

**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»

**Выполнил:**

Тошматов Хусравджон Хурshedович, студент группы N34511



(подпись)

**Проверил:**

Попов Илья Юрьевич, к.т.н.

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023г.

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

Студент Тошматов Хусравджон Хуршедович  
(Фамилия И.О)  
Факультет Безопасность информационных технологий  
Группа N34511  
Направление (специальность) 10.03.01 (Технологии защиты информации)  
Руководитель Попов Илья Юрьевич  
(Фамилия И.О)  
Должность, ученое звание, степень Доцент факультета безопасности информационных технологий  
Дисциплина Инженерно-технические средства защиты информации  
Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии  
Задание Разработать комплекс инженерно-технической защиты информации для помещения,  
в котором ведется работа с информацией типа «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**

Данная курсовая работа содержит набор мер для комплексной инженерно-технической защиты информации уровня «секретно» в помещении предприятия.

**Рекомендуемая литература**

149-ФЗ «Об информации, информационных технологиях и о защите информации».

Руководитель \_\_\_\_\_  
(Подпись, дата)  
Студент  \_\_\_\_\_  
(Подпись, дата)

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

**Студент** Тошматов Хусравджон Хуршедович  
(Фамилия И.О)

**Факультет** Безопасность информационных технологий

**Группа** N34511

**Направление (специальность)** 10.03.01 (Технологии защиты информации)

**Руководитель** Попов Илья Юрьевич  
(Фамилия И.О)

**Должность, ученое звание, степень** Доцент факультета безопасности информационных технологий

**Дисциплина** Инженерно-технические средства защиты информации

**Наименование темы** Проектирование инженерно-технической системы защиты информации на предприятии

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1.	Заполнение задания на курсовую работу	1.12.2023	5.12.2023	
2.	Анализ информации	10.10.2023	16.12.2023	
3.	Написание курсовой работы	18.10.2023	19.10.2023	
4.	Защита курсовой работы	27.12.2023	27.12.2023	

**Руководитель** \_\_\_\_\_  
(Подпись, дата)

**Студент** \_\_\_\_\_  
(Подпись, дата)

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

Студент	Тошматов Хусравджон Хуршедович (Фамилия И.О)
Факультет	Безопасность информационных технологий
Группа	N34511
Направление (специальность)	10.03.01 (Технологии защиты информации 2019)
Руководитель	Попов Илья Юрьевич (Фамилия И.О)
Должность, ученое звание, степень	Доцент факультета безопасности информационных технологий
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической системы защиты информации на предприятии

1. Цель и задачи работы	Повышение защищенности рассматриваемого помещения
2. Характер работы	Отчетная курсовая работа
3. Содержание работы информации и выбор мер защиты информации	<u>Анализ защищаемого помещения, оценка каналов утечки</u>
4. Выводы	<u>В результате работы был произведен комплексный анализ</u> возможных технических каналов утечки информации в предложенных помещениях, предложены меры пассивной и активной защиты информации

Чел

## СОДЕРЖАНИЕ

Введение .....	6
1 Анализ технических каналов утечки информации.....	7
2 Руководящие документы .....	10
3 Сведения об организации .....	12
4 Анализ защищаемых помещений.....	14
4.1 Описание помещения .....	16
4.2 Анализ возможных утечек информации.....	17
4.3 Выбор средств защиты информации.....	17
5 Анализ и сравнение технических средств защиты информации .....	19
5.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации .....	19
5.2 Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации .....	20
5.3 Защита от утечек по каналам побочных электромагнитных излучений .....	22
5.4 Защита от утечек по оптическому каналу .....	23
6 Описание расстановки технических средств .....	24
Заключение.....	27
Список использованных источников.....	28

## **ВВЕДЕНИЕ**

В современном мире на вооружении шпионов, недобросовестных конкурентов и просто злоумышленников находятся самые разные средства проникновения на объекты противоправных интересов и получения конфиденциальной информации. В этих условиях в интересах обеспечения информационной безопасности необходимы адекватные по назначению технические средства защиты.

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

В данной научно-исследовательской работе будет разработан комплекс инженерно-технической защиты информации.

Цель работы - повышение защищенности рассматриваемого помещения путем внедрения инженерно-технических средств защиты информации.

Задачи:

- анализ защищаемого помещения;
- изучение нормативно-правовой базы;
- оценка каналов утечки информации;
- анализ и сравнение технических средств;
- проектирование системы защиты 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.

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 её источника.



Рисунок 1 – Структура технического канала утечки информации

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.

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

- оптические;
- радиоэлектронные;
- электрические;
- электромагнитные;
- индукционные;
- акустические;
- акустоэлектрические;
- виброакустические;
- материально-вещественные.

Непосредственно сам человек может стать инициатором (намеренным или случайным) утечки информации. Поэтому работу некоторых систем связи необходимо контролировать, чтобы, с одной стороны, обеспечить безопасную, надежную и точную передачу информации, а с другой, защитить ее от незаконного доступа. И если канал должным образом не защищен, и передача информации из исходной точки в другую происходит без ведома источника, то такой канал можно называть каналом утечки информации.

Защита от утечки информации требует проведения обязательных организационных и технических мер, которые позволят выявить вероятные технические каналы утечки информации, чтобы избежать их возможного использования.

