

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

Факультет безопасности информационных технологий

КУРСОВАЯ РАБОТА

По дисциплине:

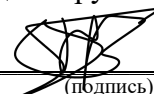
«Инженерно-технические средства защиты информации»

На тему:

**«Проектирование системы защиты от утечки информации по
различным каналам»**

Выполнил:

Василев Васил Николаев, студент группы N34511



(подпись)

Проверил:

Попов И. Ю., преподаватель ФБИТ

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023 г.

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент	Василев Васил Николаев
	(Фамилия И.О.)
Факультет	Безопасности информационных технологий
Группа	N34481
Направление (специальность)	10.03.01 Информационная безопасность
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ Университета ИТМО
	(Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование системы защиты от утечки информации по различным каналам
Задание	Разработка комплекса инженерно-технической защиты информации, составляющей государственную тайну с уровнем «секретно».

Краткие методические указания

1. Курсовая работа выполняется в рамках изучения дисциплины «Инженерно-технические средства защиты информации».
2. Порядок выполнения и защиты курсовой работы представлен в методических указаниях, размещённых на коммуникационной площадке дисциплины.
3. Объект исследований курсовой работы ограничивается заданным помещением

Содержание пояснительной записки

Включает разделы – введение, анализ технических каналов утечки информации, перечень руководящих документов, анализ выбранных помещений, анализ технических каналов утечки информации и выбор средств защиты информации, описание расстановки технических средств защиты, заключение, список использованных источников


Рекомендуемая литература

Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с

Руководитель Попов Илья Юрьевич

(Подпись, дата)

Студент Василев Васил Николаев


(Подпись, дата)

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Василев Васил Николаев

(Фамилия И.О.)

Факультет Безопасности информационных технологий

Группа N34481

Направление (специальность) 10.03.01 Информационная безопасность

Руководитель Попов Илья Юрьевич, к.т.н., доцент ФБИТ Университета ИТМО

(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование системы защиты от утечки информации по различным каналам

№ п/п	Наименование этапа	Дата завершения	
		Планируемая	Фактическая
1.	Разработка и утверждение задания и календарного плана на курсовую работу	19.09.2023	19.09.2023
2.	Создание плана курсовой работы	24.09.2023	24.09.2023
3.	Анализ теоретической составляющей	26.10.2023	26.10.2023
4.	Разработка комплекса инженерно-технической защиты информации в заданном помещении	23.11.2023	23.11.2023
5.	Представление выполненной курсовой работы	19.12.2023	19.12.2023

Руководитель Попов Илья Юрьевич

(Подпись, дата)

Студент Василев Васил Николаев

(Подпись, дата)

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ

Студент Василев Васил Николаев

(Фамилия И.О.)

Факультет Безопасности информационных технологий

Группа N34481

Направление (специальность) 10.03.01 Информационная безопасность

Руководитель Попов Илья Юрьевич, к.т.н., доцент ФБИТ Университета ИТМО

(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование системы защиты от утечки информации по различным каналам

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

**1. Цель и задачи
работы**

- ☐ Предложены студентом ☐ Сформулированы при участии студента
☒ Определены руководителем

Цель данной работы –

**2. Характер
работы**

- ☐ Расчет ☒ Конструирование
☐ Моделирование ☐ Другое Исследование

3. Содержание работы

Введение; Анализ технических каналов утечки информации; Перечень руководящих документов; Анализ выбранных помещений; Анализ технических каналов утечки информации и выбор средств защиты информации; Анализ технических средств защиты информации; Описание расстановки технических средств защиты; Заключение; Список использованных источников

4. Выводы

В результате работы была предложена защита от утечек информации техническим каналам, обеспечена защита от ПЭМИН

Руководитель Попов Илья Юрьевич

(Подпись, дата)

Студент Василев Васил Николаев

(Подпись, дата)

«_____» _____ 2023 г.

СОДЕРЖАНИЕ

Содержание	5
Введение	6
1 Постановка задач	7
1.1 Цель курсовой работы	7
1.2 Задачи, решаемые в ходе выполнения работы	7
2 Анализ технических каналов утечки информации	8
2.1 Утечки информации в радиоэлектронном канале	9
2.2 Утечки информации в оптическом канале	10
2.3 Утечки информации в радиоэлектронном канале	10
2.4 Утечки информации в электромагнитном канале	10
2.5 Утечки информации в электрическом канале	10
2.6 Утечки информации в акустическом канале	11
2.7 Утечки информации в акустоэлектрическом канале	11
2.8 Утечки информации в виброакустическом канале	11
2.9 Утечки информации в материальном канале	11
3 Перечень руководящих документов	13
4 Анализ выбранных помещений	16
4.1 Обоснование секретности	16
4.2 Описание помещения	18
5 Анализ технических каналов утечки информации и выбор средств защиты информации	21
6 Анализ технических средств защиты информации	22
6.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации	22
6.2 Устройства для перекрытия электрического, акустического и электромагнитного каналов утечки информации	25
6.3 Защита от ПЭМИН	27
6.4 Защита от утечек по оптическому каналу	29
7 Описание расстановки технических средств защиты информации	31
Заключение	34
Список использованных источников	35

ВВЕДЕНИЕ

В истории было много случаев кражи информации, которые оказывали негативное влияние на их владельцев. Поэтому необходимо позаботиться о защите информации.

Информация передается по различным каналам связи, но она должна быть должным образом защищена. Если защита этих каналов слабая, информация может быть предоставлена неуполномоченным лицам. Чтобы устранить эту ситуацию, были использованы различные технические средства для обеспечения того, чтобы информация не распространялась за пределы определенной области. Канал, который распространяет информацию за пределами зоны контроля, называется каналом утечки информации. Здесь рассматривается процесс разработки комплекса инженерно-технической защиты информации, составляющего государственную тайну на уровне "секретно" в информационном объекте. Охраняемые объекты включают в себя 9 помещений: кабинет директора, конференц-зал, рабочие кабинеты, место для отдыха, серверное помещение, туалет и коридор.

Работа состоит из 5 глав. В первой главе анализируются технические каналы утечки информации. Второй включает перечень административных документов, а третий включает анализ охраняемых объектов с точки зрения возможной утечки информации и технических средств, необходимых для защиты. В главе 4 анализируется рынок различных типов технических средств защиты информации, а глава 5 посвящена разработке плана размещения выбранных технических средств в защищаемом помещении.

