

**Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

Факультет безопасности информационных технологий

Дисциплина:

«Инженерно-технические средства защиты информации»

КУРСОВАЯ РАБОТА

На тему:

«Проектирование инженерно-технической защиты информации на предприятии»

Выполнил:

Кориненко Даниил Трофимович, студент группы N34471



(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	Кориненко Даниил Трофимович
	(Фамилия И.О.)
Факультет	Безопасность информационных технологий
Группа	N34471
Направление (специальность)	Информационная безопасность
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 инженерно-технической системы защиты информации на предприятии. Вариант 30
Задание	Разработать системы инженерно-технической защиты информации на предприятии


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, размещенных на коммуникационной площадке дисциплины.
3. Объект исследований курсовой работы ограничивается заданным помещением.

Содержание пояснительной записки

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.

Рекомендуемая литература

Руководитель		(Подпись, дата)
Студент		17.12.2023
		(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Кориненко Даниил Трофимович
(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34471

Направление (специальность) Информационная безопасность


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 инженерно-технической системы защиты информации на предприятии. Вариант 30

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируема я	Фактически я	
1	Разработка и утверждение задания и календарного плана на курсовую работу	24.10.2023	24.10.2023	
2	Анализ теоретической составляющей	25.10.2023	25.10.2023	
3	Разработка комплекса инженерно-технической защиты информации в заданном помещении	26.10.2023	27.11.2023	
4	Представление выполненной курсовой работы	19.12.2023	19.12.2023	

Руководитель _____
(Подпись, дата)

Студент  17.12.2023
(Подпись, дата)

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

Студент Кориненко Даниил Трофимович

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34471

Направление (специальность) Информационная безопасность

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 инженерно-технической системы защиты информации на предприятии. Вариант 30

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

**1. Цель и задачи
работы**

☐ Предложены студентом

☐ Сформулированы при участии студента

☒ Определены руководителем

Целью работы является проектирование комплексных средств защиты информации. Задачами является анализ защищаемого помещения, оценка каналов утечки информации и выбор мер пассивной и активной защиты информации.

**2. Характер
работы**

☐ Расчет

☒ Конструирование

☐ Моделирование

Другое _____

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.

Выводы

В результате работы был проведен анализ потенциальных путей утечки информации в предлагаемых помещениях, а также предложены стратегии пассивной и активной защиты данных.

Руководитель

Студент



(Подпись, дата)

17.12.2023

(Подпись, дата)

СОДЕРЖАНИЕ

Введение	7
1 Организационная структура предприятия	8
1.1 Структура предприятия.....	8
1.2 Структура информационных потоков предприятия	9
2 Обоснование защиты информации	11
2.1 Руководящие документы	11
2.2 Обоснование уровня защищенности	12
2.3 Требования к СЗИ.....	14
3 Анализ защищаемого помещения	16
3.1 Схема помещения	16
3.2 Описание помещения	19
3.3 Анализ возможных каналов утечки информации	20
4 Анализ рынка технических средств	23
4.1 Защита от утечки информации по акустическим и виброакустическим каналам	23
4.2 Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам	27
4.3 Защита от утечек посредством ПЭМИН	29
4.4 Защита от утечек информации по оптическим каналам	32
5 Описание расстановки технических средств	33
Заключение.....	37
Список использованных источников.....	38

ВВЕДЕНИЕ

Средства защиты информации (СЗИ) — это технологические и организационные меры, принимаемые для обеспечения конфиденциальности, целостности и доступности информации. Они направлены на предотвращение несанкционированного доступа (НСД), утечек данных, а также обеспечение надежности информационных систем. СЗИ делятся на организационные, программно-аппаратные, криптографические, а также инженерно-технические, которые служат для защиты каналов связи, по которым передается информация, от утечек, изменения, блокирования, копирования. В современной обстановке повышен риск атак на предприятия с целью получения НСД, поэтому наличие СЗИ как никогда актуально.

В данной работе рассмотрен процесс разработки комплекса инженерно-технической защиты информации, составляющей государственную тайну с уровнем «секретно» на объекте информатизации. Защищаемый объект состоит из десяти помещений и представляет собой офис предприятия с переговорной, кабинетом директора, двумя санузлами, тремя кабинетами, двумя коридорами, кухней и холлом-прихожей.

Данная работа состоит из пяти глав. В первой главе произведен анализ технических каналов утечки информации. Во второй приведён перечень управляющих документов, в третьей – анализ защищаемых помещений с точки зрения возможных утечек информации и требуемых для защиты технических средств. Четвертая глава представляет собой анализ рынка технических средств защиты информации разных категорий, и пятая глава посвящена разработке схем расстановки выбранных технических средств в защищаемом помещении.

1 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

1.1 Структура предприятия

В данном разделе курсовой работы будет описана организационная структура предприятия, в котором обрабатывается государственная тайна третьего уровня. На рисунке 1 представлена иерархия персонала организации, который состоит из 54 человек и включает в себя:

- СТО;
- CEO;
- Руководитель RnD;
- команда контента — 7 человек;
- команда разработки — 10 человек;
- отдел маркетинга — 5 человек;
- отдел дизайна — 8 человек;
- юридический отдел — 3 человека;
- финансовый отдел — 3 человека;
- отдел инфраструктуры — 5 человек;
- отдел ИБ — 5 человек;
- отдел поддержки — 5 человек.

