

**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:**

студент группы N34471,

Смирнов Д.А.

  
(подпись)

**Проверил:**

доцент ФБИТ, к.т.н.,

Попов И.Ю.

---

(отметка о выполнении)

---

(подпись)

Санкт-Петербург

2023 г.

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

**ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ**

**Студент**    Смирнов Даниил Александрович

(Фамилия И.О.)

**Факультет**    Безопасность Информационных Технологий

**Группа**    N34471

**Направление (специальность)**    10.03.01 (Технологии защиты информации 2020)

**Руководитель**    Попов Илья Юрьевич, к.т.н., доцент ФБИТ

(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**    Разработать инженерно-техническую систему защиты информации для предприятия

**Краткие методические указания**

**Рекомендуемая литература**

**Руководитель**

(Подпись, дата)

**Студент**     16.12.2023

(Подпись, дата)

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

**ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

**Студент** Смирнов Даниил Александрович  
(Фамилия И.О.)

**Факультет** Безопасность Информационных Технологий

**Группа** N34471

**Направление (специальность)** 10.03.01 (Технологии защиты информации 2020)


**Руководитель** Попов Илья Юрьевич, к.т.н., доцент ФБИТ  
(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		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Исследование организации и обрабатываемой информации	15.11.2023	15.11.2023	
2	Выявление обоснования для разработки инженерно-техническую систему защиты информации	20.11.2023	20.11.2023	
3	Изучение плана предприятия	28.11.2023	28.11.2023	
4	Анализ рынка инженерно-технических средств защиты информации	01.12.2023	01.12.2023	
5	Разработка итоговой инженерно-технической системы защиты информации	16.12.2023	16.12.2023	

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

**Студент**  16.12.2023  
(Подпись, дата)

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ**

Студент	Смирнов Даниил Александрович
	(Фамилия И.О.)
Факультет	Безопасность Информационных Технологий
Группа	N34471
Направление (специальность)	10.03.01 (Технологии защиты информации 2020)
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ
	(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

Исследовать роль и обязанности администратора информационной безопасности, оценить влияние на обеспечение безопасности информационных ресурсов, изучить используемые методы и инструменты, анализировать законодательные нормы и требования.

- 2. Характер работы**
- ☐ Расчет    ☐ Конструирование  
☐ Моделирование    ☒ Другое

**3. Содержание работы**

1. Введение
2. Организационная структура предприятия
3. Обоснование защиты информации.
4. Анализ защищаемых помещений.
5. Анализ рынка технических средств.
6. Описание расстановки технических средств.
7. Заключение.
8. Список литературы

**4. Выводы**

В ходе работы была разработана инженерно-техническая система защиты информации для предприятия, исследован рынок актуальных решений.

Руководитель	
Студент	 16.12.2023
	(Подпись, дата)
	(Подпись, дата)

## СОДЕРЖАНИЕ

Введение .....	6
1      Организационная структура предприятия .....	7
2      Обоснование защиты информации. ....	8
3      Анализ защищаемых помещений.....	10
4      Анализ рынка .....	15
5      Описание расстановки технических средств .....	20
Заключение.....	22
Список литературы.....	23

## **ВВЕДЕНИЕ**

В современном информационном обществе, где технологии занимают центральное место в повседневной деятельности предприятий, обеспечение надежной защиты информации становится критической задачей. Развитие информационных технологий неизбежно сопровождается возрастающими угрозами безопасности, что требует системного и комплексного подхода к обеспечению конфиденциальности, целостности и доступности данных.

Целью данной курсовой работы является исследование и проектирование инженерно-технических средств защиты информации на предприятии с целью обеспечения устойчивости информационной инфраструктуры и минимизации рисков связанных с утечкой, повреждением или несанкционированным доступом к конфиденциальной информации.

В ходе работы будет исследована структура организации, приведено обоснование защиты информации, проанализированы защищаемое помещение и рынок технических средств, описана расстановка выбранных технических средств.

# 1 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

**Наименование организации:** Paper planes

**Область деятельности:** Разработка и производство высокотехнологичного оборудования для авиационной индустрии.

**Основные закрытые информационные потоки в организации:**

- государственная тайна – проекты, чертежи, тех. характеристики, технологии производства и разработки;
- коммерческая тайна – планы развития предприятия, бизнес-процессы
- персональные данные сотрудников.

