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
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: Разработка программного продукта для расчета защищенности помещения от утечки информации по электромагнитному каналу

Исполнитель
студент группы 455 об _____ А.А. Цыплухина
(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 Цыплухиной Анастасии Александровны

1. Тема бакалаврской работы: Разработка программного продукта для расчета защищенности помещения от утечки информации по электромагнитному каналу

(утверждено приказом от 22.05.2018 № 1109-уч)

2. Срок сдачи студентом законченной работы _____

3. Исходные данные к бакалаврской работе: отчет о прохождении преддипломной практики, разработка проекта системы расчета и его реализация.

4. Содержание бакалаврской работы: анализ предметной области; проектирование информационной системы; разработка информационной системы; анализ угроз; рекомендации по обеспечению безопасности на предприятии.

5. Перечень материалов приложения: таблицы, программный код.

6. Консультанты по бакалаврской работе: консультант по безопасности и экологичности, А.Б. Булгаков, доцент, канд. техн. наук.

7. Дата выдачи задания: _____

Руководитель бакалаврской работы: Самохвалова Светлана Геннадьевна, доцент, канд. техн. наук.

Задание принял к исполнению_____ А.А. Цыплухина

РЕФЕРАТ

Бакалаврская работа содержит 67 с., 17 рисунков, 19 источников, 3 приложения.

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ, ЗАЩИТА ИНФОРМАЦИИ, КОНТРОЛИРУЕМАЯ ЗОНА, НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ, ИНФОРМАЦИЯ, СИСТЕМА, МЕТОД, МОДУЛЬ, БАЗА ДАННЫХ, ИНТЕРФЕЙС, УГРОЗЫ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, ЭЛЕКТРОМАГНИТНЫЕ ИЗЛУЧЕНИЯ, СРЕДСТВА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Защищенность – способность информационной системы противостоять утечке информации, несанкционированному доступу к программам, информации, умышленному или случайному их искажению или разрушению.

Целью работы является разработка программного продукта для расчета защищенности информации по электромагнитному каналу. Для достижения этой цели необходимо выполнить некоторые задачи: анализ и разработка проекта защиты информации, включающий следующие функции:

– расчет данных;

– перерасчет данных;

– вывод результата;

– подсчет расстояния, необходимого для обеспечения безопасности;

– формирование отчётов.

На основе теории был создан программный продукт, соответствующий поставленной задаче. Для создания программного обеспечения была использована среда разработки Visual Studio 2017.

СОДЕРЖАНИЕ

НОРМАТИВНЫЕ ССЫЛКИ

В настоящей бакалаврской работе использованы ссылки на следующие стандарты и нормативные документы:

СТО СМК 4.2.3.21-2018 Оформление выпускных квалификационных и курсовых работ (проектов)

ГОСТ Р 51275-2006 Объект информатизации. Факторы, воздействующие на информацию

ФСТЭК РФ 15.02.2008 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных

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

ФСТЭК РФ 12.01.2016 № 240/24/87 Информационное сообщение по вопросу продления сроков действия сертификатов соответствия на средства активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок, и средства активной акустической и вибрационной защиты акустической речевой информации, эксплуатируемые на объектах информатизации

Федеральный закон от 21.12.1994 № 68-ФЗ О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера

ФСТЭК РФ 14.06.2017 № 240/24/2816 Информационное сообщение по вопросу продления сроков действия сертификатов соответствия на средства активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок, и средства активной акустической и вибрационной защиты акустической речевой информации, эксплуатируемые на объектах информатизации

ФСТЭК РФ 28.12.2016 № 240/24/6312 Информационное сообщение по вопросу продления сроков действия сертификатов соответствия на средства защиты информации от утечки по техническим каналам

СПИСОК ОБОЗНАЧЕНИЙ И СОКРАЩЕНИЙ

ТСПИ – технические средства приема информации;

ЭМИ – электромагнитные излучения;

ТСОИ – технические средства обработки информации;

ПЭМИН – побочные электромагнитные излучения и наводки;

СВТ – средства вычислительной техники;

ПЭВМ – персональная электронно-вычислительная машина;

ТС – технические средства;

КЗ – контролируемая зона;

ПО – программное обеспечение;

ОС – операционная система;

ОТСС – основные технические средства и системы;

НСД – несанкционированный доступ;

ВДТ – видеодисплейный терминал;

ПДК – предельно-допустимая концентрация.

ВВЕДЕНИЕ

Широкое применение вычислительной техники и электроники во всех сферах деятельности человека является в нынешнее время приоритетным.

Масштабы и сферы применения этой техники таковы, что возникают проблемы обеспечения безопасности, циркулирующей в ней информации. В истории известно множество случаев кражи информации, которые приводили к негативным последствиям для ее владельцев. Технологические, производственные и коммерческие данные, которые используют предприятия, обладают высокой стоимостью, а их утрата или утечка может привести к серьезным финансовым потерям. На любом предприятии очень важно выявить и исключить все возможные угрозы утечки информации. Злоумышленники, ради получения конфиденциальной информации, готовы использовать разные способы ее получения:

- технические средства перехвата;
- программно-математические;
- использование нетрадиционных информационных каналов;
- непосредственный доступ в операционную среду.

Информация передается по различным каналам связи, которые должны быть защищены надлежащим образом. В случае слабой защиты этих каналов, информация может стать доступной для посторонних лиц. Для устранения таких ситуаций используются различные технические средства, которые не позволяют информации распространяться дальше заданной зоны. Каналы, по которым информация распространяется за пределы контролируемой зоны, называются каналами утечки информации. Один из преимущественно уязвимых каналов передачи информации является электромагнитный. Самое важное понять причины возникновения электромагнитных излучений и изучить устройства, использующиеся для перехвата информации.

Целью бакалаврской работы является разработка программного продукта, позволяющего оценить защищенность помещения от утечки информации по электромагнитному каналу.

Задачами бакалаврской работы, в связи с указанной целью, являются:

– анализ предметной области;

– проектирование информационной системы;

– разработка информационной системы;

– исследование угроз утечки информации;

– разработка рекомендаций по обеспечению безопасности на предприятии.

Создание данного программного продукта позволит обеспечить быстрый расчет с предоставлением рекомендаций по необходимому расстоянию до границы контролируемой зоны, если по результатам расчета этого расстояния будет недостаточно.

1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

1.1 Электромагнитный канал утечки информации

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Канал утечки информации (или технический канал утечки) – это путь информации, который она может пройти от источника информации до приемника/получателя в процессе случайной утечки или целенаправленного несанкционированного получения закрытой информации. Если меры по защите информации не были приняты заранее, то могут быть задействованы любые каналы утечки. Если же защита информации предусмотрена – то будет задействован наиболее слабозащищенный канал.

Причиной утечек информации может стать: использование ошибочных норм защиты информации, их нарушение или же полное несоблюдение. Малейшие отступления от правил работы с критически важными документами, техникой, продукцией и прочими конфиденциальными материалами чреваты возникновением канала утечки информации ограниченного доступа.

В некоторых ТСПИ (например, системах звукоусиления) носителем информации является электрический ток, параметры которого (сила тока, напряжение, частота и фаза) изменяются по закону изменения информационного речевого сигнала. При протекании электрического тока по токоведущим элементам ТСПИ и их соединительным линиям в окружающем их пространстве возникает переменное электрическое и магнитное поле. В силу этого элементы ТСПИ можно рассматривать как излучатели электромагнитного поля, модулированного по закону изменения информационного сигнала.

Электромагнитная энергия, определяемая электрической и магнитной компонентой электромагнитного поля низкой частоты, колеблется около излучателя.

Магнитная и электрическая составляющие электромагнитного поля убывают обратно пропорционально соответственно третьей и второй степеням от расстояния. Характер и структура поля определяется величиной тока точечного излучателя, суммарной площадью его витков, через которые протекает ток, количеством точечных излучателей, и их взаимным расположением относительно точки, в которой находится измерительный преобразователь. Известны методы, позволяющие снизить значение напряженности электромагнитного поля в разумных пределах. Локализация полей обеспечивает снижение напряженности электромагнитного поля экранированием источника излучения с использованием электромагнитных НЧ экранов различной степени сложности их конструкций. Решая задачу ослабления уровней полей, экраны оказывают влияние на параметры экранируемых полей. Такое влияние может быть существенным при локализации магнитного поля головок громкоговорителей, так как помимо магнитного поля, экран ослабляет акустическое поле либо существенно ослабляет его при ненайденном компромиссном решении (максимум ослабления магнитного поля при минимуме ослабления и искажения акустического поля).

К аппаратуре, предназначенной для эксплуатации на подвижных объектах и особенно летательных и космических аппаратах, предъявляются жесткие требования по габаритновесовым характеристикам. В то же время экранирующие свойства экранов улучшаются с утолщением экранов и увеличением их радиусов. Характеристики пермалоевых экранов резко ухудшаются при воздействии на них вибрации и ударов в условии эксплуатации. В этой связи возникла новая проблема локализации магнитных полей в ближней зоне точечных источников без ухудшения габаритновесовых характеристик аппаратуры, а также качества излучения акустических полей акустическими излучателями. Для решения указанной проблемы следует исследовать распределения магнитного поля от одного, двух, четырех n источников, расположенных в ограниченном объеме путем решения задачи создания приемников электрического и магнитного полей, не подверженных влиянию внешних помех, обеспечивая при этом высокую точность оценки параметров полей.

1.2 Требования к средствам измерения побочных электромагнитных излучений и наводок средств вычислительной техники и условиям проведения измерений

Подготовка эталонных образов и сигналов исследуемых технических средств:

– автоматизированное (без участия оператора) обнаружение, распознавание (определение принадлежности к исследуемому техническому средству) и измерение уровней сигналов;

– полуавтоматическое (с участием оператора) обнаружение и измерение уровней сигналов технических средств;

– анализ электромагнитной обстановки в месте проведения контроля;

– обработка результатов измерений и расчет зон возможного перехвата ПЭМИН, затухания в линиях;

– формирование протокола измерений и передача его в выбранный редактор для коррекции и вывода на печать.

В электромагнитных каналах утечки информации носителем информации являются электромагнитные излучения (ЭМИ), возникающие при обработке информации техническими средствами. Основными причинами возникновения электромагнитных каналов утечки информации в ТСОИ являются:

– побочные электромагнитные излучения, возникающие вследствие протекания информативных сигналов по элементам ТСОИ;

– модуляция информативным сигналом побочных электромагнитных излучений высокочастотных генераторов ТСОИ (на частотах работы высокочастотных генераторов);

– модуляция информативным сигналом паразитного электромагнитного излучения ТСОИ (например, возникающего вследствие самовозбуждения усилителей низкой частоты).

Побочным электромагнитным излучением (ПЭМИ) ТСОИ называется нежелательное радиоизлучение, возникающее в результате нелинейных процессов в блоках ТСОИ.

Побочные электромагнитные излучения возникают при следующих режимах обработки информации средствами вычислительной техники:

– вывод информации на экран монитора;

– ввод данных с клавиатуры;

– запись информации на накопители;

– чтение информации с накопителей;

– передача данных в каналы связи;

– вывод данных на периферийные печатные устройства – принтеры, плоттеры; запись данных от сканера на магнитный носитель и т.д.

При каждом режиме работы СВТ возникают ПЭМИ, имеющие свои характерные особенности. Диапазон возможных частот побочных электромагнитных излучений СВТ может составлять от 10 кГц до 2 ГГц.

Паразитным электромагнитным излучением ТСОИ называется побочное радиоизлучение, возникающее в результате самовозбуждения генераторных или усилительных блоков ТСОИ из-за паразитных связей. Наиболее часто такие связи возникают за счёт случайных преобразований отрицательных обратных связей (индуктивных или ёмкостных) в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов. Частота автогенерации (самовозбуждения) лежит в пределах рабочих частот нелинейных элементов усилителей (например, полупроводниковых приборов). В ряде случаев паразитное электромагнитное излучение модулируется информативным сигналом (модуляцией называется процесс изменения одного или нескольких параметров электромагнитного излучения (например, амплитуды, частоты или фазы) в соответствии с изменениями параметров информативного сигнала, воздействующих на него).

Для перехвата побочных электромагнитных излучений СВТ используются специальные стационарные, перевозимые и переносимые приёмные устройства, которые называются техническими средствами разведки побочных электромагнитных излучений и наводок (ТСР ПЭМИН).

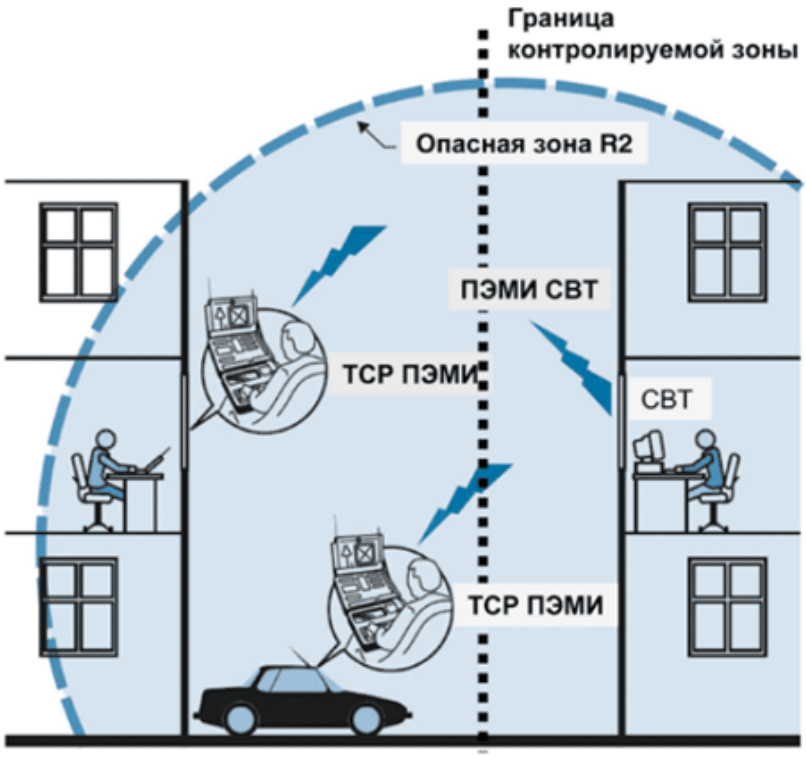

Рисунок 1 – Перехват побочных электромагнитных излучений (ПЭМИ) средств вычислительной техники (СВТ) техническими средствами разведки побочных электромагнитных излучений (ТСР ПЭМИН)

Типовой комплекс разведки ПЭМИ включает: специальное приёмное устройство, ПЭВМ (или монитор), специальное программное обеспечение и широкодиапазонную направленную антенну. В качестве примера на рис. 3 приведён внешний вид одного из таких комплексов.

Средства разведки ПЭМИ могут устанавливаться в близлежащих зданиях или машинах, расположенных за пределами контролируемой зоны объекта. Это наглядно показано на рисунке 1.

Наиболее опасным (с точки зрения утечки информации) режимом работы СВТ является вывод информации на экран монитора. Учитывая широкий спектр ПЭМИ видеосистемы СВТ ($DF_c > 100$ МГц) и их незначительный уровень, перехват изображений, выводимых на экран монитора ПЭВМ, является довольно трудной задачей.

Дальность перехвата ПЭМИ современных СВТ, как правило, не превышает 30-50 м.

Качество перехваченного изображения значительно хуже качества изображения, выводимого на экран монитора ПЭВМ, как показано на рисунке 2.

Особенно трудная задача - перехват текста, выводимого на экран монитора и написанного мелким шрифтом. Это представлено на рисунке 3.

Рисунок 2 – Тестовое изображение, выведенное на экран монитора и изображение, перехваченное средством разведки ПЭМИ

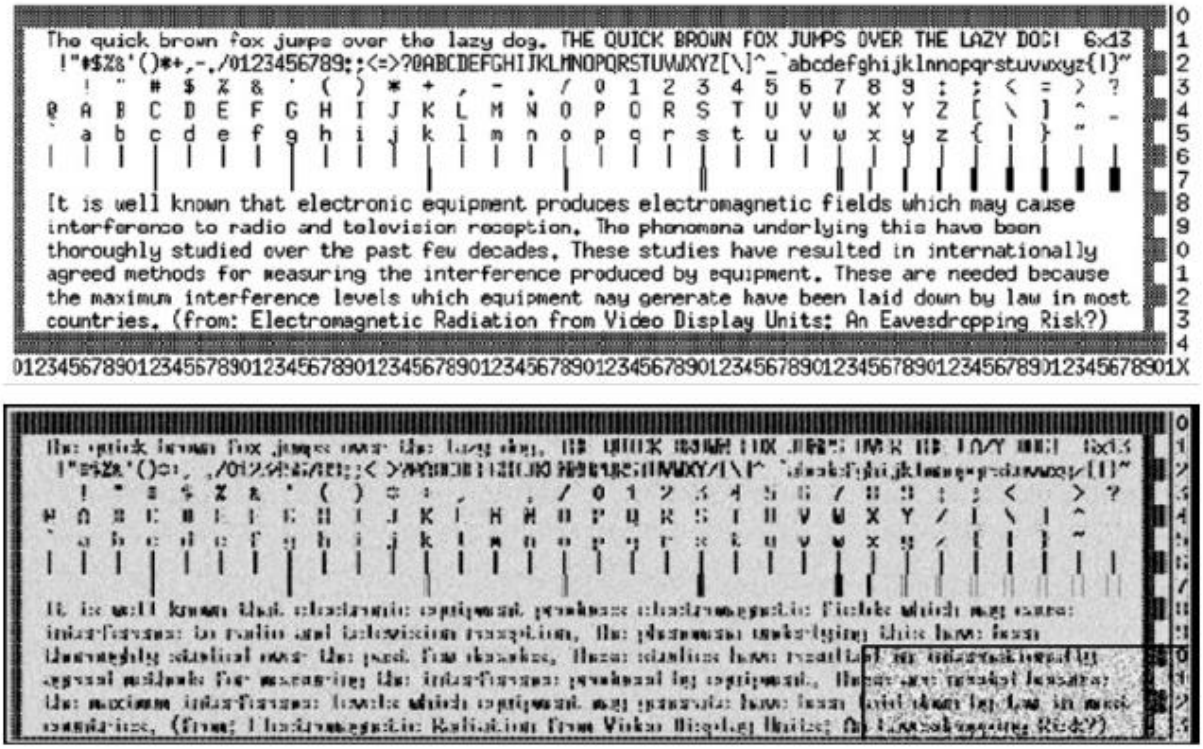

Рисунок 3 – Исходный текст, выведенный на экран монитора (режим работы VGA монитора 800*600 @ 75Hz, тактовая частота F_m= 49,5МГц, размер букв 6 х 13 пикселей) и текст, перехваченный средством разведки ПЭМИ (DFпр = 200 МГц)

1.3 Показатели эффективности защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

В качестве показателя оценки эффективности защиты информации от утечки по техническим каналам используется вероятность правильного обнаружения информативного сигнала (P_0) приёмным устройством средства разведки.