1 ПОСТАНОВКА ЗАДАЧ

1.1 Цель курсовой работы

Цель курсовой работы это - разработка комплекса инженерно-технической защиты информации, составляющей государственную тайну с уровнем «секретно».

1.2 Задачи, решаемые в ходе выполнения работы

1. Произвести анализ технических каналов утечки информации;
2. Составить перечень управляющих документов;
3. Проанализировать защищаемые объекты с точки зрения возможной утечки информации и технических средств, необходимых для защиты;
4. Проанализировать рынок технических средств защиты информации разных категорий;
5. Разработать схемы расстановки выбранных технических средств в защищаемом помещении.

2 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Утечка конфиденциальной информации — это неконтролируемое разглашение конфиденциальной информации за пределами организации или компании, которым доверено обслуживание или которые известны во время работы. Утечка может быть вследствие разглашения конфиденциальной информации, ухода по каналам связи, несанкционированного доступа к конфиденциальной информации различными методами.

В курсовой работе рассматриваться только утечку информации по техническим каналам.

Технический канал утечки информации (ТКУИ) - совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация [1].

Утечка (информации) по техническому каналу - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации [2]. На рисунке 1 приведена структура технического канала утечки информации.

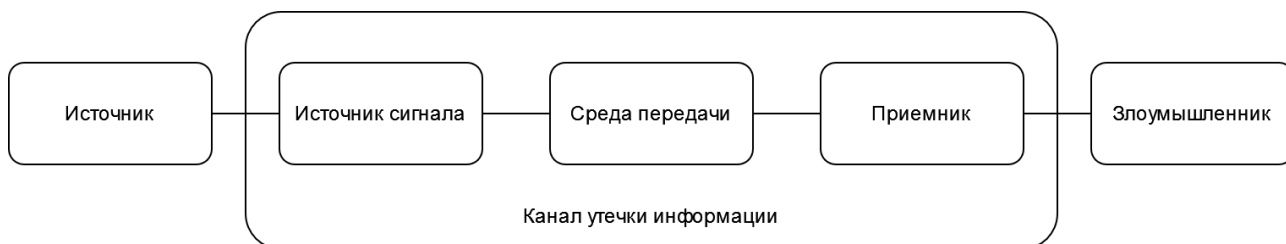


Рисунок 1 – Структура технического канала утечки информации

На вход ТКУИ поступает информация в виде первичного сигнала, представляющего собой носитель с информацией от её источника. Источниками сигнала могут быть:

- объект наблюдения, отражающий электромагнитные и акустические волны;
- объект наблюдения, излучающий собственные (тепловые) электромагнитные волны в оптическом и радиодиапазонах;
- передатчик функционального канала связи;
- закладное устройство;
- источник опасного сигнала;
- источник акустических волн, модулированных информацией.

Поскольку информация из источника передается на вход канала на исходном языке, передатчик преобразует полученную информацию в формат, который записывает ее на носитель, подходящий для среды распространения. Среда распространения сигнала - это

физическая среда, в которой информационные сигналы могут распространяться и записываться приемником. Он характеризуется набором физических параметров, которые определяют условия движения сигнала. Основными параметрами, которые следует учитывать при описании среды распространения, являются:

- физические препятствия для субъектов и материальных тел;
- мера ослабления сигнала на единицу длины;
- частотная характеристика;
- вид и мощность помех для сигнала.

Приемник после этого производит следующие действия:

- выбор носителя с нужной получателю информацией;
- усиление принятого сигнала до значений, обеспечивающих съем информации;
- съем информации с носителя;
- преобразование информации в форму сигнала, доступную получателю (человеку, техническому устройству), и усиление сигналов до значений, необходимых для безошибочного их восприятия.

Классификация технических каналов утечки информации приведена на рисунке 2.

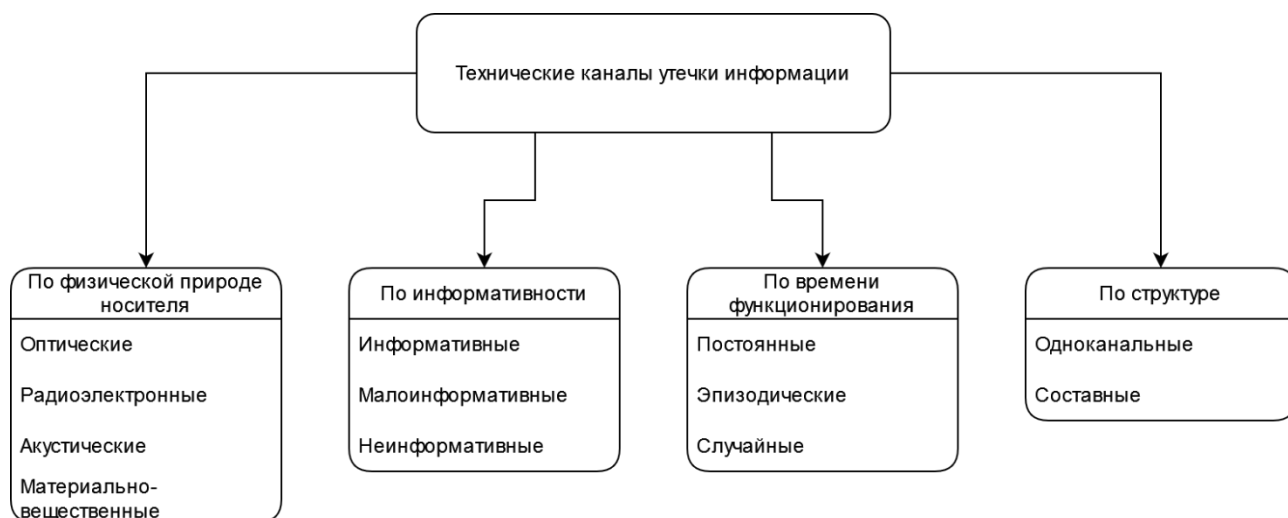


Рисунок 2 – Классификация технических каналов утечки информации

2.1 Утечки информации в радиоэлектронном канале

Утечки информации в радиоэлектронном канале в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток, распространяющийся по металлическим проводам. Акустические ТКUI в свою очередь делятся на акустоэлектрическом, виброакустическом и акустические.