**Основные открытые информационные процессы и потоки в организации:**

- Отчеты о финансовом состоянии компании, пресс-релизы, рекламные материалы, налоговые и пенсионные отчисления.

Таким образом, можно изобразить схему информационных потоков предприятия. Красным обозначены закрытые потоки, зеленым - открытые (рисунок 1).

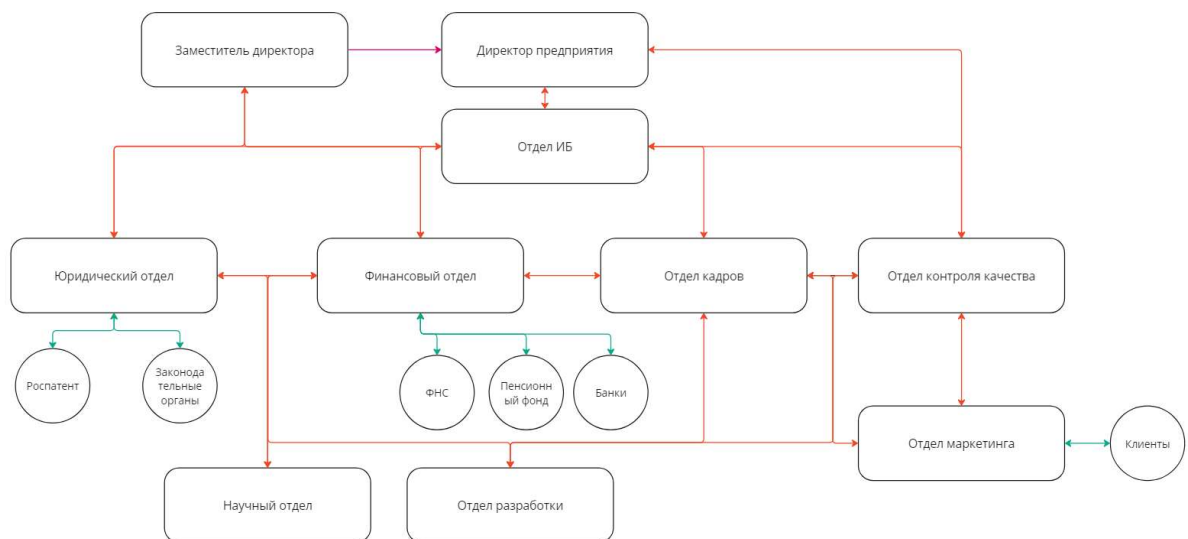


Рисунок 1 – Информационные потоки предприятия

## **2      ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ.**

Поскольку в информационной системе предприятия содержатся секретные сведения, составляющие государственную тайну, возникает необходимость руководствоваться соответствующими нормативно-правовыми актами.

В соответствии с постановлением Правительства РФ от 4 сентября 1995 г. N 870 "Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности":

Сведения, отнесенные к государственной тайне, по степени секретности подразделяются на сведения особой важности, совершенно секретные и секретные.

– К сведениям особой важности следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из указанных областей.

– К совершенно секретным сведениям следует относить сведения 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.

– К секретным сведениям следует относить все иные сведения из числа сведений, составляющих государственную тайну. 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-разыскной области деятельности.

Таким образом, сведения, отнесенные к государственной тайне на рассматриваемом предприятии, могут быть отнесены к категории «секретно».

НПА, определяющие требования к защите такой информации, являются следующими:

- Закон РФ «О государственной тайне» от 21.07.1993 N 5485–1;
- Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;



- Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера»;
- Указ Президента РФ от 06.10.2004 N 1286(ред. от 02.04.2012)"Вопросы Межведомственной комиссии по защите государственной тайны"
- Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
- Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства РФ от 22.11.2012 N 1205"Об утверждении Правил организации и осуществления федерального государственного контроля за обеспечением защиты государственной тайны"
- Постановление Правительства РФ от 06.02.2010 N 63(ред. от 01.11.2012)"Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне"
- Приказ ФСТЭК «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. №644;
- 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";
- 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.
- "Инструкция о порядке проведения специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну"(утв. ФСБ РФ 23.08.1995 N 28)

### 3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

Для выявления потенциальных каналов утечки информации следует подробнее рассмотреть план помещения (рисунок 2).