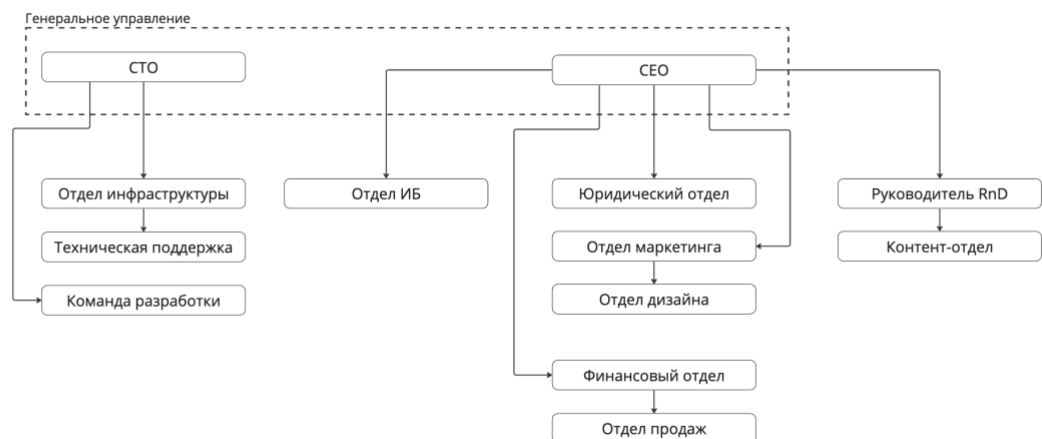


Рисунок 1 – Организационная структура предприятия

Данное предприятие не имеет единственного руководителя, все ключевые решения принимаются советом генерального управления, которое состоит из CEO и СТО.

1.2 Структура информационных потоков предприятия

Информационный поток – это совокупность циркулирующих в логистической системе, между логистической системой и внешней средой сообщений, необходимых для управления и контроля логистических операций. Информационный поток может существовать в виде бумажных, электронных носителей, звука, сигналов.

Информационные потоки могут быть классифицированы по-разному, в рамках данной курсовой работы выделены следующие типы информационных потоков: внешние (открытые и закрытые) и внутренние (открытые и закрытые).

Внешние потоки представляют из себя информацию, которая передается между компанией и внешними актёрами, например клиентами, а также банками и государственными органами. К открытым потокам относится отчетная информация о налоговых выплатах и финансовых операциях – не требуют специального уровня доступа. К закрытым потокам относятся персональные данные, коммерческая тайна, передача которых должна осуществляться в защищенной среде.

Внутренние потоки представляют из себя информацию, которая не должна быть доступна лицам, не являющимися сотрудниками компании. Данная информация необходима для успешного протекания рабочих процессов. Любая внутренняя информация должна быть защищена от любого внешнего воздействия. К открытым данным относится информация, которая не требует специальных разрешений и доступна всем сотрудникам, например, дизайн и контент будущих продуктов. К закрытой информации относятся финансовые данные, персональные записи, интеллектуальная собственность, а также данные, составляющие гостайну (разработки внутри компании), несанкционированный доступ к которым, может нанести ущерб предприятию и, следовательно, интересам Российской Федерации.

На рисунке 2 представлена схема потоков внутри защищаемой организации. Так, например, данные о разрабатываемом ПО доступна только техническому персоналу компании, так как именно он будет поддерживать корректное функционирование и безопасность ПО.

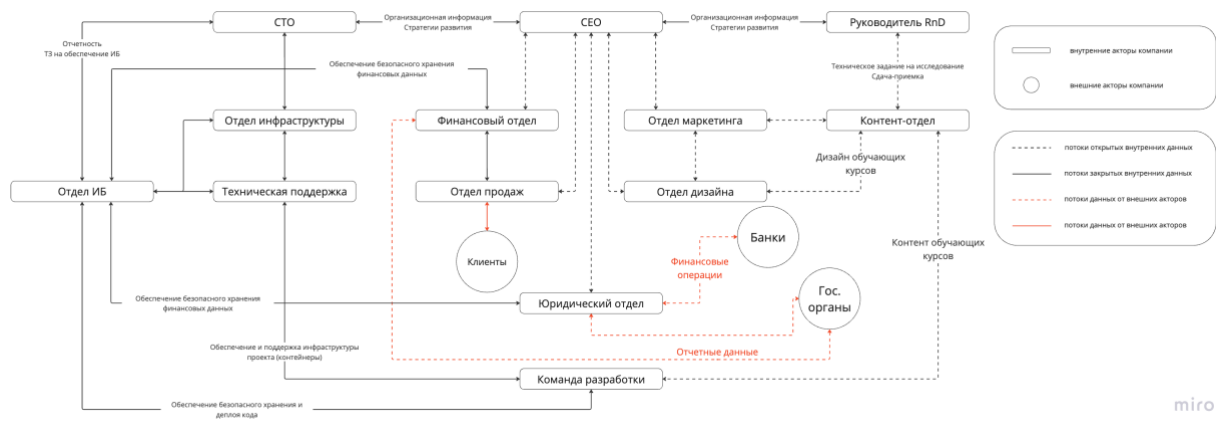


Рисунок 2 – Информационные потоки в предприятии

2 ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

2.1 Руководящие документы

Необходимость наличия средств защиты информации, содержащей гостайну, а также порядок их установки и аттестации регламентируется нормативными актами, регламентами и руководящими документами, представленными в следующем перечне:

1. Указы Президента РФ:

- «Вопросы Государственной технической комиссии при Президенте Российской Федерации» от 19 февраля 1999 г. №212
- «Вопросы защиты государственной тайны» от 30.03.1994 г. №614
- «Об утверждении перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г. №1203.
- «О межведомственной комиссии по защите государственной тайны» от 8 ноября 1995 г. №1108.
- «Вопросы Межведомственной комиссии по защите государственной тайны» от 20 января 1996 г. №71 с изменениями, внесенными Указами Президента Российской Федерации от 21 апреля 1996 г. №573, от 14 июня 1997 г. №594.
- «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. №644.
- «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. №188.
- Указ Президента РФ от 06.10.2004 N 1286(ред. от 02.04.2012)"Вопросы Межведомственной комиссии по защите государственной тайны"

2. Постановления Правительства Российской Федерации:

- Постановление Правительства РФ от 15.04.1995 N 333 (ред. от 05.05.2012)"О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны"
- Постановление Правительства РФ от 04.09.1995 N 870 (ред. от 22.05.2008)"Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности"

- 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"

- Постановление Правительства РФ от 22.11.2012 N 1205 "Об утверждении Правил организации и осуществления федерального государственного контроля за обеспечением защиты государственной тайны"

3. Федеральные законы

- «О государственной тайне» от 21 июля 1993 г. №5151-1
- «Об информации, информатизации и защите информации» от 20 февраля 1995 г. №24-ФЗ
- «О безопасности» от 5 марта 1992 г. №2446-1.