В качестве критерия обнаружения наиболее часто используется критерий «Неймана-Пирсона». В зависимости от решаемой задачи защиты информации пороговое значение вероятности обнаружения информативного сигнала может составлять от 0,1 до 0,8, полученное при вероятности ложной тревоги от 10^{-3} до 10^{-5}.

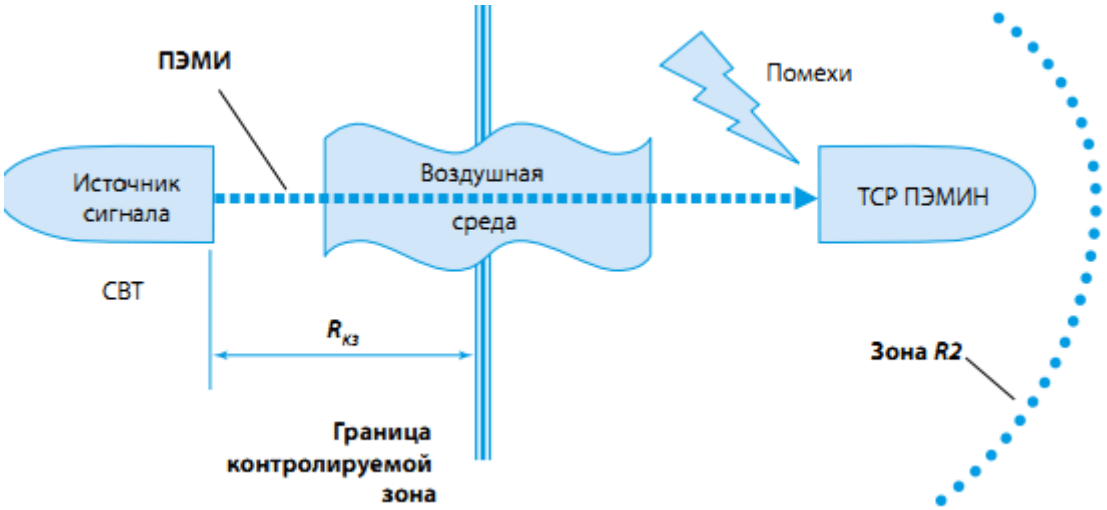

Рисунок 4 – Схема технического канала утечки информации, возникающего за счёт побочных электромагнитных излучений СВТ (схема электромагнитного канала утечки информации)

Зная характеристики приёмного устройства и антенной системы средства разведки, можно рассчитать допустимое (нормированное) значение напряжённости электромагнитного поля, при котором вероятность обнаружения сигнала приёмным устройством средства разведки будет равна некоторому (нормированному) значению ($P_0 = P_П$).

Пространство вокруг ТСОИ, на границе и за пределами которого напряжённость электрической (E) или магнитной (H) составляющей электромагнитного поля не превышает допустимого (нормированного) значения ($E \leq E_n$; $H \leq H_n$, называется опасной зоной 2 (R2).

Зона R2 для каждого СВТ определяется инструментально-расчётным методом при проведении специальных исследований СВТ на ПЭМИ и указывается в предписании на их эксплуатацию или сертификате соответствия.

Таким образом, для возникновения электромагнитного канала утечки информации необходимо выполнение двух условий:

– первое – расстояние от СВТ до границы контролируемой зоны должно быть менее зоны R2 R < R2);

– второе – в пределах зоны R2 возможно размещение стационарных или перевозимых (переносимых) средств разведки ПЭМИН.

Наглядно это видно на рисунке 4.

1.4 Оценочный расчет защищенности помещения от утечки информации

Обобщенный электромагнитный канал (канал побочных электромагнитных излучений и наводок – ПЭМИН) состоит из каналов утечки, причинами возникновения которых являются:

– излучения и окружающее пространство (в дальней зоне) электромагнитных полей технических средств (ТС) и соединяющих их линий связи (например, электромагнитное поле монитора и других устройств ПЭВМ);

– излучение в окружающее пространство (в ближней зоне) электрической составляющей электромагнитного поля ТС (например, электрическое поле, излучаемое клавиатурой);

– излучение в окружающее пространство (в ближней зоне) магнитной составляющей электромагнитного поля ТС (например, магнитное поле усилителя звуковой частоты);

– паразитные наводки на отходящие и проходящие вблизи от ТС провода и кабели, на расположенные рядом внешние технические средства связи, взаимные наводки между линиями связи

В свою очередь, паразитные наводки могут обусловливаться:

– непосредственными электрической и магнитной паразитными связями в ближней зоне (например, наводки на провода электропитания, заземления (зануления), выходящие из ПЭВМ линии связи – сетевой адаптер, модем);

– емкостной и индуктивной паразитными связями по посторонним проводам, проходящим рядом с ПЭВМ (например, проходящие вблизи ПЭВМ телефонные провода и стоящие рядом телефонные аппараты, провода и кабели от других устройств и т. п.);

– паразитной связью через электромагнитное поле излучения в дальней зоне (например, наводки на провода, кабели ТС, расположенные на значительном удалении от ПЭВМ, но проходящие в непосредственной близости от линий передачи данных (телефонных проводов и кабелей ЛВС) и проводов электропитания, выходящих из ПЭВМ;

– паразитными связями через общее полное сопротивление (например, наводки на провода электропитания, осуществляются через элементы фильтров питания).

Наличие сигналов, несущих конфиденциальные сообщения, на границе и за пределами контролируемой зоны (КЗ) создает условия для утечки сообщений за счет перехвата этих сигналов злоумышленниками.

Совокупность источника информативного сигнала, среды распространения этого сигнала и приемника перехвата злоумышленника представляет собой «канал утечки» сообщений, эффективность которого определяется следующими факторами:

– уровень информативного канала от источника;

– ослабление и искажение сигнала в среде его распространения;

– технические характеристики приемного устройства, используемого злоумышленником.

Чем ближе приемник сигнала к источнику, тем эффективнее работает канал утечки. Системным показателем качества перехвата утечки является отношение сигнал/помеха на входе приемника перехвата, которое определяется соотношениями параметров всех элементов канала утечки.

При организации защитных мероприятий исходят из того, что приемное устройство для перехвата информативных сигналов реализует потенциальную помехоустойчивость и может быть размещено в любом месте за пределами контролируемой зоны, вплоть до ее границы. При этом считается, что наблюдение и перехват могут осуществляться непрерывное течение времени любой продолжительности.

Определяющий вид помех в канале утечки сообщений – аддитивные помехи, характеризующиеся тем, что смесь сигнала s(t) и помехи n(t) на входе приемника представляют собой их сумму: x(t)= s(t)+ n(t).

Примером аддитивных помех являются:

– атмосферные помехи, обусловленные электрическими процессами в атмосфере, прежде всего грозовыми разрядами;

– космические помехи, вызванные радиоизлучением Солнца и других небесных тел;

– внутренние шумы радиоприемника, обусловленные хаотическим движением носителей заряда в самом приемнике;

– индустриальные помехи, обусловленные работой электрических устройств и агрегатов;

– помехи от посторонних радиостанций.

Атмосферные помехи – тот вид помех, который всегда присутствует в окружающем пространстве, поэтому при определении дальности распространения сообщений по каналу ПЭМИН необходимо учитывать не только естественное затухание сигнала, но и искажения, вносимые этими помехами. Остальные виды помех в данной лабораторной работе не учитываются.

В помещении, показанному на рисунке 5, расположена ПЭВМ, на которой обрабатываются конфиденциальные данные. Расстояние от ПЭВМ до контролируемой зоны составляет r = 15м. Граница контролируемой зоны проходит по периметру железобетонной стены толщиной 160 мм, в стене имеется оконный проем, не превышающий 30% от площади стены. Окно закрыто металлической решеткой с ячейкой 5см, соответствуя таблице А.1, пункту 6 в приложении А. Значения напряженности электромагнитного поля Е, создаваемого ПЭВМ на частотах 100 МГц, 500 МГц и 1000 МГц, берется из таблицы А.2, пункта 6 в приложении А. при определении коэффициента затухания принимаем n = 1,4. В качестве критерия защищенности помещения от утечки информации на границе контролируемой зоны отношение сигнал/шум принимается равным $\Delta \leq 1$. Расчет

среднеквадратического значения напряженности поля атмосферных помех E_a производился при T_a =293° К и $f_{пр}$ = 40 МГц.

Для расчета среднеквадратического значения напряженности поля E_a атмосферных помех используется следующая формула:

$$E_a = 10 \lg (Ta/To) – 125,5 + 20\lg f + 10\lg f_{экр}, дБ, \quad (1)$$

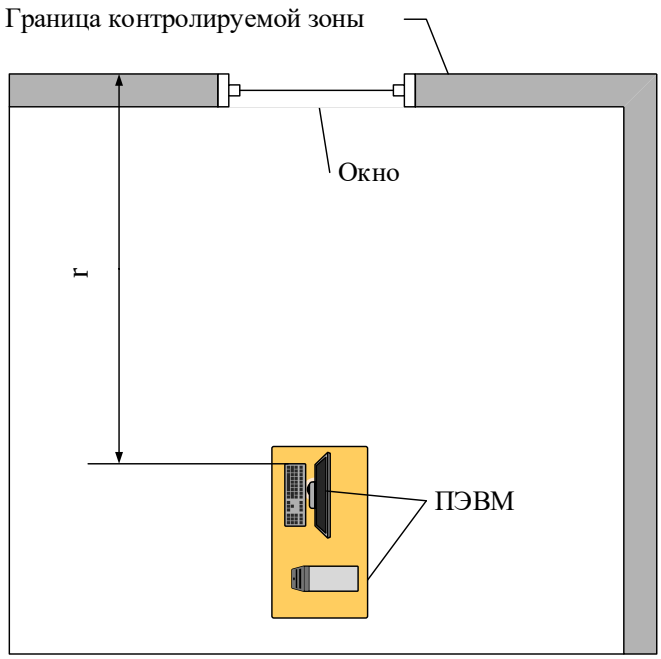

Рисунок 5 – Схема помещения для проведения расчетов

$$E_a = 10 \lg\left(\frac{293}{273}\right) – 125,5 + 20 \lg(100) + 10 \lg(40000000) = -9,2 дБ$$ (на частоте 100 МГц)

$$E_a = 10 \lg\left(\frac{293}{273}\right) – 125,5 + 20 \lg(500) + 10 \lg(40000000) = 4,8 дБ$$ (на частоте 500 МГц)

$$E_a = 10 \lg\left(\frac{293}{273}\right) – 125,5 + 20 \lg(1000) + 10 \lg(40000000) = 10,8 дБ$$ (на частоте 1000 МГц)

где f – частота (МГц);

$f_{экр}$ – ширина полосы пропускания приемника (Гц);

Та – эквивалентная шумовая температура, характеризующая интенсивность помех; То = 273 °К.

Ширина полосы пропускания приемника $f_{пр}$ в диапазоне частот выше 30 МГц должна быть не менее 40 МГц, что соответствует характеристикам целого ряда устройств, предназначенных для съема и анализа информации с ПЭВМ.

Измеренные в дБ значения необходимо перевести в мкВ/м:

$$E_a = 10^{0,05E(дБ)} \text{ (мкВ/м)}$$

В соответствии с выражением (1) и значениях T_a =293° К, $f_{пр}$ = 40 МГц среднеквадратическая напряженность поля E_a:

– на частоте 100 МГц – E_a = - 9.2 дБ (0,346 мкВ/м);

– на частоте 500 МГц – E_a = 4.8 дБ (1,738 мкВ/м);

– на частоте 1000 МГц – E_a = 10.8 дБ (3,467 мкВ/м).

Электромагнитное поле, создаваемое промышленными ВЧ-установками, затухает со средним коэффициентом:

$$k_з = 1/r^n, \qquad (2)$$

$$k_з = \frac{1}{15^{1,4}} = 0,0226$$

где r – расстояние от источника;

n = 1,3 … 2,8 (n = 1,3 – для открытых сельских районов;

n = 2,8 – для интенсивно застроенных городских районов).

Напряженность электромагнитного поля, создаваемого ПЭВМ, сертифицированной по ЭМС в соответствии с требованиями CISPR, не должна превышать:

– в диапазоне 30-230 МГц – 630,5 мкВ/м;

– в диапазоне 230-1000 МГц – 1412,5 мкВ/м.

Электромагнитное поле также затухает с коэффициентом $k_{экр}$ при распространении через ограждающие конструкции. Значения коэффициентов экранирования некоторых ограждающих конструкций приведены в таблице А.1, приложении А.

Значения коэффициентов экранирования некоторых ограждающих конструкций на частотах 100, 500 и 1000 МГц

Напряженность электромагнитного поля Е на границе контролируемой зоны вычисляется по следующей формуле:

$$E_{кз} = E * k_з / k_{экр} \text{ (мкВ/м)}, \quad (3)$$

$$E_{кз} = 610 * \frac{0,0226}{39,8} = 0,346 \text{ мкВ/м (на частоте 100 МГц)}$$

$$E_{кз} = 1370 * \frac{0,0226}{22,4} = 1,38 \text{ мкВ/м (на частоте 500 МГц)}$$

$$E_{кз} = 1390 * \frac{0,0226}{17,8} = 1,76 \text{ мкВ/м (на частоте 1000 МГц)}$$

где Е – напряженность электромагнитного поля непосредственно у ПЭВМ;

$k_з$ – коэффициент затухания (2);

$k_{экр}$ – коэффициент экранирования из таблицы А.1, приложения А.

Для определения отношения сигнал/шум используем выражение, которое определяется отношением напряженности электромагнитного поля на границе контролируемой зоны к среднеквадратическому значению напряженности поля:

$$\Delta = \frac{E_{кз}}{E_а}. \quad (4)$$

Для практического применения формулы (4) необходимо определить максимальное значение Δ, при котором исключается определение злоумышленником содержания (смысла) перехваченного сообщения, т. е. определить смысловой критерий безопасности сообщений.

Известно, что значение Δ не должно превышать значения 1,0 для важной информации (5) и значения 0,7 – для весьма важной информации (6).

$$\Delta = \frac{0{,}346}{0{,}346} = 0{,}999 \approx 1 \text{ (на частоте 100 МГц)}$$

$$\Delta = \frac{1{,}38}{1{,}738} = 0{,}79 \text{ (на частоте 500 МГц)}$$

$$\Delta = \frac{1{,}76}{3{,}467} = 0{,}51 \text{ (на частоте 1000 МГц)}$$

Вывод: Расчеты показали, что на всех частотах значение $\Delta \leq 1$. следовательно, расстояние до границы контролируемой зоны достаточно для обеспечения безопасности сообщений, излучаемых в окружающее пространство ПЭВМ. Дополнительных мер по обеспечению защиты помещения от утечки информации не требуется.

Если $\Delta > 1$, приравниваем значение $E_{кз}$ к $E_а = 0{,}346$ и делаем перерасчет r по формуле:

$$r = \sqrt[n]{\frac{E}{E_{кз} * k_{экр}}}$$

При частоте кадровой развертки 85 Гц и просмотре изображения в течение 15с отношение сигнал/шум Δ на границе контролируемой зоны должно быть не более 0,04. Время, равное 15 с, выбрано из тех соображений, что устройства, осуществляющие накопление сигналов на фоне помех, эффективно работают только в течение первых 10-15с после перехвата сообщений. Результаты расчета приводятся в таблице А.3, приложении А.

Для автоматизации расчетов защищенности помещения необходимо создать программный продукт, который облегчит и ускорит процесс ручного подсчета.

2 ПРОЕКТИРОВАНИЕ ПРОГРАММНОГО ПРОДУКТА

Проектируемая программу имеет базу данных, в которой хранятся данные и формулы, а также пользовательский интерфейс. Программа должна будет загружать данные из файла, производить расчет и выдавать результат. При желании, пользователь может сохранить результат в виде отчета. Структурная схема работы программы показана на рисунке 6.

Рисунок 6 – Структурная схема работы программы

Для системы необходимо, чтобы пользователь вводил свои данные. На основе них и производятся расчеты. Далее пользователь выбирает, сохранять результат или нет. Также необходимо программное и техническое обеспечение для непосредственной работы системы. Функциональная модель программы представлена на рисунке 7, а ее декомпозиция на рисунке 8.