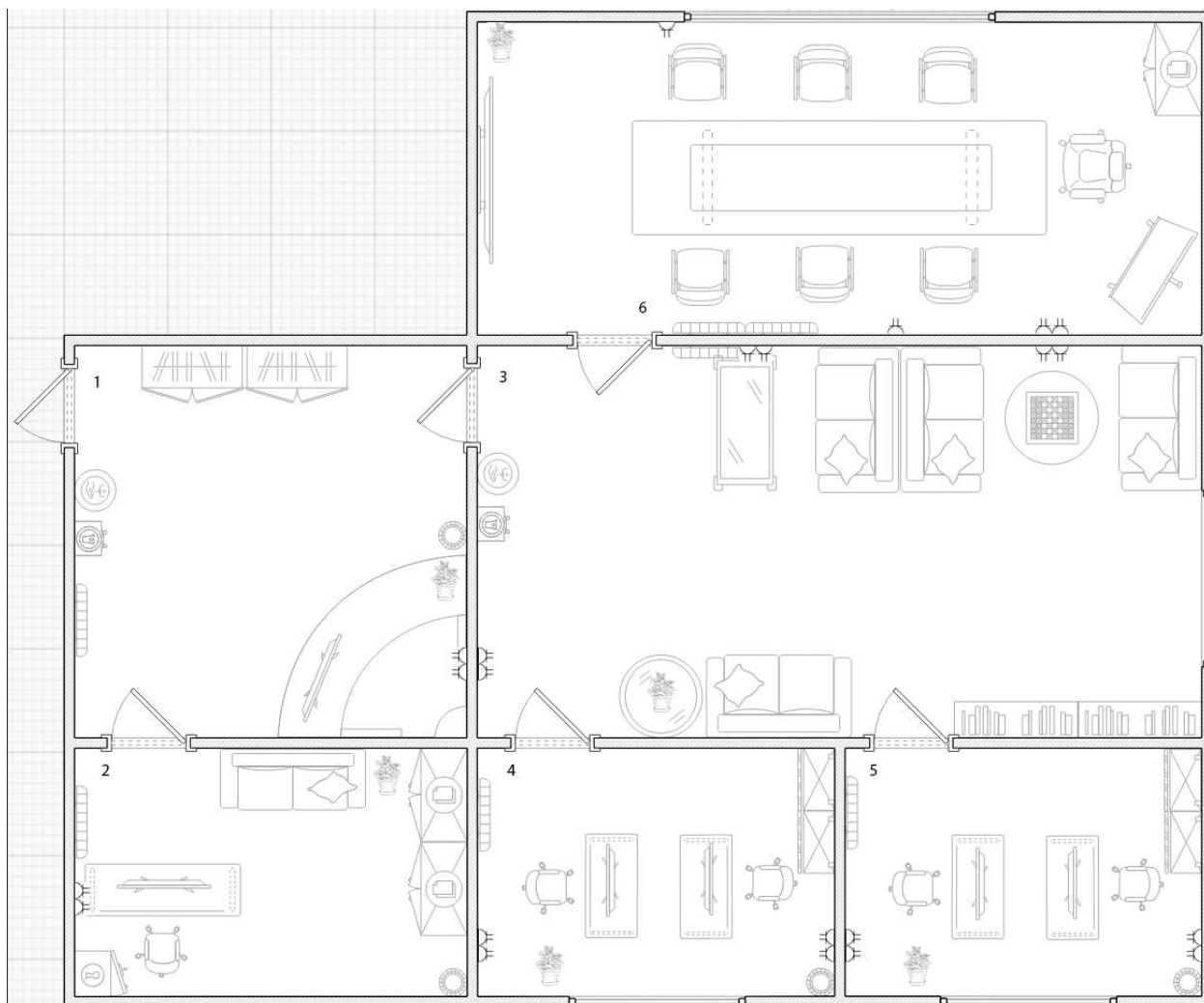



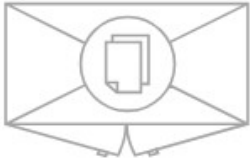
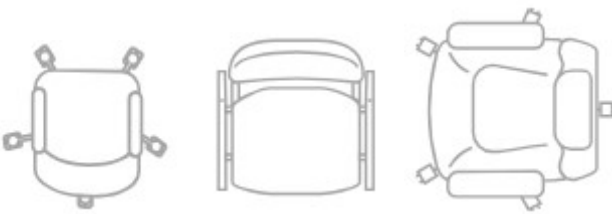