4. Документы ФСТЭК

- 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
- 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.

2.2 Обоснование уровня защищенности

Объектом защиты является фирма ООО "StopY", занимающаяся созданием и продажей образовательных материалов по информационной безопасности в виде сервиса-платформы для корпоративных клиентов и государственных структур.

Согласно Руководящему документу Государственной технической комиссией при Президенте РФ «Классификация автоматизированных систем и требований по защите

информации» от 30 марта 1992 г.: «При разработке АС, предназначенной для обработки или хранения информации, являющейся собственностью государства и отнесенной к категории секретной, необходимо ориентироваться в соответствии с РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» на классы защищенности АС не ниже (по группам) 3А, 2А, 1А, 1Б, 1В».

Таблица 1 – Классы защищенности автоматизированных систем

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

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

- особой важности: сведений в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации.

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

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

Соответственно класс защищенности у рассматриваемой организации 1В, так как в ней обрабатывается секретная информация и предприятие является многопользовательской АС, где не все пользователи имеют права доступа ко всей информации.

2.3 Требования к СЗИ

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

1. В помещениях для работы с государственной тайной и хранилищах секретных документов устанавливаются усиленные двери, обеспечивающие надежное закрытие. Двери с двух сторон обшиваются металлическим листом не менее 2 мм толщиной, внутри — звукоизоляционный материал, сама дверь должна иметь толщину не менее 4 см. Дверь устанавливается на металлический каркас.

2. Обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании.
3. 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.
4. Все режимные помещения оборудуются аварийным освещением.
5. Оборудование помещений для работы с государственной тайной по требованиям технической безопасности, вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемым к оснащению защищенных и выделенных помещений.
6. 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.

3 АНАЛИЗ ЗАЩИЩАЕМОГО ПОМЕЩЕНИЯ

3.1 Схема помещения

Для корректного размещения технических средств защиты информации на объекте необходимо провести анализ защищаемого помещения. На рисунке 3 представлен план помещения офисного типа. В таблице 1 представлено описание используемых обозначений.

Компания “StopY” имеет несколько офисов-помещений для каждого отдела внутри одного бизнес-центра. Так как планы офисов имеют максимальную схожесть, будет рассмотрена защита только на одном плане, чтобы избежать дублирования.

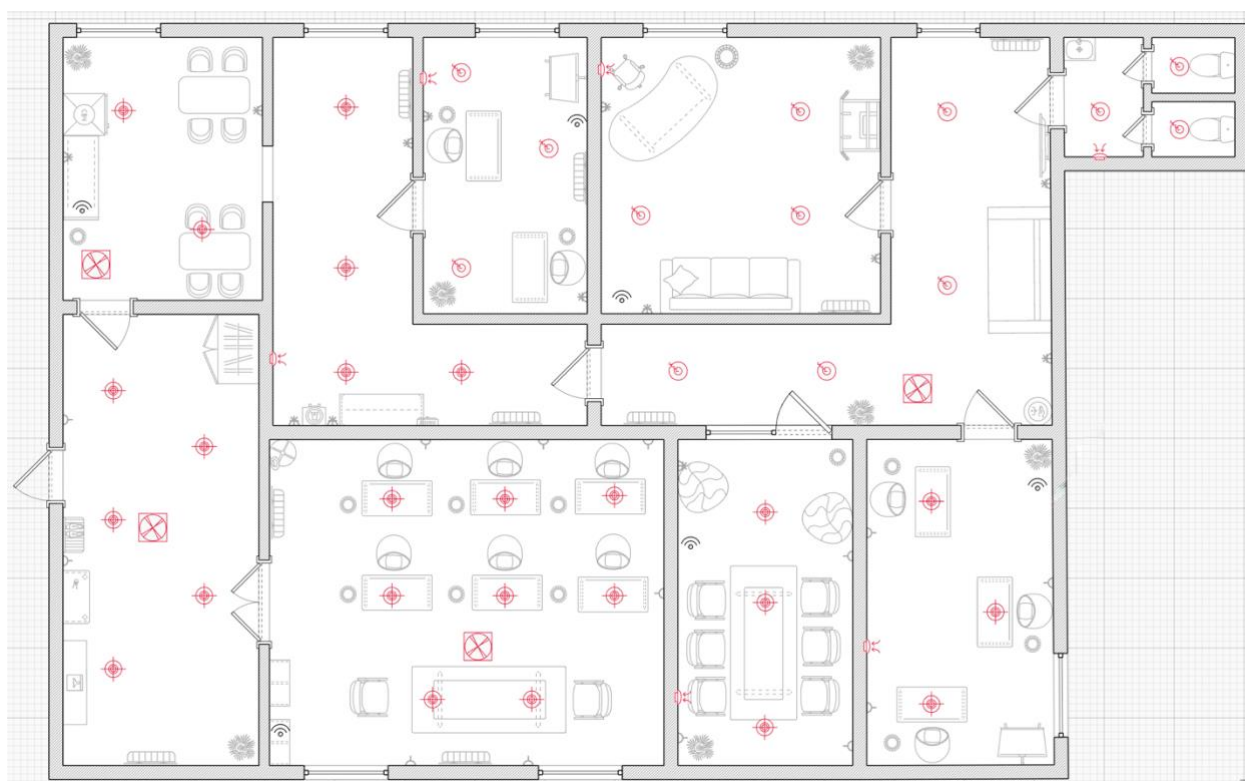
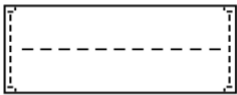
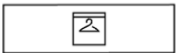















