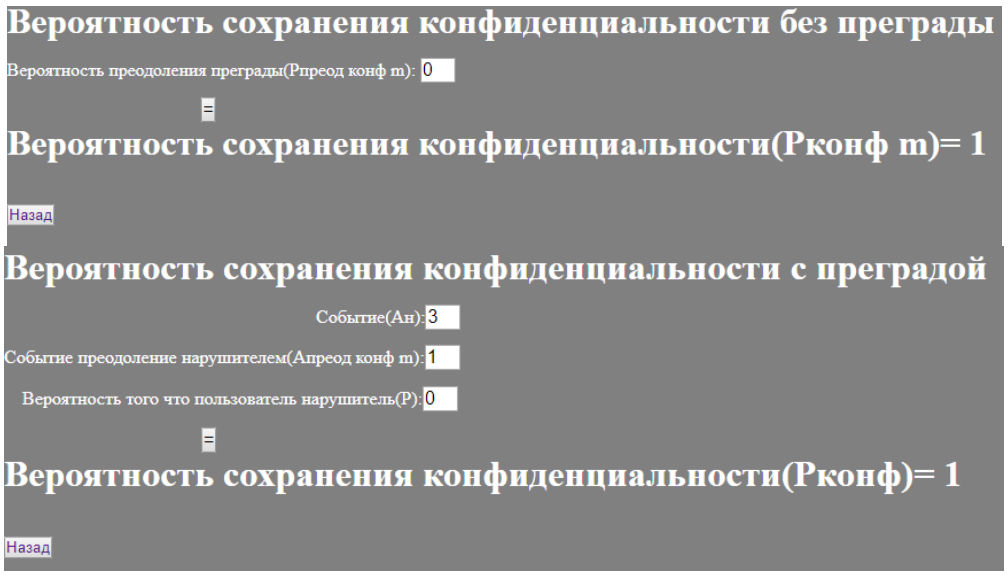

Рисунок 19 – Расчет вероятности сохранения конфиденциальности с преградой и без преграды

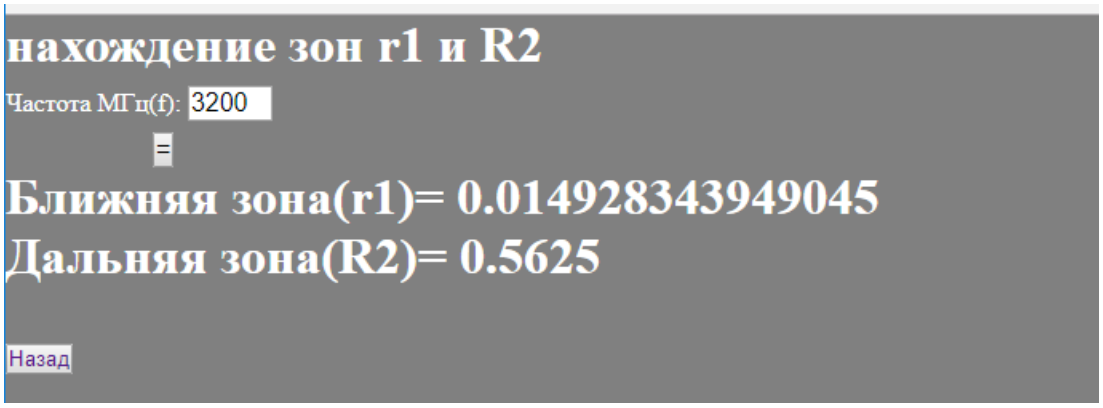

Рисунок 20 – Расчет дальней R2 и ближней зоны r1

4 БЕЗОПАСНОСТЬ И ЭКОЛОГИЧНОСТЬ

Трудовая деятельность требует от человека высокой подвижности нервных процессов, быстрых и точных движений, повышенной активности восприятия, внимания, памяти, мышления, эмоциональной устойчивости. В целом ее можно разделить на умственный (интеллектуальный) и физический труд.

Важным моментом в трудовой деятельности, направленных на совершенствование условий труда являются мероприятия по охране труда. Охрана труда – система сохранения жизни и здоровья работников в процессе трудовой деятельности, включающие в себя правовые, социально-экономические, организационно-технические, санитарно- гигиенические, лечебно-профилактические, и иные мероприятия. Существуют нормативно-правовые акты, принятые в нашей стране, направлены на обеспечение условий труда, отвечающих требованиям сохранения жизни и здоровья работников в процессе трудовой деятельности. Они содержат ряд важных положений, обеспечивающих для работающих гарантии прав на охрану труда. Обеспечение здоровых и безопасных условий труда главная задача предприятия.