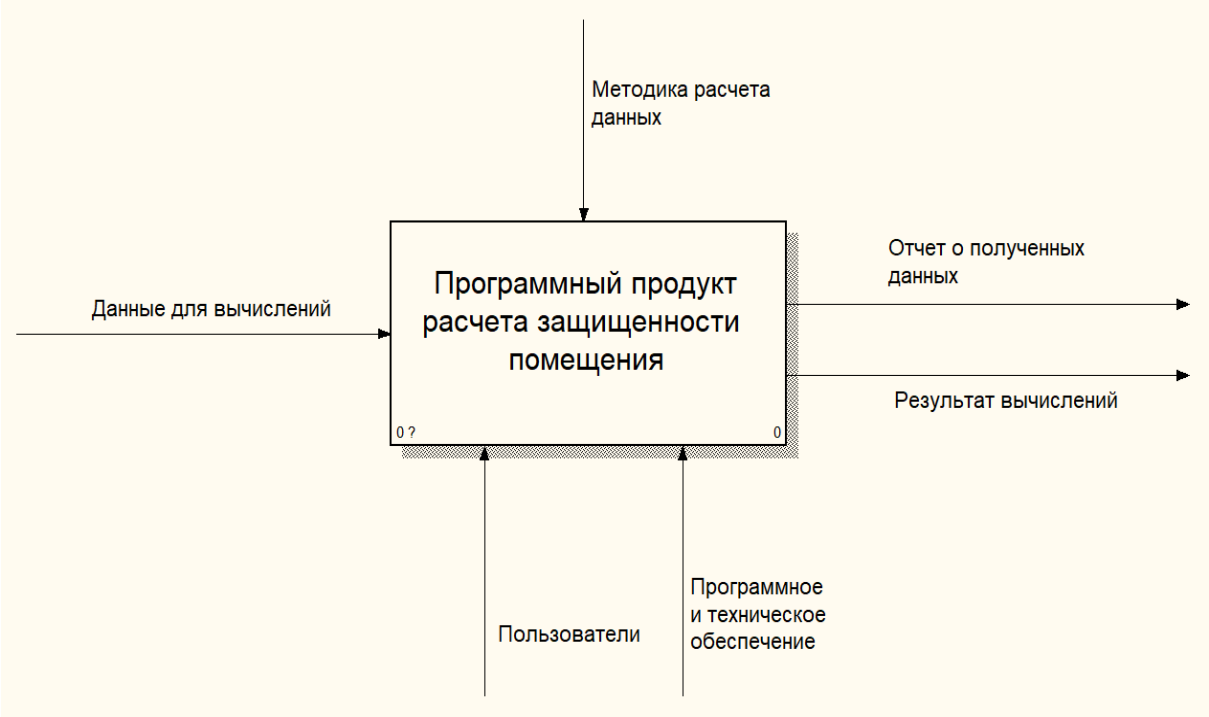

Рисунок 7 – Функциональная модель программы в нотации IDEF0

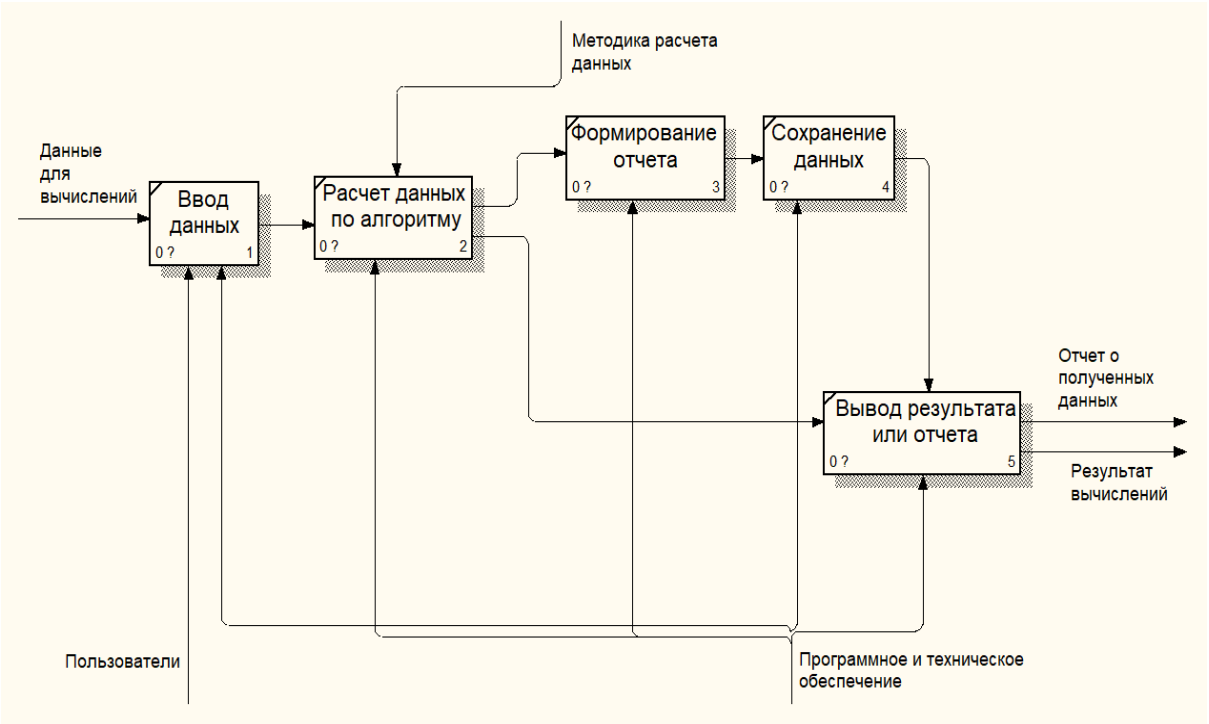

Рисунок 8 – Декомпозиция функциональной модели программы

2.1 Цели и назначение программы

Программа предназначена для расчета защищенности помещения от утечки информации по электромагнитному каналу.

Цели создания программы- расчет расстояния до границы контролируемой зоны, для обеспечения безопасности сообщений, излучаемых в окружающее пространство ПЭВМ, а также определение смыслового критерия безопасности сообщений.

Основные задачи программы:

– расчет коэффициента затухания

– расчет напряженности электромагнитного поля

– определение среднеквадратической напряженности

– расчет отношения сигнал/шум

– вывод результата с рекомендациями

2.2 Характеристика функциональных модулей программы

Главные функции программы:

– функция «ввод и вывод данных» обеспечивает пользователю возможность ввода необходимых данных для получения результата расчета

– функция «расчет данных» отвечает за правильное применение системой алгоритма подсчета

– функция «установка минимальных и максимальных значений» предназначена для соотнесения значений уровня децибел на каждой из трех частот

– функция «обработчик события» позволяет присваивать необходимые переменные в зависимости от выбранного типа данных

На основе этих функций можно выделить модули:

– модуль расчета данных – программный код, реализующий расчет по данным, вводимых пользователем и имеющихся в базе данных программы.

– модуль вывода отчетности – программный код, реализующий составление и сохранение отчета по проводимому расчету отдельным файлом на компьютере.

Эти модули необходимы для корректной работы программы. Далее следует определить этапы работы модулей.

Этапы работы модуля расчета данных:

– этап 1 – ожидание ввода значений от пользователя, а по окончании ввода происходит переход на этап 2;

– этап 2 – расчет коэффициента затухания, переход на этап 3;

– этап 3 – расчет напряженности электромагнитного поля, переход на этап 4;

– этап 4 – определение среднеквадратичной напряженности, переход на этап 5;

– этап 5 – расчет отношения сигнал/шум, Δ. Если значение Δ меньше необходимого уровня, то переходим к этапу 7, а если Δ больше, то переходим к этапу 6;

– этап 6 – перерасчет расстояния r, необходимого для обеспечения безопасной дистанции до границы контролируемой зоны, переход на этап 7;

– этап 7 – вывод результата.

Диаграмма деятельности модуля показана рисунке 9.

Этапы работы модуля вывода отчетности:

– этап 1 – ожидание действия пользователя по сохранению отчета, переход к этапу 2;

– этап 2 – вставка данных в шаблон, переход к этапу 3;

– этап 3 – сохранение отчета в отдельный файл.

Диаграмма деятельности модуля показана рисунке 10.

2.3 Требования к программе

2.3.1 Общие требования

Проектируемая программа должна содержать следующие компоненты:

– модуль расчета данных.

– модуль вывода отчетности.

Данный программный продукт может подвергаться модифицированию и улучшению на основе потребностей заинтересованных лиц, имеющих официальное разрешение.

Пользователями системы могут быть разные люди, в том числе не имеющие особых профессиональных навыков в области защиты и безопасности.

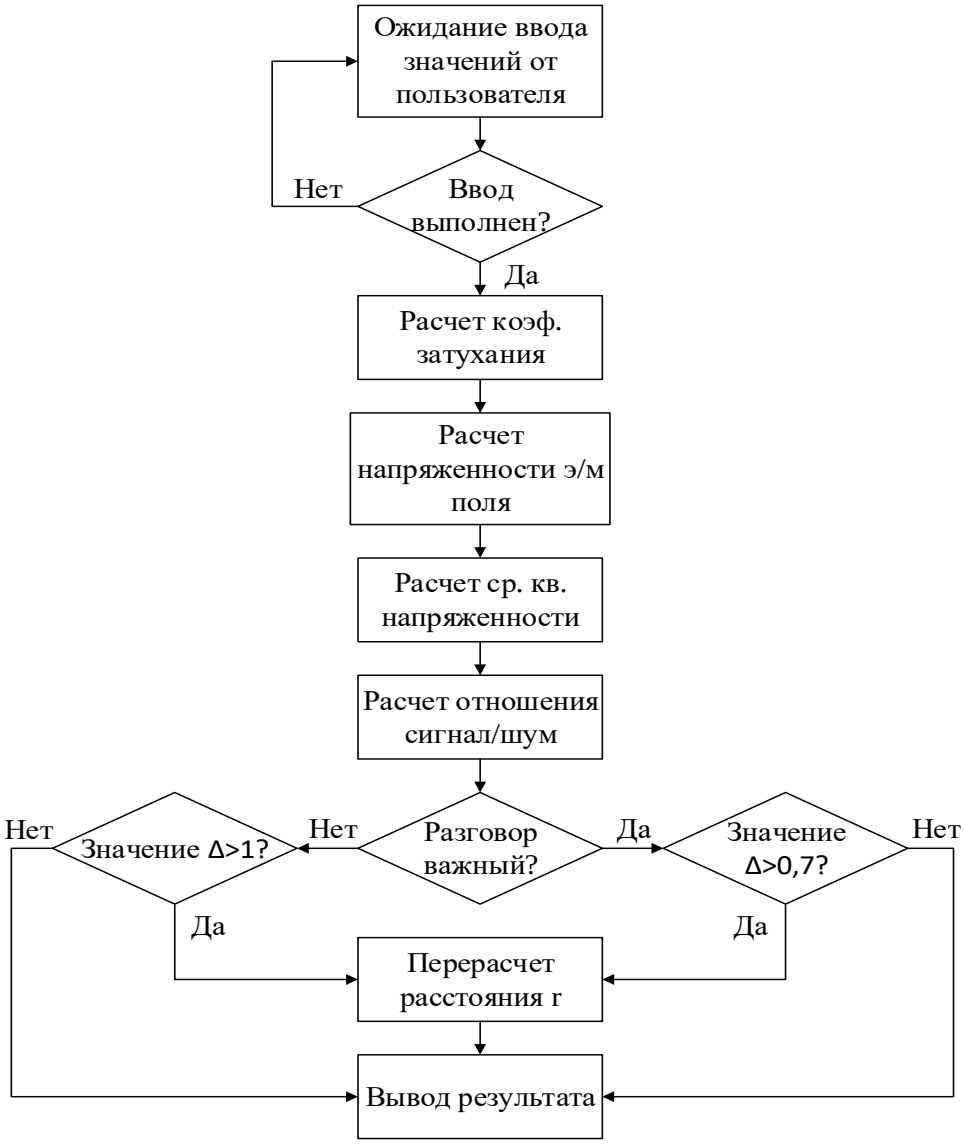

Рисунок 9 – Диаграмма деятельности модуля расчета данных

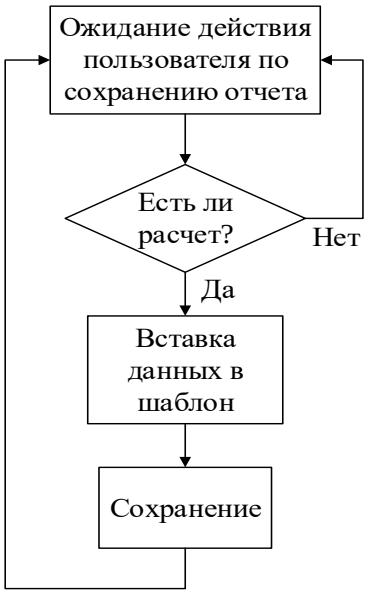

Рисунок 10 – Диаграмма деятельности модуля вывода отчетности

На каждый программный продукт должен быть только один пользователь.

Требования к надежности оборудования и ПО:

– проведение комплекса мероприятий отладки, поиска и исключения ошибок;

– использование сертифицированных средств вычислительной техники, их комплектующих и средств передачи данных;

– необходимо использование программ защиты от компьютерных вирусов;

– обеспечение защиты от перехвата информации по техническому каналу;

– с целью повышения отказоустойчивости системы в целом необходима обязательная комплектация серверов источником бесперебойного питания с возможностью автономной работы системы не менее 20 минут.

Требования к интерфейсу:

– интерфейс должен быть простым и понятным, чтобы пользователю не требовалось объяснять, как им пользоваться;

– удобство интерфейса и его элементов обеспечивает высокую скорость работы пользователя;

– обеспечение защиты от человеческих ошибок;

– быстрое обучение пользователя за счет эргономичности интерфейса;

– цветовая гамма интерфейса должна быть приятной глазу и настраивать на рабочий лад;

– возможность ввода данных с помощью клавиатуры и использование компьютерной мыши.

2.3.2 Требования к лингвистическому обеспечению

Программа должна быть полностью на русском языке. Ввод данных производится только арабскими цифрами и буквами русского алфавита.

Для разработки программы выбран объектно- ориентированный язык программирования- C#.

2.3.3 Требования к информационному обеспечению

Программный продукт не нуждается в хранении большого объема данных, поэтому создание отдельной базы данных не требуется. В данном случае ресурсов компьютера будет достаточно.

2.3.4 Требования к математическому обеспечению

Разрабатываемая программа не требует специальное математическое обеспечение.

2.3.5 Требования к программному обеспечению

Основой разрабатываемой программы является операционная система. Выбор ОС, на которых работает эта система, разнообразен, но лучше всего использовать ОС Windows 7 компании Microsoft, поскольку она имеет следующие достоинства:

– стабильная работа системы

– большая производительность

– многозадачность

– эргономичность интерфейса

Отчет сохраняется в Microsoft word – текстовый редактор, предназначенный для создания, просмотра и редактирования текстовых документов, с локальным применением простейших форм таблично-матричных алгоритмов.

2.3.6 Требования к техническому обеспечению

Разрабатываемая программа не требует много места на компьютере и сильной загрузки процессора, ограничиваясь самыми минимальными требованиями, поэтому она более доступна для любого пользователя. Таким образом, минимальными требованиями к ПЭВМ пользователей будут следующими:

– процессор – Intel Pentium 1.5 ГГц;

– объем оперативной памяти – 256 Мб;

– дисковая подсистема – 24 Гб;

– устройство для работы с USB Flash носителями;

– сетевой адаптер – 100 Мбит;

– устройство чтения и записи компакт-дисков.

3 ОПИСАНИЕ РАЗРАБОТАННОГО ПРОГРАММНОГО ПРОДУКТА

3.1 Обоснование выбора языка программирования и среды разработки

C# – это объектно-ориентированный язык со строгой типизацией, позволяющий разработчикам создавать различные безопасные и надежные приложения, работающие на платформе. Синтаксис C# очень богат, но при этом прост и удобен в изучении.

C# поддерживает универсальные методы и типы, которые обеспечивают более высокий уровень безопасности и производительности, а также итераторы, позволяющие определять в классах коллекций собственное поведение итерации, которое может легко применить в клиентском коде.

C# поддерживает указатели и понятие "небезопасного" кода для тех случаев, в которых критически важен прямой доступ к памяти.

Процесс построения в C# проще по сравнению с C или C++, но более гибок, чем в Java. Отдельные файлы заголовка не используются, и нет необходимости объявлять методы и типы в определенном порядке. Исходный файл C# может определить любое число классов, структур, интерфейсов и событий.
Также этот язык программирования имеет поддержку Microsoft и постоянно развивается благодаря усилиям этой компании.

Средой разработки был выбран Visual Studio 2017. Преимуществами данной среды являются:

– наличие в Visual Studio интегрированного Web-сервера позволяет запускать Web-сайт прямо из среды проектирования, а также повышает безопасность, исключая вероятность получения доступа к тестовому Web-сайту с какого-нибудь внешнего компьютера, поскольку тестовый сервер может принимать соединения только с локального компьютера.

– поддержка множества языков при разработке. Visual Studio позволяет писать код на своем языке или любых других предпочитаемых языках, используя все время один и тот же интерфейс (IDE).

– интуитивный стиль кодирования. По умолчанию Visual Studio форматирует код по мере его ввода, автоматически вставляя необходимые отступы и применяя цветовое кодирование для выделения элементов типа комментариев. Такие незначительные отличия делают код более удобным для чтения и менее подверженным ошибкам.

– более высокая скорость разработки за счет удобных функций, вроде функции IntelliSense (которая умеет перехватывать ошибки и предлагать правильные варианты), функции поиска и замены (которая позволяет отыскивать ключевые слова как в одном файле, так и во всем проекте) и функции автоматического добавления и удаления комментариев (которая может временно скрывать блоки кода), позволяют разработчику работать быстро и эффективно.

– возможности отладки.

3.2 Описание модулей программного продукта

При разработке программного продукта были выделены модули, на основе которых созданы следующие классы:

SetE – реализует модуль «расчет данных»;

SaveFile – реализует модуль «вывод отчетности»;

MainWindow – метод инициализации пользовательского интерфейса;

Button_Click – метод разработчик события клика по кнопке "Расчет";

SetK – метод установки минимальных и максимальных значений дБ для трех основных частот;

ComboBox_SelectionChanged – метод обработчик события изменения типа окна/стены/разговора.

Работа программного продукта показана на рисунке В.1, рисунке В.2 и рисунке В.3 в приложении В.

