

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

Факультет безопасности информационных технологий

КУРСОВАЯ РАБОТА

По дисциплине:

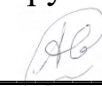
«Инженерно-технические средства защиты информации»

На тему:

«Проектирование инженерно-технической системы защиты информации на
предприятии. Вариант 132»

Выполнил:

Аверин Н. О., студент группы N34521


(подпись)

Проверил:

Попов Илья Юрьевич, к.т.н., доцент 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	Аверин Никита Олегович
	(Фамилия И.О.)
Факультет	Безопасности Информационных Технологий
Группа	N34521
Направление (специальность)	Эксплуатация транспортно-технологических машин и комплексов
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 инженерно-технической системы защиты информации на предприятии. Вариант 132
Задание	Проанализировать всевозможные каналы утечки данных в помещении, провести анализ рынка технических средств защиты информации разных категорий, разработать схему расстановки выбранных технических средств в защищаемом помещении

Краткие методические указания

Рекомендуемая литература

Руководитель	Попов Илья Юрьевич
	(Подпись, дата)
Студент	
	(Подпись, дата)

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»
ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

Студент Аверин Никита Олегович

(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34521

Направление (специальность) Эксплуатация транспортно-технологических машин и комплексов

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 инженерно-технической системы защиты информации на предприятии. Вариант 132

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Разработка и утверждение задания и календарного плана на курсовую работу	08.11.2022	08.11.2022	
2	Анализ литературы	08.11.2022	08.11.2022	
3	Разработка комплекса инженерно-технической защиты информации в заданном помещении	13.11.2022	13.11.2022	
5	Презентация КР перед аудиторией	19.12.2022	19.12.2022	

Руководитель Попов Илья Юрьевич

(Подпись, дата)

Студент

(Подпись, дата)

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»
АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ**

Студент	Аверин Никита Олегович
	(Фамилия И.О.)
Факультет	Безопасности Информационных Технологий
Группа	N34521
Направление (специальность)	Эксплуатация транспортно-технологических машин и комплексов
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 инженерно-технической системы защиты информации на предприятии. Вариант 132

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

1. Цель и задачи работы

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

Цель данной работы – повышение защищенности рассматриваемого помещения. Задачами является анализ Защищаемого помещения, оценка каналов утечки информации и выбор мер пассивной и активной защиты информации.

2. Характер работы

- ☐ Расчет ☐ Конструирование
☒ Моделирование ☐ Другое

3. Содержание работы

В результате работы был произведен комплексный анализ возможных технических каналов утечки информации в предложенных помещениях, предложены меры пассивной и активной защиты информации.

4. Выводы

В результате работы был произведен комплексный анализ возможных технических каналов утечки информации в предложенных помещениях, предложены меры пассивной и активной защиты информации

Руководитель	Попов Илья Юрьевич
	(Подпись, дата)
Студент	
	(Подпись, дата)

«___» _____ 20__ г

СОДЕРЖАНИЕ

Введение.....	2
1 Анализ технических каналов утечки информации.....	3
2 Организационная структура предприятия.....	9
3 Руководящие документы.....	11
4 Анализ защищаемых помещений.....	14
4.1 Описание помещений.....	16
4.2 Анализ потенциальных каналов утечек информации.....	18
4.3 Выбор средств защиты информации.....	19
5 Анализ рынка предлагаемых решений.....	21
5.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации.....	22
5.2 Устройства для перекрытия электрического акустоэлектрического и электромагнитного каналов утечки информации.....	24
5.3 Защита от ПЭМИН.....	26
5.4 Устройства для перекрытия визуально-оптического канала утечки информации.....	27
6 Описание расстановки технических мер защиты информации.....	28
Выводы.....	32
Использованная литература.....	33

ВВЕДЕНИЕ

В настоящее время большую роль в планировании играет информация и в подобных условиях следствием конкуренции любого вида является кража ценной информации. Поэтому стал актуальным вопрос защиты информации от несанкционированного доступа, распространения, изменения или уничтожения. В этом контексте обеспечение делится на несколько видов, которые отвечают за определённые угрозы информационной безопасности. Фундаментальную роль в обеспечении информационной безопасности и предотвращении реализации угроз играет инженерно-техническая система защиты информации.

В работе рассмотрен процесс разработки комплекса инженерно-технических мер по защите информационной безопасности на объекте работающим с государственной тайной категории «совершенно секретно». Предприятие расположено на объекте, имеющем 8 помещений, в которые входят кабинет директора, кабинет секретаря, кабинет IT отдела, кабинет бухгалтерии, офис, приёмная, коридор и санузел.

Цель работы – разработать инженерно-техническую систему защиты информации на предприятии, обеспечивающую надежную защиту данных и минимизацию рисков утечки, повреждения или несанкционированного доступа к информации.

Для достижения поставленной цели необходимо решить следующие задачи:

- Анализ технических каналов утечки информации;
- Поиск руководящих документов;
- Провести анализ защищаемых помещений;
- Выбрать инженерно-технические средства защиты информации в соответствии с существующим рынком предлагаемых решений;
- Спроектировать систему защиты информации на основе выбранных средств.

1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Утечка — это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена. Утечка информации может осуществляться по различным каналам. Каналом утечки информации называют канал коммуникации, позволяющий процессу передавать информацию путем, нарушающим безопасность системы.

Существует три формы утечки информации:

- разглашение информации;
- несанкционированный доступ к информации;
- утечка информации по техническим каналам.

Согласно теме данной работы, рассматриваться будет только утечка информации по техническим каналам.

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

Утечка - бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

Утечка (информации) по техническому каналу - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.



Рисунок 1 – Структура технического канала утечки информации

На рисунке 1 представлена схема структуры технического канала утечки информации. На вход ТКУИ поступает информация в виде первичного сигнала, представляющего собой носитель с информацией от ее 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.