Безопасность жизнедеятельности – наука о комфортном и безопасном взаимодействии человека со средой обитания.

Целью раздела БЖД в ВКР является изучение вопросов техники безопасности и экологии труда сотрудников медицинских учреждений.

Поставленная цель реализуется через задачи:

– оценка безопасности работника;

– анализ экологичности;

– оценка обеспечения пожарной безопасности;

– составление комплексов физических упражнений для сохранения и укрепления индивидуального здоровья и обеспечения полноценной профессиональной деятельности

4.1 Безопасность жизнедеятельности работника

Под рабочим местом следует понимать зону трудовых действий работника или группы работников, оснащенную и оборудованную всем необходимым для выполнения своих служебных обязанностей. При организации рабочих мест медицинских работников, прежде всего учитывается тип учреждения и профиль специалиста, то есть рабочее место должно быть специализированным.

Рациональная организация любого рабочего места в лечебно-профилактическом учреждении должна предусматривать оснащение, рациональную планировку, организацию обслуживания рабочего места, соблюдение эргономических, эстетических и санитарно-гигиенических требований.

Важное значение в организации рабочего места имеет рациональное размещение медицинской мебели и оборудования во врачебном кабинете. В соответствии с эргономическими требованиями, а также исходя из наблюдений за действиями врача и медицинской сестры мебель и оборудование врачебного кабинета рекомендуется размещать, руководствуясь следующими правилами:

- рабочий стол врача и медицинской сестры должен находиться в наиболее освещенной части кабинета;

- вокруг стола необходимо иметь пространство, обеспечивающее свободное передвижение врача и медицинской сестры от стола к любому предмету в кабинете;

- кушетка для обследования пациента должна располагаться таким образом, чтобы правая половина тела пациента находилась со стороны врача; кушетку необходимо отгородить от входной двери ширмой и вплотную к ней поставить стул для пациента;

- расположение каждого предмета должно быть продумано, чтобы свести до минимума затраты на передвижения и обеспечить соблюдение эстетических требований в оформлении кабинета;

- дверь кабинета должна быть доступна обозрению, чтобы врач мог видеть входящего пациента.

Некоторые рабочие зоны могут быть одними и теми же для разных рабочих мест. Поэтому целесообразно проводить измерения сначала в основных подразделениях, а затем – во вспомогательных. Это позволит избежать проведения измерений повторяющихся факторов в одном и том же месте для различных категорий работников.

Рабочее место представляет собой совокупность факторов окружающей среды, в том числе вредных.

Вредный производственный фактор – производственный фактор, воздействие которого на работника может привести к его заболеванию (неблагоприятный микроклимат, повышенный уровень шума, вибрации, плохое освещение, неблагоприятный аэроионный состав воздуха, механические колебания, электромагнитное и ионизирующее излучение).

4.1.1 Освещение

Человеческий глаз защищается от поражения слишком ярким светом с помощью мигательного рефлекса, поворота глаз и движения головы при воздействии яркого света.

При организации рационального освещения, выборе источников света и светильников учитываются назначение помещения, его размеры и категория по взрыво- пожароопасности, возможные загрязнения (пыль, газы, пары), характеристика и разряд выполняемой работы, нормированная освещенность и цветовая отделка.

Для создания нормальной световой среды применяют различные системы освещения.

Освещение как свет от какого-либо источника, создающее освещенность поверхностей предметов и обеспечивающее зрительное восприятие этих предметов, бывает:

- естественное освещение – освещение помещений светом, исходящим от неба (прямым или отраженным), проникающим через световые проемы в наружных ограждающих конструкциях. Нормируемой характеристикой является коэффициент естественной освещенности

– искусственное освещение – освещение помещений и других мест, где недостаточно естественного освещения. Подразделяется на а) *рабочее, б) аварийное, в) охранное, г) дежурное, д) общее, е) местное и ж) комбинированное*.

При необходимости часть светильников рабочего или аварийного освещения используется для дежурного освещения.

– совмещенное – освещение, при котором недостаточное по нормам естественное освещение дополняется искусственным.