2.2 Утечки информации в оптическом канале

Носителями информации в оптическом канале являются электромагнитные поля (фотоны). Удаление информации возможно, например, наблюдая за ней, глядя в окно или слегка приоткрытую дверь. Другой способ - использовать встроенное устройство с возможностью записи фотографий или видео. Этот канал утечки связан с представлением информации в графическом формате и распространяется на все поверхности (окна, стеклянные двери и т. д.) Защита осуществляется путем установки непрозрачного покрытия жалюзи или другой формы.) если смотреть со стороны.), а также использование двери ближе.

2.3 Утечки информации в радиоэлектронном канале

В радиоэлектронном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также используется ток (поток электронов), распространяющийся по металлическому проводу. Частотный диапазон радиоэлектронных каналов занимает полосу частот от нескольких десятков ГГц до звукового.

2.4 Утечки информации в электромагнитном канале

Электромагнитный ТКУИ связан с перехватом электромагнитного излучения на частоте передатчика и средств связи системы. Используется для перехвата информации, передаваемой по радио, радиорелейным и спутниковым каналам связи. Напряженность поля в точке приема (перехвата) прямо пропорциональна величине мощности передачи, высоте приемной и передающей антенн и обратно пропорциональна расстоянию. Этот канал утечки актуален, когда в помещении есть электронно-вычислительная машина, ЭВМ или другое средство обработки информации. Электромагнитное излучение, генерируемое во время работы технического устройства, называется вторичным электромагнитным излучением и помехами (ПЭМИН), а защита — это специальное техническое устройство, создающее электромагнитный шум, который скрывает это электромагнитное излучение.

2.5 Утечки информации в электрическом канале

Электрическая ТКУИ связана со сбором информации путем подключения оборудования злоумышленника к кабельной линии связи. Электрические колебания, возникающие при работе электроприборов, содержат информацию о подключенном устройстве. Защита осуществляется специальными фильтрами для электросетей, которые скрывают электрические колебания, вызванные компьютерной техникой.

2.6 Утечки информации в акустическом канале

Носителем информации в акустическом канале является упругая звуковая волна, распространяющаяся в среде. Информация может быть удалена путем подслушивания извне помещения (при отсутствии звукоизоляции) или с помощью встроенного устройства с функцией записи звука. Этот канал утечки актуален при передаче информации в аудио формате (диалоги, встречи и т. д.). Защита осуществляется за счет использования звукоизоляционных материалов, препятствующих выходу звука за пределы помещения, а также специального программного и аппаратного обеспечения, способного идентифицировать закладки.

2.7 Утечки информации в акустоэлектрическом канале

В акустоэлектрических каналах информация представляется в виде акустических колебаний, которые в дальнейшем воздействуют на сеть электроснабжения и вызывают электрические колебания. При устранении этих колебаний можно восстановить исходный акустический сигнал. Этот канал утечки информации актуален, когда есть электрическая сеть, подключенная к внешней зоне контролируемого помещения. Например, телефонная сеть - подавая небольшое напряжение на входящую телефонную линию и снимая его на входе, мы можем получать голосовую информацию, которая распространяется в помещении. Защита осуществляется с помощью специального фильтра для электросети, который скрывает колебания, вызванные воздействием на электрическую сеть.

2.8 Утечки информации в виброакустическом канале

В виброакустических каналах информация сначала представляется в виде акустических колебаний, которые воздействуют на некоторые твердые поверхности и превращаются в виброакустические колебания. Этот канал утечки информации практически всегда актуален, поскольку связан с наличием твердой поверхности в контролируемом помещении: стен, потолков, полов, батарей отопления, оконных стекол и т.д. Защита осуществляется с помощью специального технического устройства, которое передает белый шум на защищаемую твердую поверхность, скрывающую вибрационные колебания, вызываемые звуковыми волнами.

2.9 Утечки информации в материальном канале

В материальном канале утечка информации осуществляется путем несанкционированного распространения физических носителей с защищенной информацией

за пределами зоны контроля. В качестве физических носителей чаще всего используются черновики документов и использованная копировальная бумага, портативные носители (HDD, SSD, карта памяти и т. д.). С кражей и копированием информации, записанной на материальных носителях, борются в первую очередь с помощью организационных мер, введения строгих процедур учета и обращения с этими типами носителей.

Еще одна угроза — это возможность проникновения злоумышленников на территорию охраняемой территории, поэтому не менее актуальным вопросом является изучение контроля доступа к охраняемой территории.

3 ПЕРЕЧЕНЬ РУКОВОДЯЩИХ ДОКУМЕНТОВ

Основными указами Президента Российской Федерации в области предотвращения утечки информации по техническим каналам являются:

- «Вопросы Государственной технической комиссии при Президенте Российской Федерации» от 19 февраля 1999 г. №212;
- «Вопросы защиты государственной тайны» от 30.03.1994 г. №614;
- «Об утверждении перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г. №1203;
- «О межведомственной комиссии по защите государственной тайны» от 8 ноября 1995 г. №1108;
- «Вопросы Межведомственной комиссии по защите государственной тайны» от 20 января 1996 г. №71 с изменениями, внесенными Указами Президента Российской Федерации от 21 апреля 1996 г. №573, от 14 июня 1997 г. №594;
- «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. №644;
- «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. №188.

Основными постановлениями Правительства Российской Федерации в области предотвращения утечки информации по техническим каналам являются:

- Инструкция №0126–87;
- Положение о государственной системе защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам Постановление Совета Министров – Правительства Российской Федерации от 15 сентября 1993 г. №921–51;
- «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» от 3 ноября 1994 г. №1233;
- «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 15 апреля 1995 г. №333;
- «О внесении дополнения в Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием

сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 30 апреля 1997 г. №513;

- «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 4 сентября 1995 г. №870;

- «Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам» от 2 августа 1997 г. №973;

- «О сертификации средств защиты информации» от 26 июня 1995 г. №608.