Далее полученная информация преобразуется в форму, обеспечивающую запись ее на носитель информации, соответствующий среде распространения. Среда распространения сигнала - физическая среда, по которой информативный сигнал может распространяться и регистрироваться приемником. Она характеризуется набором физических параметров, определяющих условия перемещения сигнала. Приемник после этого снимает информацию с носителя, обрабатывает полученный сигнал (усиление) и преобразует информацию в форму сигнала, доступную получателю (человеку или техническому устройству).

По физической природе носителя и виду канала связи ТКУИ делятся на:

- оптические;
- радиоэлектронные;
- электрические;
- электромагнитные;
- индукционные;
- акустические;

- акустоэлектрические;
- виброакустические;
- материально-вещественные.

Носителем информации в оптическом канале является электромагнитное поле (фотоны). Снятие информации возможно с помощью наблюдения, например, через подсматривание в окно или приоткрытую дверь. Альтернативой является использование закладного устройства с возможностью фото или видеозаписи. Данный канал утечки актуален для графической формы представления информации, защита осуществляется методом установки жалюзи или другой формой непрозрачного покрытия на все просматриваемые снаружи поверхности (окна, стеклянные двери и т. д.), а также использованием доводчиков для дверей.

В радиоэлектронном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток (поток электронов), распространяющийся по металлическим проводам. Диапазон частот радиоэлектронного канала занимает полосу частот от десятков ГГц до звукового.

Электромагнитный ТКУИ связан с перехватом электромагнитных излучений на частотах работы передатчиков систем и средств связи. Используется для перехвата информации, передаваемой по каналам радио-, радиорелейной, спутниковой связи. Напряженность электрического поля в точке приема (перехвата) будет прямо пропорциональна величине мощности передатчика, высоте приёмной и передающей антенн и обратно пропорциональна расстоянию. Данный канал утечки актуален при наличии в помещении электронной вычислительной техники, компьютеров или других средств обработки информации. Создаваемое при работе технических устройств электромагнитное излучение называют побочным электромагнитным излучением и наводками (ПЭМИН); защита осуществляется посредством специальных технических устройств,

создающих электромагнитный шум, скрывающий это электромагнитное излучение.

Электрический ТКУИ связан со съемом информации путем контактного подключения аппаратуры злоумышленника к кабельным линиям связи. Электрические колебания, появляющиеся при работе электрических приборов, содержат информацию о подключенных устройствах. Защита осуществляется посредством специальных фильтров для сетей электропитания, которые скрывают электрические колебания, вызываемые вычислительной техникой.

Индукционный ТКУИ связан с бесконтактным съемом информации с кабельных линий связи. Возможность такого съема информации возникает за счет эффекта возникновения вокруг кабеля связи электромагнитного поля, модулированного информационным сигналом. Это поле перехватывается специальным индукционным датчиком, далее усиливается и демодулируется на аппаратуре злоумышленника. Следует отметить, что бесконтактные закладные устройства обнаружить труднее всего, так как они не изменяют характеристик канала связи. Защита осуществляется посредством использования специальных программных и аппаратных средств, позволяющих выявить закладки.

Носителями информации в акустическом канале являются упругие акустические волны, распространяющиеся в среде. Снятие информации возможно либо с помощью подслушивания из-за пределов помещения (при отсутствии звукоизоляции), либо с помощью закладных устройств с функциями аудиозаписи. Данный канал утечки актуален при передаче информации в звуковой форме (диалог, совещание, др.); защита осуществляется посредством использования звукоизолирующих материалов, мешающих звуку выйти за пределы помещения, а также использованием специальных программных и аппаратных средств, позволяющих выявить закладки.

В акустоэлектрическом канале информация представлена в виде акустических колебаний, которые далее воздействуют на сети электропитания, вызывая электрические колебания. При снятии этих колебаний есть возможность восстановить исходный акустический сигнал. Данный канал утечки информации актуален, когда в контролируемом помещении есть электрические сети, связанные с внешней территорией. Например, телефонная сеть – подав небольшое напряжение на входящую телефонную линию и сняв его на входе, мы сможем получить распространяющуюся в помещение звуковую информацию. Защита осуществляется посредством использования специальных фильтры для сетей электропитания, скрывающих колебания, вызванные воздействием на электрические сети.

В виброакустическом канале информация изначально представлена в виде акустических колебаний, которые воздействуют на некоторую твердую поверхность, превращаясь в вибрационные колебания. Данный канал утечки информации актуален практически всегда, так как связан с наличием твёрдых поверхностей в контролируемом помещении, в т. ч. стен, потолка и пола, батарей отопления, оконных стёкол. Защита осуществляется путем использования специальных технических устройства, которые передают на защищаемую твердую поверхность белый шум, который скрывает вибрационные колебания, вызванные акустическими волнами.

В материально-вещественном канале утечка информации производится путем несанкционированного распространения за пределы контролируемой зоны вещественных носителей с защищаемой информацией. В качестве вещественных носителей чаще всего выступают черновики документов и использованная копировальная бумага, портативные носители информации (HHD, SSD, проч. карты памяти). С кражей или копированием информации, зафиксированной на материальных носителях, борются в первую очередь организационными мерами, вводя строгий порядок учета и работы с данными видами носителей.

Помимо вышеперечисленного, также выделяют оптико-электронные ТКУИ, связанные с перехватом акустических сигналов путём лазерного зондирования оконных стекол.

Отдельной угрозой является возможность проникновения злоумышленника на территорию охраняемого помещения, так что не менее актуальным вопросом является рассмотрение контроля доступа на охраняемую территорию.

2 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

Наименование предприятия: Общество с ограниченной ответственностью “Ромашково” (далее - ООО "Ромашково", Предприятие).