Существует искусственное освещение двух систем: общее (равномерное и локализованное) и комбинированное. Большинство производственных помещений оборудуют системами общего искусственного освещения – когда светильники располагаются в верхней (потолочной) зоне. Если расстояние между светильниками принимается одинаковым, то освещение считают равномерным, если светильники располагают ближе к производственному оборудованию, то освещение называют локализованным. Комбинированным называют такое искусственное освещение, когда к общему добавляется местное.

Характер работы участковых терапевтов требует высоких уровней как естественного, так и искусственного освещения. При этом согласно СНиП II-4-79 "Естественное и искусственное освещение. Нормы проектирования" нормируемые значения коэффициента естественного освещения (КЕО) составляют 1,5 - 2,0; искусственная освещенность на уровне поверхности стола должна составлять не менее 300 лк и обеспечивается за счет общего освещения. Во время исследования освещенности была измерена реальная освещенность люксметром, которая составила 390 лк. Это значение находится в пределах нормы.

4.1.2 Механические колебания

К механическим колебаниям относятся шум и вибрация. Шум — беспорядочное сочетание различных по уровню и частоте звуков. Шум является одной из причин быстрого утомления работающих, может вызвать головокружение, что в свою очередь может привести к несчастному случаю. Вибрация — механические колебания упругих тел при низких частотах (3—100 Гц) с большими амплитудами (0,5— 0,003 мм).

Систематическое воздействие вибрации вызывает вибрационную болезнь (неврит) с потерей трудоспособности. Эта болезнь возникает постепенно, вызывая головные боли, боли в суставах, судороги пальцев, спазмы сосудов и нарушение питания тканей тела. В особо тяжелых случаях в организме человека наступают необратимые изменения, приводящие к инвалидности.

Согласно ГОСТу 12.1.003-76 "Шум. Общие требования безопасности" уровень шума в кабинетах не должен превышать 30 дБ, а в помещениях для приема больных на шумных производствах уровни шума не должны превышать 50 дБ.

Бактериальная обсемененность воздуха рабочих помещений должна составлять не выше 4000 колоний на куб. м бактерий и 50 колоний на куб. м представителей гемолитической микрофлоры.

При проведении соревнований не имеется шумящего оборудования, уровни шума которого превышают нормативные, а также используемые ПЭВМ и оргтехника имеют уровень шума и вибрации в пределах нормы.

4.1.3 Микроклимат

Микроклимат производственных помещений — это климат внутренней среды данных помещений, который определяется совместно действующими на организм человека температурой, относительной влажностью и скоростью движения воздуха, а также температурой окружающих поверхностей (ГОСТ 12.1.005 "Общие санитарно-гигиенические требования к воздуху рабочей зоны").

Поддержание микроклимата рабочего места в пределах гигиенических норм является важнейшей задачей охраны труда.

Оптимальная температура воздуха в кабинете согласно ГОСТу 12.1.005-76 "Воздух рабочей зоны. Общие санитарно-гигиенические требования" в холодные и переходные периоды года должна находиться в пределах 20 - 23 °С, в теплый период года - 20 - 25 °С при относительной влажности 60 - 40% и скорости движения воздуха не более 0,2 м/с во все периоды года. Во избежание нарушения теплового равновесия и охлаждения пациентов

при физикальном обследовании необходимо, чтобы разница температур воздуха по горизонтали (от наружных стен до любой точки внутри помещения) и вертикали (между полом и высотой 1,5 - 2 м) не превышали 1 - 2 °С. Кратность воздухообмена в кабинете не менее 1 раза в час обеспечивается использованием естественного проветривания.

В помещениях, оборудованных ПЭВМ, должна проводится ежедневная влажная уборка и систематическое проветривание после каждого часа работы на ПЭВМ.

При анализе помещения для проведения соревнований было выявлено, что температура воздуха составляет +24°С, относительная влажность - 45%. Также было выявлено, что помещение проветривают каждые пол часа, проводится ежедневная вечерняя влажная уборка помещения, в помещении имеется вентиляция.