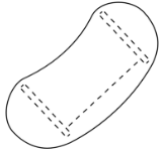
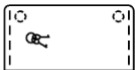
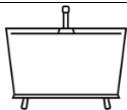







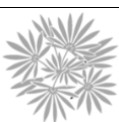





Рисунок 3 – План защищаемого помещения

Таблица 2 – Расшифровка обозначений

Обозначение	Описание
	Барный стол (для кофе-брейка)
	Вешалка для вещей

Обозначение	Описание
	Встраиваемый светильник
	Диван
	Информационная ТВ-панель
	Кондиционер
	Кресло директора
	Кресло сотрудника
	Кресло-мешок в переговорной
	Кулер
	Обувная полка
	Подвесной светильник
	Рабочий стол сотрудника
	Раковина
	Розетка
	Турник

Обозначение	Описание
	Станция обработки рук
	Унитаз
	Рабочий стол директора
	Столик в прихожей
	Интерактивный флипчарт
	Шкаф для одежды
	Щиток электрический
	Вентиляция потолочная
	Вентиляция настенная
	Диван в приемной
	Стул офисный
	Стол офисный
	Цветок напольный
	Мусорное ведро
	Батарея отопления

Обозначение	Описание
	Wi-fi роутер

3.2 Описание помещения

На рассматриваемом предприятии в рамках курсовой работы имеются следующие помещения, подлежащие инженерно-технической защите:

- кабинет директора (15,9 м²);
- переговорная комната (8,3 м²);
- кабинет 1 (16,2 м²);
- кабинет 2 (35 м²);
- кабинет 3 (16 м²);
- коридор 1 (14,0 м²);
- коридор-приемная (15 м²);
- главный холл (19,4 м²);
- туалетная комната (11,1 м²);
- кухня (12 м²).

Кабинет директора включает в себя: одно рабочее кресло, один рабочий стол, один диван для отдыха, три розетки, три подвесных светильника, одну дверь и одно окно.

Переговорная комната представляет из себя помещение без окон, с одной дверью, одним встроенным светильником, четырьмя розетками, переговорным столом, шестью стульями и двумя креслами-мешками.

Кабинет 1 содержит два рабочих места (два рабочих кресла и рабочих стола). Также присутствует две розетки, один кондиционер, интерактивный флипчарт, окно и три встроенных светильника.

Первый коридор соединяет холл, офис, а также зону работы директора и переговорную комнату. В нем содержится четыре встроенных светильника, один дверной проем, две двери, три окна, электрический щиток, две розетки и зона кофе-брейка (кулер, барный стол).

Коридор-приемная – это место ожидания приема у директора, которое содержит в себе 4 подвесных светильника, зону обработки рук, информационную ТВ-панель, две розетки, диван и одно окно.

Главный холл – место, через которое персонал попадает в офис компании, для входа в него есть одна дверь, также присутствует окно, кондиционер, две розетки, шкаф для вещей, вешалка для вещей, полочка для обуви и столик для прихожей.

Туалетная комната состоит из двух кабинок с унитазами и раковиной, также присутствует три подвесных светильника мощности.

Кабинет 2 представляет собой open-space пространство, в котором есть шесть одноместных столов, один двухместный стол, а также восемь офисных стульев и восемь светильников.

Кабинет 3 содержит три рабочих места (офисный стул, офисный стол), а также интерактивный флипчарт, три розетки и три светильника.

В кухне находится два обеденных стола, восемь стульев, а также колонна для хранения, поверхность для приготовления пищи, две розетки и СВЧ-печь.

Помещения находятся на 13 этаже бизнес-центра, окна помещения 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 выполнены из железобетона и имеют толщину не менее 13 см. Внутренние перегородки толщиной не менее 5 см выполнены из газобетона. Во всех помещениях присутствует настенная, или потолочная вентиляция.

3.3 Анализ возможных каналов утечки информации

Для того, чтобы определить состав средств защиты информации, которые необходимо установить, сначала нужно выделить возможные каналы утечки информации, которые делятся на следующие типы.

- акустические (акустоэлектрические) – утечка по такому каналу возможна, например, из-за закладных устройств, которые могут быть спрятаны в системах хранения, цветах или вентиляционных шахтах;
- вибрационные (виброакустические) – утечка через стекла, тонкие стены, батареи, любой твердый предмет, совершающий вибрации;
- электромагнитные (электрические) – утечки, связанные с электронными устройствами: АРМ, бытовая техника, а также розетки и проводка;
- визуально-оптические – утечка через открытые окна, прозрачные перегородки и незакрытые двери;

– материально-вещественные – хищение имущества, в рамках данной курсовой работы не рассматривается, так как подразумевается, что взаимодействие с физическими носителями информации строго регулируется политикой компании.

В таблице 3 представлены возможные каналы утечки информации для данного помещения, вероятные источники данных утечек, а также необходимые СЗИ, в соответствии с типом конфиденциальной информации – государственная тайна типа «секретно».