Также на сайте ФСТЭК существует отдельный раздел, содержащий специальные нормативно-технические документы ФСТЭК России – нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации:

- СТР Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам;

- СТР-К. Специальные требования и рекомендации по технической защите конфиденциальной информации;

- Методика сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров;

- Временные методики сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров по требованиям безопасности информации;

- Временный порядок аттестации объектов информатизации по требованиям безопасности информации;

- Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения;

- Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации;

- Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации;

- Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники;

- Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации;

- Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования;

- Руководящий документ Гостехкомиссии России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей;

- Руководящий документ. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам.

Также, необходимо обратить внимания на законы Российской Федерации:

- «О государственной тайне» от 21 июля 1993 г. №5151–1;
- «Об информации, информатизации и защите информации» от 20 февраля 1995 г. №24-ФЗ;

- «О безопасности» от 5 марта 1992 г. №2446–1;
- «О федеральных органах правительственной связи и информации» от 19 февраля 1993 г. №4524–1;

- «О связи» от 16 февраля 1995 г. №15-ФЗ;
- «Об участии в международном информационном обмене» от 4 июля 1996 г. №85-ФЗ.

4 АНАЛИЗ ВЫБРАННЫХ ПОМЕЩЕНИЙ

4.1 Обоснование секретности

Объектом защиты является фирма ООО «Мрежа1», занимающаяся поддержкой сетевого оборудования для бизнес-клиентов и государственных структур.

Согласно [3] Руководящему документу Государственной технической комиссией при Президенте РФ «Классификация автоматизированных систем и требований по защите информации» от 30 марта 1992 г.: «При разработке АС, предназначенной для обработки или хранения информации, являющейся собственностью государства и отнесенной к категории секретной, необходимо ориентироваться в соответствии с РД «Средства вычислительной техники».

Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» на классы защищенности АС не ниже (по группам) 3А, 2А, 1А, 1Б, 1В».

Таблица 1 – Классы защищенности автоматизированных систем

Первая группа (многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, и не все пользователи имеют право доступа ко всей информации АС)	1А	В случае обработки секретной информации с грифом «особая важность»
	1Б	В случае обработки секретной информации с грифом не выше «совершенно секретно»
	1В	В случае обработки секретной информации с грифом не выше «секретно»
	1Г	АС, в которых циркулирует служебная информация
	1Д	АС, в которых циркулируют персональные данные
Вторая группа (АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности)	2А	Информация, составляющая гостайну
	2Б	Служебная тайна или персональные данные
Третья группа (многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, и не все пользователи имеют право доступа ко всей информации АС)	3А	Информация, составляющая гостайну
	3Б	Служебная тайна или персональные данные

информации АС)		
----------------	--	--

По постановлению Правительства РФ от 4 сентября 1995 г. N 870 "Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности" к секретным сведениям следует относить все сведения, отличные от сведений:

1. Особой важности: сведений в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации.
2. Совершенно секретных: сведений в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб интересам государственного органа или отрасли экономики Российской Федерации в одной или нескольких из указанных областей.

Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности.

Класс защищенности у фирмы ООО «Мрежа1» 1В, так как предприятие является многопользовательской АС и хранится информация разных уровней конфиденциальности, и не все пользователи имеют право доступа ко всей информации АС и в ней обрабатывается секретная информация.

Информационные потоки для ООО «Мрежа1» показаны на рисунке 3. Красные стрелки соответствуют внутренним информационным потокам, а зеленые – внешним

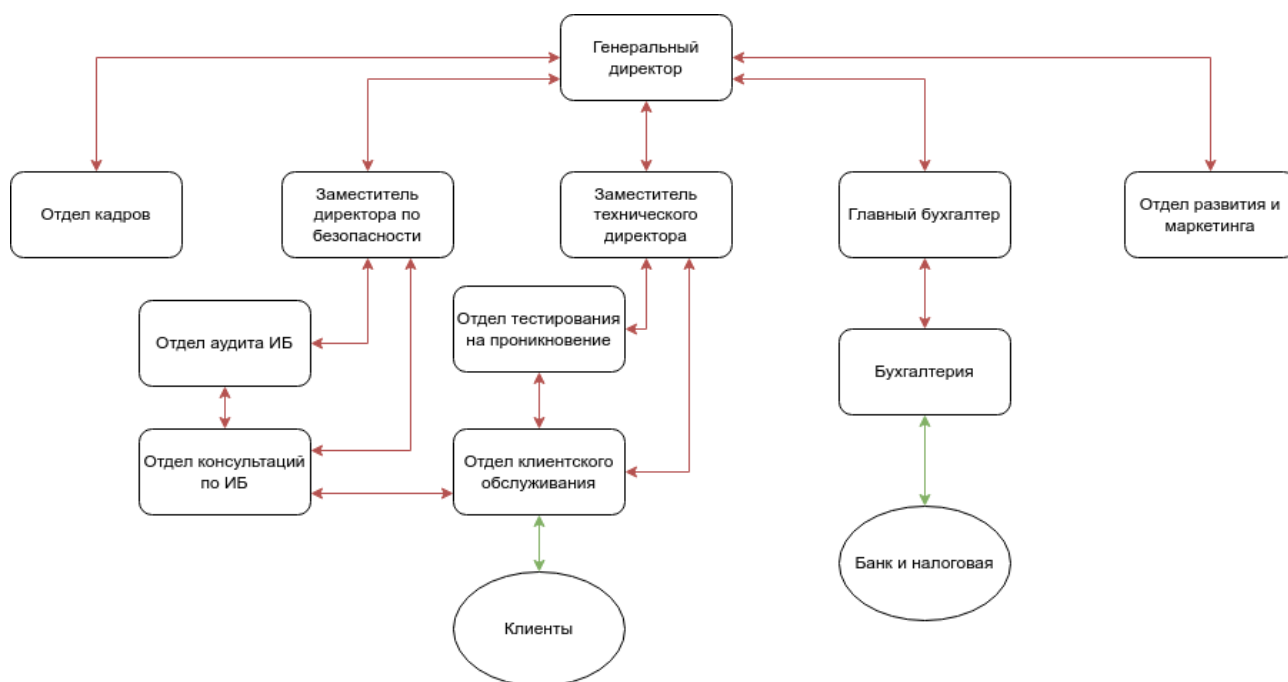


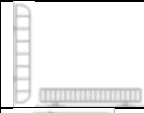

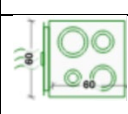

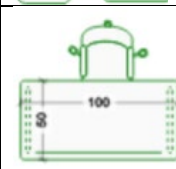

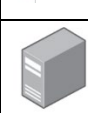
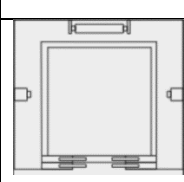
Рисунок 3 – Информационные потоки ООО «Мрежа1»