К примеру, чтобы предотвратить утечку информации по акустическому каналу, необходимо снизить или исключить возможность выхода информации за счет контроля акустических полей. В этом случае профессионалы проводят сразу комплекс мероприятий – архитектурную перепланировку пространства, повышение звукоизоляции, звукопоглощения, звукоподавления, а также проводят режимные меры по строгому контролю пребывания людей в отслеживаемой зоне.

В качестве защиты от утечки информации по визуально-оптическому каналу следует снизить освещенность защищаемого объекта и его отражательные свойства, использовать различные пространственные ограждения (ширмы, экраны, шторы, ставни, темные стекла),



применять специальную маскировку и средства сокрытия защищаемых объектов (аэрозольные завесы, сетки, краски, укрытия).

Ключевым способом защиты от утечки информации по электромагнитным каналам считается экранирование аппаратуры и ее элементов. Электростатическое, магнитостатическое и электромагнитное экранирование позволяет предохранить объект от воздействия и электромагнитных, и акустических сигналов. Таким образом, оно обеспечивает надежную защиту информации от утечки по ПЭМИН.

Материально-вещественные каналы также нуждаются в защите, так как различные материальные носители могут содержать в себе важнейшую секретную информацию. К примеру, любое производственное предприятие имеет отходы, в которых могут содержаться различные испорченные документы, бракованные детали, жидкости или газообразные вещества, и часто они бесконтрольно отправляются за пределы контролируемой зоны. Для защиты материально-вещественных каналов от утечки информации разрабатывается целый комплекс организационных мер.

К основным причинам образования технических каналов утечки информации (ТКУИ) относятся:

- несовершенство элементной базы;
- несовершенство схемных решений;
- эксплуатационный износ;
- злоумышленные действия;

Показатели ТКУИ, позволяющие оценить риск утечки информации:

- пропускная способность ТКУИ;
- длина ТКУИ;
- относительная информативность ТКУИ.

Носителем информации в визуально-оптическом канале является электромагнитное поле (фотоны).

В электромагнитном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток (поток электронов), распространяющийся по металлическим проводам.

Носителями информации в акустическом канале являются упругие акустические волны, распространяющиеся в среде.

## 2 РУКОВОДЯЩИЕ ДОКУМЕНТЫ

Основными документами в области защиты информации являются:

Основными нормативно-правовыми 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».
- 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. N 152-ФЗ «О персональных данных».
- Постановление Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- 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.
- РД. Защита от несанкционированного доступа к информации. Термины и определения.
- РД. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.

- РД. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
- РД. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации.
- РД. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники.
- РД. Защита информации. Специальные защитные знаки. Классификация и общие требования.
- РД. Гостехкомиссии России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей.
- РД. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам.
- Закон РФ «О государственной тайне» от 21.07.1993 N 5485–1.
- Межведомственная комиссия по защите государственной тайны решение N 199 от 21.01.2011г. "О типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними".

### 3 СВЕДЕНИЯ ОБ ОРГАНИЗАЦИИ

Организация «Evelation» занимается разработкой программного обеспечения и поставкой ИТ-услуг исключительно для гос. структур. Специализируется на создании и внедрении технологий сбора, обработки и анализа данных, автоматизации бизнес-процессов и разработки системных решений для сложных аналитических задач в сфере тарифного и таможенно-тарифного регулирования. Данная информация является сведениями в области экономики РФ и попадает под статью 5 закона N 5485–1 «Перечень сведений, составляющих государственную тайну». Степень секретности – «секретно».

Структурная схема организации представлена на рисунке 2. Она разбита на 3 сектора: производственный, коммерческий и бэк-офис, с соответствующим директором в главе каждого.