Таблица 3 – Каналы утечки и соответствующие СЗИ

Каналы	Источники	Пассивная защита	Активная защита
Акустические (акустоэлектрические)	Вентиляционная шахта, проводка, открытые двери и окна, тонкие стены	Звукоизоляция, фильтры для сетей электропитания	Устройства акустического зашумления
Вибрационные (виброакустические)	Твердые поверхности, тонкие стены	Изолирующие звук и вибрацию обшивки стен и пола	Устройства вибрационного зашумления
Электромагнитные (электрические)	Розетки, бытовая техника (СВЧ), АРМ, офисная техника (ТВ-панель, интерактивный флипчарт)	Фильтры для сетей электропитания, защитные экраны	Устройства электромагнитного зашумления
Визуально-оптические	Окна, двери, прозрачные перегородки	Жалюзи / шторы на окнах, тонирующие пленки на окна, доводчики на дверях	Бликующие устройства

Средства защиты информации можно разделить на активные и пассивные. К пассивным средствам технической защиты относятся разнообразные экранирующие устройства, маски различного назначения, разделительные устройства в сетях электроснабжения, защитные фильтры и другие средства. Основная цель пассивного подхода заключается в максимальном ослаблении сигнала от источника информации. Например, это может достигаться за счет применения звукопоглощающих материалов при отделке стен или экранирования технических устройств. В отличие от этого, активные технические средства защиты предоставляют устройства, способные создавать активные помехи (или их имитации) для средств технической разведки. Такие устройства могут также нарушать нормальное функционирование средств негласного сбора информации. Активные методы предупреждения утечки информации могут включать в себя обнаружение и нейтрализацию этих устройств.

4 АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ

4.1 Защита от утечки информации по акустическим и виброакустическим каналам

Принцип работы канала основан на способности звуковой волны вызывать механические колебания в препятствиях (в т. ч. воздухе), через которые она проходит при распространении. Эти колебания при помощи оборудования преобразуются в связный текст. Для снижения риска утечки информации по виброакустическому каналу требуется максимально ослабить акустический сигнал от источника звука, подающийся на коммуникации, служащие средой его распространения, где он может быть перехвачен. Пассивная защита акустического и виброакустического каналов утечки информации представляет собой:

- усиленные двери;
- тамбурное помещение перед переговорной;
- дополнительная отделка переговорной звукоизолирующими материалами.

Активная защита представляет собой систему виброакустического зашумления, т. е. необходимо сгенерировать в среде распространения сильный помеховый сигнал, который невозможно доступными злоумышленнику техническими средствами отфильтровать от информационного. Для защиты помещения для работы с государственной тайной уровня «секретно» рассматриваются технические средства активной защиты информации для объектов информатизации категории не ниже 1В. В таблице 4 приведен сравнительный анализ подходящих средств активной защиты помещений по виброакустическому каналу.

Таблица 4 – Перечень возможных средств виброакустической защиты

Модель	Цена, руб	Характеристики	Состав
ЛГШ-404	35 100 (минимальная комплектация)	Диапазон воспроизводимого шумового сигнала: 175–11200 Гц. До 40 преобразователей (до 20 на канал) Сертифицирован	Вибровозбудитель «ЛВП-10» - 1 шт. Акустический излучатель «ЛВП-2а» - 1 шт. Виброзэкран «ЛИСТ-1» - 1 шт. Размыкатель «ЛУР» - 1 шт.

Модель	Цена, руб	Характеристики	Состав
		<p>ФСТЭК России по 2 классу защиты</p> <p>Органы регулировки выходного шумового сигнала защищены от несанкционированного изменения и обнаружение несанкционированного доступа к ним</p> <p>Возможность регулировки уровня шумового сигнала и частотной коррекции сигнала для каждого выхода в отдельности, а также возможность дистанционного включения и выключения при помощи проводного пульта ДУ</p>	
Соната АВ-4Б	44 200	<p>Диапазон воспроизводимого шумового сигнала: 175–11200 Гц.</p> <p>Максимальное количество излучателей: 239 шт.</p> <p>Мониторинг с помощью СПО «Инспектор»</p> <p>Сертификат ФСТЭК</p> <p>Световая и звуковая индикация</p> <p>8 шагов регулировки уровней шума в каждой октавной полосе</p>	<p>БПУ «Соната-ИП4.3»</p> <p>Генераторы-акустоизлучатели «СА-4Б», «СА-4Б1»</p> <p>Генератор-вибровозбудитель «СВ-4Б»</p> <p>Размыкатель телефонной линии «Соната-ВК4.1»</p> <p>Размыкатель слаботочной линии «Соната-ВК4.2»</p> <p>Размыкатель линии Ethernet «Соната-ВК4.3»</p>

Модель	Цена, руб	Характеристики	Состав
		10 шагов регулировки интегральных уровней шума	Пульт управления «Соната-ДУ4.3» Блоки сопряжения с внешними устройствами «Соната-СК4.1», Соната-СК4.2 Техническое средство защиты речевой информации от утечки по оптико-электронному (лазерному) каналу «Соната-АВ4Л»: Генераторный блок «АВ-4Л» + вибровозбудитель «СП-4Л»
Камертон-5	46 000	Диапазон воспроизводимого шумового сигнала: 90–11200 Гц. 1 класс защиты Сертификация ФСТЭК Максимальное количество подключаемых модулей: ВД-80/ВД-120 = 4шт.; АС-Ш/АСП = 4шт Интерфейс управления: пленочная клавиатура + ЖК экран Индикация: световая, звуковая, ЖК	Виброизлучатель (ВД-80 и ВД-120): 2 шт. Акустоизлучатель (АС-Ш и АСП): 2 шт. Размыкатель локальной сети Р-8И: 2 шт. Распределительная коробка РК-1: 1 шт. Остальные компоненты докупаются отдельно
SEL SP-157 ШАГРЕНЬ	47 400	Диапазон воспроизводимого	Вибропреобразователь SEL SP-157VP