Исходный код программы указан в приложении Б.

Существует достаточно много угроз, направленных на перехват информации по электромагнитному каналу. Данная программа была разработана для того, чтобы рассчитывать максимально безопасное расстояние от источника

угроз до границы контролируемой зоны. В следующей главе будут рассмотрены основные угрозы утечки информации по электромагнитному каналу.

4 УГРОЗЫ УТЕЧКИ ИНФОРМАЦИИ ПО ЭЛЕКТРОМАГНИТНОМУ КАНАЛУ

4.1 Технические средства перехвата информации

Угрозы утечки защищаемой информации по каналам ПЭМИН связаны с электрическими информативными сигналами технических средств обработки информации и автоматизированных систем. Генерация, обработка, передача этих сигналов сопровождается побочными (не связанными с прямым функциональным назначением аппаратуры) электромагнитными излучениями, которые распространяются как в объекте информации, так и за его пределами. Это излучения элементов технических средств (клавиатуры, принтера, монитора, накопителей, линий связи и передачи данных, систем звукоусиления, магнитофонов, систем громкоговорящей связи и т.д.).

Регистрация ПЭМИН осуществляется с целью перехвата информации, циркулирующей в технических средствах, обрабатывающих ПДн (в средствах вычислительной техники, информационно-вычислительных комплексах и сетях, средствах и системах передачи, приема и обработки ПДн, в том числе в средствах и системах звукозаписи, звукоусиления, звуковоспроизведения, переговорных и телевизионных устройствах, средствах изготовления, тиражирования документов и других технических средствах обработки речевой, графической, видео- и буквенно-цифровой информации). Для регистрации ПЭМИН используется аппаратура в составе радиоприемных устройств и оконечных устройств восстановления информации. Кроме этого, перехват ПЭМИН возможен с использованием электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПДн.

Регистрация ПЭМИН может вестись с использованием аппаратуры следующих видов:

– стационарной аппаратурой, размещаемой в близлежащих строениях (зданиях) с неконтролируемым пребыванием посторонних лиц;

– портативной возимой аппаратуры, размещаемой в транспортных средствах, осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями;

– портативной носимой аппаратурой – физическими лицами в непосредственной близости от ИСПДн;

– автономной автоматической аппаратурой, скрытно устанавливаемой физическими лицами в непосредственной близости от ИСПДн.

Перехват электромагнитных излучений может осуществляться:

– программно-аппаратными комплексами перехвата;

– портативными сканерными приёмниками;

– цифровыми анализаторами спектра, управляемыми компьютером со специальным программным обеспечением.

Могут использоваться и параметрические каналы утечки информации, формируемые в результате высокочастотного облучения элементов технических средств обработки информации, в которых проводится обработка информативных сигналов, и приема переизлученного сигнала средствами, аналогичными средствам перехвата ПЭМИН. Схема представлена на рисунке 11.

Для съема информации с проводных линий могут использоваться следующие средства перехвата и съёма наведенных сигналов:

– с аппаратуры основных технических средств связи (ОТСС), средств обработки информации и вспомогательных технических средств, линий связи и передачи данных, выходящих за пределы контролируемой зоны (токовые трансформаторы, пробники);

– с цепей электропитания и шин заземления, представленных на рисунке 12;

– с инженерных коммуникаций, представленных на рисунке 13.

ПЭМИН от ОТСС могут перехватываться закладочными электронными устройствами, размещаемыми в пределах объекта информатизации, либо в рядом расположенных.

Для волоконно-оптической системы передачи данных угрозой утечки информации является утечка оптического излучения, содержащего защищаемую информацию, с боковой поверхности оптического волокна.

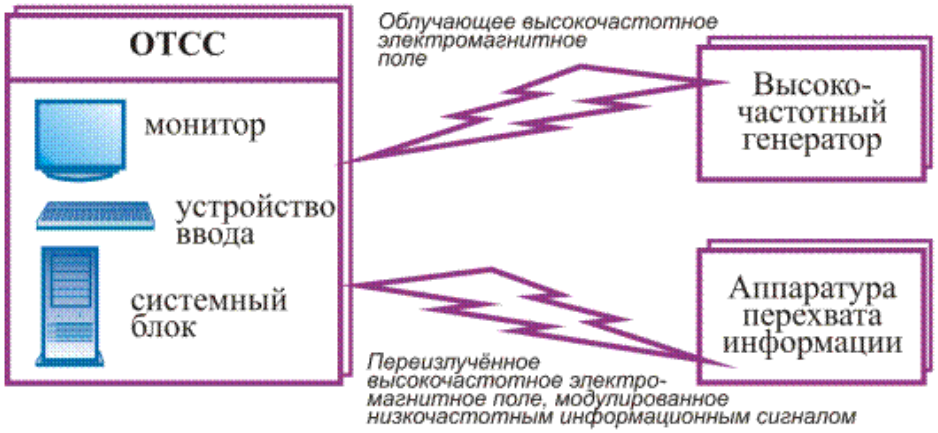

Рисунок 11 – Схема съема информационных сигналов по параметрическому электромагнитному каналу, реализуемого путем высокочастотного облучения

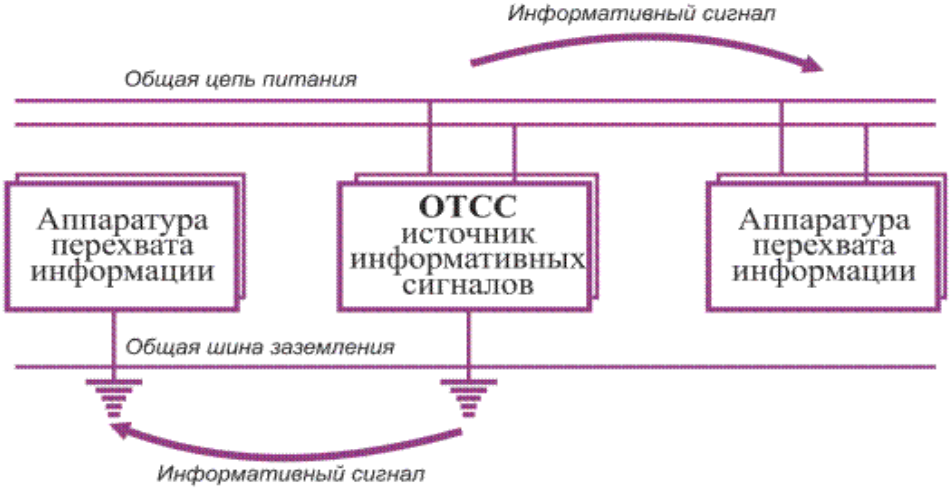

Рисунок 12 – Схема съема информативных сигналов по электрическому каналу с цепей заземления и питания

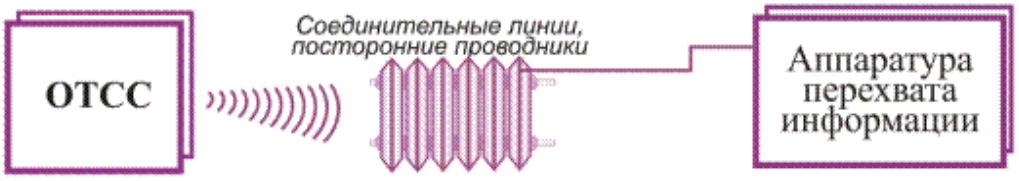

Рисунок 13 – Прямые электрические каналы утечки информации, возникающие за счет электромагнитных наводок в посторонних проводниках

Появление новых каналов связи – сотовой связи, спутниковых и беспро-

водных сетей передачи данных – привело к развитию специализированных систем и средств контроля и перехвата информации, ориентированных на используемые в них информационные технологии, в том числе средств: перехвата сотовой связи; перехвата информации в каналах передачи данных вычислительных сетей.

В *радиозакладках* для передачи информации используется энергия электромагнитных волн, не влияющих на органы чувств человека, способных распространяться на значительные расстояния, преодолевая естественные и искусственные препятствия. Благодаря этим двум свойствам радиозакладные устройства позволяют с помощью специальной приемной аппаратуры вести скрытное наблюдение за интересующим объектом практически из любой удаленно точки.

С технической точки зрения, закладки могут работать практически в любом диапазоне радиоволн. Однако из конструктивных соображений наиболее используемые частоты – от 100 до 1000 МГц.

В *инфракрасных закладках* для передачи информации также используется энергия электромагнитных волн, но не радиодиапазона, а невидимой части оптической области спектра – инфракрасного диапазона. Благодаря малой длине такие волны распространяются узким пучком в заданном направлении, и их трудно обнаружить даже с помощью специальной аппаратуры. Дальность передачи информации от инфракрасных ЗУ достигает 500 м.

Однако высокая скрытность таких устройств существенно усложняет их применение. Так, инфракрасная закладка должна постоянно находиться в зоне прямой видимости приемника оптического излучения, а случайно попавший на линию визирования предмет, человек или автомобиль, а также изменившиеся погодные условия могут привести к существенному ухудшению качества или даже пропаданию сигнала в аппаратуре регистрации. Естественно, что такие ЗУ совершенно не применимы на мобильных объектах. В силу перечисленных недостатков инфракрасные закладки редко используются в практике промышленного шпионажа.

Любое электронное устройство при работе создает так называемые побочные электромагнитные излучения и наводки (ПЭМИН). Не является исключением и *телефонный аппарат*. При наборе номера и ведении переговоров, благодаря техническим особенностям блока питания, вся информация излучается на десятках частот в средневолновом, коротковолновом и ультракоротковолновом диапазонах. Это излучение может быть зафиксировано на расстоянии до 200 м. В случае применения подобного телефона радиозакладки совсем не нужны. Хочется отметить, что получившие широкое распространение телефонные аппараты с радиоудлинителем (Cordless Telephone) тоже значительно облегчают жизнь специалистам от промышленного шпионажа, так как дальность несанкционированного перехвата их довольно мощного сигнала достигает 400-800 м.

Конечно, приведенные примеры относятся к крайностям, но перехват излучений может осуществляться с помощью малогабаритного индуктивного датчика, позволяющего «улавливать» побочные электромагнитные колебания практически любого телефонного аппарата на расстоянии до метра. При этом кроме речевых сигналов регистрируются также и сигналы набора номера. В качестве датчика используется катушка индуктивности. Она может быть плоской и устанавливаться там, где ее никто искать не будет, например, под основанием телефонного аппарата или под настольным письменным прибором, а также параллельно телефонному проводу внутри стен, под карнизами и плинтусами. Недостаток способа - появление наводок от посторонних источников.

Кроме самого аппарата, телефонные *провода и кабели связи* тоже создают вокруг себя магнитные и электрические поля, образующие каналы утечки информации за счет наводок на другие провода и элементы аппаратуры в ближней зоне.

Также для перехвата информации могут использоваться анализаторы спектра, приемные антенны, устройства цифровой обработки сигналов и ТС.

4.2 Угрозы программно-математического воздействия

Программно-математическое воздействие – это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой называют некоторую самостоятельную программу

(набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

– скрывать признаки своего присутствия в программной среде;

– обладать способностью к самодублированию, ассоциированию себя другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;

– разрушать (искажать произвольным образом) код программ в оперативной памяти;

– выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);

– сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

– искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

Вредоносные программы могут быть внесены (внедрены) преднамеренно или случайно в компьютерное программное обеспечение в процессе его разработки, сопровождения, модификации и настройки. Кроме этого, они могут быть внесены в процессе эксплуатации с внешних носителей информации или посредством сетевого взаимодействия как в результате НСД, так и случайно пользователями компьютера.

Наличие в компьютере вредоносных программ может способствовать возникновению скрытых, в том числе нетрадиционных каналов доступа к информации, позволяющих вскрывать, обходить или блокировать защитные механизмы, предусмотренные в системе, в том числе парольную и криптографическую защиту.

Основными видами вредоносных программ являются:

– программные закладки;

– классические программные (компьютерные) вирусы;

– вредоносные программы, распространяющиеся по сети (сетевые черви);

– другие вредоносные программы, предназначенные для осуществления НСД (например, подбора и вскрытия паролей, осуществления сетевой атаки).

В связи с усложнением и возрастанием разнообразия программного обеспечения число вредоносных программ быстро возрастает. Вместе с тем, далеко не все из них представляют реальную угрозу. Во многих случаях устранение уязвимостей в системном или прикладном программном обеспечении привело к тому, что ряд вредоносных программ уже не способны внедриться в систему компьютера. Часто основную опасность представляют новые вредоносные программы.

4.3 Угрозы нетрадиционных информационных каналов

Нетрадиционный информационный канал - это канал скрытной передачи информации с использованием традиционных каналов связи и специальных преобразований передаваемой информации, не относящихся к криптографическим методам, т.е. метода скрытной передачи полезного сообщения в безобидных видео, аудио, графических и текстовых файлах.

Особенностью технологии является использование для передачи данных канала ПЭМИН, что значительно затрудняет обнаружение самого факта несанкционированной передачи по сравнению с традиционной компьютерной стеганографией. Действительно, если для предотвращения несанкционированной передачи данных по локальной сети или сети Интернет существуют аппаратные и программные средства (FireWall, Proxy server и т.п.), то средств для обнаружения скрытой передачи данных по ПЭМИН нет, а обнаружить такое излучение в общем широкополосном спектре (более 1000 МГц) паразитных излучений ПК без знания параметров полезного сигнала весьма проблематично.

При использовании в информационных каналах некоторых разделяемых ресурсов возможна их манипуляция. При этом в каналах, использующих временные характеристики, осуществляется модуляция по времени занятости разделяемого ресурса (например, модулируя время занятости процессора, приложения

могут обмениваться данными). В каналах памяти ресурс используется как промежуточный буфер (например, приложения могут обмениваться данными путем помещения их в имена создаваемых файлов и директорий). В каналах баз данных и знаний используют зависимости между данными, возникающими в реляционных базах данных и знаний.

Нетрадиционные информационные каналы могут быть сформированы на различных уровнях работы компьютерной системы:

– аппаратном;

– микрокодов и драйверов устройств;

– операционной системы;

– прикладного программного обеспечения;

– функционирования каналов передачи данных и линий связи.

Эти каналы могут использоваться как для скрытной передачи скопированной информации, так и для скрытной передачи команд на выполнение деструктивных действии, запуска приложении и т.п. Для его реализации, как правило, надо внедрить в компьютерную систему программную или программно-аппаратную закладку, обеспечивающую формирование нетрадиционного канала, существующего в системе непрерывно или с активацией одноразово или по заданным условиям. При этом возможно существование обратной связи с субъектом НСД.

Эффективная защита от рассмотренных угроз безопасности и целостности информации может реализоваться только через комплексную систему защиты. Это совокупность правовых, организационных мероприятий, технических средств, программно-технических методов, организуемых и поддерживаемых для предупреждения разрушения, утечки или модификации защищаемой информации в вычислительной системе.

4.4 Защита от угроз

4.4.1 Организационные мероприятия

Целью этих мероприятий является создание организационной защиты, предотвращающей доступ посторонних лиц к компьютерам, на которых хранится и обрабатывается сетевая информация, а также к средствам и линиям связи в сети.

К числу основных таких мер можно отнести:

– организация режима и охраны для исключения тайного проникновения на территорию и в помещения посторонних лиц; обеспечение контроля прохода и перемещения сотрудников, посетителей и др.;

– создание отдельных рабочих зон (выделенные помещения);

– контроль и соблюдение временного режима труда и пребывания на территории сотрудников организации;

– проведение работы с сотрудниками: подбор и расстановка персонала; ознакомление, изучение, обучение правилам работы с информацией ограниченного доступа; оповещение о мерах ответственности за нарушение правил защиты информации и др.;

– организация специального делопроизводства и документооборота, разработка технологий использования документов и носителей информации ограниченного доступа, их учета, исполнения, возврата, хранения и уничтожения;

– использование сертифицированных технических средств сбора, обработки, накопления и хранения информации ограниченного доступа;

– анализ внутренних и внешних угроз информации ограниченного доступа и выработка мер по обеспечению ее защиты;

– проведение систематического контроля за работой персонала с информацией ограниченного доступа, порядком учета, хранения и уничтожения документов и технических носителей.

В каждом случае организационные мероприятия по форме и содержанию являются специфическими для данной организации и обеспечивают безопасность информации в конкретных условиях.

4.4.2 Технические средства защиты

Для решения задач обеспечения безопасности и целостности информации в арсенале специалистов службы безопасности и защиты информации имеется широкий набор технических средств и методов, среди которых два направления занимают важное место:

– обнаружение, идентификация, локализация (определение местоположения) подслушивающих устройств и других средств несанкционированной передачи информации из контролируемых помещений;

– организация технической защиты информации на основе специальных технических средств, методов и оборудования.

Например, используются генераторы шума. Они могут быть аппаратными и объектовыми. Основная задача зашумления эфира - это поднять уровень электромагнитного шума и тем самым препятствовать радиоперехвату информационных сигналов. Техническое средство вычислительной техники является защищенным, если зона зашумления будет больше зоны его «опасного» излучения.

Также используются следующие средства защиты от перехвата информации: фильтры сетевые помехоподавляющие; генераторы радиошума с регулировкой мощности (например, «Баррикада»); маскираторы побочных электромагнитных излучений и наводок (например, «Маис-М»); система защиты информации от утечки за счет ПЭМИН (например, «Стикс-4»); широкополосные генераторы радиошума малой мощности; генераторы шума по цепям электропитания, заземления и ПЭМИ.

4.4.3 Пассивные методы защиты

Электрические токи различных частот, протекающие по элементам средства обработки информации, создают побочные магнитные и электрические поля. Это причина возникновения электромагнитных и параметрических каналов утечки, а также наводок информационных сигналов в посторонних токоведущих линиях и конструкциях.

Ослабление ПЭМИН осуществляется экранированием и заземлением средств и их соединительных линий.

Экранируют источник излучения технического средства, то есть СВТ размещают в экранированном шкафу или в экранированном помещении целиком. Экранируется каждое ТС входящее в состав СВТ.