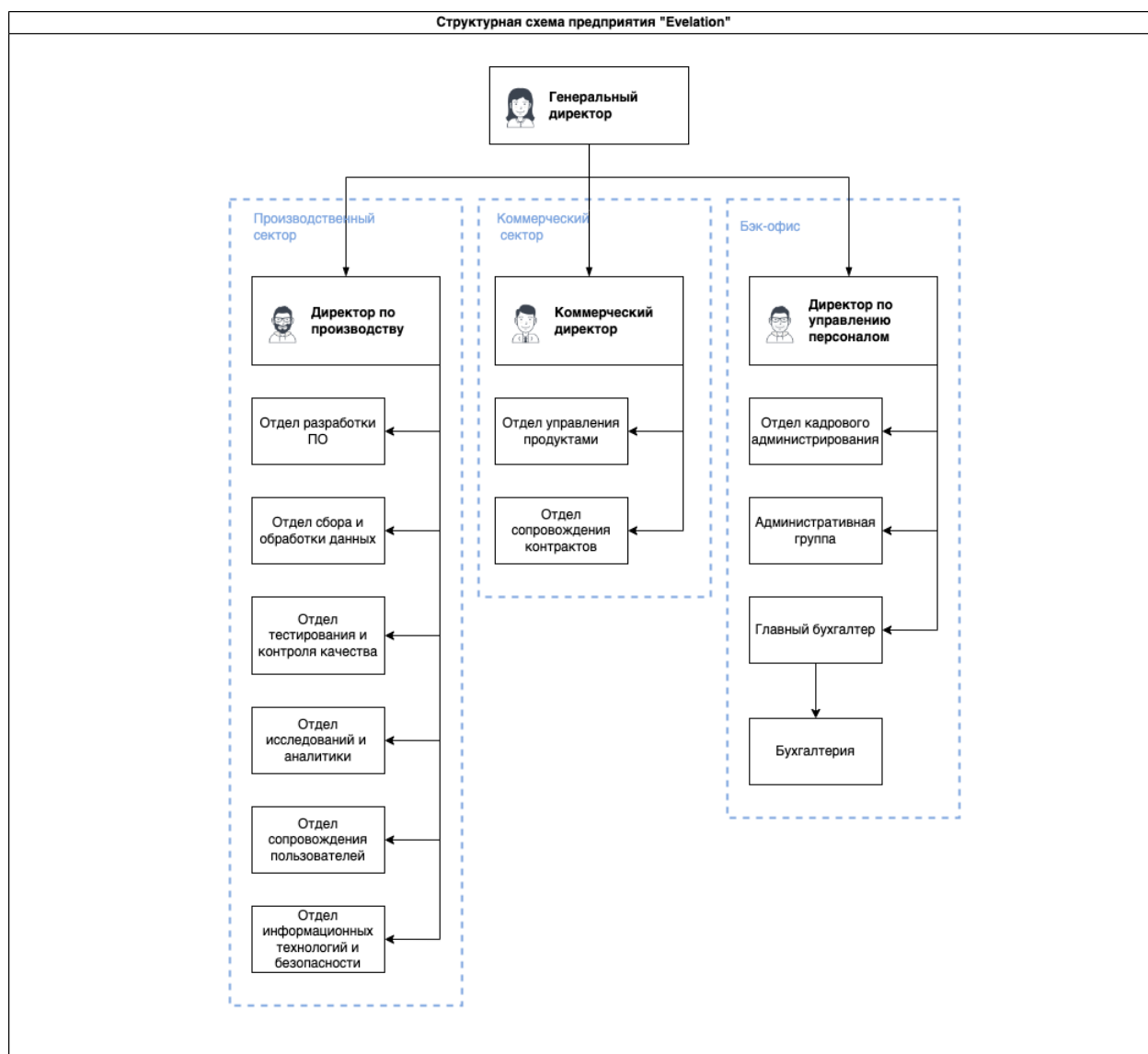


Рисунок 2 – Структурная схема предприятия

На основе структурной схемы рассмотрим информационные потоки организации (рисунок 3). Сплошной линией обозначены закрытые потоки, пунктирной – открытые. Среди закрытых потоков отдельно выделена информация с грифом «секретно» - красная сплошная линия.