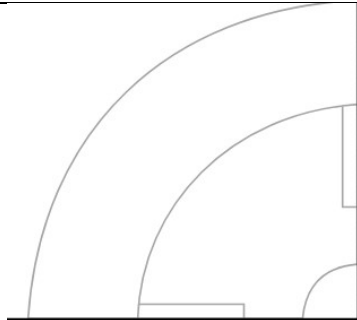
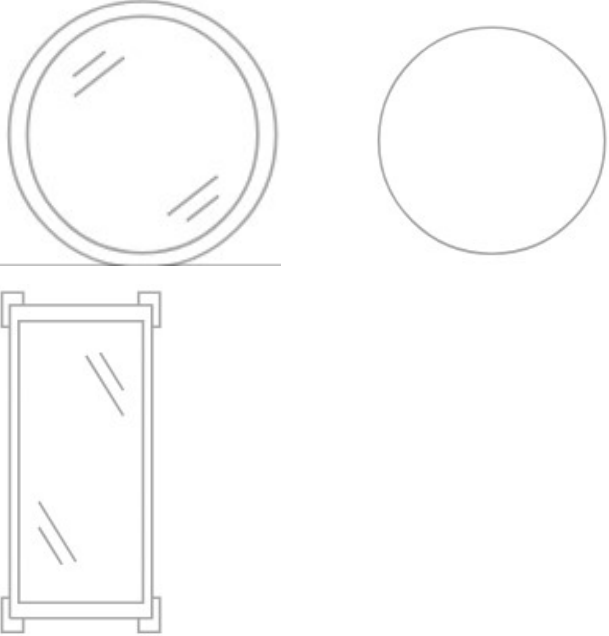
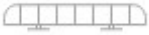



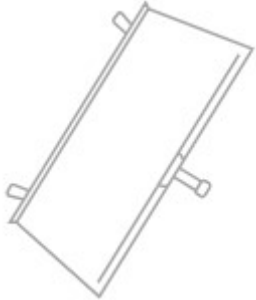


Рисунок 2 – План помещения

Обозначение	Описание
	Гардероб
	Санитайзер
	Кулер

	Мусорная корзина
	Монитор
	Диван
	Шкаф офисный
	Стул
 	Стол
	Сейф
	Книжный шкаф
	Административная стойка

	Журнальный стол
	Радиатор отопления
	Розетка
	Шахматы
	Цветок
	Флип-чарт

Предприятие арендует помещение на восьмом этаже тридцатизэтажного здания – не имеет собственной охраны, туалет находится вне офиса.

Легенда помещения:

1 – Административная стойка с монитором, общее пространство с гардеробом

2 – Кабинет директора, где может происходить работа с гос. тайной, ее хранение на бумажных и электронных носителях, ее обсуждение

3 – Пространство для отдыха, не предназначенное для работы с гос. тайной, но находящиеся вблизи с комнатами, в которых может происходить работа с гос. тайной, присутствуют окна

4 – Рабочий офис, где может происходить работа с гос. тайной, ее хранение на бумажных и электронных носителях, ее обсуждение, присутствуют окна

5 - Рабочий офис, где может происходить работа с гос. тайной, ее хранение на бумажных и электронных носителях, ее обсуждение, присутствуют окна

6 – Переговорная, где может происходить обсуждение гос. тайны, изображение информации, представляющей гос. тайну, на флип-чарте и экране для презентаций, присутствуют окна.

В помещениях присутствуют розетки, радиаторы отопления и иные элементы, которые могут косвенно способствовать утечки информации через вибрационный канал и ПЭМИН. Возможна установка закладочных устройств. Незакрытые двери и окна могут быть причиной утечки по оптическому и акустическому каналам.