Экранирование уменьшает емкостные связи между защищаемыми элементами, накапливает статическое электричество на экране с последующим отводом зарядов на землю. Высокочастотное электромагнитное поле ослабляется полем обратного направления, создаваемым вихревыми токами, наведенными в металлическом сплошном или сетчатом экране, располагающемся на всех элементах помещения.

Просачивание в цепи электропитания предотвращается фильтрацией информационных сигналов, а для маскирования ПЭМИН используются системы зашумления.

Экранирование эффективно только при правильном заземлении аппаратуры и соединительных линий. Система заземления должна состоять из общего заземления, заземляющего кабеля, шин и проводов, соединяющих заземлитель с объектами. Качество электрических соединений должно обеспечивать минимальное сопротивление контактов, их надежность и механическую прочность в условиях вибраций и жестких климатических условиях. В качестве заземляющих устройств запрещается использовать «нулевые» провода электросетей, металлоконструкции зданий, оболочки подземных кабелей, трубы систем отопления, водоснабжения, сигнализации.

5 БЕЗОПАСНОСТЬ НА ПРЕДПРИЯТИИ

5.1 Экологичность

Согласно требованиям, ГОСТ 12.1.003–99 «Шум. Общие требования безопасности», в помещениях с ЭВМ, где работают инженерно – технические работники, уровень шума не должен превышать 60 дБА.

В ПК источниками шума являются вентиляторы, трансформаторы, винчестеры, DVD-ROM. Для уменьшения шумов необходимо применять специально разработанные корпуса ПК, выполняющиеся в виде активного элемента охлаждающей системы. Все вентиляторы в системном блоке заменяются на радиаторы с теплоотводящими трубками. Все трубки имеют тепловые интерфейсы с корпусом, что позволяет удалять тепло от источников. Данный корпус не имеет ни одного вентилятора, т.е. шум, производимый работой ПК, сведен практически к нулю.

Использование лазерного принтера или размещение принтера вне кабинета позволит устранить излишние шумы от принтера.

Шум, создаваемый в люминесцентных лампах нового образца, почти сведен к нулю.

Оператор ПЭВМ подвергается электромагнитному излучению компьютера, результат которого зависит от напряженностей электрического и магнитного полей, индивидуальных особенностей организма и времени воздействия. Наиболее интенсивно электромагнитные поля воздействуют на органы с большим содержанием воды или со слабо развитой сосудистой системой.

Источником излучения электромагнитных волн в ЭВМ является электронно-лучевая трубка (ЭЛТ) дисплея и трансформаторы блоков питания.

В современных мониторах электромагнитное излучение невелико благодаря использованию защитных экранов. Для сведения излучения к нулю рекомендуется использовать жидкокристаллический монитор, поскольку его излучение значительно меньше.

Пользователя следует удалить от монитора на расстоянии не менее 500 мм

(оптимальное расстояние - 600-700 мм).

ПК (монитор, системный блок, клавиатура, мышь) содержит, помимо ничтожного количества ценных металлов, много разных тяжелых химических соединений: ртуть; кадмий; мышьяк; свинец; цинк; никель и другие. Попадая на стихийную свалку, эти вещества под влиянием солнечного ультрафиолета и агрессивного атмосферного воздействия разлагаются и становятся токсичными. Впитываясь в грунт, через некоторое время они попадают в растительные продукты питания.

Порядок утилизации компьютеров:

– первый шаг – создание комиссии на предприятии, имеющем технику, подлежащую утилизации. Это внутренняя комиссия, которая создается для коллективного принятия решения о том, какая именно техника может быть списана;

– составление экспертного заключения о том, что техника действительно «отжила свое» и должна быть списана. В качестве эксперта может выступать как независимый специалист, так и сотрудник компании, имеющий диплом, подтверждающий его компетентность в работе с данной техникой;

– составление акта технической экспертизы, подтверждающего, что техника уже вышла из строя и не подлежит ремонту либо же что ремонт её уже нецелесообразен;

– составление акта списания компьютерной техники с обязательным отображением в бухгалтерском учете предприятия;

– утилизация техники на соответствующем предприятии, имеющем право на переработку компьютеров;

– получение официального подтверждения в виде документа, сообщающего о том, что техника была утилизирована в соответствующем порядке и опасные отходы не будут загрязнять окружающую среду.

5.2 Безопасность

5.2.1 Эргономичность интерфейса

Интерфейс разработанной программы показан на рисунке 14.

Под эргономичностью интерфейса понимается удобство общения пользователя с программным продутом. Чтобы оценить эти удобства введены критерии эргономичности интерфейса, это интуитивность (естественность), непротиворечивость (последовательность), визуализация, система навигации, гибкость, поддержка пользователя. Все эти критерии в большей степени зависят от интеллектуальности самой программы, но это уже другая история.

Интуитивность иди естественность – это свойство программного продукта, адаптироваться под требования пользователя, а именно:

– общение происходит при помощи языка пользователя (в разработанной программе используется русский язык);

– отсутствуют жёсткие требования к порядку ведения диалога пользователя с машиной (пользователь сам строит диалог по мере решения задачи);

– не требуется предварительная обработка данных перед вводом их пользователем в систему (это влияет на быстродействие и исключает появления ошибок).

Непротиворечивость или последовательность ведения диалога гарантирует единство общих принципов работы с системой. Данный критерий содержит:

– последовательность в интерпретации команд;

– последовательность в использовании форматов данных – в одном формате должны представляться аналогичные;

– последовательность в размещении информации на экране –информативность сообщения, должна предоставляться пользователю по степени важности (предупреждение об ошибке появится в центре экрана, а вспомогательная информация в нижнем правом углу).

Выделение элементов интерфейса актуализирует внимание пользователя на конкретной информации:

– цвет (создание интерфейсов, более интересных для пользователя. Он используется для группировки информации, выделения различий между информацией, выделения простых сообщений (ошибки, состояния)).

– форма (вид символа, шрифт, начертание, размер).

– окружение (подчеркивание, рамки, инвертированное изображение).

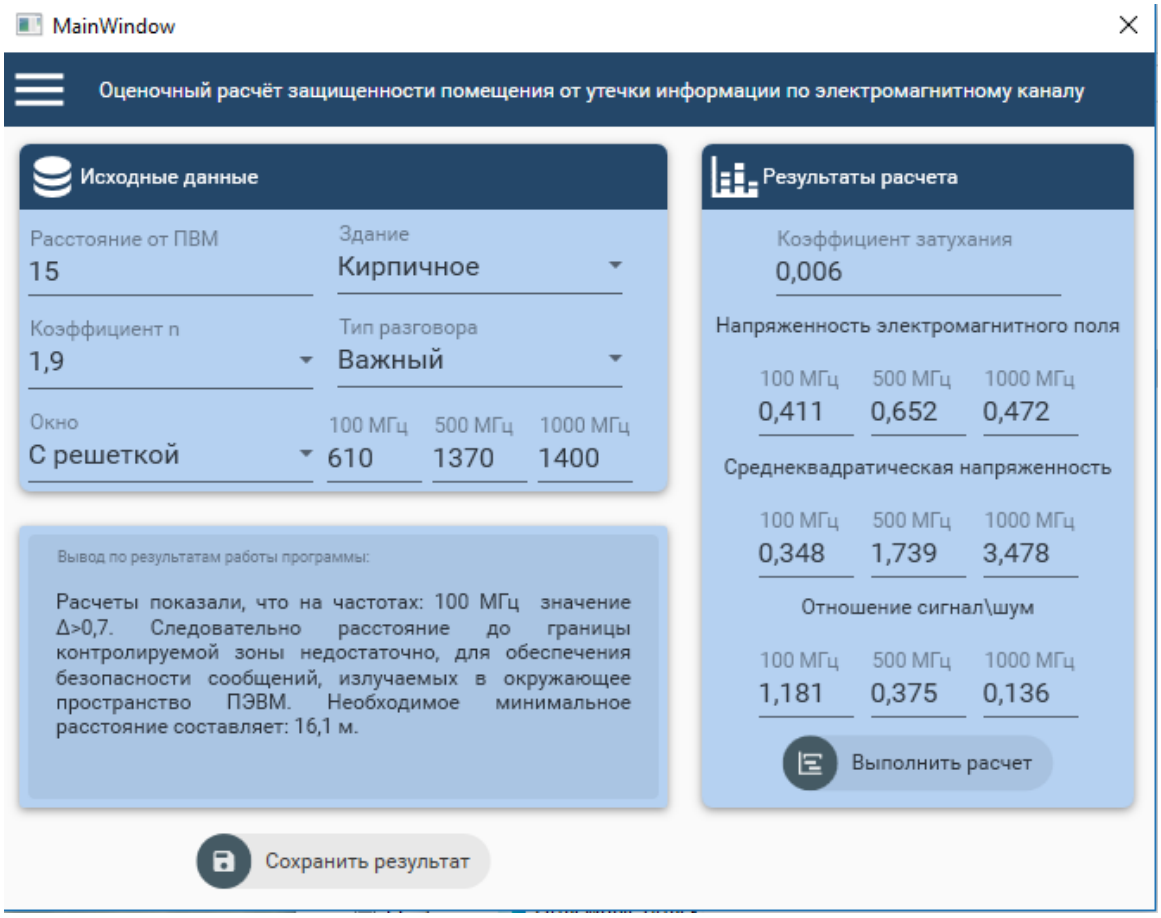

Рисунок 14 – Интерфейс пользователя

Поддержка пользователя во время диалога - это мера помощи, которую диалог оказывает пользователю при его работе с системой. Она включает в себя:

– инструкции пользователю – необходимы для направления пользователя в нужную сторону, подсказок и предупреждений для выполнения необходимых действий на пути решения задачи. Инструкции обеспечены в форме диалога, экранных заставок, справочной информации и т.п. Они могут предложить пользователю: выбрать из предложенных альтернатив некую опцию или набор опций; ввести некоторую информацию; выбрать опцию из набора опций, которые могут изменяться в зависимости от текущего контекста; подтвердить фрагмент введенной информации перед продолжением ввода;

– подтверждение действий системы - используется, чтобы пользователь мог убедиться, что система выполняет, выполнила или будет выполнять требуемое действие;

– сообщения об ошибках - должны объяснить, в чем ошибка, и указать, как ее исправить.

Гибкость диалога - это мера того, насколько хорошо диалог соответствует различным уровням подготовки и производительности труда пользователя. При этом диалог может подстраивать свою структуру или входные данные. Гибкость диалога проявляется в способности диалоговых систем адаптироваться либо с помощью пользователя, либо самостоятельно к любому возможному уровню подготовки оператора.

5.2.2 Эргономичность рабочего места

Требования к ПЭВМ:

– ПЭВМ должны соответствовать требованиям настоящих санитарных правил, и каждый их тип подлежит санитарно-эпидемиологической экспертизе с оценкой в испытательных лабораториях, аккредитованных в установленном порядке;

– концентрации вредных веществ, выделяемых ПЭВМ в воздух помещений, не должны превышать предельно допустимых концентраций (ПДК), установленных для атмосферного воздуха;

– конструкция ПЭВМ должна обеспечивать возможность поворота корпуса в горизонтальной и вертикальной плоскости с фиксацией в заданном положении для обеспечения фронтального наблюдения экрана ВДТ. Дизайн ПЭВМ должен предусматривать окраску корпуса в спокойные мягкие тона с диффузным рассеиванием света. Корпус ПЭВМ, клавиатура и другие блоки и устройства ПЭВМ должны иметь матовую поверхность с коэффициентом отражения 0,4-0,6 и не иметь блестящих деталей, способных создавать блики;

– конструкция ВДТ должна предусматривать регулирование яркости и контрастности.

Требования к освещению на рабочих местах, оборудованных ПЭВМ:

– естественное и искусственное освещение должно соответствовать требованиям действующей нормативной документации. Окна в помещениях, где экс-

плуатируется вычислительная техника, преимущественно должны быть ориентированы на север и северо-восток. Оконные проемы должны быть оборудованы регулируемыми устройствами типа: жалюзи, занавесей, внешних козырьков и др.;

– рабочие столы следует размещать таким образом, чтобы видеодисплейные терминалы были ориентированы боковой стороной к световым проемам, чтобы естественный свет падал преимущественно слева;

– освещенность на поверхности стола в зоне размещения рабочего документа должна быть 300-500 лк. Освещение не должно создавать бликов на поверхности экрана. Освещенность поверхности экрана не должна быть более 300 лк;

– общее освещение при использовании люминесцентных светильников следует выполнять в виде сплошных или прерывистых линий светильников, расположенных сбоку от рабочих мест, параллельно линии зрения пользователя при рядном расположении видеодисплейных терминалов. При периметральном расположении компьютеров линии светильников должны располагаться локализованно над рабочим столом ближе к его переднему краю, обращенному к оператору.

Общие требования к организации рабочих мест пользователей ПЭВМ:

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

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

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

– конструкция рабочего стула (кресла) должна обеспечивать поддержание

рациональной рабочей позы при работе на ПЭВМ, позволять изменять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления. Тип рабочего стула (кресла) следует выбирать с учетом роста пользователя, характера и продолжительности работы с ПЭВМ. 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;

– модульными размерами рабочей поверхности стола для ПЭВМ, на основании которых должны рассчитываться конструктивные размеры, следует считать: ширину 800, 1000, 1200 и 1400 мм, глубину 800 и 1000 мм при нерегулируемой его высоте, равной 725 мм.

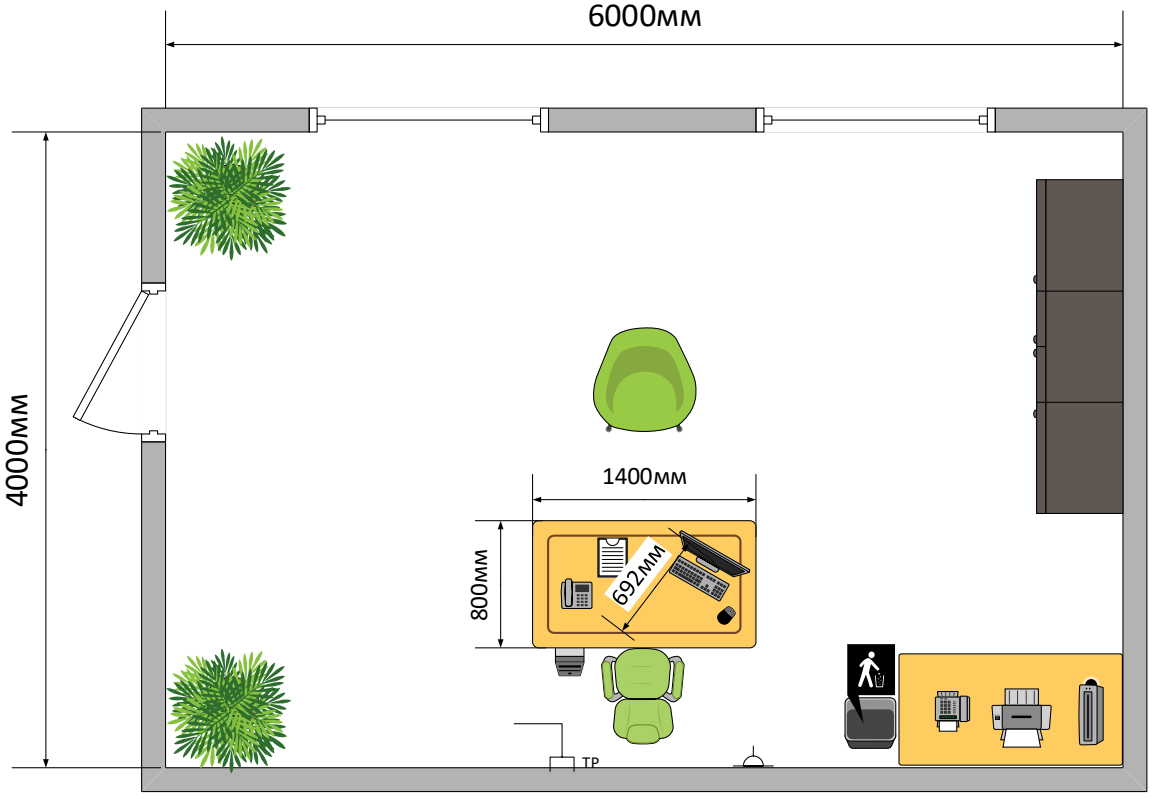

Рисунок 15 – Эргономичное расположение рабочего места

Как мы видим на рисунке 15 и рисунке 17, рабочая поверхность, расположение ПЭВМ относительно окна и относительно человека соответствует норме.

Расположение ламп указано на рисунке 16. Они находятся на достаточном

расстоянии друг от друга, а количество испускаемого света достаточно для корректной работы.