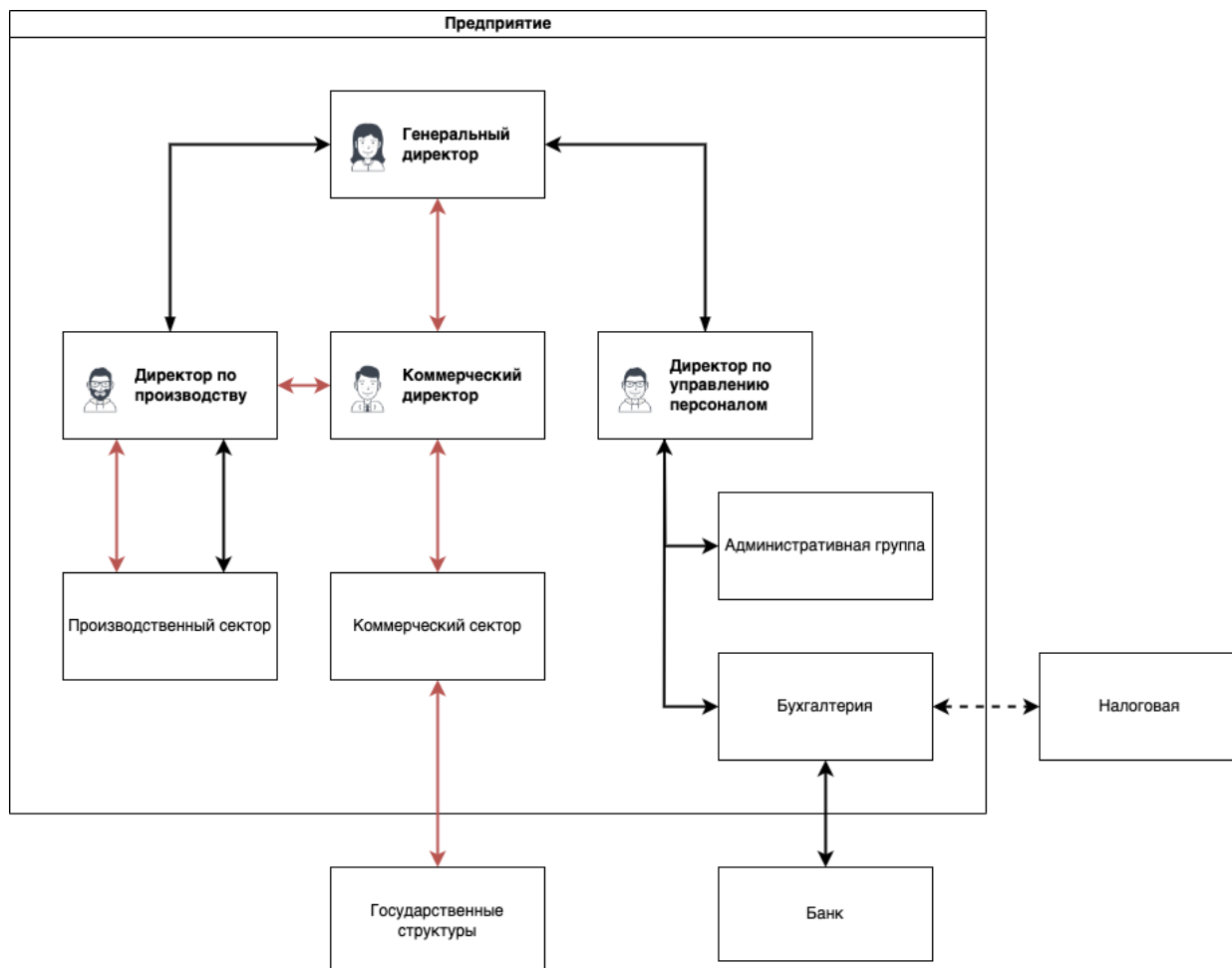


Рисунок 3 – Информационные потоки предприятия

## 4 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

Перед тем как приступим к проектированию технических средств защиты на объекте, проведем анализ защищаемых помещений. На рисунке 4 представлен план защищаемого помещения. В таблице 1 представлена легенда плана защищаемого помещения.

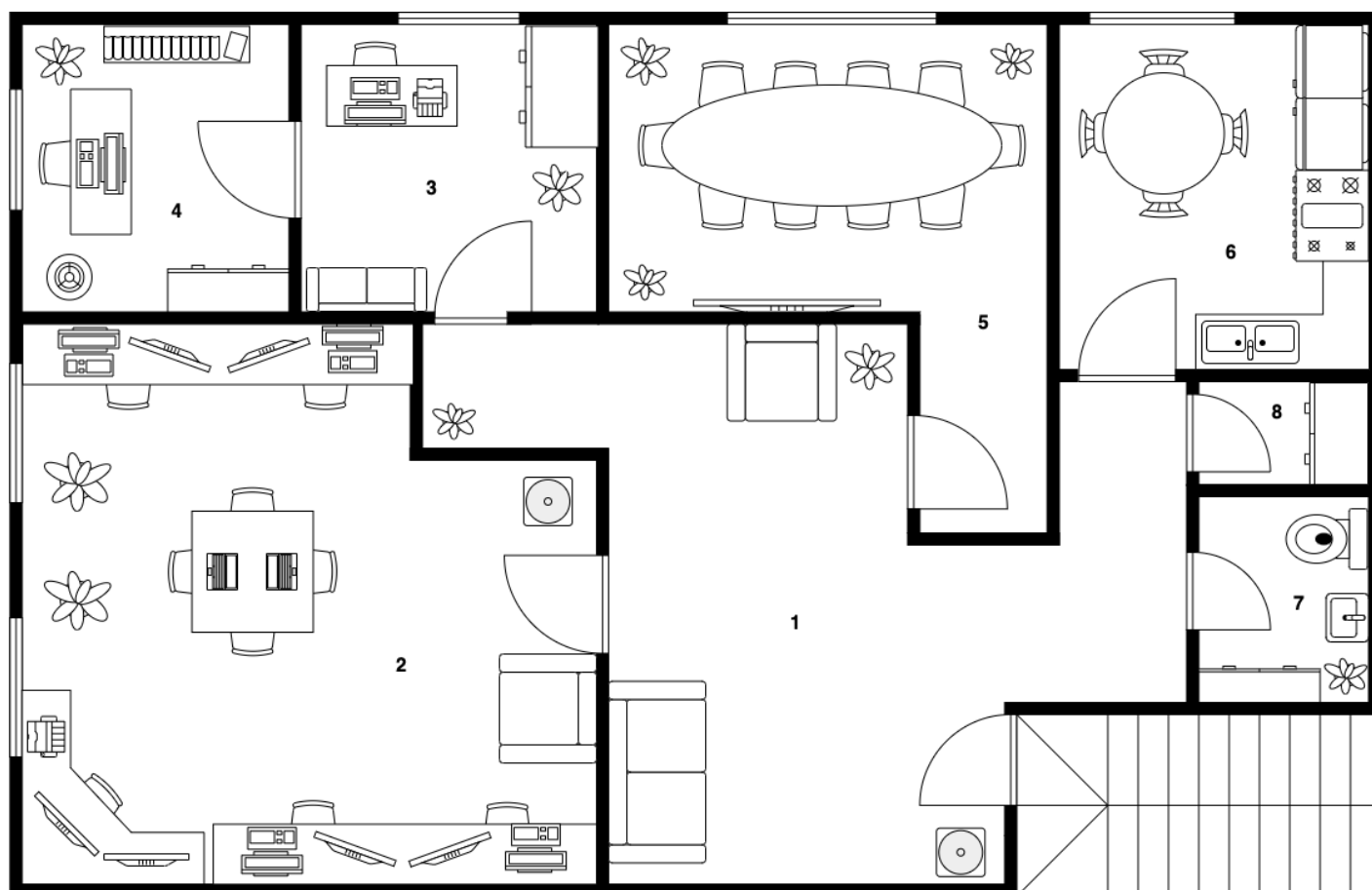

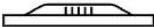
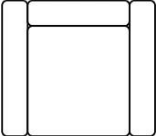
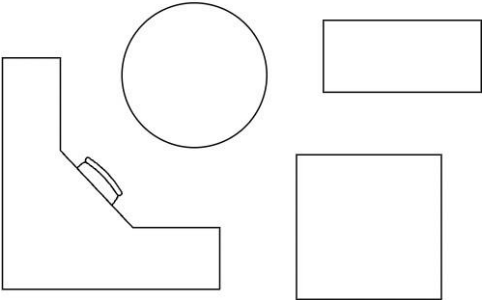