4.2 Описание помещения

На рисунке 3 представлен план защищаемого помещения с учетом мебелировки. В таблице 2 приведены помещения и их краткое описание, а в таблице 3 описание элементы, изображенных на плане помещения. Офис находится в здании на 4-ем этаже из 6-х. Здание имеет железобетонные стены 10-15 см. В близости нет околных зданий. На здании нет балконов или других фасадных элементов.

Таблица 2 – Помещения

№	Размер в м ²	Описание
1	14.77	Кабинет директора
2	14.53	Туалет
3	3.15	Лифт
4	10.75	Серверное помещение
5	33.95	Офис
6	18.39	Переговорная
7	32.38	Офис
8	26.86	Кухня/Комната отдыха
9	27.1	Коридор

	Батарея
	Холодильник
	Духовка
	Раковина
	Рабочее бюро со стулом
	Магнитно-маркерная доска
	Сервер
	Лифт

5 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ И ВЫБОР СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

В помещениях есть декоративные элементы, в которых можно спрятать закладное устройство. В каждом помещении присутствуют розетки, сетевое оборудование, поэтому актуальны электрический и электромагнитный каналы утечки информации. Также есть угроза снятия информации по вибрационному и оптическому каналам. В таблице 4 приведено описание активных и пассивных защит информации.

Таблица 4 – Активная и пассивная защита информации

Канал утечки	Источники	Пассивная защита	Активная защита
Акустический, акустоэлектрический	Окна, двери, электрические сети, проводка и розетки	Звукоизоляция переговорной, фильтры для сетей электропитания	Звуко-подавление, защищенные акустические системы
Вибрационный, виброакустический	Батареи и все твердые поверхности помещений	Максимальное снижение уровня перехватываемого сигнала	Устройства вибрационного зашумления
Электромагнитный, электрический	Розетки, АРМы, бытовая техника	Экранирование, заземление, фильтрация, развязка	Устройства электромагнитного зашумления
Визуально-оптический	Окна, двери	Снизить освещенность защищаемого объекта и его отражательные свойства	Средства сокрытия защищаемых объектов

6 АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Согласно заданию на курсовую работу, создаваемая система защиты информации предназначена для информации, составляющей государственную тайну уровня «секретно». Согласно требованиям «Типовых норм и правил проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними», утвержденных Решением Межведомственной комиссии по защите государственной тайны от 21.01.2011 N 199, защита рассматриваемых помещений должна удовлетворять следующим критериям:

3. В помещениях для работы с государственной тайной и хранилищах секретных документов устанавливаются усиленные двери, обеспечивающие надежное закрытие. Двери с двух сторон обшиваются металлическим листом не менее 2 мм толщиной, внутри — звукоизоляционный материал, сама дверь должна иметь толщину не менее 4 см. Дверь устанавливается на металлический каркас.
4. Обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании.
5. По требованиям безопасности режимных помещений, если окна комнат и хранилищ находятся рядом с водостоком, эвакуационной лестницей, крышами стоящих вблизи зданий, на первом или последнем этаже, каждое окно оборудуется выдвижными ставнями или створками с металлической решеткой, которая крепится к железным конструкциям оконного проема в стене.
6. Все режимные помещения оборудуются аварийным освещением.
7. Оборудование помещений для работы с государственной тайной по требованиям технической безопасности, вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемым к оснащению защищенных и выделенных помещений.
8. Перед началом эксплуатации необходимо проверить выделенные и иные режимные помещения проверить на предмет наличия «жучков» и иных средств несанкционированного получения информации. В дальнейшем такие проверки желательно проводить периодически, чтобы исключить возможность утечки.

6.1 Устройства для перекрытия акустического и виброакустического канала утечки информации

Таблица 5 – Сравнительный анализ средств активной защиты по виброакустическому каналу

Устройство	Сертификат ФСТЭК	Диапазон частот (Гц)	Характеристики	Цена (руб.)
Система защиты речевой информации "Соната-АВ" модель "4Б"	Да	175 - 11200	<p>Имеет ряд преимуществ перед "классическим" подходом - "центральный генератор + электроакустические преобразователи":</p> <p>Есть возможность подключения к одному питающему шлейфу. Это делает легче процесс проектирования и монтажа</p> <p>Индивидуальная регулировка интегрального уровня и корректировка спектра каждого генератора улучшает действие системы</p> <p>Улучшенная аппаратная настройка элементов модели 4Б позволяет связывать источник электропитания с другими для обмена информацией. Это дает возможность:</p> <p>Создать систему автоматического контроля всех элементов</p> <p>Снизить время на конфигурирование и тестирование системы</p> <p>Изменить настройки генераторов и построить гибкую систему виброакустической защиты</p> <p>Уменьшить затраты благодаря использованию единой линии связи и электропитания</p>	44 200
Генератор шума ЛГШ-402	Да	175 - 11200	<p>Соответствует типу «А» - средства акустической и вибрационной защиты информации с центральным генераторным блоком и подключаемыми к нему по линиям связи пассивными (не содержащими в своей конструкции индивидуальные задающие источники шума требующие электропитания) преобразователями.</p> <p>Оснащено визуальной системой индикации</p>	18 200