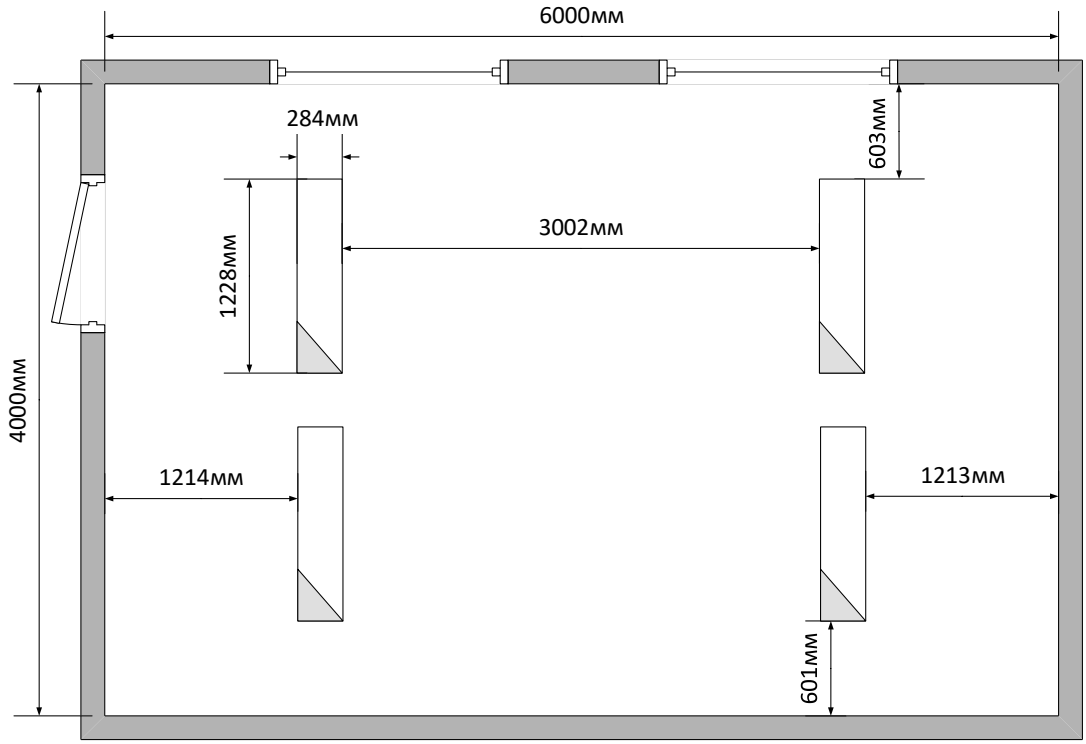

Рисунок 16 – Расположение ламп в помещении

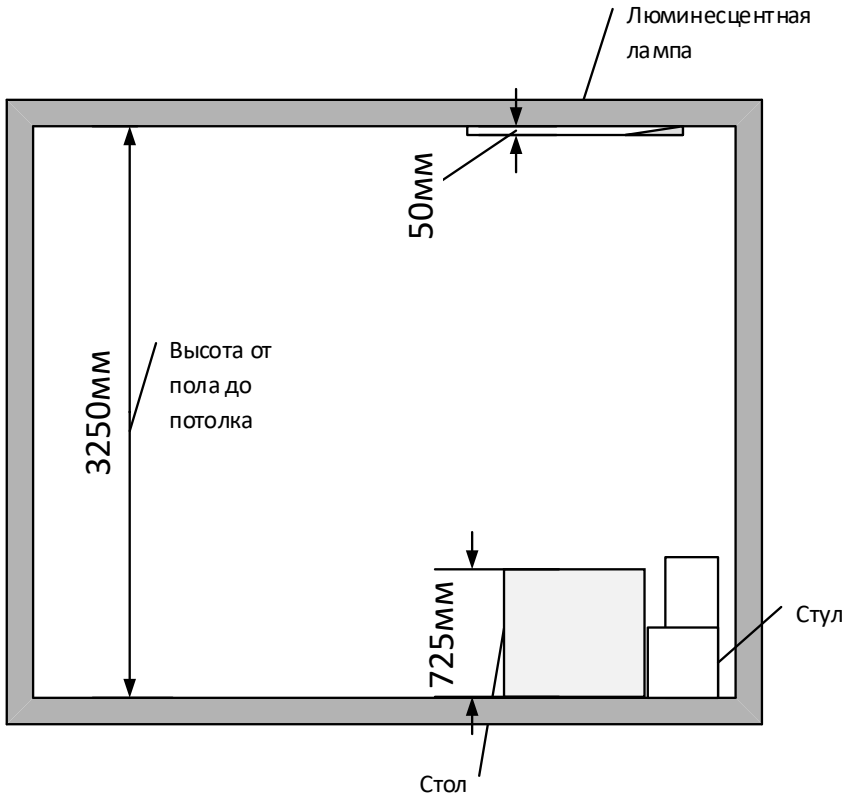

Рисунок 17 – Вид рабочего места сбоку

5.3 Чрезвычайные ситуации

Чрезвычайные ситуации, возникающие на предприятии:

– пожары, взрывы, угроза взрывов – самые распространённые ЧС в современном индивидуальном обществе наиболее часто встречающиеся и, как правило, с тяжёлыми социальными, экономическими последствиями;

– угрозы терроризма;

– наводнения, ураганы, торнадо, землетрясения – наименее популярные ЧС, но не менее опасные;

– угрозы выброса химических веществ на близлежащих промышленных предприятиях.

Федеральный закон от 21.12.1994 № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера», который в настоящий момент действует в редакции от 23.06.2016, обязывает организации к следующему:

– планировать и принимать меры по защите своих сотрудников от чрезвычайных ситуаций;

– планировать и устраивать мероприятия для повышения устойчивости работы своей организации в случае ЧС;

– обеспечивать создание и поддержание в полной готовности сил и средств предупреждения и ликвидации чрезвычайной ситуации, а также теоретическую и практическую подготовку своих сотрудников (инструктажи, специальные курсы, учения и тренировочные мероприятия);

– создавать и поддерживать в постоянной готовности системы оповещения о ЧС;

– руководствуясь планами действий по предупреждению и ликвидации последствий, обеспечивать проведение аварийно-спасательных и других работ на предприятии;

– финансировать мероприятия по защите своих работников от чрезвычайных ситуаций;

– обеспечить создание финансовых и материальных резервов для ликвидации последствий;

– обеспечивать своих работников информацией о защите населения и территорий от ЧС, а также оповещать об угрозе их возникновения или о возникновении; оказывать содействие федеральным органам, осуществляющим защиту населения и территорий от ЧС, в деле установки средств оповещения, распространения информации и так далее.

При угрозе возникновения или возникновении чрезвычайной ситуации на территории организации ее руководителю вменяется в обязанность:

– ввести режим повышенной готовности;

– проинформировать о ситуации органы управления и силы единой государственной системы предупреждения и ликвидации последствий;

– принять решение об установлении уровня реагирования и других мер с целью защиты от чрезвычайной ситуации своих сотрудников и других лиц на территории организации.

5.4 Снижение негативного воздействия компьютера на глаза

Чтобы уменьшить отрицательное влияние компьютера на глаза и сохранить зрение, необходимо придерживаться простых правил, которые заключаются в следующем:

– расстояние от Вас до монитора должно составлять минимум 60 сантиметров. Если при этом Вы плохо видите информацию на экране, следует поменять размер шрифта;

– монитор необходимо располагать прямо перед собой. Он не должен стоять наискосок, иначе для просмотра изображения на нем Вам придется постоянно поворачивать голову. А это может привести к усталости глаз;

– необходимо установить монитор так, чтобы угол падения взгляда на него был равен примерно 15 градусам. То есть верхняя кромка экрана должна быть чуть ниже уровня глаз;

– периодически протирайте монитор, не трогайте его руками. Для чистки

можно воспользоваться безворсовыми сухими салфетками и специальной жидкостью;

– обратите внимание на освещение в рабочем помещении. Оно не должно быть слишком ярким или тусклым. Отдайте предпочтение приглушенному рассеянному свету. Не работайте за компьютером в темноте;

– установите минимальный уровень яркости экрана. Не следует увеличивать контрастность изображения. Для обработки текста на светлом фоне можно притушить яркость монитора, а при просмотре видео – сделать ярче;

– старайтесь избегать длительной работы с сайтами с неудачной цветовой гаммой. Чтобы разглядеть маленькие желтые буквы на белом фоне придется сильно напрячь глаза, это большая нагрузка для них;

– при работе за компьютером следует чаще моргать. Так Вы обеспечите глазам постоянное увлажнение и предотвратите высыхание роговицы, что может привести к раздражению;

– считается, что взрослый человек может беспрерывно проводить за компьютером не более 2 часов. При этом в день рекомендуется отводить ему не более 6 часов.

5.5 Упражнения для глаз и тела при работе с компьютером

Выполняйте эти упражнения во время регулярных перерывов при работе с компьютером.

Общие правила выполнения упражнений:

– для того, чтобы дать вашим глазам эффективный отдых, переместитесь на участок с освещением, отличным от вашего рабочего места, снимите очки или контактные линзы, если вы их носите;

– при выполнении упражнений с телом – не фиксируйте взгляд так же, как это было при работе на компьютере. Наоборот, смотрите вдаль. Или закройте глаза. Для детей во время перерывов полезны (для отдыха глаз) такие игры, при которых надо следить глазами за быстро перемещающимися объектами.

Комплексы упражнений для глаз:

- самый простой (для глаз). Закройте глаза ладонями. Всматривайтесь в эту

темноту в течение тридцати секунд, затем закройте глаза, перед тем как убрать руки, и медленно откройте их;

– немного сложнее (для глаз): зажмурьте глаза на ~ 10 секунд; быстро моргайте в течении ~5-10 сек; сделайте несколько круговых движений глазами; несколько раз поменяйте фокус, для этого смотрите сначала на какую-либо точку на окне (если оно очень чистое, можно приклеить маленькую бумажку) а потом в даль (на облака, далёкий дом и т.д.).

Упражнения можно выполнять, не вставая с кресла, легко, без напряжения. Примите удобное положение, спина прямая, глаза открыты, взгляд устремлен прямо.

Комплекс упражнений только для глаз №1:

1) снимаем нагрузку с мышц, участвующих в движении глазного яблока: взгляд влево - прямо, вправо - прямо, вверх - прямо, вниз - прямо, без задержки в отведенном положении. Круговые движения глаз -от 1 до 10 кругов влево и вправо. Сначала быстрее, потом - как можно медленнее;

2) изменение фокусного расстояния: посмотрите на кончик носа, затем вдаль. Посмотрите на кончик пальца или карандаша, удерживаемого на расстоянии 30 см от глаз, затем вдаль. Повторите упражнение несколько раз;

3) сожмите веки, затем моргните несколько раз.

Комплекс упражнений только для глаз №2:

1) горизонтальные движения глаз: направо-налево;

2) движение глазными яблоками вертикально вверх-вниз;

3) круговые движения глазами: по часовой стрелке и в противоположном направлении;

4) интенсивные сжимания и разжимания глаз в быстром темпе;

5) движение глаз по диагонали: скосить глаза в левый нижний угол, затем по прямой перевести взгляд вверх. Аналогично в противоположном направлении;

6) сведение глаз к носу. Для этого к переносице поставьте палец и посмотрите на него - глаза легко "соединятся";

7) частое моргание глазами;

8) работа глаз "на расстояние". Подойдите к окну, внимательно посмотрите на близкую, хорошо видимую деталь: ветку дерева, растущего за окном, или на царапинку на стекле. Можно наклеить на стекло крохотный кружок из бумаги. Затем направьте взгляд вдаль, стараясь увидеть максимально удаленные предметы.

Каждое упражнение следует повторять не менее 6 раз в каждом направлении.

Комплекс упражнений только для глаз №3:

1) смотрите вдаль прямо перед собой 2-3 секунды. Поставьте палец на расстояние 25-30 см. от глаз, смотрите на него 3-5 секунд. Опустите руку, снова посмотрите вдаль. Повторить 10-12 раз;

2) перемещайте карандаш от расстояния вытянутой руки к кончику носа и обратно, следя за его движением. Повторить 10-12 раз;

3) прикрепите на оконном стекле на уровне глаз круглую метку диаметром 3-5 мм. Переводите взгляд с удаленных предметов за окном на метку и обратно. Повторить 10-12 раз;

4) открытыми глазами медленно, в такт дыханию, плавно рисуйте глазами «восьмерку» в пространстве: по горизонтали, по вертикали, по диагонали. Повторить 5-7 раз в каждом направлении;

5) поставьте большой палец руки на расстоянии 20-30 см. от глаз, смотрите двумя глазами на конец пальца 3-5 секунд, закройте один глаз на 3-5 секунд, затем снова смотрите двумя глазами, закройте другой глаз. Повторить 10-12 раз;

6) смотрите 5-6 секунд на большой палец вытянутой на уровне глаз правой руки. Медленно отводите руку вправо, следите взглядом за пальцем, не поворачивая головы. То же выполните левой рукой. Повторить 5-7 раз в каждом направлении;

7) не поворачивая головы, переведите взгляд в левый нижний угол, затем - в правый верхний. Потом в правый нижний, а затем - в левый верхний. Повторить 5-7 раз, потом - в обратном порядке.

Гимнастика для усталых глаз № 4:

1) глубоко вдохните, зажмурив глаза как можно сильнее. Напрягите мышцы шеи, лица, головы. Задержите дыхание на 2-3 секунды, потом быстро выдохните, широко раскрыв на выдохе глаза. Повторить 5 раз;

2) закройте глаза, помассируйте надбровные дуги и нижние части глазниц круговыми движениями - от носа к вискам;

3) закройте глаза, расслабьте брови. Повращайте глазными яблоками слева направо и справа налево. Повторить 10 раз;

4) поставьте большой палец руки на расстоянии 25-30 см. от глаз, смотрите двумя глазами на конец пальца 3-5 секунд, закройте один глаз на 3-5 секунд, затем снова смотрите двумя глазами, закройте другой глаз. Повторить 10 раз;

5) положите кончики пальцев на виски, слегка сжав их. 10 раз быстро и легко моргните. Закройте глаза и отдохните, сделав 2-3 глубоких вдоха. Повторить 3 раза.

В обычных условиях человек последовательно смотрит то на близкие предметы, то на отдаленные. Это заставляет мышцы, управляющие хрусталиком, растягиваться и сокращаться; так сохраняется необходимая эластичность мышц и возможность фокусировки глаза. В том случае, когда человек долгое время смотрит на статичный объект, находящийся все время на одном и том же расстоянии (книга, тетрадь, монитор компьютера), начинает развиваться близорукость (миопия) – глаз постепенно теряет способность рассматривать предметы на большом расстоянии в связи с атрофией мышц хрусталика. А ведь именно за компьютером некоторые люди часто сидят не отрываясь, часами напролет.

Комплекс комбинированных (с элементами движения рук) упражнений для профилактики близорукости (миопии):

– исходное положение сидя, каждое упражнение повторяется 5-6 раз. Указанные упражнения желательно повторять через каждые 40-50 минут работы за компьютером. Продолжительность однократной тренировки 3-5 минут;

– откинувшись на спинку стула, сделать глубокий вдох, наклонившись вперед сделать выдох;

– откинувшись на спинку стула, прикрыть веки, крепко зажмурить глаза и затем открыть веки. Повторить 5-6 раз;

– руки – на пояс, повернув голову вправо, посмотреть на локоть правой руки, повернуть голову влево, посмотреть на локоть левой руки, вернуться в исходное положение. Повторить 5-6 раз;

– поднять глаза кверху, сделать ими круговые движения по часовой стрелке, за тем – против часовой стрелки. Повторить 5-6 раз;

– руки – вперед, посмотреть на кончики пальцев, поднять руки вверх (вдох), следить глазами за руками, не поднимая головы, руки опустить (выдох). Повторить 4-5 раз;

– смотреть прямо перед собой на дальний предмет 2-3 секунды, перевести взгляд на кончик носа на 3-5 секунд. Повторить 6-8 раз;

– закрыть веки, в течение 30 секунд массировать их кончиками указательных пальцев.

Еще варианты простых упражнений для глаз:

1) «бабочка». Часто-часто похлопайте ресничками, то есть поморгайте. Оказывается, перед монитором глаза ленятся и перестают моргать, а это вредит нашему зрению;

2) «вверх-вниз». Голову держите прямо, не запрокидывайте. Смотрите прямо перед собой. Медленно поднимите взгляд на потолок, задержите на пару секунд, затем также медленно опустите его на пол и тоже задержите. Голова во время выполнения упражнения остается неподвижной;

3) «маятник». Голову держите прямо, смотрите перед собой. Посмотрите влево, затем медленно переведите взгляд вправо. Голова неподвижна, работайте только глазами. Во время выполнения упражнения следите за состоянием мышц глазных яблок, не перенапрягайте их;

4) «восьмерка». Голову держите прямо, смотрите перед собой. Мысленно представьте себе горизонтальную восьмерку (или знак бесконечности) максимального размера в пределах вашего лица и плавно опишите ее глазами. Повто-

рите упражнение несколько раз в одну сторону, затем в другую. После этого часто-часто поморгайте;

5) «циферблат». Представьте перед собой большой циферблат золотого цвета (ученые считают, что именно этот цвет способствует восстановлению зрения). Выполняйте круговые движения глазными яблоками, оставляя при этом голову неподвижной;

6) «карандаш». Возьмите карандаш в правую руку и вытяните ее, подняв карандаш на уровне глаз. Смотрите на кончик карандаша и медленно отводите руку вправо, затем влево, провожая пишущий предмет глазами, но не двигая головой;

7) «прекрасное далеко». Подойдите к окну и посмотрите вдаль, затем на кончик носа – это тренирует глазную мышцу. Повторите упражнение несколько раз;

8) «с широко закрытыми глазами». Закройте глаза и попробуйте описать ими воображаемый круг, затем горизонтальную восьмерку, потом крестик;

9) «жмурки». Несколько раз сильно зажмурьтесь, потом просто закройте глаза и посидите 20-30 секунд;

10) «эстафета взгляда». Отметьте в воображении несколько точек на своем рабочем месте. Начните с какого-нибудь предмета, который находится вблизи, например, с компьютерной клавиатуры или с кончика своего большого пальца. Следующая точка может находиться на мониторе, рядом с экраном. Теперь переместите взгляд на какой-нибудь предмет, который находится на вашем письменном столе, что-нибудь вроде линейки, бумаги для записей, штемпельной подушечки, подставки с карандашами и т.д. Ищите предметы, которые расположены на различных расстояниях по отношению к вам. Пусть ваш взгляд немного задержится на каждом предмете. Затем переведите взгляд на цветы на подоконнике, на оконную раму, затем за окно, на дерево или куст, на дом, который располагается напротив, - все дальше, до тех пор, пока взгляд не достигнет неба. Затем по отмеченным точкам последовательно вернитесь обратно к вашей клавиатуре или пальцу. Если у вас близорукость, во время передвижения взгляда с

ближнего расстояния на дальнее выдыхайте, а на обратном пути - вдыхайте. Если у вас дальнозоркость, выдыхайте, когда ваш взгляд перемещается с предметов, расположенных вдали, на предметы, расположенные вблизи. Если у вас нормальное зрение, выберите удобный ритм дыхания. Переводите взгляд всякий раз, когда у вас возникает такое желание. Не забывайте глубоко дышать

Напряженные мышцы, особенно в области шеи и плеч, являются частой причиной головной боли. В перерывах работы с компьютером выполняйте растягивающие упражнения, чтобы расслаблять их - это поможет снять стресс и предупредит возникновение головной боли.