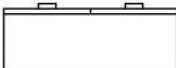

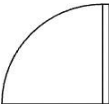
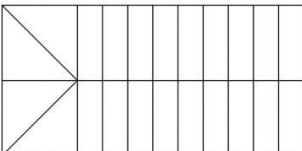

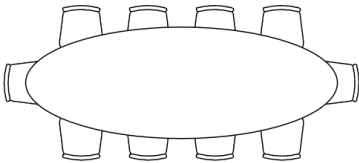
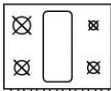



Рисунок 4 – План защищаемого помещения

Таблица 1 – Описание условных обозначений на рисунке 4

	Стена
	Окно
	Персональный компьютер
	Ноутбук

	Принтер
	Экран (монитор)
	Диван/кресло
	Стол
	Стулья
	Кулер с водой
	Цветок (растение)
	Шкаф
	Книжный шкаф
	Дверь
	Лестница
	Раковина

	Стол для переговоров
	Кухонная плита
	Сортир

#### 4.1 Описание помещения

Помещение состоит из 8 комнат:

1. Коридорное помещение – 56 кв. м. (231 – все остальное)
2. Рабочая зона – 62 кв. м. (8.3 на 7.9 - 2.2 на 1.7)
3. Приемная – 18,5 кв. м. (4.4 на 4.2)
4. Кабинет директора – 17 кв. м. (4.1 на 4.2)
5. Переговорная – 30 кв. м. (6.2 на 4.2 + 1.5 на 3)
6. Кухня – 21 кв. м. (4.4 на 4.8)
7. Уборная – 8 кв. м. (2.7 на 3)
8. Кладовая – 4 кв. м. (2.7 на 1.5)

Защите подлежат следующие из них: рабочая зона, приемная, кабинет директора, переговорная. Проведем анализ каждой зоны.

Для работы сотрудников выделена рабочая зона. В ней находится 7 рабочих мест, 5 из которых оснащены персональным компьютером и дополнительным монитором, 2 предназначены для работы на личных устройствах, 1 дополнительно оснащено принтером. Также в помещении имеется 2 горшка с цветами, кулер с водой, диван, 2 окна и 7 розеток.

В приемной директора находится рабочий стол, стул, персональный компьютер, принтер, диван, шкаф, горшок с цветком, окно и 4 розетки.

Кабинет директора оснащен рабочим столом, стулом, персональным компьютером, цветком в горшке, напольной лампой, шкафом для хранения вещей и книжным шкафом, а также 4 розетками и окном.

Для переговоров выделено отдельное помещение, в котором находится длинный стол, 10 стульев, 3 цветка в горшке, экран для презентаций, окно и 8 розеток.



На кухне находятся круглый стол, 4 стула, кухонный гарнитур, включающий в себя 2 раковины, холодильник, микроволновую печь, плиту и шкаф. Также в комнате присутствует окно и 4 розетки.

Помещение расположено на втором этаже малоэтажного бизнес-центра, окна выходят в закрытый контролируемый двор. Окна не соседствуют с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и прочими элементами, с которых в помещения могут проникнуть посторонние лица. Стены здания и внутренние перегородку железобетонные и имеют толщину не менее 10 см.

#### 4.2 Анализ возможных утечек информации

Почти во всех помещениях присутствуют декоративные элементы, где можно спрятать закладное устройств, например, горшки с цветами. Помещения содержат розетки и персональные компьютеры, а значит, актуальны электрические и электромагнитные каналы утечки информации.

Таким образом, актуальны следующие угрозы:

- 1) Электрические и электромагнитные каналы утечки информации;
- 2) Вибрационные и виброакустические каналы утечки;
- 3) Оптические каналы утечки;
- 4) Акустические, акустоэлектрические каналы утечки.

Материально-вещественный канал утечки информации регулируется строгой политикой компании в отношении физических носителей информации.

#### 4.3 Выбор средств защиты информации

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

Таблица 2 - Средства инженерно-технической защиты информации

Каналы	Источники	Пассивная защита	Активная защита
Электрический и электромагнитный	ПК, сервер, розетки, принтеры, телефон, электрические приборы	Сетевые фильтры (фильтры для сетей электропитания)	Устройство электромагнитного зашумления
Вибрационный и виброакустический	Твердые поверхности: стены, батареи	Изоляция стен, усиленные двери со изоляцией	Устройство вибрационного зашумления
Оптический	Окна, двери	Жалюзи на окнах и доводчики	Блокирующие устройства

Акустический и акустоэлектрический	Окна, двери, электрические сети, проводка, розетки	Звукоизоляция	Устройство акустического зашумления
---------------------------------------	--	---------------	---

## **5 АНАЛИЗ И СРАВНЕНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**

Требования к режимным помещениям и их оборудованию содержатся в решении N 199 от 21.01.2011г. "О типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними". Для степени секретно должны быть соблюдены следующие требования:

- 1) Стены или перегородки между обычными и защищенными помещениями должны быть бетонными, железобетонными или металлическими с толщиной стен – от 10 см, или кирпичные с толщиной стен от 12 см.
- 2) Все режимные помещения оборудуются аварийным освещением.
- 3) Вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемыми к оснащению защищенных и выделенных помещений.