			<p>нормального режима работы</p> <p>Общее количество вибропреобразователей, подключаемых к генератору - 8 шт</p>	
Камертон-5	Да	100-11200	<p>Является техническим средством активной защиты типа "А":</p> <p>1 класса защиты (для выделенных помещений до 1 категории включительно, не оборудованных системами звукоусиления);</p> <p>2 класса защиты (для выделенных помещений до 2 категории включительно, оборудованных системами звукоусиления)</p> <p>предназначено для обеспечения защиты акустической речевой информации от утечки по акустическому и вибрационному каналам, за счет акустоэлектрических преобразований во вспомогательных технических средствах и системах, блокирует применение направленных и лазерных микрофонов</p>	46 000
Система акустической и виброакустической защиты речевой информации SEL SP-157 "Шагренъ"	Да	90 - 11200	<p>Система акустической и виброакустической защиты речевой информации (генератор виброакустического шума) SEL SP-157 предназначена для защиты речевой информации в помещениях от её утечки по техническим каналам: акустическому, вибрационному и лазерному путём создания маскирующих акустических помех в смежных воздушных пространствах и маскирующих вибрационных помех в ограждающих конструкциях и инженерно-технических коммуникациях.</p> <p>Особенности системы:</p> <p>Жидкокристаллический двухстрочный экран.</p> <p>Защита паролем настроек системы.</p> <p>Отсчёт времени наработки генерации</p>	47 400

			шума по каждому каналу с выводом на экран. Непрерывный контроль состояния системы и каждого отдельного излучателя. Возможность регулировки уровня шума каждого излучателя. Возможность дистанционного управления (проводного и по ИК-каналу)	
--	--	--	---	--

По результатам анализа была выбрана система Соната «АВ» модель 4Б, так как:

- Есть возможность подключения к одному питающему шлейфу. Это делает легче процесс проектирования и монтажа;
- Индивидуальная регулировка интегрального уровня и корректировка спектра каждого генератора улучшает действие системы;
- Дает возможность создать систему автоматического контроля всех элементов
- Имеет среднюю цену из представленных средств активной защиты, а также позволяет уменьшить затраты благодаря использованию единой линии связи и электропитания.

6.2 Устройства для перекрытия электрического, акустического и электромагнитного каналов утечки информации

В таблице 6 приведен сравнительный анализ средств активной защиты помещений по электрическому каналу.

Таблица 6 – Сравнительный анализ средств активной защиты по электрическому каналу

Устройство	Характеристики	Цена (руб.)
Генератор шума SEL SP-44	Наличие сертификата ФСТЭК, разрешающего использование устройства в выделенных помещениях 3-1 категорий 2-канальный цифровой генератор шумовых сигналов в диапазоне 10кГц-400МГц Активная защита конфиденциальных сведений от утечки по проводам электропитания 2 независимых друг от друга формирователей шума Возможность регулировки уровня ВЧ и НЧ шумов Световая и текстовая индикация работы	26 000

	Звуковой сигнал при переходе в аварийный режим Функция самодиагностики для оперативного выявления неисправностей и сбоев в работе	
Генератор шума ЛГШ-221	Сертификат ФСТЭК - «продлен до 2024 года» Сетевой генератор шума – средство защиты информации от утечки через электропроводку; Принцип работы – генерация электромагнитных помех; Устройство оснащено счетчиком отработанных часов; Устройство оснащено световым и звуковым индикаторами работы; Ресурс работы генератора шума – минимум 27000 часов; Возможность управления устройством с помощью пульта ДУ;	36 400
Генератор шума СОНАТА-РС3	Устройство для активной защиты информации от утечки по сети электропитания Предназначено для подключения к 3-проводной сети (энергосеть с проводом заземления); Звуковая и световая индикация работы; Возможно дистанционное управление посредством проводного пульта; Работа от сети 220В и 50Гц; Потребляемая мощность – 10Вт; Сертифицировано ФСТЭК.	32 400
Генератор шума СОНАТА-РС2	Предназначен для активной защиты объектов ВТ (объектов вычислительной техники) или, другими словами, переговорных помещений от утечки информации через линии электропитания и заземления. Отличается от прибора Соната РС-1 только наличием модуля ИК-управления, что позволяет дистанционное включение прибора с пульта управления. Тогда как Соната РС-1 включается только в розетку Данный прибор больше не поставляется и заменен новой версией	23 600

После проведенного анализа был выбран генератор шума Соната-РС3. Конструктивные особенности этого устройства делают его эффективным и недорогим решением при больших количествах компьютерных комплексов. Эта модель также оказалась самым популярным устройством для активной защиты информации от утечки по сети электропитания, совместимым с моделью Соната «АВ» модель 4Б, и была выбрана в качестве генератор шума.

К активной защите следует установить фильтры для сетей электропитания во всех помещениях

6.3 Защита от ПЭМИН

ПЭМИН - побочные электромагнитные излучения и наводки. Вариант защиты компьютерной информации методом радиомаскировки. В таблице 7 представлено сравнение устройств генератора шума.

Таблица 7 – Сравнительный анализ средств активной защиты от ПЭМИН

Устройство	Характеристики	Диапазон частот	Цена (руб.)
СОНАТА-РЗ	<p>Соната-РЗ Может применяться в выделенных помещениях до 1 категории включительно</p> <p>Средство активной защиты информации</p> <p>Изделие обеспечивает защиту от утечки за счет побочных электромагнитных излучений и наводок путем излучения в окружающее пространство электромагнитного поля шума, а также наводок на линии сети электропитания и заземления путем индуцирования в них маскирующих шумовых напряжений</p> <p>Сертификат ФСТЭК</p> <p>Изделие представляет собой систему из трёх устройств "Соната-РЗ.1", расположенных во взаимно перпендикулярных плоскостях и работающих в одинаковом диапазоне частот</p> <p>Правильно установленное и отрегулированное Изделие позволяет блокировать каналы утечки информации за счет ПЭМИН</p> <p>Устройство "Соната-РЗ.1" конструктивно выполнено в виде моноблока с сетевым шнуром</p>	0,01 - 200 МГц	97 200
Генератор шума ЛГШ-503	<p>Генератор белого шума ЛГШ-503 соответствует требованиям документа «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, 2014) – по 2 классу защиты.</p> <p>Оснащен визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа).</p>	10 кГц - 1800 МГц	44 200