Попробуйте выполнить *упражнение для мышц шеи*, называющееся «шейные круги». Для максимальной пользы его следует выполнить несколько раз в течение примерно пяти минут: Поставьте ноги на ширине плеч. Медленно опустите подбородок на грудь и останьтесь в этом положении на несколько секунд. Глубоко дыша, выполните круговое движение головой вправо, пытаясь коснуться ухом плеча. Задержитесь в этом положении на несколько секунд, затем поверните голову влево, к левому плечу, опять делая паузу. Когда вы почувствуете, что мышцы расслаблены, начните медленно выполнять вращательные движения толовой вначале вправо три-пять раз, затем то же число раз влево. Закончите растягивающее упражнение (все еще глубоко дыша), подняв плечи вверх, пытаясь достать ими ушей, затем медленно опустите их. Повторите 5 раз.

Упражнение для расслабления шеи: сядьте или встаньте прямо. Голову держите прямо. Сделайте выдох и поверните голову направо; сделайте вдох и снова верните голову в исходное положение; сделайте выдох и поверните голову налево. Во время выдоха еще раз поверните голову направо. Сделайте вдох и опять верните голову в исходное положение. Сделайте выдох и поверните голову налево. Во время выдоха наклоните голову к правому плечу; сделайте вдох и держите голову прямо; сделайте выдох и наклоните голову к левому плечу. Сделайте выдох - голова наклоняется вправо, сделайте вдох - выпрямляется, сделайте выдох - голова наклоняется влево. Затем медленно начинайте вращения

головой. Не отклоняйте голову слишком сильно назад. Потом выполните вращательные движения головой в другом направлении.

Гимнастическое упражнение для расслабления плеч: приподнимите плечи, насколько это возможно, и напрягите всю область шеи и плен. Расслабьтесь и опустите плечи. Повторите упражнение 3 раза. Несколько раз сделайте вращательные движения плечами назад, а потом вперед. Теперь выполните попеременные вращения плечами, как при плавании кролем, руки должны быть совершенно расслаблены. Затем энергично встряхнитесь.

Упражнения для рук (в том числе для профилактики туннельного синдрома):

1) встряхните руки;

2) сжимайте пальцы в кулаки (~10 раз);

3) вращайте кулаки вокруг своей оси;

4) надавливая одной рукой на пальцы другой руки со стороны ладони, как бы выворачивая ладонь и запястье наружу.

Разминка для голеностопного сустава:

– сядьте и примите расслабленное положение. Одну стопу отставьте на полу, другую сгибайте в голеностопном суставе вверх и вниз, вправо и влево. Пару раз выполните круговые вращения стопой во всех направлениях. Затем пошевелите пальцами ног и расслабьте их. Повторите то же самое с другой стопой, затем обеими стопами одновременно;

– сгибание ног. Сядьте поудобнее на стул. Вытяните правую ногу вперед. Согните ногу в колене и подтяните к груди, затем вытяните ее обратно. Опустите ногу на пол, повторите упражнение для левой ноги, затем для обеих ног;

– покачивание тазом в положении сидя. Сядьте прямо. Таз выдвиньте немного вперед. Позвоночник становится совершенно прямым и переходит в легкий изгиб крестцового отдела. Отодвиньте таз назад. При этом немного сгорбится нижняя часть спины. Вдыхайте, когда выдвигаете таз; выдыхайте, когда отодвигаете его. Выполните несколько раз эти движения. Напрягайте ягодичные мышцы и снова расслабляйте.

Комплекс для улучшения состояния легких, глаз, мышц шеи и кистей рук в перерывах между работы на компьютере:

1) поставьте ноги на ширине плеч. Руки опустите вниз перед собой, сцепите пальцы «в замок» и выверните сцепленные кисти (ладони будут расположены плоскостью вниз);

2) одновременно с глубоким вдохом поднимите сцепленные руки вверх и максимально отведите их назад, прогибаясь всем туловищем назад и максимально растягивая все мышцы в паузу после достижения максимальной амплитуды движения («стиль» этого растягивания позаимствован у кошки - то, как она потягивается после сна);

3) вместе с глубоким (и шумным – со звуком) выдохом закройте глаза, полностью расслабьтесь, расцепите кисти, опустите их за шею и дайте им свободно упасть вниз вдоль вашего туловища. Одновременно расслабьте голову и дайте ей упасть вперед. В конце медленного выдоха немного согнитесь вперед в пояснице и подожмите живот (напрягите брюшные мышцы) для того, чтобы диафрагмой выжать весь «застоявшийся» воздух из ваших легких – такое глубокое завершение выдоха можно осуществить несколькими шумными выдыхательными движениями;

4) сделайте несколько таких медленных дыхательных циклов в начале и в конце комплекса упражнений. Степень сгибания рук в локтевом суставе при их поднятии и траектория их падения при выдохе может варьировать в зависимости от ощущений наибольшей «приятности» от различных способов выполнения этих движений. Упражнение лучше делать, вдыхая свежий воздух у открытого окна или форточки, а еще и на балконе. Полезно при этом еще и «поглазеть», что происходит на улице: перевод взгляда с одного отдаленного объекта на другой является хорошим упражнением для глаз после их длительной фиксации на близких объектах на экране монитора.

ЗАКЛЮЧЕНИЕ

В наше время значение информации многократно возросло по сравнению с прошлыми столетиями. Более того, в наше время бытует весьма распространенная поговорка, что кто владеет информацией, тот владеет миром. Естественно, что на сегодняшний день весьма актуальным является вопрос защиты важных данных, которые в подавляющем большинстве случаев хранятся на персональном компьютере. Стоит заметить, что кража конфиденциальных данных возможна не только посторонними злоумышленниками, скажем через глобальную сеть Интернет, но и собственными сотрудниками компании. Как показывает практика, такие случаи весьма нередки во многих крупных компаниях мира.

Также многочисленные мошенники на сегодняшний день успешно зарабатывают неплохие деньги, занимаясь промышленным шпионажем. Они крадут информацию, находящуюся на персональных компьютерах. А затем перепродают ее заинтересованным лицам.

На каждый метод получения информации существует метод противодействия, часто не один, который может свести угрозу к минимуму. При этом успех зависит от двух факторов - от компетентности в вопросах защиты информации (либо от компетентности тех лиц, которым это дело поручено) и от наличия оборудования, необходимого для защитных мероприятий. Первый фактор важнее второго, так как самая совершенная аппаратура останется мертвым грузом в руках дилетанта.

При выполнении бакалаврской работы был проведён анализ предметной области; определены требования к средствам измерения побочных электромагнитных излучений и наводок средств вычислительной техники и условиям проведения измерений; установлены показатели эффективности защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами; проведен оценочный расчет; спроектирована и разработана система расчета; изучены угрозы утечки информации, а также установлены рекомендации по безопасности на предприятии.

В качестве средств реализации компоненты были выбраны:

– среда разработки Visual Studio 2017;

– язык программирования C#.

Разработанный программный продукт позволил определить степень защищенности помещения от утечки информации по электромагнитному каналу и условия, при которых защита будет наиболее успешной.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Хорев, А.А. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники // Специальная техника, 2010. – №2. – С. 53–56.

2 Основы защиты информации: Учебное пособие. Изд. 2-е, исправ. и доп. / под ред. К.М. Бондаря. – Хабаровск: Дальневосточный юридический институт МВД РФ, 2011. – 130 с.

3 Биттерлих [Электронный ресурс]. – Режим доступа: http://bitterlikh.com/kompyuter-i-zdorove/138-uprazhneniya-dlya-glaz-i-tela-pri-rabote-s-kompyuterom.html. – 2.05.2018

4 Хорошее зрение [Электронный ресурс]. – Режим доступа: https://www.horosheezrenie.ru/uprazhneniya-dlya-glaz-za-kompyuterom/ – 2.05.2018

5 Хорев, А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации/ А.А. Хорев. – М.: Гостехкомиссия РФ, 1998. – 320 с.

6 Емцева, Е.Д. Моделирование и анализ бизнес-процессов/ Е.Д. Емцева. – Владивосток: Изд-во ВГУЭС, 2012. – 156 с.

7 Волобуев, С.В. Безопасность социотехнических систем/ С.В. Волобуев. – Обнинск: Викинг, 2000. – 340 с.

8 Романцев, Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романцев, П.А. Тимофеев, В.Ф. Шаньгин – М.: Радио и связь, 1999. – 328 с.

9 Защита информации и информационная безопасность / И.Н. Кузьмин – Благовещенск: АмГУ, 2002. – 49 с.

10 Каторин, Ю.Ф. Защита информации техническими средствами / Каторин Ю.Ф., Разумовский А.В., Спивак А.И. – СПб: НИУ ИТМО, 2012. – 416 с.

11 Защита информации от утечки по техническим каналам: учебное пособие / В. К. Железняк. – СПб.: ГУАП, 2006. – 188 с.

12 Мельников, В.В. Защита информации в компьютерных системах/ В.В.

Мельников. – М.: Финансы и статистика, 1997. – 368 с.

13 Хаббард, Дж. Автоматизированное проектирование баз данных/ Дж. Хаббард. – М.: ИНФРА-М, 1984. – 432 с.

14 Рудикова, Л.В. Базы данных. Разработка приложений/ Л.В. Рудикова. – СПб.: БХВ-Петербург, 2006. – 496 с.

15 Хорев, А.А. Техническая защита информации. В 3 т. Том 1. Технические каналы утечки информации/ А.А. Хорев. – М.: НПЦ «Аналитика», 2008. – 436 с.

16 Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации/ А.А. Малюк. – М.: Горячая линия-Телеком. – 280 с.

17 Рембовский, А.М. Радиомониторинг: задачи, методы, средства / А.М. Рембовский, А.В. Ашихмин, В.А. Козьмин. – М.: Горячая линия – Телеком, 2010. – 680 с.

18 Зайцев, А.П. Технические средства и методы защиты информации / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков, А.А. Солдатов. – М.: Машиностроение, 2010. – 616 с.

19 Бедрина, Е.А. Методические указания по выполнению раздела «Безопасность жизнедеятельности» в выпускных квалификационных работах специальностей факультета «Информационные системы в управлении» / Е.А. Бедрина, Д.С. Алешков. – Омск: СибАДИ, 2012. – 17 с.

ПРИЛОЖЕНИЕ А

Таблица А.1 – Значения коэффициентов экранирования некоторых ограждающих конструкций на частотах 100, 500 и 1000 МГц

Тип здания	Экранирование (дБ) (коэффициент экранирования kэкр), на частотах:		
	100 МГц	500 МГц	1000 МГц
Деревянное здание с толщиной стен 20 см:			
Окно без решетки	5 - 7 (1,8 -2,2)	7 - 9 (2,2 – 2,8)	9 – 11 (2,8 – 3,5)
Окно закрыто решеткой с ячейкой 5 см	6 - 8 (2,0 -2,5)	10 - 12 (3,2 – 4,0)	12 - 14 (4,0 -5,0)
Кирпичное здание с толщиной кирпичной стены 1.5 кирпича:			
Окно без решетки	13 - 15 (4,5 – 5,6)	15 - 17 (5,6 -7,0)	16 - 19 (6,3 -8,9)
Окно закрыто решеткой с ячейкой 5 см	17 - 19 (7,0 – 8,9)	20 - 22 (10,0-12,6)	22 - 25 (12,6 - 17,8)
Железобетонные здания с ячейкой арматуры 15х15 см и толщиной 160 мм:			
Окно без решетки	20 - 25 (10,0 -17,8)	18 - 19 (8,0 -8,9)	15 - 17 (5,6 -7,0)
Окно закрыто решеткой с ячейкой 5 см	28 - 32 (25,1 -39,8)	23 - 27 (14,1-22,4)	20 - 25 (10,0 - 17,8)
Примечание: оконный проем составляет не более 30% от площади стены			

Таблица А.2 – Значения напряженности электромагнитного поля Е, создаваемого ПЭВМ

Значения электромагнитного поля Е (мкВ/м) на частотах		
1	2	3
100 МГц	500 МГц	1000 МГц
630	1400	1400
610	1370	1390
620	1420	1400

Продолжение таблицы А.2

1	2	3
610	1360	1400
600	1360	1390
630	1410	1400

Таблица А.3 – Результаты расчета

Ход вычислений	Данные, полученные из таблиц или в результате расчетов, на частотах		
	100 МГц	500 МГц	1000 МГц
Значения электромагнитного поля Е, создаваемого ПЭВМ, мкВ/м	610	1370	1390
Коэффициент затухания	0,0226		
Максимальные значения коэффициента экранирования kэкр	39,8	22,4	17,8
Напряженность электромагнитного поля на границе КЗ, мкВ/м	0,346	1,38	1,76
Среднеквадратическое значение напряженности поля Еа атмосферных помех	0,346	1,738	3,467
Определяем отношение сигнал/шум на границе контролируемой зоны по формуле Δ = Екз/Еа	0,999 ≈ 1	0,79	0,51

Программный продукт.