Для помещений с уровнем «секретно» подойдут устройства для класса информатизации не ниже 1В согласно РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

### **5.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации**

Пассивная защита представляет собой:

- установка усиленных двери,
- тамбурное помещение перед переговорной,
- дополнительная отделка переговорной звукоизолирующими материалами.

Тамбурное помещение перед переговорное сделать невозможно в силу планировки, поэтому в качестве пассивной защиты я выбрал установку усиленных дверей и шумоизоляции в кабинет директора и переговорную комнату. В кабинете директора потребуется покрыть 50 метров, в переговорной 70.

Активная защита представляет собой систему виброакустического зашумления.

В таблице 3 приведен сравнительный анализ подходящих средства активной защиты помещений по виброакустическому каналу.

Таблица 3 – Сравнительный анализ виброакустических средства защиты

<b>Средство защиты</b>	<b>Цена</b>	<b>Описание и характеристики</b>
------------------------	-------------	----------------------------------

БАРОН-S1 категория 1	33500 руб.	Диапазон частот 60–16000 Гц. Виброгенератор БАРОН-S1, кабель для подключения к ПЭВМ, сетевой шнур, техническое описание; дополнительно устройство контроля эффективности помех Барон-К, Барон-ДК, устройство дистанционного включения Барон-В
ЛГШ-404	35100 рублей	Изделие 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. Изделие «ЛГШ-404» может устанавливаться в выделенных помещениях до 2 категории включительно.
«Соната-АВ» модель 4Б	44200 рублей	Система защиты речевой информации от утечки по техническим каналам "Соната-АВ" модель 4Б, предназначена для защиты речевой информации в выделенных помещениях, от утечки по акустическим, виброакустическим, акустоэлектрическим и оптико-электронным (лазерным) каналам. Комплекс виброакустической защиты помещения — это комплект, состоящий из устройств СВ-4Б, СА-4Б, Соната ИП-4.3, Соната-ДУ-4.3 и набора креплений для установки

По результатам анализа было выбрано средство виброакустической защиты СОНАТА «АВ» модель версии 4Б, так как имеется возможность изменить настройки генераторов. Аппаратная настройка элементов модели 4Б позволяет связывать источник электропитания с другими для обмена информацией. Это дает возможность создать гибкую систему с уменьшенными затратами на электропитание.

## **5.2 Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации**

Пассивная защита основывается на установке фильтров для сетей электропитания во всех помещениях.

Активная защита основывается на создании в сети белого шума, который скрывает колебания, порождаемые воздействием звуковой волны или работающей электрической техникой. Для этого разберем устройства для создания электрического зашумления. В таблице 4 представлен анализ средств активной защиты электрических каналов.

Таблица 4 – Сравнительный анализ средств активной защиты от утечек

Средство защиты	Цена	Описание
СОНАТА-РСЗ	32400 руб.	<p>Устройства для защиты линий электропитания, заземления от утечки информации "Соната-РСЗ" предназначены для защиты объектов ВТ (объектов вычислительной техники) от утечки информации за счет наводок на линии электропитания и заземления и могут использоваться в выделенных помещениях до 1 категории включительно.</p> <p>Изделия рассчитаны на подключение к 3-проводной сети энергоснабжения ("Фаза", "Ноль" и "Защитное заземление") и обеспечивают формирование несинфазных токов и синфазных и паразитных составляющих шумового напряжения во всех проводниках.</p> <p>Может применяться в выделенных помещениях до 1 категории включительно.</p> <p>Диапазон частот 0.01-2000МГц</p>
ЛГШ-503	44200 рублей	<p>Система представляет собой генератор шума по цепям электропитания, заземления и ПЭМИН. Генераторы радиопомех предназначены для работы в составе систем активной защиты информации (САЗ), обеспечивая защиту информации от утечки по каналам ПЭМИН путем создания на границе контролируемой зоны широкополосной шумовой электромагнитной помехи, которая зашумляет побочные излучения защищаемого объекта.</p> <p>Изделие «ЛГШ-503» может устанавливаться в выделенных помещениях до 2 категории включительно.</p> <p>Изделие «ЛГШ-503» оснащено визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа).</p> <p>Изделие «ЛГШ-503» оснащено счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы Изделия в режиме формирования маскирующих помех.</p> <p>Конструкция Изделия «ЛГШ-503» обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного</p>

		<p>изменения и обнаружение несанкционированного доступа к ним.</p> <p>Имеет сертификат соответствия требованиям по безопасности информации №3519, выданный ФСТЭК России 12 февраля 2016 г., срок действия продлён до 12 февраля 2024 г.</p> <p>Диапазон частот 0.01–1800 МГц.</p>
ЛГШ-513	39000 рублей	<p>Генератор шума по цепям электропитания, заземления и ПЭМИ «ЛГШ-513» предназначен для использования в целях защиты информации, содержащей сведения, составляющие государственную тайну и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет побочных электромагнитных излучений и наводок путем формирования маскирующих шумоподобных помех.</p> <p>Изделие «ЛГШ-513» оснащено визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа).</p> <p>Изделие «ЛГШ-513» оснащено счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы Изделия в режиме формирования маскирующих помех.</p> <p>Конструкция Изделия «ЛГШ-513» обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним.</p> <p>Диапазон частот 0.009–1800 МГц.</p>

В ходе анализа средств защиты от утечки по электрическим, акустоэлектрическим и электромагнитным каналам был выбран СОНАТА-РС3. Производитель генератора такой же, как и у системы виброакустической защиты, что Диапазон частот шире, чем у ЛГШ – от 0.01 до 2000МГц. Имеет приятную цену.