4.1.5 Организация рабочего места

В соответствии с «Санитарно-эпидемиологические правила и нормативы СанПиН 2.2.2/2.4.1340-03»:

– площадь на одно рабочее место пользователей ПЭВМ с периферийными устройствами или орг.техникой в помещениях культурно-развлекательных учреждений и с ВДТ на базе плоских дискретных экранов (жидкокристаллические, плазменные) $S_{1р.м.} = 6$ м^2;

– расстояние между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора и тыла поверхности другого видеомонитора) принимается равным 1200 мм;

– расстояние между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора и экрана другого видеомонитора) принимается равным 2000 мм;

– высота рабочей поверхности стола для взрослых пользователей принимается равной 680-800 мм;

– глубина рабочей поверхности стола для взрослых пользователей принимается равной 800-1000 мм;

– ширина рабочей поверхности стола для взрослых пользователей принимается равной 1000-1200 мм;

– экран видеомонитора должен находиться от глаз пользователя на расстоянии равным 600-700 мм, но не ближе 500 мм;

– лица, работающие с ПЭВМ более 50 % рабочего времени, должны проходить обязательные предварительные при поступлении на работу и периодические медицинские осмотры в установленном порядке;

– женщины со времени установления беременности переводятся на работу, не связанные с использованием ПЭВМ, или для них ограничивается время с работой ПЭВМ (не более 3-х часов за рабочую смену) при условии соблюдения гигиенических требований, установленных настоящими Санитарными правилами

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

рабочий стул (кресло) должен быть подъемно-поворотным, регулируемым по высоте и углам наклона сиденья и спинки, а также расстоянию спинки от переднего края сиденья, при этом регулировка каждого параметра должна быть независимой, легко осуществляемой и иметь надежную фиксацию.

4.2 Экологичность

Так как результатом разработки бакалаврской работы является организация безопасности информации в медицинском учреждении.

Рассмотрим вопросы связанные с условием временного хранения и удаления отходов. В соответствии с нормами СанПин 2.1.7.728 выделяют следующие условия:

– открытое хранение и контакт персонала с отходами классов Б, В, Г вне помещений медицинского подразделения не допускается;

– хранение и транспортирование отходов по территории лечебно - профилактического учреждения классов А, Б, В допускается только в герметичных многоразовых контейнерах. Смещение потока удаления отходов класса В с другими потоками не допускается;

– при транспортировании отходов класса А разрешается применение автотранспорта, используемого для перевозки твердых отходов;

– использование автомашин, предназначенных для перевозки отходов класса классов Б и В для других целей, не допускается;

– хранение отходов класса Г производится в специально отведенных для этой цели вспомогательных помещениях;

– отходы класса А могут быть захоронены на обычных полигонах по захоронению твердых бытовых отходов. Отходы классов Б,В необходимо уничтожать на специальных установках по обезвреживанию отходов ЛПУ термическими отходами;

– обезвреживание отходов класса Б, В может осуществляться децентрализованным или централизованным способами;

– при отсутствии установки по обезвреживанию эпидемиологически безопасные патологоанатомические и органические операционные отходы (органы, ткани и т.п.) захораниваются на кладбищах в специально отведенных могилах;

– транспортирование, обезвреживание и захоронение отходов класса Г осуществляется в соответствии с гигиеническими требованиями, предъявляемыми к порядку накопления, транспортирования, обезвреживания и захоронения токсичных промышленных отходов.

Согласно требованиям СанПиН 2.1.7.1322-03 сбор и временное хранение ртутьсодержащих отходов должны осуществляться следующим образом:

– специализированном контейнере с чехлом, расположенном в отдельном помещении с ограниченным доступом персонала. Помещение должно быть сухим и светлым, иметь естественную и принудительную вентиляцию. Допускается хранение отработанных ртутьсодержащих ламп в неповрежденной таре из-

под новых ламп или в другой таре, обеспечивающей их сохранность при хранении, погрузочно-разгрузочных работах и транспортировании;

– место временного хранения должно быть промаркировано и оборудовано средствами локализации и удаления загрязнения ртутью при разрушении ламп или других приборов (демеркуризационным набором);

– хранение поврежденных ртутьсодержащих ламп должно осуществляться в специальной таре, не допускается совместное их хранение с неповрежденными лампами [20].

За использование, функционирование и утилизацию приборов освещения несет ответственность организация, предоставляющее помещение для проведения соревнований.

Также деятельность при проведении соревнований связана с документами, поэтому необходимо утилизировать бумажные документы при помощи шредера.

4.3 Чрезвычайные ситуации

Пожарная безопасность – это состояние объекта, при котором исключается возможность пожара, а в случае его возникновения используются необходимые меры по устранению негативного влияния опасных факторов пожара на людей, сооружения и материальные ценности.

Пожарная безопасность может быть обеспечена мерами пожарной профилактики и активной пожарной защиты. Пожарная профилактика включает комплекс мероприятий, направленных на предупреждение пожара или уменьшение его последствий.