	<p>Оснащен счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы в режиме формирования маскирующих помех.</p> <p>Конструкция генератора обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним.</p> <p>Прибор имеет возможность подключения проводного дистанционного управления и контроля, в качестве которого может использоваться программно-аппаратный комплекс «Паутина».</p>		
<p>Генератор шума</p> <p>ГАММА</p> <p>ГШ-18</p>	<p>Является средством активной защиты информации типа «А» и типа «Б» 2 класса защиты</p> <p>Предназначен для маскировки ПЭМИН персональных компьютеров, рабочих станций компьютерных сетей и комплексов на объектах вычислительной техники второй, третьей и четвертой категорий, путем формирования и излучения в окружающее пространство электромагнитного поля шума (ЭМПШ) и наведения шумового сигнала на токопроводящие линии и инженерно-технические коммуникации, включая цепи электропитания и заземления, в широком диапазоне частот</p> <p>В генераторе установлен счетчик наработки времени с дисплеем (количество часов работы учитывается и прописывается в формуляре изделия);</p> <p>В генераторе предусмотрена плавная регулировка уровня выходного сигнала (осуществляется встроенным аттенуатором в пределах не менее 20 дБ)</p>	<p>0,009 - 6000 МГц</p>	<p>29 400</p>
<p>Генератор шума</p> <p>ПУЛЬСАР</p>	<p>Имеет диапазоны частот от 10 кГц до 6 ГГц</p> <p>2 съемные антенны, счетчик наработки</p> <p>Индикаторы нормального режима работы (диод) и аварийного режима (свет и звук)</p> <p>Имеет защиту регулятора уровня выходного шумового сигнала от нелегального доступа (и сигнализирует об этом)</p> <p>Соответствует требованиям документа «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК</p>	<p>10 кГц - 6 ГГц</p>	<p>24 525</p>

	России) – по 2 классу защиты Можно применять в выделенных помещениях до 2 категории включительно		
--	---	--	--

После проведенного анализа был выбран генератор шума Соната-РЗ из-за совместимости с уже выбранных решений и высокой оценки потребителей.

6.4 Защита от утечек по оптическому каналу

Для защиты информации от утечки по оптическому каналу рекомендуется:

- располагать объекты защиты так, чтобы исключить отражение света в стороны возможного расположения злоумышленника (пространственные ограждения);
- уменьшить отражательные свойства объекта защиты;
- уменьшить освещенность объекта защиты (энергетические ограничения);
- использовать средства преграждения или значительного ослабления отраженного света: ширмы, экраны, шторы, ставни, темные стекла и другие преграждающие среды, преграды;
- применять средства маскирования, имитации и другие с целью защиты и введения в заблуждение злоумышленника;
- использовать средства пассивной и активной защиты источника от неконтролируемого распространения отражательного или излученного света и других излучений;

Наиболее приемлемый вариант защиты — применение жалю-зи на окнах (Таблица 8).

Таблица 8 – Сравнительный анализ средств активной защиты от утечек по оптическому каналу

Меры	Преимущества	Недостатки
Шторы	исключают возможность наблюдения за объектами защиты в кабинете	ухудшают естественную освещенность кабинета накапливают пыль
Жалюзи	исключают возможность наблюдения через окно	
Тонированные пленки	исключают возможность наблюдения за объектами защиты в кабинете	незначительно уменьшают освещенность кабинета позволяют легко выявить окна

		помещений с повышенными требованиями к безопасности информации
--	--	--



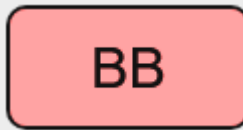

7 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ




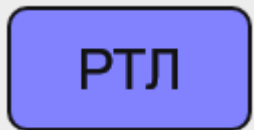


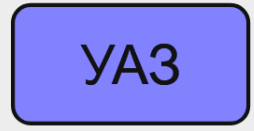

Согласно информации, приведённой в предыдущих пунктах, выбранные средства защиты информации включают в себя:

- усиленные двери (4 мм+), обшитые металлом (2 мм+) со звукоизолирующей прокладкой на металлическом каркасе – 3 шт., в переговорную, в серверном и кабинет директора;
- генератор шума СОНАТА-РС3;
- устройство активной защиты от ПЭМИН СОНАТА-Р3;
- 8 комплектов жалюзи на 8 окон;
- доводчики 430 ISPARUS на 8 дверей.

Перейдём к оценке количества компонентов и расстановке выбранных технических средств. Согласно руководству по эксплуатации [4] «Система виброакустической и акустической защиты "Соната-АВ". Руководство по эксплуатации» для предварительной оценки необходимого количества излучателей необходимо исходить из следующих норм (таблица 9).

Таблица 9 – Описание расстановок технических средств на помещении и их означении

Средство защиты	Установка	Условное обозначение	Количество
Блок электропитания и управления «Соната-ИП4.3»	У стен;		1
«Соната-СА-4Б1» генератор-акустоизлучатель	Один на каждый вентиляционный канал или дверной тамбур; один на каждые 8...12 м ³ надпотолочного пространства или др. пустот;		19
«Соната-СВ-4Б» генератор-вибровозбудитель (двери, окна, батареи)	Один на окно (при установке на оконный переплет);		26
«Соната-СВ-4Б» генератор-вибровозбудитель (пол,	Один на каждые 15...25 м ² перекрытия;		24

потолок)			
«Соната-СВ-4Б» генератор- вибровозбудитель (стены)	Один на каждые 3...5 метров периметра для капитальной стены при условии установки излучателей на уровне половины высоты помещения;		31
«Соната-СВ-4Б» генератор- вибровозбудитель (трубопровод)	Один на каждую вертикаль (отдельную трубу) вида коммуникаций.		9
Дверь звукоизолирующая	На двери;		5
Размыкатель телефонной линии	Около каждого телефона;		3
Размыкатель слаботочной линии	подключена к системе электропитания согласно рекомендациям производителя;		1
Размыкатель линии Интернета	в розетку, подключение к 3- проводной сети (энергосеть с проводом заземления)		1
Устройство активной защиты от ПЭМИН СОНАТА-РЗ	«Соната-РЗ» подключена непосредственно к «Соната-ИП4.3»		1
Генератор шума СОНАТА-РСЗ	подключается к системе электропитания в соответствии с рекомендациями производителя		1

Каждое окно оснащено жалюзи, а каждая дверь - доводчиком. Расположение компонентов комбинированной системы Соната «АБ» 4Б показано на рис. 5. «Соната-РЗ» подключена непосредственно к «Соната-ИП4.3». «Соната-РСЗ» подключается к системе электропитания в соответствии с рекомендациями производителя.