### 5.3 Защита от утечек по каналам побочных электромагнитных излучений

Для реализации активной защиты от ПЭМИН было выбрано устройство Соната-РЗ.1. Данный выбор обоснован тем, что устройство может быть встроено в систему «Соната АВ-4Б», выбранную как реализация активной защиты по виброакустическому каналу. Помимо этого, устройство СОНАТА-РС3, выбранное в качестве активной защиты от утечек

по электрическим, акустоэлектрическим и электромагнитным каналам, уже содержит в себе активную защиту от утечек за счет ПЭМИН.

#### **5.4 Защита от утечек по оптическому каналу**

Для обеспечения защиты помещения от утечки по оптическим каналам необходимо установить рулонные шторы блэкаут Inspire Belem. Их стоимость приблизительно 900 рублей/штуку. Всего понадобится 5 штук. Также используются доводчики для плотного закрывания дверей, которые были установлены бизнес-центром.

## 6 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

В ходе анализа и сравнения технических средств защиты информации от утечек по техническим каналам были выбраны следующие средства:

- НПО Соната «АВ» модель АВ-4Б;
- Шумоизоляция Steico Therm;
- Усиленные двери Torex Super Omega PRO PP;
- Рулонные шторы блэкаут Inspire Belem;
- Соната-РС3;
- Соната-Р3.1.

В комплекс СОНАТА АВ-4Б входит:

- 1) Блок электропитания и управления – "Соната-ИП4.3"
- 2) Генератор-акустоизлучатель – "СА-4Б"
- 3) Генератор-вибровозбудитель – "СВ-4Б"
- 4) Размыкатель телефонной линии – "Соната-ВК4.1"
- 5) Размыкатель слаботочной линии – "Соната-ВК4.2"
- 6) Размыкатель линии Ethernet – "Соната-ВК4.3"
- 7) Пульт управления – "Соната-ДУ4.3"
- 8) Блок сопряжения с внешними устройствами – "Соната-СК4.2"

Оценим количество компонентов и расстановке выбранных технических средств.

Ориентировочное количество аудиогенераторов-излучателей "СА-4Б"/"СА4Б1" может быть определено исходя из следующих норм:

- 1) один "СА-4Б" на каждый вентиляционный канал,
- 2) один "СА-4Б" на дверной тамбур или входную дверь;
- 3) один "СА-4Б" на каждые 8...12 м<sup>2</sup> надпотолочного пространства или других пустот.

Для оценки необходимого количества виброгенераторов-излучателей "СВ-4Б" необходимо исходить из следующих норм:

- 1) при установке на стену – один "СВ-4Б" на каждые 15...25 м<sup>2</sup> площади поверхности стены (при этом излучатели должны устанавливаться на уровне половины высоты стены при высоте стены менее 5 м или на высоте от пола помещения не менее 2.5 м при высоте стены 5 м и более, далее – через каждые 5 м высоты);
- 2) при установке на потолок (пол) – один "СВ-4Б" на каждые 15...25 м<sup>2</sup> плиты перекрытия;



- 3) при установке на оконный переплет - один "СВ-4Б" на каждое окно или раздельную раму;
- 4) при установке на дверь – один "СВ-4Б" на каждое полотно двери;
- 5) при установке на трубы систем водо-, тепло- или газоснабжения – один "СВ-4Б" на каждую отдельную трубу перед выходом из помещения.
- 6) Ориентировочное количество "СВ-4Б" определяется из расчета: один "СВ-4Б" на каждый элемент остекления.

В таблице 5 посчитаем итоговую стоимость выбранных технических средств для рассматриваемого предприятия.

Таблица 5 – Оценка итоговой стоимости всех технических средств

<b>СЗИ</b>	<b>Цена за штуку</b>	<b>Количество</b>	<b>Итого</b>
Пульт управления – "Соната-ДУ4.3"	7 500	1	7 500
Блок электропитания и управления – "Соната-ИП4.3"	21 500	1	21 500
Генератор-акустоизлучатель "СА-4Б"	7 500	12	90 000
Генератор-вибровозбудитель – "СВ-4Б"	7 500	28	210 000
Размыкатель телефонной линии	6 000	1	6 000
Размыкатель слаботочной линии	6 000	1	6 000
Размыкатель линии Ethernet	6 000	2	12 000
Усиленные двери Torex Super Omega PRO PP	56 000	2	112 000
Соната-РС3	33 000	3	99 000
Соната-РЗ.1	33 000	1	33 000
Звукоизоляция стен за 1 кв. м.	1 000	130	130 000
Шторы рулонные блэкаут Inspire Belem	1000	5	5 000
<b>Итого</b>			<b>731 000</b>

На рисунке 5 представлен план помещения с расставленными на нем выбранными средствами защиты информации. На рисунке 6 представлены условные обозначения.