Причины возникновения пожара делятся на:

– неэлектрические;

– электрические.

К неэлектрическим причинам относится: неосторожное и халатное обращение с огнем, неисправность оборудования и нарушение режима производственного процесса, самовоспламенение и самовозгорание отдельных веществ и т.д.

К причинам электрического характера относят короткое замыкание, перегрузки, большие переходные сопротивления, искрение и электрические дуги, статическое электричество и т.д.

Для предотвращения пожароопасных ситуаций должны применяться следующие меры:

– необходимо следить за исправным состоянием электропроводки, выключателей, розеток, с помощью которых в сеть включается оборудование, и аппаратуры;

– необходимо обеспечить возможность эвакуации людей;

– должны быть установлены пожарные сигнализации и средства пожаротушения;

– должны быть отведены места для курения;

– должны регулярно проводится противопожарный инструктаж сотрудников и занятия по пожарно-техническому минимуму.

Для обеспечения пожарной безопасности поликлиника ООО «АНКОР» оборудован огнетушителями, пожарными кранами и щитами. Все помещения оснащены автоматической системой пожаротушения, дымовыми датчиками, пожарной сигнализацией, звуковыми извещателями. По всему учреждению размещены планы помещения, эвакуационные выходы.

4.4 Комплексы физических упражнений для сохранения и укрепления индивидуального здоровья и обеспечения полноценной профессиональной деятельности

Для предупреждения преждевременной утомляемости пользователей ПЭВМ рекомендуется организовывать рабочую смену путем чередования работ с использованием ПЭВМ и без него. В качестве рекомендации предлагается:

– проведение упражнений для глаз через каждые 20 – 25 мин. работы за ПЭВМ;

– проведение упражнений физкультминутки в течение 1 - 2 мин. для снятия локального утомления, которые выполняются индивидуально при появлении начальных признаков усталости.

4.4.1 Упражнения для глаз

Упражнения для глаз необходимо выполнять сидя или стоя, отвернувшись от экрана монитора при ритмичном дыхании, с максимальной амплитудой движения глаз. Комплекс упражнений для глаз при работе с компьютером помогает уменьшить нагрузку на глаза и укрепляет глазные мышцы. Каждое упражнение повторяется 10 – 12 раз. Для гимнастики глаз рекомендуется выполнить следующие упражнения:

– закрыть рукой один глаз, затем посмотреть вдаль прямо перед собой 2-3 секунды;

– поставить карандаш на расстояние 15-20 см от глаз, смотреть на его кончик 3-5 секунд; затем перевести взгляд вдаль;

– перемещать карандаш от расстояния вытянутой руки к кончику носа и обратно, следя за его движением;

– открытыми глазами медленно, в такт дыханию, плавно рисовать глазами «восьмерку» в пространстве: по горизонтали, по вертикали, по диагонали;

– поставить карандаш на расстоянии 20-30 см от глаз, смотреть двумя глазами на конец карандаша 3-5 секунд, закрыть один глаз на 3-5 секунд, затем снова смотреть двумя глазами, закрыть другой глаз;

– смотреть 5-6 секунд на карандаш, расположив его на уровне глаз на расстоянии вытянутой руки, медленно отводить руку вправо, следить взглядом за карандашом, не поворачивая головы, повторить влево;

– сделать движения глазами.

4.4.2 Упражнения для снятия локального утомления

При офисной работе в сидячем положении, активность в мышцах значительно снижается, вследствие чего мышцы начинают ослабевать. Со временем их сокращения становится все медленнее, серьезно препятствуя циркуляция крови. Для того что бы сократить вероятность появления различных недугов, необходимо выполнять гимнастику для тела.

4.4.2.1 Упражнения для рук

Во время работы в офисе руки могут затекать из-за постоянного одинакового положения. Для предотвращения этого необходимо выполнять действия, представленные на рисунке 21.