Основное правило, которого следует придерживаться при выборе мест установки излучателей в каждом конкретном помещении, — это обеспечение максимального уровня

вибрации и акустического шума на предполагаемых путях утечки информации и в то же время обеспечение допустимого уровня мешающего акустического шума в защищаемом помещении. Контроль уровня вибрации и акустического шума в помещениях рекомендуется осуществлять в соответствии с методиками и рекомендациями ФСТЭК (Гостехкомиссии) РФ.

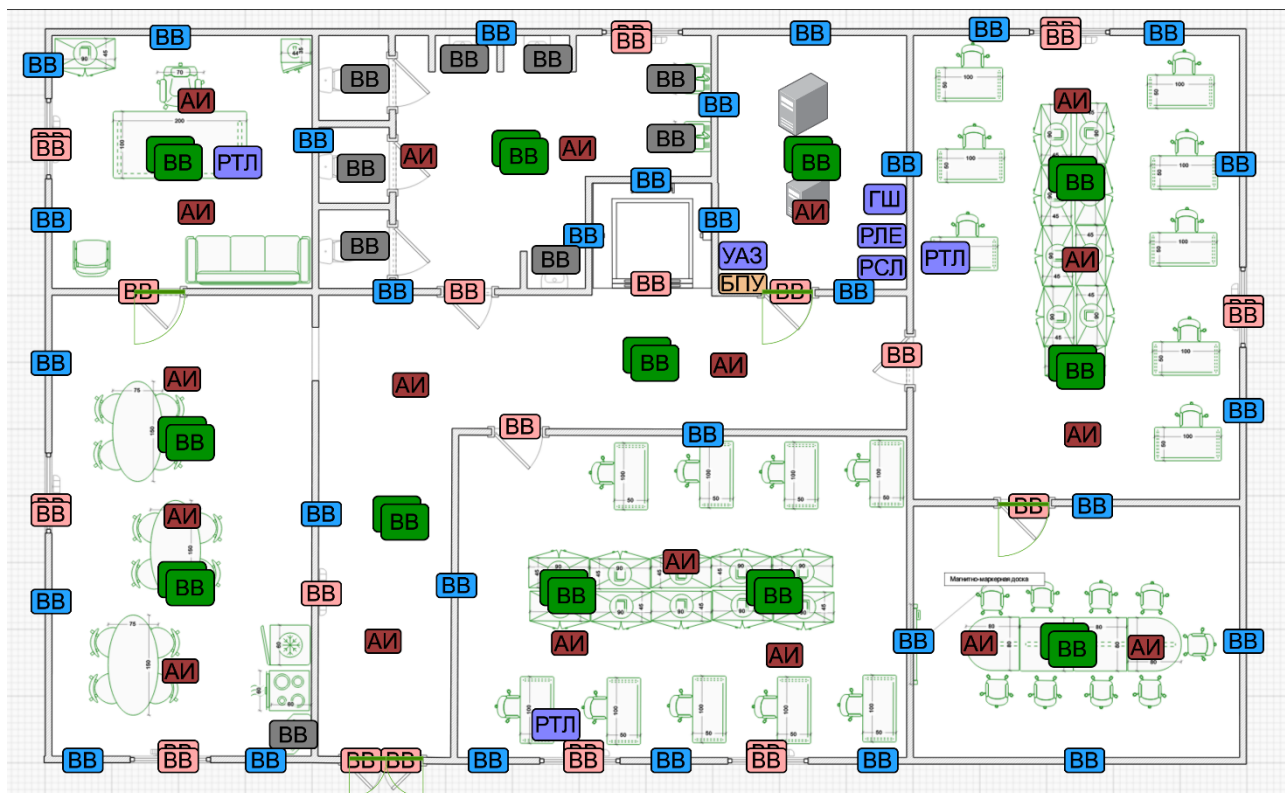


Рисунок 5 – План помещения после расстановки защитных средств

В таблице 10 приведена смета затрат на выбранные средства защиты информации.

Таблица 10 – Смета на выбранные средства защиты информации

Средство защиты	Цена (руб.)	Количество	Стоимость (руб.)
«Соната-СА-4Б1» генератор-акустоизлучатель	3 540	19	67 260
«Соната-СВ-4Б» генератор-вибровозбудитель	7 440	90	669 600
Соната «АВ» модель 4Б	44 200	1	44 200
Рычажная тяга Tantos TS-DC - рычаг	1120	8	8 960
«Соната-РС3»	32 400	1	32 400
«Соната-Р3»	97 200	1	97 200
Жалюзи	1 980	8	15 840
Дверь звукоизолирующая	78 400	5	392 000
Доводчик 430 ISPARUS	1680	8	13 440
Итого:			1 340 900

ЗАКЛЮЧЕНИЕ

В результате этой работы был проведен теоретический анализ технических каналов утечки информации. Кроме того, были определены руководящие документы, проанализированы объекты защиты, оценены пути утечки информации, выбраны пассивные и активные меры защиты информации.

По окончании работ была составлена смета на основе текущих цен на технические средства защиты информации, и итоговая стоимость составила 1 340 900 рублей и был разработан план установки мер защиты.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждено 30.08.2002 приказом Председателя Гостехкомиссии России No 282.
2. ГОСТ Р 50.1.056–2005 «Техническая защита информации. Основные термины и определения».
3. Руководящий документ Государственной технической комиссии при Президенте РФ «Классификация автоматизированных систем и требований по защите информации» от 30 марта 1992 г.
4. «Система виброакустической и акустической защиты "Соната-АВ". Руководство по эксплуатации» - Москва.
5. Решение Межведомственной комиссии по защите государственной тайны от 21 января 2011 г. N 199 "О Типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними".
6. Detector System. Средства защиты переговоров [HTML] (https://detsys.ru/catalog/sredstva_zashchity_peregovorov/) (Дата обращения: 17.12.2023).
7. Кармановский Н.С., Михайличенко О.В., Савков С.В. Организационно-правовое и методическое обеспечение информационной безопасности / Учебное пособие. – СПб: НИУ ИТМО, 2013. – 148 с
8. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.