Область деятельности: Производство и строительство железных дорог необщего пользования.

Структура Предприятия представлена на Рисунке 2.

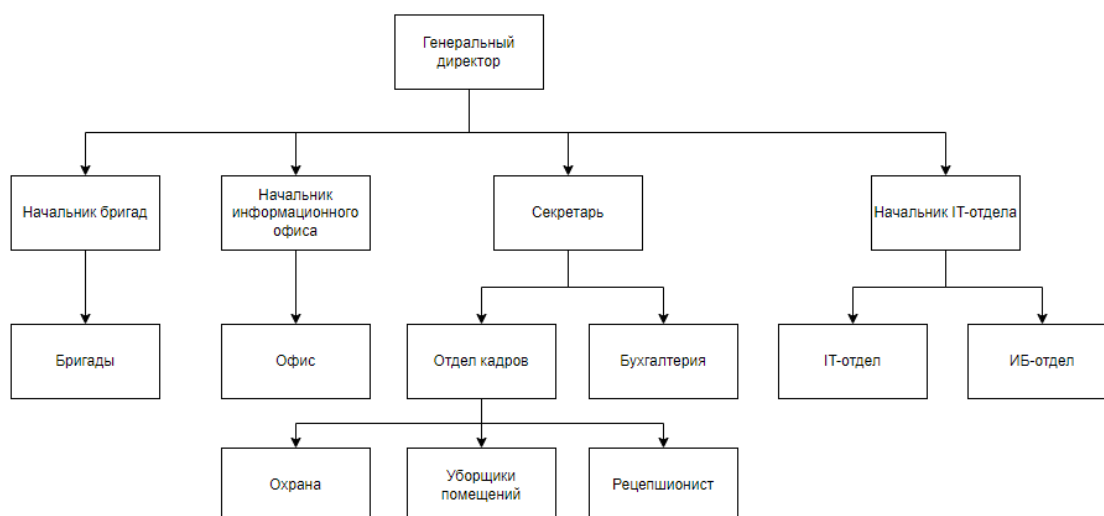


Рисунок 2 – Структура Предприятия

Основные информационные процессы и потоки в организации, включая описание информации ограниченного доступа:

В организации обрабатывается информация конфиденциального характера:

- персональные данные лиц, являющихся и не являющихся работниками Предприятия;
- сведения, отнесенные к коммерческой тайне организации, включающие в себя деловые секреты, финансово-экономическую, технологическую информацию, технологические секреты организации (ноу-хау), сведения, содержащиеся в служебной документации Предприятия, кроме официально публикуемых,

идеи и разработки, полученные сотрудниками в процессе трудовой деятельности;

- сведения, отнесённые к государственной тайне с уровнем «совершенно секретно», включающие в себя обсуждение, разработку и проектирование зданий и помещений для государственных нужд.

Внутренние и внешние информационные потоки внутри Предприятия представлены на Рисунке 3, который демонстрирует, как данные и информация циркулируют внутри компании и за её пределами.

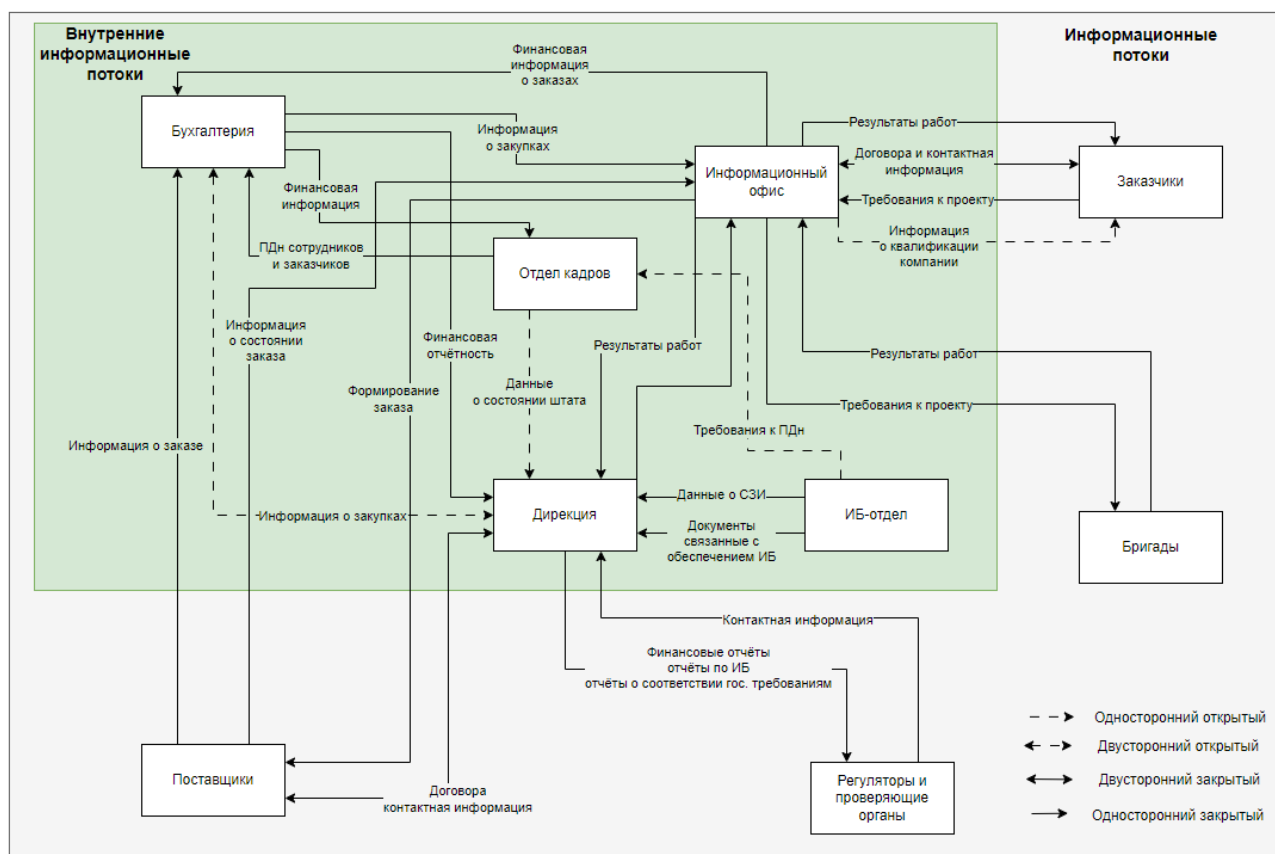


Рисунок 3 – Информационные потоки

3 РУКОВОДЯЩИЕ ДОКУМЕНТЫ

Основными документами в области защиты информации являются:

- Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера».
- Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
- Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации».
- Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне».
- Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) «О сертификации средств защиты информации».
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
- Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Закон РФ «О государственной тайне» от 21.07.1993 N 5485-1.
- МЕЖВЕДОМСТВЕННАЯ КОМИССИЯ ПО ЗАЩИТЕ ГОСУДАРСТВЕННОЙ ТАЙНЫ РЕШЕНИЕ № 199 от 21.01.2011г. "О Типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними".

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.

4 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

Перед тем как перейдем к проектированию технических средств защиты на объекте, сначала проведем анализ защищаемых помещений.

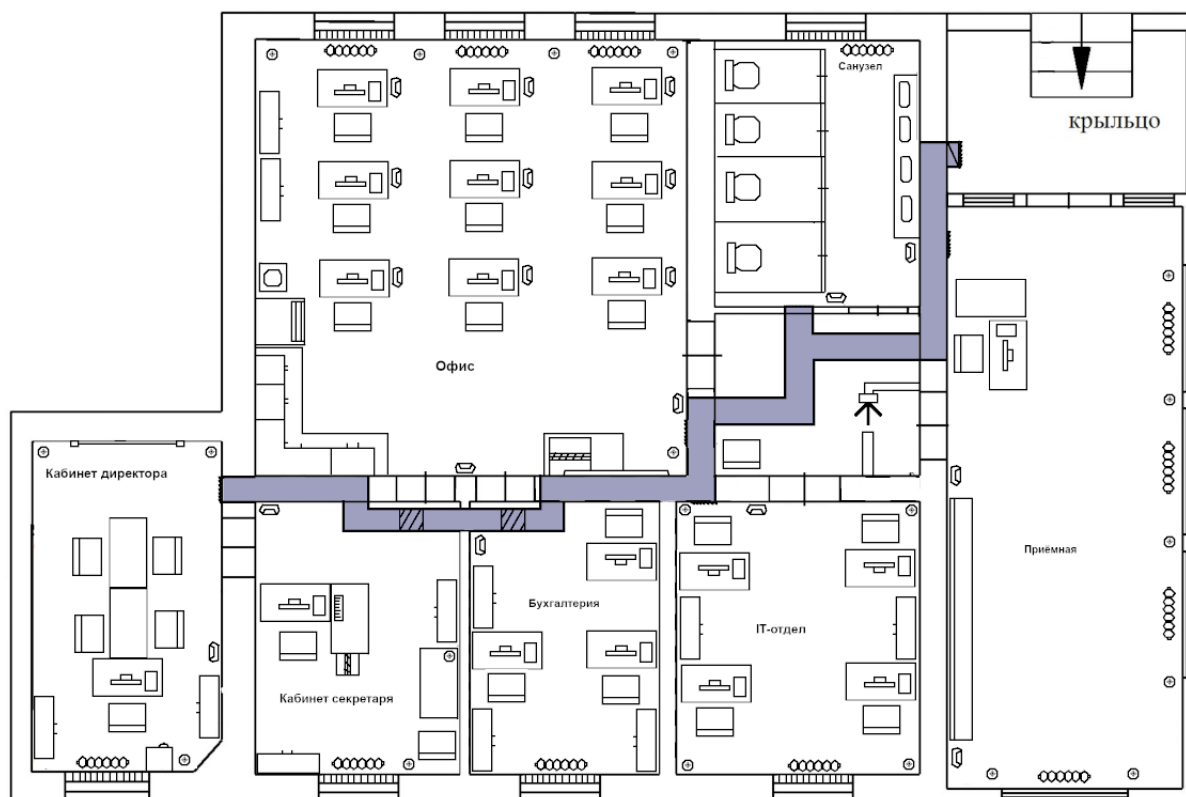
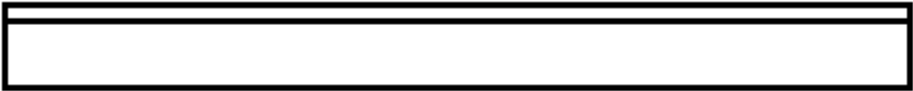

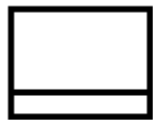
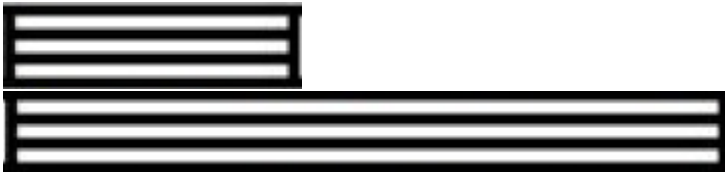