Модель	Цена, руб	Характеристики	Состав
		<p>шумового сигнала: 90–11200 Гц</p> <p>Максимальное количество излучателей: 64 шт</p> <p>Индикация: диодная + звуковая + ЖК</p> <p>Сертификат ФСТЭК 2 конструктивно-независимых выхода, по 4 канала на каждом</p> <p>Средство виброакустической защиты 1 класса комбинированного типа</p> <p>Жидкокристаллический двухстрочный экран.</p> <p>Защита паролем настроек системы.</p> <p>Непрерывный контроль состояния системы и каждого отдельного излучателя.</p> <p>Возможность регулировки уровня шума каждого излучателя.</p> <p>Возможность дистанционного управления (проводного и по ИК-каналу)</p>	<p>Вибропреобразователь SEL SP-157VPS</p> <p>Акустоизлучатель SEL SP-157AS</p> <p>Регулятор выносной SEL SP-157P</p> <p>Все устройства от 1 шт. – дополнительные устройства приобретаются отдельно</p>

По результатам анализа для установки была выбрана система Соната АВ-4Б, так как она имеет максимальное количество подключаемых устройств, что позволит сэкономить на закупках дополнительных источников электропитания, а также существенно упрощает

взаимодействие с системой. Кроме того, в данном решении наиболее простое расширение системы за счет специальных блоков сопряжения с внешними устройствами. К тому же Соната имеет достаточную комплектацию по сравнению с остальными вариантами и оптимальную цену.

В качестве средства пассивной защиты информации будут использованы укрепленные двери, отделанные звукоизолирующим материалом.

4.2 Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам

Пассивная защита сети 220 В заключается в использовании сетевых помехоподавляющих фильтров. Такие фильтры не пропускают информативные сигналы, возникающие при работе средств оргтехники. Причём, правильно установленный фильтр также защищает средства оргтехники от вредного влияния внешних помех. Следует учитывать, что для эффективной работы помехоподавляющих фильтров необходимо качественное заземление.

К активным методам защиты сети переменного тока (220 В) относятся методы, предусматривающие формирование специальными генераторами шумового сигнала, превосходящего по уровню сигналы устройств съёма информации или информативные сигналы. В таблице 5 представлены средства активной защиты от утечек по электрическому каналу.

Таблица 5 – Средства защиты информации от утечек по электрическому каналу

Модель	Цена	Особенности
Сетевой генератор шума «ЛГШ-221»	36 400	Сертификат ФСТЭК (2 класс защиты) Визуальная система индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа). Конструкция обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним. Спектральная плотность напряжения шумового сигнала в диапазоне частот 10–500 кГц: от 10 до 55 дБ

Модель	Цена	Особенности
		Спектральная плотность напряжения шумового сигнала в диапазоне частот 0,5–30 МГц: от 10 до 58 дБ Спектральная плотность напряжения шумового сигнала в диапазоне частот 30–400 МГц: от 10 до 47 дБ Диапазон регулировки уровня выходного шумового сигнала: от 20 дБ Рабочий диапазон частот: от 0,01 до 400 МГц Время непрерывной работы: ~ 12 ч Количество фаз: 1 Напряжение: 187–242 В Потребляемая мощность: 45 ВА (~ 36 Вт)
Генератор шума «Соната-РС3»	32 400	Рабочий диапазон частот: до 2 ГГц (как в модели РС2), регулировка уровня шума в 3 частотных полосах Количество фаз: 1 Ток нагрузки: сеть ~220 В +10%/-15%, 50 Гц Виды индикации: световая, звуковая (исправность / отказ) Потребляемая мощность: не более 10 Вт Продолжительность непрерывной работы: не менее 8 ч Потребляемая мощность: ~ 10 Вт
Генератор шума «SEL SP-44»	26 000	Сертификат ФСТЭК Управление: ручное, ДУ, RS-485 Уровень шума / затухания: 12–90 дБ Напряжение: 220 В ± 10% 50 Гц Рабочий диапазон частот: от 0,01 до 400 МГц Количество фаз: 1 Диапазон регулировки уровня шума в каждом поддиапазоне: от 20 дБ

Из всех представленных вариантов, был выбран генератор шума «Соната-РС3» по нескольким причинам:

– кратно больший диапазон охватываемых частот по сравнению с конкурентами;

- более простая интеграция с элементами компании «Соната», которые были выбраны ранее, что позволит сэкономить время на установке;
- упрощённое управление с помощью пультов ДУ;
- малая потребляемая мощность (10 Вт против 35 Вт).

В качестве средства пассивной защиты информации был выбран сетевой фильтр ЛФС-40-1Ф, который может быть использован в сетях до 40 А стоимостью 70 200 руб.

4.3 Защита от утечек посредством ПЭМИН

ПЭМИН – канал утечки информации через излучение элементов компьютера. Принимая и декодируя эти излучения, можно получить сведения обо всей информации, обрабатываемой в компьютере. Приемные электронные устройства устанавливаются в компьютер, параллельно подсоединяются к сетям электропитания или заземления, просто размещаются недалеко от работающего оборудования или перехватывают данные при помощи антенны. Чаще всего перехватываются и дешифровываются излучения, вырабатываемые:

- при выводе данных на монитор;
- при вводе информации с клавиатуры;
- при записи данных на жесткий диск или при их копировании со съемных носителей.

В качестве активной защиты также используются генераторы радиопомех, обеспечивающие защиту информации от утечки путем создания на границе контролируемой зоны широкополосной шумовой электромагнитной помехи, которая зашумляет побочные излучения защищаемого объекта. В таблице 6 представлен перечень подобных СЗИ.