Исходный код.

```
using Microsoft.Win32;
using System;
using System.Collections.Generic;
using System.IO;
using System.Linq;
using System.Runtime.Serialization.Formatters.Binary;
using System.Text;
using System.Threading.Tasks;
using System.Windows;
using System.Windows.Controls;
using System.Windows.Data;
using System.Windows.Documents;
using System.Windows.Input;
using System.Windows.Media;
using System.Windows.Media.Imaging;
using System.Windows.Navigation;
using System.Windows.Shapes;
namespace SpaceSecurity
{
   public partial class MainWindow : Window
   {
                    // глобальные переменные программы
      private double n = 1.3; // нужно вынести как поле для ввода юзером
      private byte _window = 0; // без решетки = 0, с решеткой = 1
      private byte _building = 0; // дерево = 0, кирпичное = 1, железобетонное = 2
      private double _TalkLevel = 0.7; // важность разговора
      BinaryFormatter formatter = new BinaryFormatter(); // дичь)
      // 3 экземпляра класса Core - описан снизу
      private Core MGz100;
      private Core MGz500;
      private Core MGz1000;
```

```
            // метод инициализации пользовательского интерфейса
        public MainWindow()
        {
            InitializeComponent();
        }
            // метод рбработчик события клика по кнопке "Расчет"
        private void Button_Click(object sender, RoutedEventArgs e)
        {
                // создаем 3 объекта класса Core
            MGz100 = new Core(Convert.ToInt32(textBox100M.Text));
            MGz500 = new Core(Convert.ToInt32(textBox500M.Text));
            MGz1000 = new Core(Convert.ToInt32(textBox1000M.Text));
                // расчитываем коэффициент затухания и выводим его в текстовое
поле
            var k = 1 / Math.Pow(Convert.ToDouble(textBoxRadius.Text), n);
            k = Math.Round(k,3);
            MGz100.k = k; MGz500.k = k; MGz1000.k = k;
            textBoxKzat.Text = k.ToString();
                // вызываем метод установки минимальных и максимальных зна-
чений Db для 3 экземпляров Core
            SetK();
                // производим расчеты для каждого экземпляра класса
        Core
            MGz100.SetE(100); MGz500.SetE(500); MGz1000.SetE(1000);
                // выводим результаты в текстовые поля графического интерфейса
            textBox100M_E.Text = MGz100.E.ToString();
            textBox500M_E.Text = MGz500.E.ToString();
            textBox1000M_E.Text = MGz1000.E.ToString();
            textBox100M_E_Copy.Text = MGz100.Ea.ToString();
            textBox500M_E_Copy.Text = MGz500.Ea.ToString();
            textBox1000M_E_Copy.Text = MGz1000.Ea.ToString();
            textBox100M_E_Copy1.Text = MGz100.Delta.ToString();
            textBox500M_E_Copy1.Text = MGz500.Delta.ToString();
```

```
            textBox1000M_E_Copy1.Text = MGz1000.Delta.ToString();
            // расчет дельты и вывод результата
            if (MGz100.Delta <= _TalkLevel & MGz500.Delta <= _TalkLevel & MGz1000.Delta
<= _TalkLevel)
               TextBox_Out.Text = $"Расчеты показали, что на всех частотах значение
Δ≤{_TalkLevel}. Следовательно, расстояние до границы контролируемой зоны достаточно,
для обеспечения безопасности сообщений, излучаемых в окружающее пространство ПЭВМ.
Дополнительных мер по обеспечению защиты помещения от утечки информации не требу-
ется.";
            else
            {
               string summ="";
               if (MGz100.Delta > _TalkLevel)
                  summ += "100 МГц ";
               if (MGz500.Delta > _TalkLevel)
                  summ += "500 МГц ";
               if (MGz1000.Delta > _TalkLevel)
                  summ += "1000 МГц ";
               double newr = Math.Pow((Convert.ToInt32(textBox100M.Text) / (MGz100.Ea *
MGz100.maxDb)),1/n);
               newr = Math.Round(newr,1);
               TextBox_Out.Text = $"Расчеты показали, что на частотах: {summ} значение
Δ>{_TalkLevel}. Следовательно расстояние до границы контролируемой зоны недостаточно,
для обеспечения безопасности сообщений, излучаемых в окружающее пространство ПЭВМ.
Необходимое минимальное расстояние составляет: {newr} м.";
            }
         }
               // метод устанавливающий мин и макс значения Db для 3х экземпляров
класса Core
         void SetK()
         {
            if (_building == 0) // если дерево
            {
```

```
    if (_window == 0)
    {
        MGz100.minDb = 1.8f;
        MGz100.maxDb = 2.2f;
        MGz500.minDb = 2.2f;
        MGz500.maxDb = 2.8f;
        MGz1000.minDb = 2.8f;
        MGz1000.maxDb = 3.5f;
    }
    Else
    {
        MGz100.minDb = 2.0f;
        MGz100.maxDb = 2.5f;
        MGz500.minDb = 3.2f;
        MGz500.maxDb = 4.0f;
        MGz1000.minDb = 4.0f;
        MGz1000.maxDb = 5.0f;
    }
}
else if (_building == 1) // если кирпич
{
    if (_window == 0)
    {
        MGz100.minDb = 4.5f;
        MGz100.maxDb = 5.6f;
        MGz500.minDb = 5.6f;
        MGz500.maxDb = 7.0f;
        MGz1000.minDb = 6.3f;
        MGz1000.maxDb = 8.9f;
    }
    else
    {
        MGz100.minDb = 7.0f;
```

```
                MGz100.maxDb = 8.9f;
                MGz500.minDb = 10.0f;
                MGz500.maxDb = 12.6f;
                MGz1000.minDb = 12.6f;
                MGz1000.maxDb = 17.8f;
            }
        }
        else // если железобетон
        {
            if (_window == 0)
            {
                MGz100.minDb = 10.0f;
                MGz100.maxDb = 17.8f;
                MGz500.minDb = 8.0f;
                MGz500.maxDb = 8.9f;
                MGz1000.minDb = 5.6f;
                MGz1000.maxDb = 7.0f;
            }
            else
            {
                MGz100.minDb = 25.1f;
                MGz100.maxDb = 39.8f;
                MGz500.minDb = 14.1f;
                MGz500.maxDb = 22.4f;
                MGz1000.minDb = 10.0f;
                MGz1000.maxDb = 17.8f;
            }
        }
    }
            // метод обработчик события изменения типа окна
    private void comboMesto_SelectionChanged(object sender, SelectionChangedEven-
tArgs e)
    {
```

```
            var k = (ComboBoxItem)e.AddedItems[0];
            if (k.Content == null)
                n = 1.3;
            else
                n = Convert.ToDouble(k.Content);
        }
                // метод обработчик события изменения типа окна
        private void ComboBox_SelectionChanged(object sender, SelectionChangedEventArgs
e)
        {
            var k = (ComboBoxItem)e.AddedItems[0];
                // в зависимости от выбранного типа окна, присваиваем переменной
_window значение
            switch (k.Content)
            {
                case "Без решетки": _window = 0; break;
                case "С решеткой": _window = 1; break;
            }
        }
                // метод обработчик события изменения типа стены здания
        private void ComboBox_SelectionChanged_1(object sender, SelectionChangedEven-
tArgs e)
        {
            var k = (ComboBoxItem)e.AddedItems[0];
                // в зависимости от выбранного типа стены, присваиваем переменной
_building значение
            switch (k.Content)
            {
                case "Деревянное": _building = 0; break;
                case "Кирпичное": _building = 1; break;
                case "Железобетонное": _building = 2; break;
            }
        }
```

```
                // метод обработчик события изменения типа разговора
            private void ComboBox_SelectionChanged2(object sender, SelectionChangedEven-
tArgs e)
            {
                var k = (ComboBoxItem)e.AddedItems[0];
                // в зависимости от выбранного типа разговора, присваиваем переменной
_TalkLevel значение
                switch (k.Content)
                {
                    case "Важный": _TalkLevel = 0.7; break;
                    case "Обычный": _TalkLevel = 1; break;
                }
            }
            private void Button_Click_Save(object sender, RoutedEventArgs e)
            {
                SaveFileDialog sv = new SaveFileDialog
                {
                    //InitialDirectory = dir + "\\Images",
                    Filter = "Txt files (*.txt)|*.txt;"
                };
                sv.ShowDialog();
                if (sv.FileName != "")
                {
                    //formatter.Serialize(fs, "Привет");
                    try
                    {
                        string text = $"Исходные данные:\nРасстояние от ПВМ - {textBoxRa-
dius.Text}\nКоэфициент n - {n.ToString()}\nТип окна - {comboWin.SelectionBox-
Item.ToString()}\n" +
                            $"Тип здания - {comboTower.SelectionBoxItem.ToString()}\nВажность
разговора - {comboTalkLvl.SelectionBoxItem.ToString()}\n" +
                            $"100 МГц - {textBox100M.Text}\n500 МГц - {textBox500M.Text}\n1000
МГц - {textBox1000M.Text}\n\n" +
```

```
                $"Результаты расчета:\nКоэффициент затухания - {MGz100.k.ToString()}\n" +
                $"Напряженность электромагнитного поля: \n100 МГц - { MGz100.E.ToString()}\n500 МГц - { MGz500.E.ToString()}\n1000 МГц - { MGz1000.E.ToString()}\n" +
                $"Среднеквадратическая напряженность: \n100 МГц - { MGz100.Ea.ToString()}\n500 МГц - { MGz500.Ea.ToString()}\n1000 МГц - { MGz1000.Ea.ToString()}\n" +
                $"Отношение сигнал \\ шум: \n100 МГц - { MGz100.Delta.ToString()}\n500 МГц - { MGz500.Delta.ToString()}\n1000 МГц - { MGz1000.Delta.ToString()}\n\n" +
                $"Вывод:\n{TextBox_Out.Text}";
            File.WriteAllText(sv.FileName, text, Encoding.UTF8);
            MessageBox.Show("Файл отчета успешно сохранен", "Готово");

        }
        catch (Exception ex)
        {
            MessageBox.Show(ex.ToString(), "Ошибка");
        }
      }
    }
}
// описание класса одного расчета
public class Core
{
        // его свойства \ поля \ переменные
    public int MGz { get; set; }
    public double minDb { get; set; }
    public double maxDb { get; set; }
    public double E { get; set; }
    public double Ea { get; set; }
    public double k { get; set; }
```

```
        public double Fecv { get; set; }
        public double Delta { get; set; }
        public int F { get; set; }
    // конструктор класса принимающий значение частоты
        public Core(int MGz)
        {
            this.MGz = MGz;
        }
    // метод производящий все расчеты
        public void SetE(int f)
        {
            F = f;
            Fecv = 40000000f;
            E = MGz * k / maxDb;
            E = Math.Round(E, 3);
            Ea = (10 * Math.Log10(293f / 273f) - 125.5f + (20 * Math.Log10(f)) + (10 *
Math.Log10(Fecv)));
            Ea = Math.Pow(10, (float)(0.05* Ea));
            Ea = Math.Round(Ea, 3);
            Delta = E / Ea;
            Delta = Math.Round(Delta, 3);
        }
    }
}
```

ПРИЛОЖЕНИЕ В

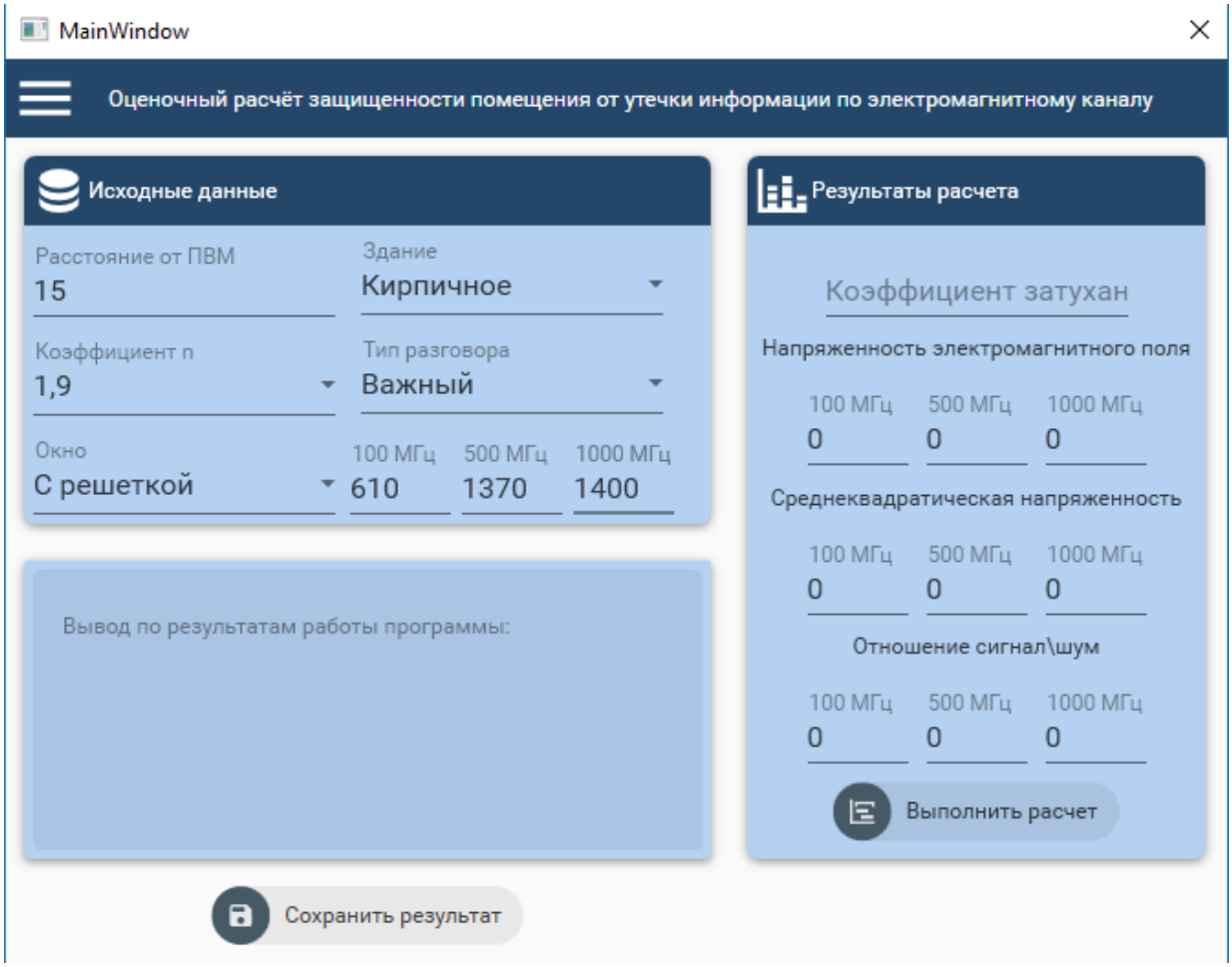

Рисунок В.1 – Вид программы до расчета данных

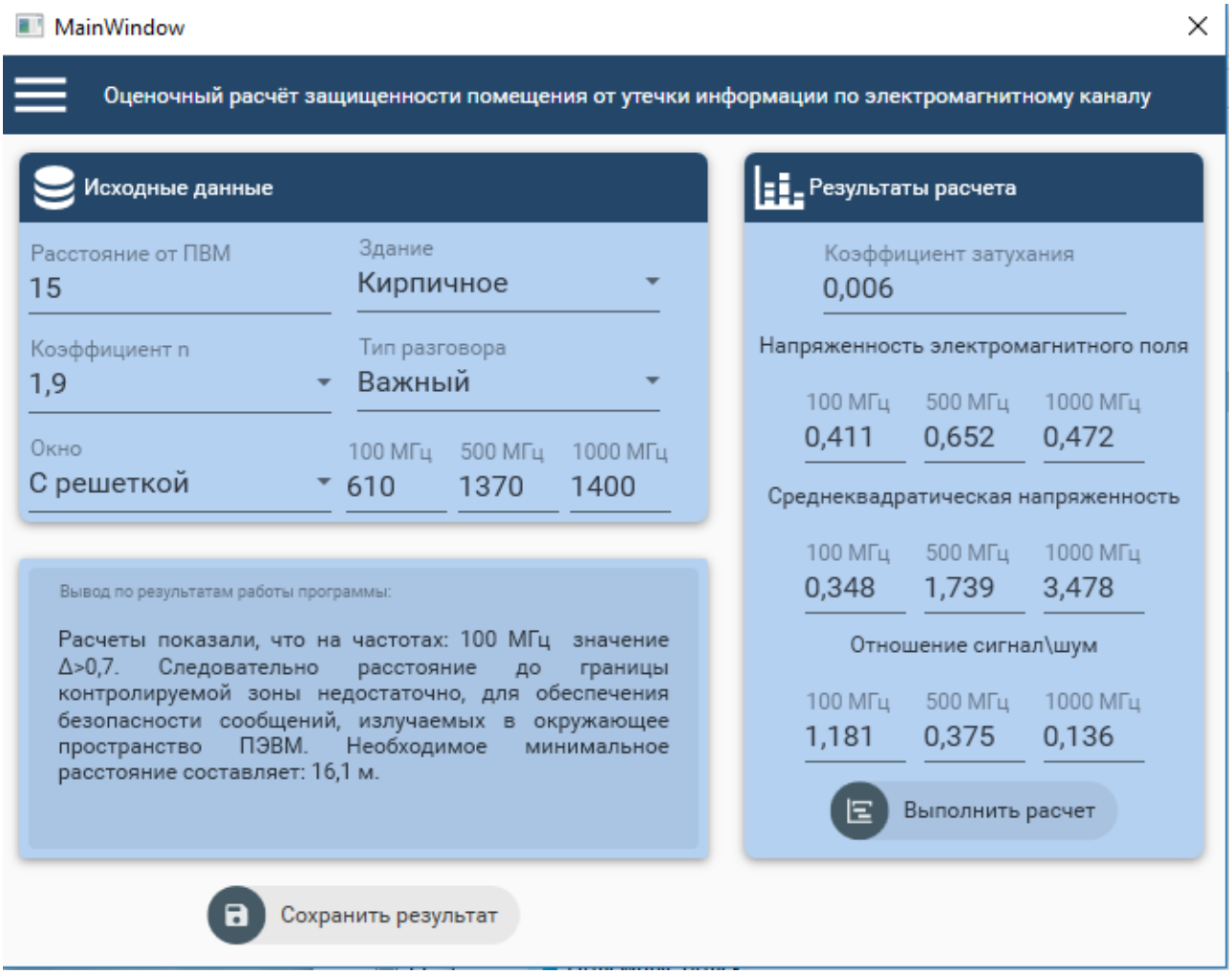

Рисунок В.2 – Вид программы после расчета данных

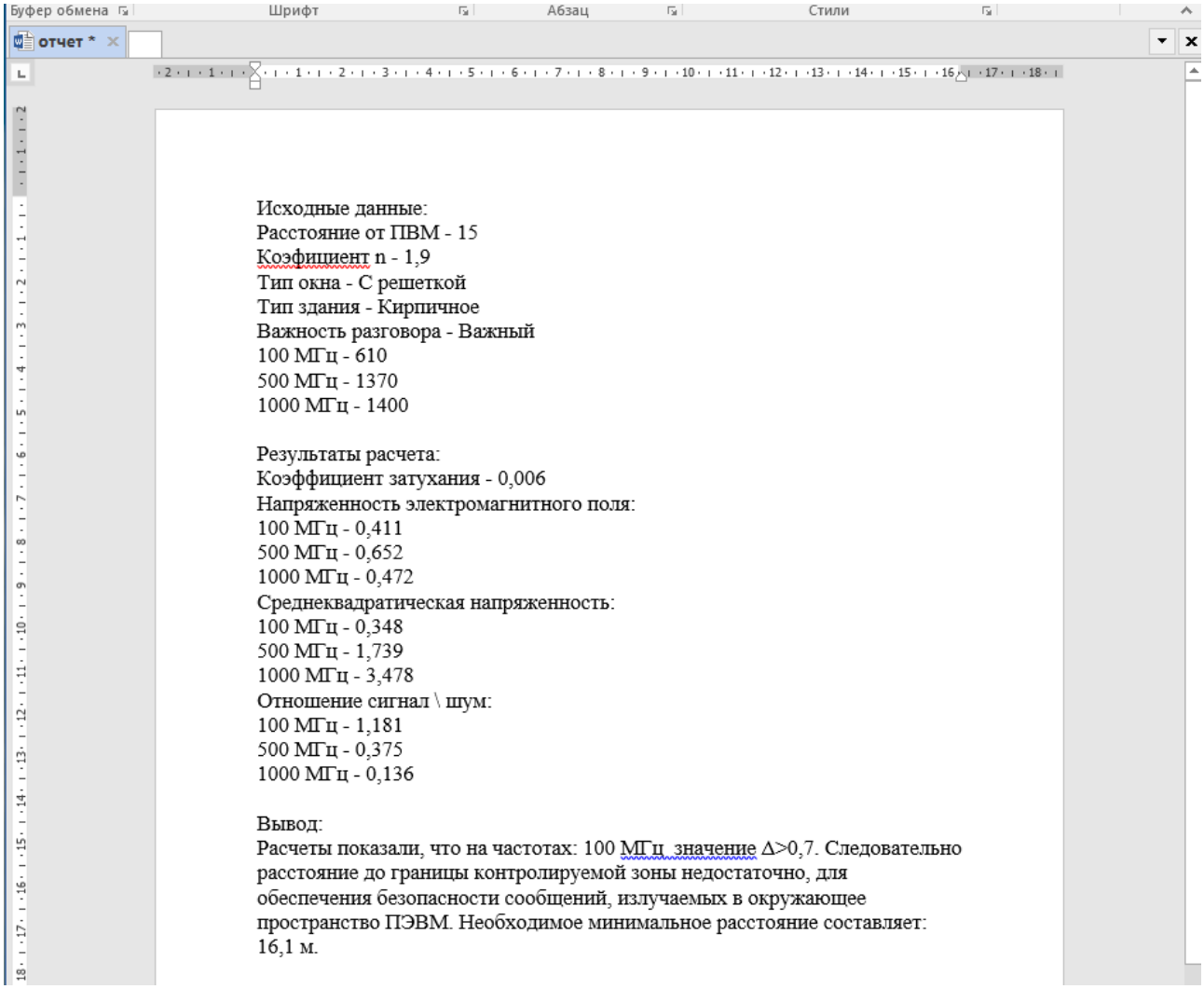

Рисунок В.3 – Отчет по расчету данных