Таким образом, можно выделить возможные технические каналы утечки информации в конкретных комнатах помещения:

Номер Комнаты	Оптический	Акустический	Виброакустический	ПЭМИН
1	-	+	+	+
2	-	+	+	+
3	+	+	+	-
4	+	+	+	+
5	+	+	+	+
6	+	+	+	+

Для предотвращения утечек по указанным каналам необходимо рассмотреть возможные способы и средства защиты:

Каналы	Источники	Пассивная защита	Активная защита
Акустический, акустоэлектрический	окна, двери, проводка	звукоизоляция переговорной, фильтры для сетей электропитания	устройства акустического зашумления

Виброакустический	все твердые поверхности помещения, батареи	изолирующие звук и вибрацию обшивки стен	устройства вибрационного зашумления
ПЭМИН	розетки, АРМы	фильтры для сетей электро- питания	устройства электро-магнитного зашумления
Оптический	окна, двери	Жалюзи / шторы на окнах, тонирующие пленки	-

## 4 АНАЛИЗ РЫНКА

Согласно решению Межведомственной комиссии по защите государственной тайны от 21.01.2011 N 199 о «Типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними»:

- 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.

- Все режимные помещения оборудуются аварийным освещением.

- 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.

- Для предотвращения доступа посторонних лиц в режимные помещения требуется установить замки. Для более надежной защиты можно устанавливать кодовые и электронные замки, а также автоматические турникеты.

С учетом рассмотренных норм можно определить пассивную защиту от утечек по имеющимся каналам:

- усиленные двери толщиной 4 см, с двух сторон обшитые металлическим листом 2 мм, имеющие звукоизоляционный материал внутри и установленные на металлический каркас;

- двойные окна;

- дополнительная звукоизолирующая обшивка переговорной;

- сетевые фильтры для цепей электропитания, экранирование металлическим материалом.

- Тонирующие пленки и шторы на окнах. Закрытие штор по время переговоров

В качестве защиты от утечек по виброакустическому, акустоэлектрическому и ПЭМИН необходимо отдельно рассмотреть актуальные активные средства защиты.

Таблица 1 – Средства виброакустического зашумления

Название устройства	Цена, руб.	Описание
ЛГШ-404	35 100	Диапазон рабочих частот 175-11200 Гц Потребляемая мощность 25 Вт Электропитание 220 В, 50 Гц Габаритные размеры генераторного блока 188х160х60 мм Количество подключаемых излучателей на канал до 20 шт.
Соната АВ-4Б	44 200	Диапазон рабочих частот 175-11200 Гц Количество октавных полос для регулировки уровня мощности шума 6 шт Максимальное количество излучателей 239 шт Электропитание сеть 220В/50Гц Удаленный мониторинг Ethernet + СПО "Инспектор" для блока управления версии "Соната-ИП4.2" Защита от использования оптико-электронных средств "Соната-АВ4Л": Генераторный блок "АВ-4Л" + вибровозбудители "СП-4Л"
Буран-2	45 000	Диапазон рабочих частот 180-11200 Гц Электропитание сеть переменного тока напряжением 220 В + 10% с частотой 50-60 Гц число помеховых каналов – три (виброакустических – 2, акустических – 1); возможность дистанционного включения системы по проводному каналу.

После анализа выбрал ЛГШ-404, так как в комплекте с ним идут:

- Вибровозбудитель «ЛВП-10» - для установки на стены, трубы и окна
- Акустический излучатель «ЛВП-2а» - для возбуждения маскирующих акустических помех
- Виброэкран «ЛИСТ-1» - для защиты от налюдения и акустических микрофонов
- Размыкатель «ЛУР» - для размыкания слаботочных линий

Данный комплект выигрывает по цене и по покрытию всех возможных конструкций, с которых возможно снятие вибраций.



Таблица 2 – Средства акустоэлектрического зашумления

Название устройства	Цена, руб.	Описание
ЛГШ-221	36 400	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 наводок путем формирования маскирующих шумоподобных помех. Рабочий диапазон частот не менее 0,01 и не более 400 МГц
ЛФС-40-1Ф	70 200	Предназначен для защиты информации, обрабатываемой техническими средствами и системами и содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа от утечки по каналам побочных электромагнитных наводок на линии электропитания напряжением 220 В с частотой 50 Гц.
СОНАТА-РС3	32 400	Предназначен для активной защиты информации от утечки по сети электропитания Работа от сети 220В и 50Гц Потребляемая мощность – 10Вт;

После сравнения выбрал прибор ЛГШ-221 из-за возможности интеграции в программно-аппаратный комплекс ДУ и наличия более подробного описания в отличие от конкурентов.