Таблица 6 – Средства активной защиты от ПЭМИН

Модель	Цена	Особенности
«ЛГШ-501»	29 900	Соответствует требованиям документа «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, 2014) – по 2 классу защиты.

Модель	Цена	Особенности
		<p>Оснащено визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа), также счетчиком учета времени наработки.</p> <p>Конструкция обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним.</p> <p>Спектральная плотность напряжения шумового сигнала в диапазоне частот (мкВ/$\sqrt{\text{кГц}}$):</p> <ul style="list-style-type: none"> - от 0,01 до 30 МГц: от 10 до 58 дБ - от 30 до 400 МГц: от 10 до 47 дБ <p>Спектральная плотность напряженности электрического поля шума в диапазоне частот (мкВ/м*$\sqrt{\text{кГц}}$):</p> <ul style="list-style-type: none"> - от 0,01 до 0,8 МГц: от 20 до 58 дБ - от 0,8 до 1000 МГц: от 20 до 75 дБ - от 1000 до 1800 МГц: от 15 до 50 дБ <p>Спектральная плотность напряженности магнитного поля шума в диапазоне частот от 0,01 до 30 МГц: от 20 до 65 дБ</p> <p>Диапазон регулировки уровня: ~ 20 дБ</p> <p>Показатель электромагнитной совместимости: ~ 70 м</p> <p>Наработка до отказа: ~ 12 000 ч</p> <p>Срок службы: ~ 7 лет</p> <p>Ресурс: ~ 27 000 ч</p>
«ЛГШ-503»	44 200	Сопоставимые с «ЛГШ-501»

Модель	Цена	Особенности
Генератор шума «Покров»	32 800	Сертификат ФСТЭК (2 класс защиты) Вид индикации: светодиоды Управление: Ethernet Диапазон частот: 0,01–6000 МГц Электропитание выполнен в виде сетевого удлинителя с 5 розетками типа F Мощность: 15 Вт Наработка на отказ: 50000 ч Диапазон шумового сигнала: - для электрической составляющей: 0,01– 3000 МГц - для магнитной составляющей: 0,01–30 МГц - для электрических сигналов, наведённых на цепи электропитания: 0,01–400 МГц
«Соната-Р3.1»	33 120	Продолжительность непрерывной работы: не менее 8 ч Возможность: повышения уровня излучаемого электромагнитного поля шума в диапазоне частот 0,01...200 МГц за счет применения дополнительной антенны ВЕРР Мощность: 10 Вт Диапазон частот: соответствует требованиям документа "Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок" (ФСТЭК России, 2014) - по 2 классу защиты

В результате анализа к использованию был выбран генератор «ЛГШ-501», который в сравнении с остальными моделями имеет сравнимые характеристики за меньшие деньги,

таким образом, есть возможность сэкономить, не потеряв в качестве. В отличие от, например, генератора «Покров» у него больший диапазон частот, а также большая, по сравнению с «Соната-РЗ.1» мощность.

4.4 Защита от утечек информации по оптическим каналам

Для защиты от утечек по оптическим каналам, т. е. несанкционированной фото- и видеосъемки, или визуального «контакта» будут использованы защитные жалюзи (для окон), а также доводчики на дверях.

5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

В предыдущей главе были выбраны следующие средства защиты, которые планируются к установке в офисе компании «StopY»:

- виброакустическая защита «Соната АВ-4Б»;
- усиленные двери со звукоизолирующей прокладкой на металлическом каркасе: Experience 70;
- генератор шума «Соната-РС3»;
- сетевой фильтр ЛФС-40-1Ф;
- устройство активной защиты от ПЭМИН «ЛГШ-501»;
- защитные жалюзи;
- доводчики дверные.

Далее будет определено необходимое количество каждого из средств защиты информации. Согласно информации на официальном веб-сайте производителя НПО «АННА» для системы виброакустической защиты, предварительную оценку необходимого количества вибровозбудителей «Соната СВ-4Б» можно провести, руководствуясь следующими стандартами:

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

Предварительная оценка необходимого количества акустоизлучателей «Соната СВ-4Б» может быть выполнена из следующих норм:

- один на каждый вентиляционный канал или дверной тамбур;
- один на каждые 8–12 м³ надпотолочного пространства или других пустот.

В свою очередь, усиленные двери будут установлены на помещения, в которых происходит обсуждение конфиденциальной информации, доводчики будут установлены на всех дверях. Жалюзи планируются к установке на всех окнах, исходя из максимального потребления электричества около 15 кВт потребуется два сетевых фильтра. Также будут установлены размыкатели линии Ethernet на роутеры, через которые осуществляется доступ

в интернет. Размыкатель слаботочной линии будет размещен в условном месте нахождения центра управления ТСО. Средства защиты от ПЭМИН будут установлены в помещения, где на вычислительных устройствах обрабатывается конфиденциальная информация. В таблице 7 представлен перечень необходимых СЗИ и общая стоимость системы.

Таблица 7 – Смета по СЗИ

Средство защиты	Цена, руб.	Количество, шт.	Итоговая стоимость, руб
Генератор-акустоизлучатель «Соната-СА-4Б»	7 440	22	163 680
Генератор-вибровозбудитель «Соната-СВ-4Б»	7 440	70	520 800
Система «Соната АВ-4Б»	44 200	1	44 200
Сетевой фильтр «ЛФС-40-1Ф»	70 200	2	140 400
Генератор шума «ЛГШ-501»	29 900	4	119 600
Сетевой генератор шума «Соната-РС3»	32 400	5	162 000
Размыкатель Ethernet «Соната-ВК4.3»	6 000	6	36 000
Размыкатель слаботочной линии «Соната-ВК 4.2»	6 000	1	6 000
Доводчик дверной «ISP 440”	1 640	9	14 760
Двери «Experience 70»	78 800	5	394 000
Рулонные жалюзи BlackOut	1900 руб/м ²	12,6	23 940
Итого			1 625 380

На рисунке 4 представлена схема расположения активных и пассивных СЗИ.