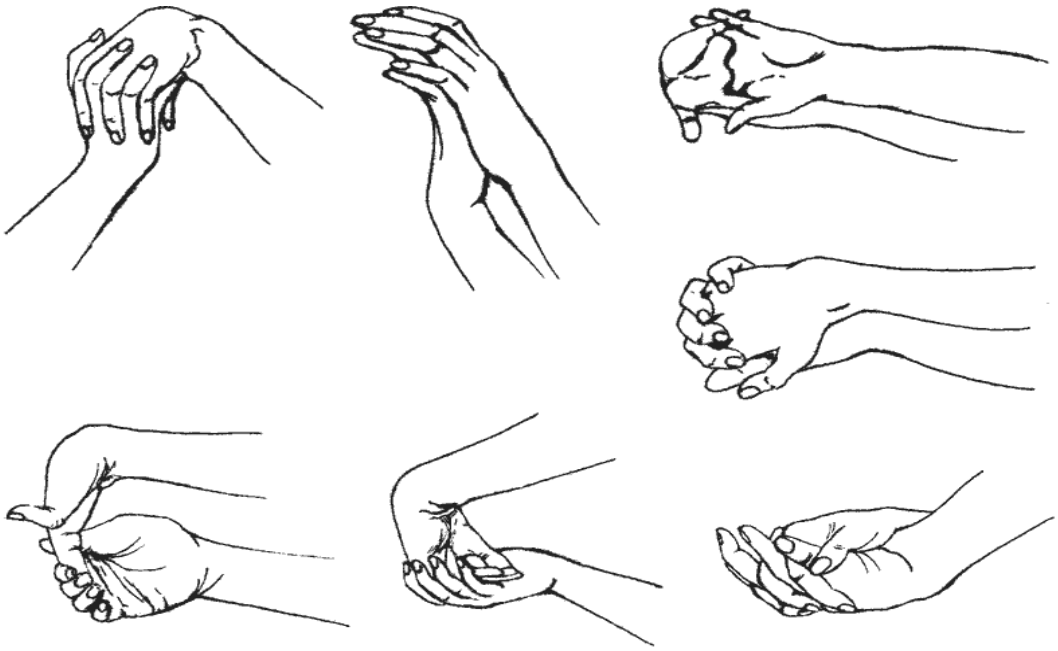

Рисунок 21 – Упражнения для рук

4.4.2.2 Упражнения для позвоночника

Основную часть нагрузки в течении всего рабочего дня несет на себе позвоночник. Для того чтобы убрать напряжение в спине, теле и суставах необходимо выполнить упражнения, представленные на рисунке 22. Каждое упражнение следует выполнять 10-12 раз.

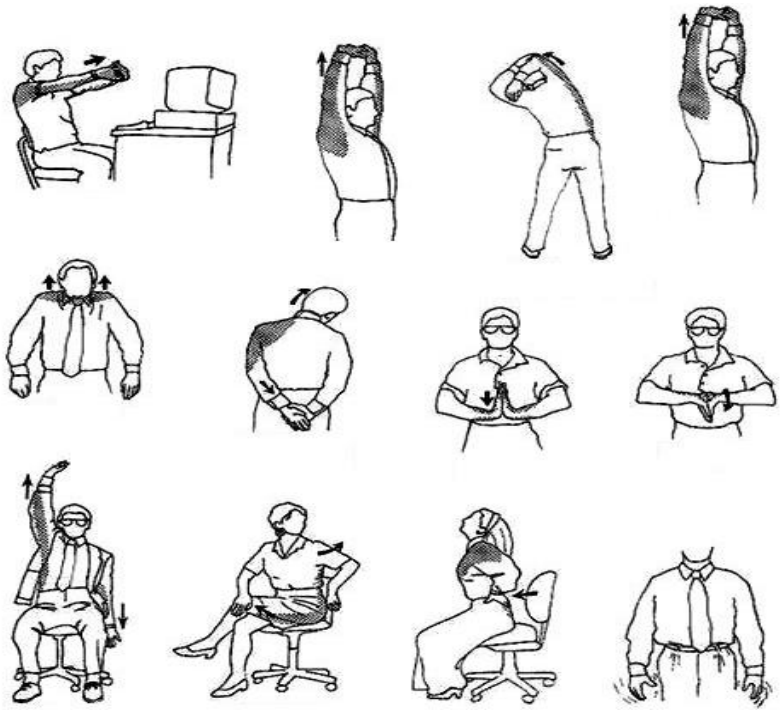

Рисунок 22 – Упражнения для позвоночника

4.4.2.3 Упражнения для ног

При сидячей работе необходимо восстанавливать кровообращение в нижней части тела, для предотвращения возникновения многих болезней. Небольшая разминка для ног на рабочем месте может включать в себя:

– поочередное поднятие носков от пола, пятки при этом двигаться не должны;

– действия аналогичные первому упражнению, но с пятками;

– попеременное сжатие и расслабление ягодиц;

– ножницы ногами: попеременное поднятие ног.