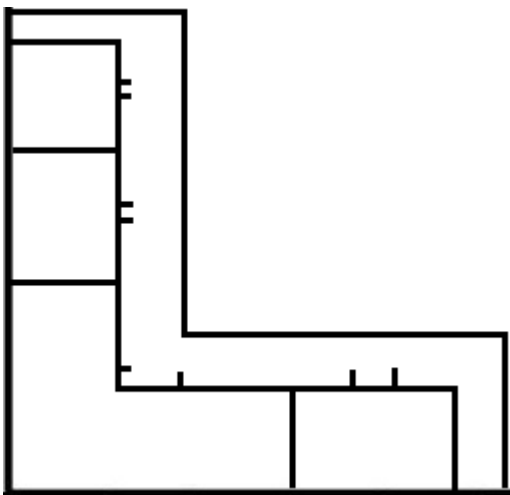











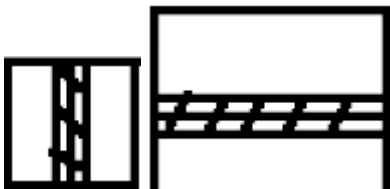





Рисунок 4 – План защищаемого помещения

Таблица 1 – Условные обозначения плана защищаемого помещения

Обозначения	Описание
	Скамья
	Стол
	Стул/кресло

	Окно
	Корзина для мусора
	Батарея центрального отопления
	<p>Кухня:</p> <ul style="list-style-type: none"> • шкафчики; • кофемашина; • чайник; • раковина; • микроволновая печь.
	Персональный компьютер
	Сейф
	Элементы санузла
	Кулер
	Шкаф
	Домашнее растение

	Стопка папок
	Вентиляционный элемент
	Вентиляционный выход
	Вендинговый автомат
	Жалюзи
	Принтер/сканер
	Проектор
	Информационная доска
	Вешалка напольная

4.1 Описание помещений

Защите подлежат следующие помещения:

- кабинет директора, 3.53 на 6.20 м (21,89 м²);
- кабинет секретаря, 3.81 на 5.12 м (19,51 м²);
- кабинет IT отдела, 4.54 на 5.12 м (23,25 м²);
- кабинет бухгалтерии, 3.53 на 5.12 м (18,07 м²);
- офис, 8.07 на 8.19 м (66,09 м²);
- приёмная, 4.44 на 10.92 м (48,49 м²);

- коридор, 3.83 на 3 м (11,49 м²);
- санузел, 3.83 на 5 м (19,15 м²);

Для ведения переговоров предназначено одно помещение (кабинет директора), там находятся три стола и пять стульев, информационная доска, проектор, персональный компьютер, ряд папок, два шкафа, сейф, три домашних растения, корзина для мусора, напольная вешалка и шесть розеток. Проход в помещение осуществляется через кабинет секретаря.

В офисе 9 рабочих мест с персональными компьютерами, 2 шкафа, кулер, принтер с функцией сканера со столом, кухня, включающая в себя шкафчики, кофемашину, чайник, раковину и микроволновая печь, информационная доска и 18 розеток.

Кухня и зона приема пищи разделены стеной, при этом проход на кухню осуществляется через столовую. В этих помещениях расположены столы, стулья, кухонные шкафы, бытовая техника и 6 розеток.

14 окон расположено в каждом из помещений кроме коридора. Под окнами расположены батареи центрального отопления. В помещениях также присутствуют столы, кресла, корзины для мусора, домашние растения. В кабинетах расположены шкафы, напольные вешалки, персональные компьютеры и розетки под них.

Помещения располагаются на первом этаже, окна выходят во двор.

Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см. Толщины стен:

- наружной стены 400 мм;
- внутренней несущей стены 380 мм;
- межкомнатных перегородок 100 мм;

Материал стен:

- наружной стены газосиликатные блоки (300х400х500);
- внутренней несущей стены кирпич силикатный полнотелый;

- межкомнатных перегородок газосиликатные перегородочные блоки (300х400х100).

4.2 Анализ потенциальных каналов утечек информации

Под окнами в помещениях расположены батареи центрального отопления, контролируемой зоной является периметр ограждающих конструкций защищаемого помещения. В кабинете директора, офисе, а также в кабинетах бухгалтера, IT-отдела и секретаря планируется обсуждать информацию служебного характера.

Основные технические средства и системы в защищаемых помещениях отсутствуют.

Акустический канал утечки информации:

- Дверь;
- Окно;
- Стены между защищаемым помещением и смежными кабинетами;
- Пол;
- Потолок;
- Вентиляционные элементы.

Виброакустический канал утечки информации:

- Дверь;
- Стены между защищаемым помещением и смежными кабинетами;
- Пол;
- Потолок;
- Вентиляционные элементы;
- Трубы центрального отопления.

Акустоэлектрический канал утечки информации:

- Извещатель пожарный.

Также может быть указан канал утечки за счет возможно внедренных в технические средства и предметы интерьера, установленные в защищаемом помещении, закладных устройств.

Возможен просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств. Также есть угроза снятия информации по вибрационному каналу.

4.3 Выбор средств защиты информации

Для обеспечения комплексной безопасности согласно типу конфиденциальной информации – государственная тайна типа «совершенно секретно», требуется оснастить помещение средствами защиты, приведенными в таблице 2.