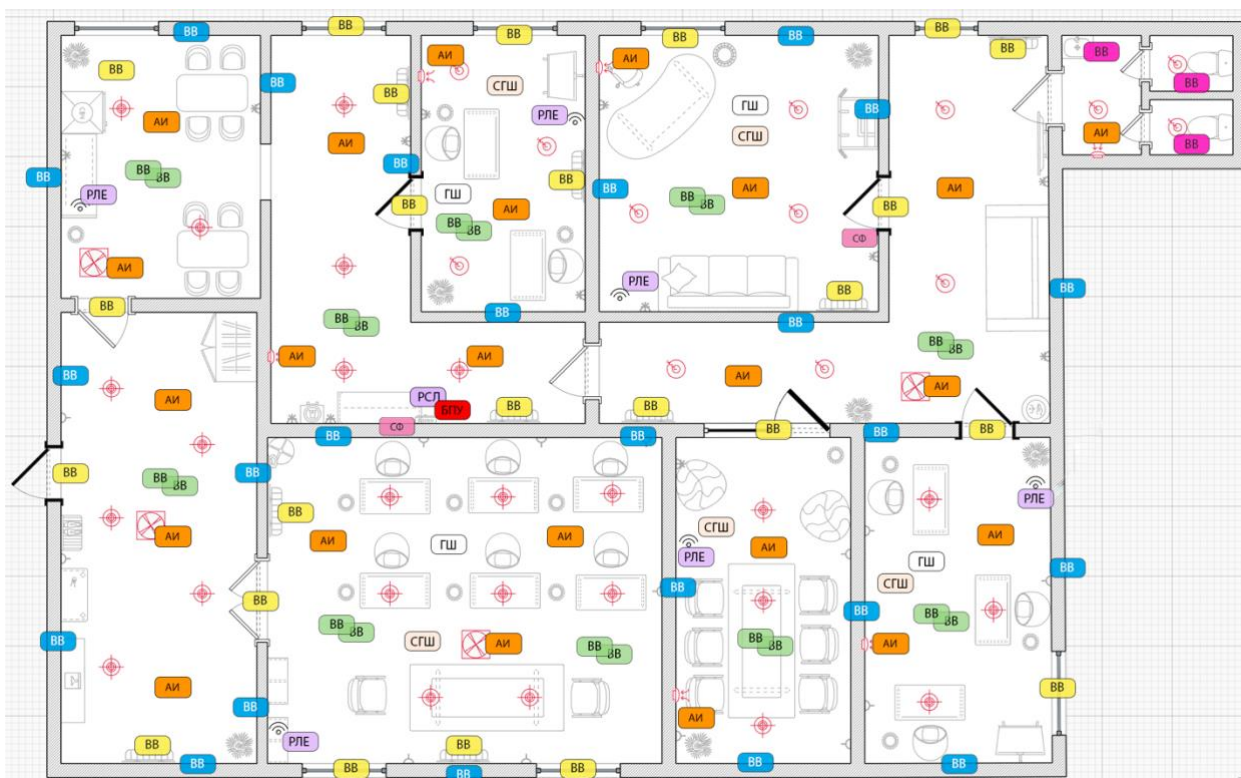





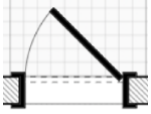



Рисунок 4 – Схема расположения СЗИ

В таблице 8 приводится расшифровка условных обозначений схемы расстановки устройств.

Таблица 8 – Условные обозначения на схеме

Условное обозначение	Средство защиты	Количество, шт.
	Блок электропитания и управления «Соната-ИП4.3»	1
	Генератор-акустоизлучатель «Соната СА-4Б»	23
	Генератор-вибровозбудитель «Соната СВ-4Б» (стены)	24
	Генератор-вибровозбудитель «Соната СВ-4Б» (потолок, пол)	20
	Генератор-вибровозбудитель «Соната СВ-4Б» (окна, двери, батареи)	24
	Генератор-вибровозбудитель «Соната СВ-4Б» (трубопровод)	3

Условное обозначение	Средство защиты	Количество, шт.
	Размыкатель линии «Ethernet» «Соната-ВК4.3»	6
	Размыкатель слаботочной линии «Соната-ВК4.2»	1
	Сетевой генератор шума «Соната-РС3»	5
	Генератор шума «ЛГШ-501»	4
	Сетевой фильтр «ЛФС-40-1Ф»	2
	Усиленные звукоизолирующие двери «Experience 70»	5
	Жалюзи BlackOut	8

ЗАКЛЮЧЕНИЕ

В рамках данной курсовой работы были выполнены такие задачи, как определение структуры и информационных потоков компании, чья деятельность связана с обработкой данных, составляющих государственную тайну уровня "секретно". Также был проведён анализ помещения, который позволил выявить возможные каналы утечки информации. После анализа рынка технических СЗИ была сформована смета, включающая устройства, рекомендованные к установке на предприятии. Таким образом, была спроектирована комплексная система защиты, способная минимизировать утечки по возможным каналам.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Кармановский Н. С., Михайличенко О. В., Савков С. В. Организационно-правовое и методическое обеспечение информационной безопасности / Учебное пособие. – СПб: НИУ ИТМО, 2013. – 148 с.
2. Международный научный журнал «Символ науки» №12–1/2016: «Исследование информационных потоков в логистической системе»: сайт. – URL <https://cyberleninka.ru/article/n/issledovanie-informatsionnyh-potokov-v-logisticheskoy-sisteme/viewer> (дата обращения: 16.12.2023). – Текст: электронный.
3. 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".