ЗАКЛЮЧЕНИЕ

Для каждого современного предприятия, компании или организации одной из самых главных задач является именно обеспечение информационной безопасности. Когда предприятие стабильно защищает свою информационную систему, оно создает надежную и безопасную среду для своей деятельности. Повреждение, утечка, неимение и кража информации – это всегда убытки для каждой компании.

Целью бакалаврской работы являлось создание комплексной защиты информации для одного из подразделений холдинга ЗАО «АНК», поликлиника ООО «АНКОР».

Для реализации поставленной задачи в рамках выполнения, бакалаврской работы были решены следующие задачи:

– проведен анализ предметной области, изучена организационная структура, рассмотрены организационные документы, внутренний и внешний документооборот;

– была рассмотрена существующая защита информации на предприятии и модернизирована;

– была проведена оценка конфиденциальности сохранения информации и написана простая программа для удобства расчета;

– были рассмотрены вопросы безопасности и жизнедеятельности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Комплексная система защиты информации на предприятии: учеб. пособие для студ. высш. учеб. заведений /В. Г.Грибунин, В.В.Чудовский. – М. : Издательский центр «Академия», 2009. – 416 с.Бейли, Л. М. Изучаем PHP и MySQL/ Л.М. Бейли. – М.: Эксмо, 2010. – 800 с.

2 Коцюба И.Ю., Чунаев А.В. – Основы проектирования информационных систем – Санкт-Петербург, 2015 – 145 с.Бенкен, Е.С. PHP, MySQL, XML: программирование для Интернета/ Е.С. Бенкен. – СПб: BHV, 2012. – 336 с.

3 Моругин, С.Л. Проектирование информационных систем. Методические указания по выполнению курсового проекта для студентов специальности 230102 (071900) - Нижний Новгород, НГТУ - 2006.

4 Маклаков С.В. BPWin и ERWin. CASE-средства разработки информационных систем.- М.: ДИАЛОГ-МИФИ, 2000 – 256 с.

5 Семененко В.А. Информационная безопасность: Учебное пособие. 2-е СЗО изд., стереот. – М.: МГИУ, 2005.- 215 с.

6 https://ru.wikipedia.org/wiki/Угрозы_информационной_безопасности#Классификация:[Электронный ресурс]: 22.05.2018.

7 Прохоров С.А., Федосеев А.А., Иващенко А.В. Автоматизация комплексного управления безопасностью предприятия / Самара: СНЦ РАН, 2008 – 55 с., ил.

8 Астахова, Л.В. Теория информационной безопасности и методология защиты информации: Конспект лекций.-Челябинск, 2006.-361 с

9 Информационная безопасность : нормативно-правовые аспекты [Текст] : учеб. пособие по специальностям 090102 «Компьютерная безопасность», 090105 "Комплексное обеспечение информ. безопасности автоматиз. систем" / Ю. А. Родичев.- СПб. и др. : Питер , 2008.-271 с.

10 Организационное обеспечение информационной безопасности [Текст] : учебник для высш. учеб. заведений по направлению «Информационная безопасность» / О.А. Романов, С.А. Бабин, С.Г. Жданов. – Ю.М. : Академия , 2008.

– 188 с.

11 Акулов О.А. Информатика: базовый курс: учебник / О.А. Акулов, Н.В. Медведев. – 4-е изд., стер. – М.: Омега-Л, 2007. – 560 с.

12 Анин Б.Ю. Защита компьютерной информации. – БХВ-Петербург, 2000. – 384 с.

13Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. — М.: Академический Проект; Гаудеамус,2004. – 544 с.

14 Информатика: учеб. пособие / С.М. Патрушина [и др.]; под ред. С.М. Патрушиной. – Изд. 2-е, перераб. и доп. – М.: МарТ; Ростов н/Д.: МарТ, 2004. – 400 с.

15Куприянов, А. И. Основы защиты информации [Текст] : учеб. пособие по специальностям «Радиоэлектрон. Системы», "Средства радиоэлектрон. борьбы" и "Информ. системы и технологии" / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов Ю.М. : Академия , 2007. – 253 с.

16 Правовое обеспечение информационной безопасности: учеб. пособие / под ред. С.Я. Казанцева. – 2-е изд., испр. и доп. – М.: Академия, 2007. – 238 с.