Таблица 2 – Активная и пассивная защита информации

Каналы утечки информации	Источники	Пассивная защита	Активная защита
Акустический, акустоэлектрический	Двери, окна, пола, стены между защищаемыми помещениями смежными кабинетами, потолок	Внедрение звукопоглощающих покрытий стен, двойных потолков, создания двойных дверей и дополнительных тамбуров дверных проемов, двойных оконных переплетов, исключающих риск снятия звуковых колебаний с оконного стекла; Блокировка и дополнительная изоляция систем ввода в помещения отопления, электропитания.	Использование средств акустического зашумления помещений и конструкций, с которых возможен перехват;
Оптический	Двери, окна	Снизить уровень отраженного света, используя ширмы, затемнение окон, матовые	Засветки изображения объекта

		перегородки, иные преграды; Размещать объекты защиты в пространстве так, чтобы избежать отражения света в сторону гипотетического нахождения злоумышленника, фотоаппарата или видеокамеры; Установить доводчики на двери.	посторонними световыми лучами — помехами; ослепления зрительной системы наблюдателя или светоприемника.
Вибрационный, виброакустический	Двери, стены, пол, потолок, трубы центрального отопления, оконные рамы	Сооружение дополнительных перегородок или повышения звукоизолирующей способности существующих перегородок	Использования средств вибрационного зашумления помещений и конструкций, с которых возможен перехват;
Электромагнитный, электрический	Розетки, АРМы	Фильтрация, комплекс мероприятий по экранированию помещения и сигнальных проводов, осуществление развязки по цепям питания	Шум-генератор

5 АНАЛИЗ РЫНКА ПРЕДЛАГАЕМЫХ РЕШЕНИЙ

Согласно исходным данным, создаваемая система защиты информации предназначена для информации, составляющей государственную тайну уровня «совершенно секретно».

Решение Межведомственной комиссии по защите государственной тайны от 21 января 2011 г. N 199 [5] "О Типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними" говорит о том, что оборудование режимных помещений должно соответствовать следующим критериям:

Стены или перегородки между обычными и защищенными помещениями должны быть бетонными, железобетонными или металлическими с толщиной стен — от 10 см, или кирпичными с толщиной стен от 12 см.

В помещениях для работы с гостайной 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.

Обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании.

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.

Все режимные помещения оборудуются аварийным освещением.

Что касается оборудование помещений для работы с гостайной по требованиям технической безопасности, вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемым к оснащению защищенных и выделенных помещений. 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.

5.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации

Пассивная защита представляет собой внедрение звукопоглощающих покрытий стен, пола, двойных потолков, создания двойных дверей и дополнительных тамбуров дверных проемов, двойных оконных переплетов, исключающих риск снятия звуковых колебаний с оконного стекла. Блокировка и дополнительная изоляция систем ввода в помещения отопления, электропитания.

Активная защита представляет собой использование средств акустического зашумления помещений и конструкций, с которых возможен перехват. Для защиты помещения для работы с государственной тайной уровня «совершенно секретно» рассматриваются технические средства активной защиты информации для объектов информатизации категории не ниже 1Б.

Ниже в таблице 3 приведен сравнительный анализ подходящих средств активной защиты помещений по виброакустическому каналу.

Таблица 3 – Сравнительный анализ средств активной защиты виброакустического канала

Модель	Цена, руб.	Диапазон частот, Гц	Состав
--------	------------	---------------------	--------

БУРАН	53 300	60 – 16 200	Имеет четыре канала формирования помех, к каждому из которых могут подключаться вибропреобразователи пьезоэлектрического или электромагнитного типа, а также акустические системы, обеспечивающие преобразование электрического сигнала, формируемого прибором, в механические колебания в ограждающих конструкциях защищаемого помещения, а также в акустические колебания воздуха
Гамма СВАЗ-01	28 600	90 – 11 200	Центральный блок управления и контроля; легкие виброизлучатели для зашумления тонких перегородок, оконных конструкций, вентиляции; тяжелые виброизлучатели для зашумления стен, труб систем коммуникаций; акустические излучатели (большие и малые);
Генератор маскирующего шума "равнина-3" (исп.4х1)	120 000	90 – 11 200	Генератор маскирующего шума «Равнина-3» (исп.4х1); Виброизлучатели ВП-3 и ВП-4, ВД-80 (средней мощности) и ВД-120 (повышенной мощности).
КАМЕРТОН-5	46 000	90 – 11 200	Блок управления и контроля системой; Блок генерации и генератор маскирующих шумов, создающий помехи в речевом диапазоне частот; Виброизлучатели разных типов, блокирующие вибрационные каналы утечки информации (стены, перекрытия, оконные рамы, прочие элементы строительной конструкции); Акустоизлучатели разных типов, создающие помехи в акустических каналах утечки данных (вентиляционная система, дверные проемы, трубы инженерных коммуникаций, пр.); Размыкатели проводных линий, перекрывающие утечку акустических сигналов по проводам телефонной связи, локальной компьютерной сети, пр.; Виброшторы, создающие надежную помеху для прослушки разговоров с помощью направленного микрофона через оконное стекло.
Соната «АВ» - 46	44 000	175–11 200	Блок электропитания и управления, генератор-акустоизлучатель, генератор- вибровозбудитель, размыкатель телефонной линии, размыкатель слаботочной линии, размыкатель линии Ethernet, пульт управления, блок сопряжения с внешними устройствами, техническое средство защиты речевой информации от утечки по

			оптико-электронному (лазерному) каналу, генераторный блок "АВ-4Л", вибровозбудитель "СП-4Л".
--	--	--	--

По результатам анализа была выбрана система НПО Соната «АВ» модель 4Б из-за ряда преимуществ:

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

5.2 Устройства для перекрытия электрического акустоэлектрического и электромагнитного каналов утечки информации

В таблице 4 приведен сравнительный анализ подходящих средств активной защиты помещений по электрическому каналу.

Таблица 4 – Активная защита от утечек по электрическим каналам

Фирма	Модель	Цена, руб.	Характеристики	Примечания
ООО "Детектор Системс"	Генератор шума СОНАТА-РС3	32 400	Диапазон частот до 2 ГГц, диапазон регулировки	Возможность регулирования уровня излучаемых электромагнитных шумов; возможность блокировки прибора от несанкционированного доступа; световой и звуковой индикаторы работы и контроля уровня излучения;

				совместимость с проводными пультами ДУ линейки СОНАТА.
ООО "Детектор Системс"	ЛГШ-221 (1)	36 400	Диапазон частот 10 кГц – 400 МГц, диапазон регулировки уровня шума не менее 20 ДБ	Световой индикатор работы в стандартном режиме; световая и звуковая сигнализация в случае отказа и перехода в аварийный режим работы; счетчик отработанных часов; возможность интеграции в программно-аппаратный комплекс ДУ и контроля «Паутина».
ООО "Детектор Системс"	SEL SP-44 (1Б)	24 000	Диапазон частот 10 кГц – 400 МГц, диапазон регулировки уровня шума не менее 20 ДБ	Генератор регулируемого шума. Индикация нормального/аварийного режима работы. Электропитание от сети переменного тока 220 В 50 Гц. Устройство имеет высший класс устойчивости к импульсным помехам и допускает длительную работу в условиях эквивалентного короткого замыкания.