Таблица 3 – Средства защиты от ПЭМИН

Название устройства	Цена, руб.	Описание
ЛГШ-501	29 900	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. Напряжение шумового сигнала - 0,01 - 400 МГц; 10 - 58 дБ. Электрическое поле - 0,01 - 1800 МГц; 15 - 75 дБ. Магнитное - 0,01 - 30 МГц; 20 - 65 дБ. Показатель электромагнитной совместимости при положении органов регулировки, обеспечивающем максимальный уровень выходного шумового сигнала, Рэмс - не менее 70 м. Ресурс изделия - 12000 ч
ЛГШ-503	44 200	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. Напряжение шумового сигнала - 0,01 - 400 МГц; 10 - 58 дБ.

		Электрическое поле - 0,01 - 1800 МГц; 15 - 75 дБ. Магнитное - 0,01 - 30 МГц; 20 - 65 дБ. Показатель электромагнитной совместимости при положении органов регулировки, обеспечивающем максимальный уровень выходного шумового сигнала, Рэмс - не менее 70 м. Ресурс изделия - 12000 ч
СОНАТА-РЗ.1	33 120	Предназначено для защиты информации от утечки информации за счет побочных электромагнитных излучений и наводок на линии электропитания и заземления, линии проводной связи и токоведущие инженерные коммуникации. Диапазон частот 0,01 - 200 МГц.
Генератор шума «Пульсар»	24 525	Диапазон частот 10 кГц - 6 ГГц. Имеет защиту регулятора уровня выходного шумового сигнала от нелегального доступа (и сигнализирует об этом). Индикаторы нормального режима работы (диод) и аварийного режима (свет и звук). ресурс изделия 27000 ч
Генератор шума «Покров»	32 800	Диапазон частот 10 кГц - 6 ГГц. Практически неотличим от сетевого удлинителя с 5 розетками. ресурс изделия 50000 ч

В качестве устройства пространственного зашумления выбрал Генератор шума «Покров» из-за более широкого диапазона частот, большого ресурса изделия и маскировки под обычный удлинитель.

Таблица 4 – Защита линий связи

Название устройства	Цена, руб.	Описание
Гранит-8	4 160	Назначение фильтра пропускать сигналы в речевом диапазоне частот при нормальном режиме работы телефонной линии и ослаблять высокочастотные сигналы, которые могут подаваться в линию при высокочастотном навязывании.
ЛУР 2	5 590	Размыкатель слаботочных линий питания (Дополнение к ЛГШ-404)
ЛУР 8	5 590	Размыкатель слаботочных линий Ethernet (Дополнение к ЛГШ-404)
Соната-ВК 4.1	6 000	размыкатель аналоговых телефонных линий + Соната-ИП4.4 (36 000 руб.) Частота - 150 Гц - 10 МГц. Интервал давления - 30-60 дБ.
Соната-ВК 4.2	6 000	размыкатель линий оповещения и сигнализации + Соната-ИП4.4 (36 000 руб.) Частота - 150 Гц - 10 МГц. Интервал давления - 30-60 дБ.
Соната-ВК 4.3	6 000	размыкатель компьютерных сетей + Соната-ИП4.4 (36 000 руб.) Частота - 150 Гц - 10 МГц.

	Интервал давления - 30-60 дБ.
--	-------------------------------

Так как ранее был выбран ЛГШ-404, защита линий связи будет обеспечена совместимыми средствами - ЛУР 2, ЛУР 8.