17Коноплева, И. А. Управление безопасностью и безопасность бизнеса [Текст] : учеб. пособие по специальности «Прикладная информатика (по обл.)» / И. А. Коноплева, И. А. Богданов .- М. : ИНФРА-М , 2008. – 446.

ПРИЛОЖЕНИЕ А

Техническое задание

1. ОБЩИЕ ДАННЫЕ

1.1. Основание для выполнения работ: Приказ руководства ООО АНКОР» о модернизации КСЗИ.

1.2. Источник финансирования:

- средства компании ООО «АНКОР».

1.3. Назначение системы: КСЗИ служит для эффективного противодействия, как известным, так и потенциально возможным атакам на защищаемые информационные ресурсы предприятия (серверы, рабочие станции, периферийное оборудование) с целью безопасного информационного взаимодействия пользователей информационной системы, организации их доступа к файловым хранилищам и удаленному терминальному серверу.

1.4. Рекомендации в соответствии, с которыми выполняется модернизация КСЗИ:

Модернизация КСЗИ необходимо осуществлять с учетом возможности использования современного оборудования, а так же при определении количества информационных ресурсов предприятия возможность их увеличения в связи с развитием предприятия или изменения назначения помещения.

Нормативные документы, в соответствии с которыми выполняются работы:

Градостроительный кодекс Российской Федерации от 29.12.2004 № 190-ФЗ;

ГОСТ 21.101-97 СПДС «Основные требования к проектной и рабочей документации»;

ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные». Классификация. Общие технические требования. Методы испытаний;

ПРИЛОЖЕНИЕ А

ГОСТ Р 50777-95 «Системы тревожной сигнализации». Часть 2. Требования к системам охранной сигнализации. Раздел 6. «Пассивные оптико-электронные инфракрасные извещатели для закрытых помещений».

Р 78.36.005-99 Выбор и применение систем контроля и управления доступом

ГОСТ Р 50571.22-2000. «Электроустановки зданий. Заземление оборудования обработки информации».

и другие действующие нормативные документы.

1.5. Состав выполняемых работ:

- Поставка оборудования.
- Монтажные работы.

2. ОБЩИЕ ТРЕБОВАНИЯ К КСЗИ

2.1. Она должна быть всеохватывающей, учитывающей все объекты и составляющие их компоненты защиты, все обстоятельства и факторы, влияющие на безопасность информации, и все виды, методы и средства защиты;

2.2 Она должна быть достаточной для решения поставленных задач и надежной во всех элементах защиты, т. е. базироваться на принципе гарантированного результата;

2.3 Она должна быть целостной: содержать все ее составляющие, иметь структурные связи между компонентами, обеспечивающие ее согласованное функционирование;

2.4. Модернизации подлежат:

2.5.1. Главный вход в предприятие (КПП).

2.5.2. Рабочие помещения предприятия.

3. ТРЕБОВАНИЯ К ПОДСИСТЕМАМ КСЗИ.

3.1. Требования к КПП предприятия.

3.1.1. КПП должно быть оснащены системами охранной сигнализации, видеонаблюдения, контроля и управления доступом.

3.1.2. Пост охраны (КПП) должно быть оснащено всем необходимым оборудованием для надежного контроля при проникновении.

3.1.3. В составе поставки специального оборудования должны входить все необходимые сервисы производителя для обеспечения гарантии не менее 1 года на ремонт и замену неисправного оборудования, техническую поддержку производителя, обновление программного обеспечения.

3.1.4 Пост охраны должен быть оборудован системами бесперебойного питания для осуществления непрерывного контроля за объектом.

3.2. Требования рабочим помещениям предприятия

3.2.1. Каждый рабочий кабинет должен быть оснащен системами пожарной, охранной сигнализации.

3.2.2 Главный коридор должен быть оснащен системами видеонаблюдения, пожарной охраны.

4. СОСТАВ И ТРЕБОВАНИЯ К ВЫПОЛНЕНИЮ РАБОТ

4.1. Пусконаладочные работы.

4.1.1. Пусконаладка оборудования должна обеспечить надежное соединение всех компонентов.

4.1.2. Должна быть проведена пусконаладка ИБП в соответствии с рекомендациями производителя, а также проверка его работоспособности в различных режимах эксплуатации, включая имитацию пропадания напряжения в сети и перехода ИБП на питание от батарей и обратно, с замером реального времени поддержки работы оборудования от батарей.