Так как по результатам выбора устройства для защиты виброакустического канала была выбрана система НПО Соната «АВ» модель 4Б, то имеет смысл и далее придерживаться данной линейки, тем более что производитель указывает на их совместимость. Данная модель также находится на первом месте в ряде популярных устройств по защите электрических каналов. Особенности конструкции устройства позволяют получать эффективные и недорогие решения при оборудовании объекта вычислительной техники с большим количеством средств вычислительной техники.

5.3 Защита от ПЭМИН

ПЭМИН - побочные электромагнитные излучения и наводки. Вариант защиты компьютерной информации методом зашумления (радиомаскировки) предполагает использование генераторов шума в помещении, где установлены средства обработки конфиденциальной информации.

Зашумление обеспечивается типами генераторов, представленными в таблице 5.

Таблица 5 – Активная защита от ПЭМИН

Название	Особенность	Цена
Генератор шума SEL SP-21B2 "Спектр"	Генератор шума переносной портативный, диапазон частот 0,1–1000 МГц.	112 000
СКИТ-МШ	Широкополосный генератор электромагнитных помех.	16 800
СОНАТА-РЗ	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 индицирования в них маскирующих шумовых напряжений	972 000
SEL SP-21B1 "Баррикада-1"	Генератор радишума, диапазон частот 10–1000 МГц.	17 500

Также выберем СОНАТА-РЗ, у которого есть сертификат ФСТЭК.

5.4 Устройства для перекрытия визуально-оптического канала утечки информации

Для прекращения функционирования оптического канала утечки информации «окно кабинета — окно противоположного жилого дома» можно применить следующие меры:

- шторы на окна;
- жалюзи;
- тонированные пленки на стеклах.

Шторы — традиционные средства для предотвращения скрытного наблюдения через окна кабинета, но они существенно ухудшают естественную освещенность кабинета и накапливают пыль.

Тонированные пленки на стеклах исключают возможность наблюдения за объектами защиты в кабинете, незначительно уменьшают освещенность кабинета, но позволяют легко выявить окна помещений с повышенными требованиями к безопасности информации, что из-за соображений скрытности защиты делать не следует. Для обеспечения скрытности защиты применять пленку надо на всех окнах, по крайней мере, этажа, а лучше здания.

Наиболее приемлемый вариант защиты — применение жалюзи на окнах. Они не только исключают возможность наблюдения через окно, но и эффективны по основному назначению — защите от солнечных лучей. Во многих помещениях они уже установлены.

Для предотвращения наблюдения через приоткрытую дверь применяют доводчик двери, который плавно закрывает дверь после ее открытия.

6 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ МЕР ЗАЩИТЫ ИНФОРМАЦИИ

Согласно информации, приведенной в 3 главе, выбранные средства защиты информации включают в себя:

- В кабинет директора устанавливаются двери толщиной не менее 4 см, обшитые металлическим листом не менее 2 мм толщиной.
- Устройство активной защиты от утечек по виброакустическому каналу: СОНАТА «АВ» модель 4Б.
- Генератор шума СОНАТА-РС3
- Устройство активной защиты от ПЭМИН СОНАТА-РЗ.
- Жалюзи на 6 окон.
- Доводчик на 8 дверей.

Согласно руководству по эксплуатации «Система виброакустической и акустической защиты "Соната-АВ". Руководство по эксплуатации» для предварительной оценки необходимого количества излучателей необходимо исходить из следующих норм:

- стены - один виброизлучатель на каждые 3...5 метров периметра для капитальной стены при условии установки излучателей на уровне половины высоты помещения;
- потолок, пол - один виброизлучатель на каждые 15...25 м² перекрытия;
- окна - один ВИ-45 на окно (при установке на оконный переплет);
- двери - один излучатель на дверь (при установке над дверным проемом);
- трубы систем водо- (тепло- и газо-) снабжения - один на каждую вертикаль (отдельную трубу) вида коммуникаций.

Ориентировочное количество пьезоизлучателей может быть определено из расчета: один ПИ-45 на каждое стекло.

Ориентировочное количество аудиоизлучателей может быть определено исходя из следующих норм:

один - на каждый вентиляционный канал или дверной тамбур;

один - на каждые 8...12 м² над потолочного пространства или других пустот.

Основным правилом, которым следует руководствоваться при выборе мест установки излучателей в каждом конкретном помещении, является обеспечение максимального уровня вибрационного и акустического шума в предполагаемом канале утечки информации при обеспечении приемлемого уровня мешающего акустического шума в защищаемом помещении. Контроль вибрационного и акустического зашумления помещений рекомендуется производить в соответствии с методиками и рекомендациями ФСТЭК (Гостехкомиссии) РФ.

На рисунке 5 изображена схема расстановки устройств.