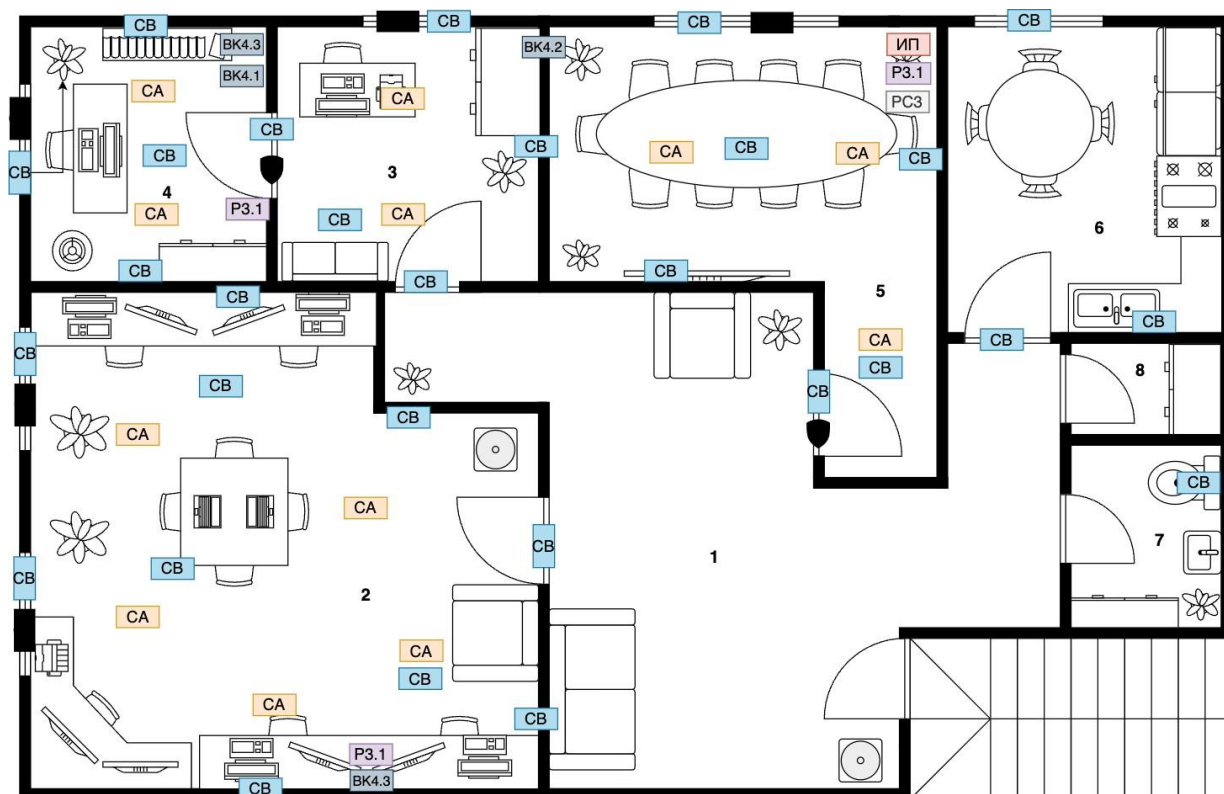


Рисунок 5 – План помещения после внедрения ИТСЗИ

ИП	Блок электропитания и управления – "Соната-ИП4.3"
CB	Генератор-вибровозбудитель – "CB-4Б"
CA	Генератор-акустоизлучатель "CA-4Б"
PC3	Соната-PC3
P3.1	Соната-P3.1
BK4.1	Размыкатель телефонной линии
BK4.2	Размыкатель слаботочной линии
BK4.3	Размыкатель линии Ethernet
	Шторы рулонные блэкаут Inspire Belem
	Усиленные двери Torex Super Omega PRO PP

Рисунок 6 – Условные обозначения СЗИ

## ЗАКЛЮЧЕНИЕ

Методы защиты важных данных предприятия представляют собой не только меры предосторожности, но и целую отрасль современной науки, которая постоянно совершенствуется и обновляется, используя передовые технологии. Мошенники при этом тоже не сидят на месте и с каждым разом придумывают все новые методы и схемы с помощью которых они производят хищение важной информации у предприятий.

Технические средства защиты информации эффективны при детальном изучении помещения, где хранятся ценные данные, а также предполагаемых зон утечки информации. В ходе курсовой 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.

Результатом работы является план защиты информации по акустическому, электромагнитному и визуальному каналам передачи данных, составляющих служебную тайну с грифом «секретно». Общая стоимость всего оборудования составила 731 000 рублей.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012. - 416 с. - экз.
2. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010.- 436 с.
3. Трунова, А. А. Анализ каналов утечки конфиденциальной информации в информационных системах предприятий / А. А. Трунова. — Текст: непосредственный // Молодой ученый. — 2016. — No 3 (107). — С. 69–72. — URL: <https://moluch.ru/archive/107/25842>.
4. Скрипник Д. Техническая защита информации. [Интернет-ресурс] URL: <https://intuit.ru/studies/courses/3649/891/info>.