Таблица 5 – Блокаторы беспроводной связи

Название устройства	Цена, руб.	Описание
ЛГШ-701	97 500	Предназначен для блокирования работы устройств несанкционированного получения информации, работающих в стандартах сетей сотовой связи и в стандартах Bluetooth и WiFi. Предназначено для блокировки (подавления) связи между базовыми станциями и пользовательскими терминалами сетей сотовой связи работающих в стандартах: <ul style="list-style-type: none"> <li>• IMT-MC-450(NMT-450i)</li> <li>• GSM900</li> <li>• E-GSM900</li> <li>• DSC/GSM1800</li> <li>• DECT1800</li> <li>• CDMA2000 1x</li> <li>• CDMA-800</li> <li>• AMPS/N-AMPS/D-AMPS-800/CDMA-800</li> </ul>
ТЕРМИНАТОР 37-5G	58 169	Предназначен для подавления беспроводного сигнала портативных устройств: сотовая связь и интернет, Wi-Fi, GPS и ГЛОНАСС, UHF и VHF
ЛГШ-702	61 100	Предназначено для блокирования (подавления) работы устройств, работающих в стандартах Bluetooth и WiFi. Диапазон рабочих частот стандарта Bluetooth, WiFi не менее 2400...2483,5 МГц

Из блокаторов выбрал ЛГШ-701, так как покрывает большее количество стандартов.

На основе представленных устройств и их описаний для защиты информации от утечек по техническим каналам были выбраны следующие средства:

Канал	Устройство	Цена, руб.
Виброакустический	ЛГШ-404	35 100
	Вибровозбудитель «ЛВП-10»	5 200
	Виброэкрэн ЛИСТ-1	12 600
	Акустический излучатель ЛВП-2А	5 200
Акустоэлектрический	ЛГШ-221	36 400
ПЭМИН	Генератор шума «Покров»	32 800
	ЛУР 2	5 590
	ЛУР 8	5 590
	ЛГШ-701	97 500

## 5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

После выбора всех средств необходимо расставить их таким образом, чтобы закрыть все возможные технические каналы утечки. Расстановка представлена на рисунке 2.