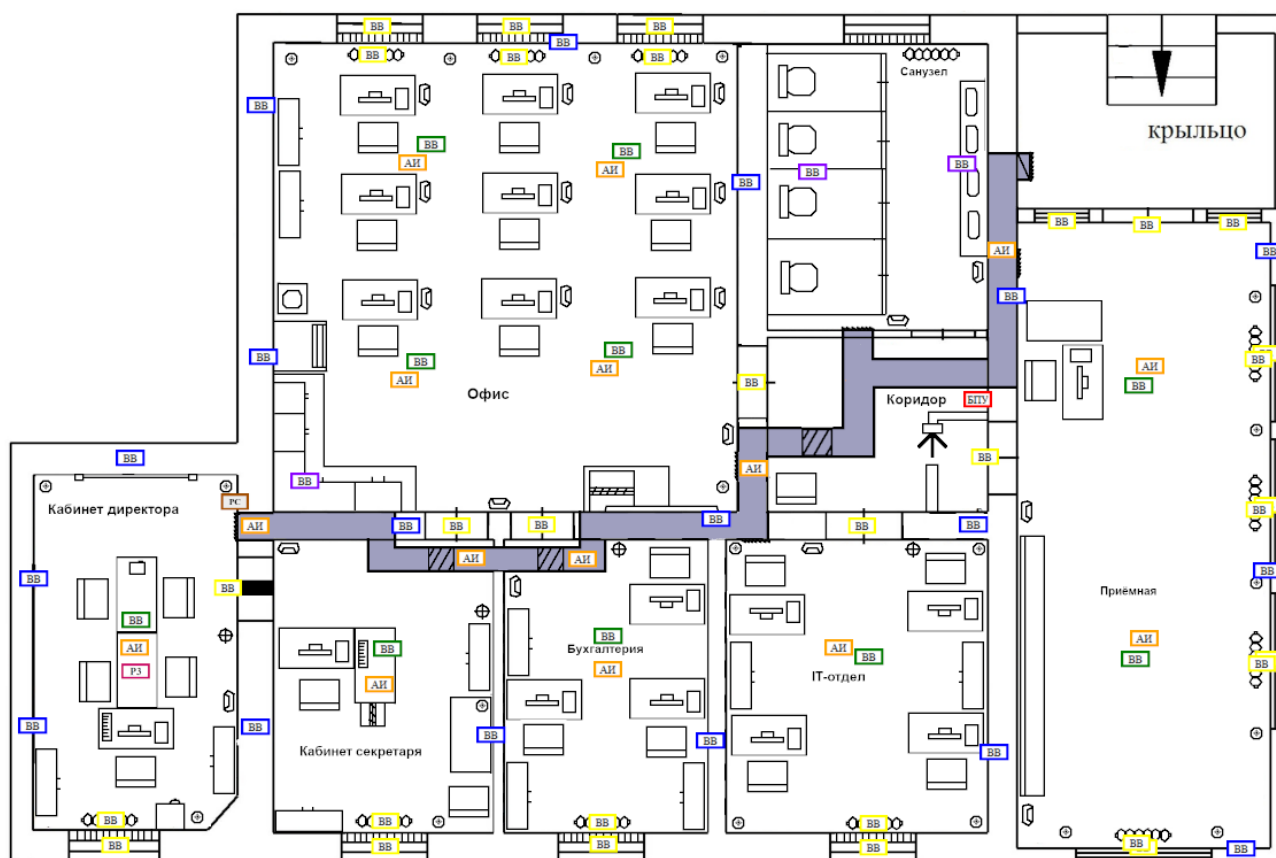





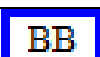
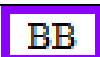




Рисунок 5 – Схема расстановки устройств

Таблица 6 – Условные обозначения схемы расстановки устройств

Устройство	Условное обозначение	Количество, шт.
Блок электропитания и управления «Соната-ИП4.3»		1
Дверь звукоизоляционная		1
«Соната-СА-4Б1» Генератор-акустоизлучатель		15
«Соната-СВ-4Б» Генератор-вибровозбудитель (двери, окна, батареи)		31
«Соната-СВ-4Б» Генератор-вибровозбудитель (пол, потолок)		10
«Соната-СВ-4Б» Генератор-вибровозбудитель (стены)		18
«Соната-СВ-4Б» Генератор-вибровозбудитель (трубопровод)		3
«Соната-РС3»		1
«Соната-РЗ»		1

Исходя из описанных выше рекомендаций и плана расстановки устройств была сформирована смета на приобретение СЗИ, представленная в таблице 7.

Таблица 7 – Смета

Мера защиты	Цена, руб.	Количество, шт.	Стоимость, руб.
Вертикальные пластиковые жалюзи «Нева»	5 725	6	34 350
Виброакустическая защита, блок питания Соната ИП-4.1	21 000	1	21 000
Виброакустическая защита Соната-СА-4Б1	7 400	15	111 000
Вибровозбудитель «Соната-СП»	840	13	10 920
Генераторный блок «Соната-АВ»	10 320	1	10 320
Дверь звукоизоляционная	18 950	1	18 950
Пульт управления «Соната-ДУ4.3»	7 680	1	7 680

«Соната-РЗ»	33 120	1	33 120
«Соната-РСЗ»	32 400	1	32 400
«Соната-СВ-4Б» генератор-вибровозбудитель	7 440	62	461 280
Тяга рычаг Geze к TS 2000/4000 белый	1 120	8	8 960
Итого, руб.	749 980		

ВЫВОДЫ

В ходе данной работы был произведен теоретический обзор существующих каналов утечки информации, анализ потенциальных каналов утечки информации в защищаемом помещении и описаны необходимые меры их защиты. Был проанализирован рынок существующих технических средств для противодействия рассматриваемым каналам утечки информации и выбраны подходящие для нашего объекта. Был разработан план установки и произведен расчет сметы затрат.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

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. «Система виброакустической и акустической защиты "Соната-АВ". Руководство по эксплуатации» - Москва.
4. Руководящий документ Государственной технической комиссии при Президенте РФ «Классификация автоматизированных систем и требований по защите информации» от 30 марта 1992 г.
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".