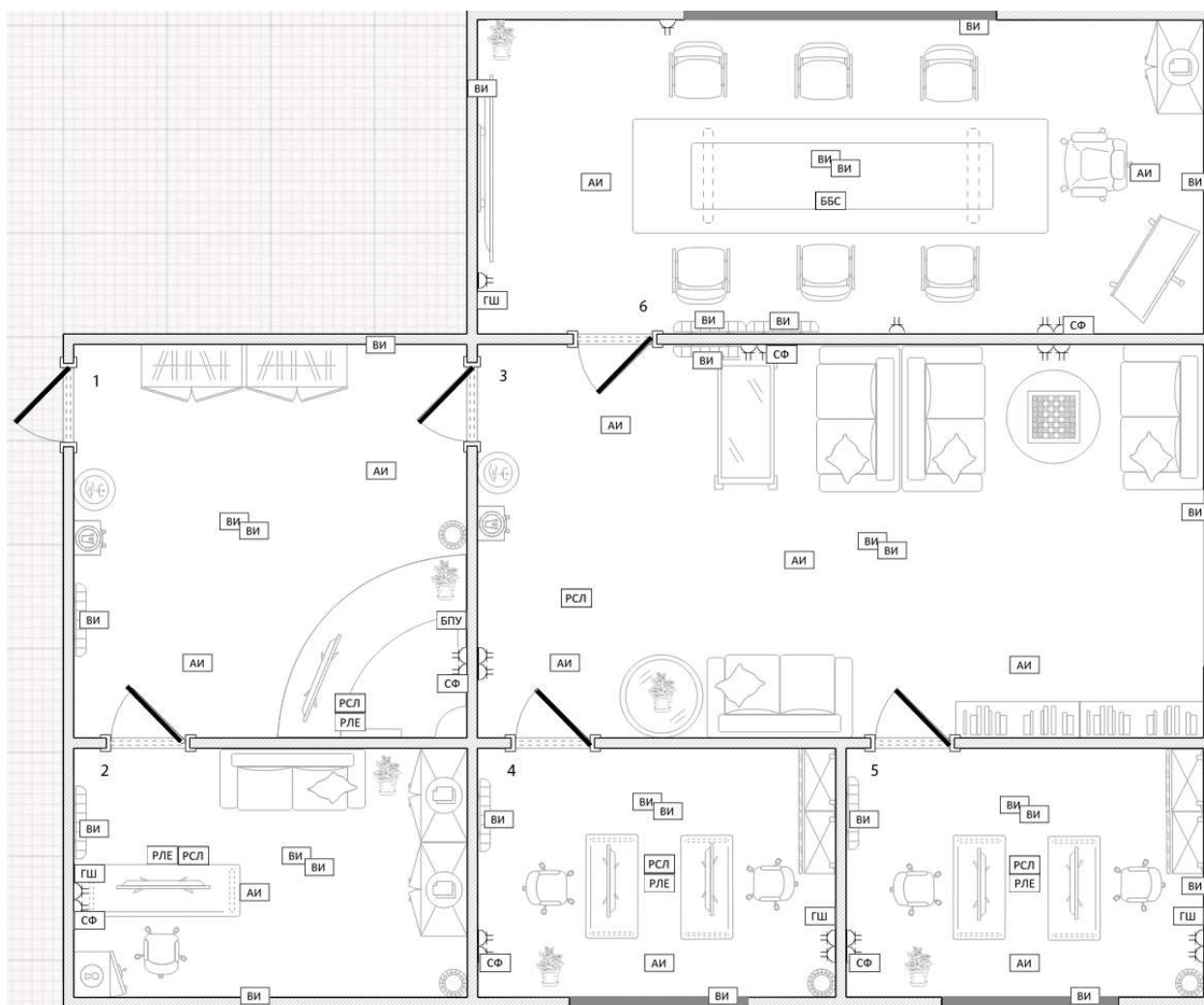




Рисунок 3 – Расстановка инженерно-технических средств защиты информации.

Таблица 6 – Условные обозначения инженерно-технических средств защиты

Обозначение	Устройство	Количество, шт.
БПУ	Блок питания управления	1
ВИ	Виброакустический излучатель	28
АИ	Акустический излучатель	11
ГШ	Генератор пространственного зашумления	4
СФ	Сетевой фильтр	6
РЛЕ	Размыкатель линии «Ethernet»	4
РСЛ	Размыкатель слаботочной линии	4
ББС	Блокатор беспроводной связи	1
	Усиленная дверь	6
	Шторы + тонированные пленки на окнах	4

Для защиты утечек по виброакустическому каналу были установлены излучатели на все поверхности, поглощающие вибрации – потолки и полы (на плане сдвоенные значки), окна, внешние стены, генераторы отопления. В качестве пассивной защиты установлены усиленные двери толщиной 4 см, с двух сторон обшитые металлическим листом 2 мм, имеющие звукоизоляционный материал внутри и установленные на металлический каркас.

Для защиты от утечек по акустоэлектрическому и ПЭМИН, были установлены генераторы пространственного зашумления, размыкатели Ethernet и слаботочных линий в комнатах, использующих ЭВМы. Сетевые фильтры – в каждой комнате. Блокатор беспроводной связи установлен под столом в переговорной.

Оптический канал защищен с помощью штор и тонированных пленок на окнах.

## **ЗАКЛЮЧЕНИЕ**

В результате выполнения курсовой работы была разработана схема инженерно-технических средств, предотвращающих утечки информации, в том числе государственной тайны, на предприятии «Paper planes», которое занимается проектированием и разработкой высокотехнологичного оборудования для авиаиндустрии. Были рассмотрены структура организации, план помещения, возможные каналы утечки информации, проанализирован рынок актуальных технических средств. Таким образом, поставленная цель и задачи выполнены.

## СПИСОК ЛИТЕРАТУРЫ

1. Нормативно-правовые акты по защите государственной тайны / [Электронный ресурс] // specotd : [сайт]. — URL: <https://specotd.admin-smolensk.ru/docs/>
2. Detector systems / [Электронный ресурс] // detsys : [сайт]. — URL: <https://detsys.ru/>
3. Лаборатория ППШ / [Электронный ресурс] // pps : [сайт]. — URL: <http://www.pps.ru/>
4. Разработки АО "НПО "ЭШЕЛОН" / [Электронный ресурс] // npo-echelon : [сайт]. — URL: <https://npo-echelon.ru/production/65/11746>
5. РАЗМЫКАТЕЛЬ ETHERNET для ответственных применений / [Электронный ресурс] // ethercut : [сайт]. — URL: <https://ethercut.ru/>
6. Защита информации от утечки по визуально-оптическим каналам / [Электронный ресурс] // anti-malware : [сайт]. — URL: <https://www.anti-malware.ru/practice/methods/protection-of-information-from-leakage-through-visual-optical-channels>