

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

Факультет безопасности информационных технологий

Дисциплина:

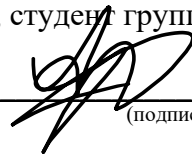
«Инженерно-технические средства защиты информации»

КУРСОВОЙ ПРОЕКТ

«Проектирование системы защиты от утечки информации по различным каналам»

Выполнили:

Алексеевко Арсений Антонович, студент группы N34471



(подпись)

Проверил:

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

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023 г.

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

Студент	Алексеев Арсений Антонович (Фамилия И.О.)
Факультет	Безопасность информационных технологий
Группа	N34471
Направление (специальность)	10.03.01 (Технологии защиты информации 2019)
Руководитель	Попов Илья Юрьевич (Фамилия И.О.)
Должность, ученое звание, степень	к.т.н., доцент ФБИТ
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование системы защиты от утечки информации по различным каналам
Задание	Проектирование системы защиты от утечки информации по различным каналам

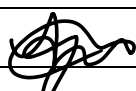
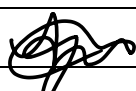
Краткие методические указания

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

1. Введение.
2. Анализ технических каналов утечки информации.
3. Руководящие документы
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	 (Подпись, дата)

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

Студент Алексеев Арсений Антонович
(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34471

Направление (специальность) 10.03.01 (Технологии защиты информации 2019)

Руководитель Попов Илья Юрьевич
(Фамилия И.О.)


Должность, ученое звание, степень к. т. н., доцент ФБИТ

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.	Разработка и утверждение задания и календарного плана на курсовую работу	13.11.2022	13.11.2022	
2.	Анализ теоретической составляющей	14.11.2022	14.11.2022	
3.	Разработка комплекса инженерно-технической защиты информации в заданном помещении	20.11.2022	20.11.2022	
4.	Представление выполненной курсовой работы	20.12.2022	20.12.2022	

Руководитель _____
(Подпись, дата)

Студент  _____
(Подпись, дата)

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

Студент	Алексеев Арсений Антонович (Фамилия И.О)
Факультет	Безопасность информационных технологий
Группа	N34471
Направление (специальность)	10.03.01 (Технологии защиты информации 2019)
Руководитель	Попов Илья Юрьевич (Фамилия И.О)
Должность, ученое звание, степень	к. т. н., доцент ФБИТ
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 Целью работы является повышение защищенности рассматриваемого помещения. Задачами является анализ защищаемого помещения, оценка каналов утечки информации и выбор мер пассивной и активной защиты информации.

2. Характер работы Конструирование

3. Содержание работы

1) Введение.

2) Анализ технических каналов утечки информации

3) Руководящие документы

4) Анализ защищаемых помещений



5) Анализ рынка технических средств

6) Описание расстановки технических средств

7) Заключение

8) Список литературы

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

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

СОДЕРЖАНИЕ

Введение	5
1 Анализ защищаемой организации.....	6
1.1 Общее описание.....	6
1.2 Информационные потоки	6
1.3 Защищаемое помещение	8
1.4 Качественная оценка угроз	13
1.4.1 Оптический канал	13
1.4.2 Акустический и виброакустический каналы.....	13
1.4.3 Электромагнитный канал.....	13
1.4.4 Закладные устройства.....	14
1.4.5 Материально-вещественный канал	14
2 Перечень руководящих документов	15
3 Выбор средств защиты информации	16
3.1 Оптический канал.....	16
3.1.1 Шторы	16
3.1.2 Доводчики на двери.....	16
3.2 Акустический и виброакустический канал	17
3.2.1 Излучатели виброакустических помех	17
3.2.2 Пассивная звукоизоляция	18
3.3 Электромагнитный канал.....	19
3.3.1 ПЭВМ.....	19
3.3.2 Защита от ПЭМИН	20
3.4 Защита от закладных устройств	21
4 Размещение средств защиты.....	23
Заключение.....	26
Список использованных источников.....	27

ВВЕДЕНИЕ

Информационная безопасность занимает ключевую позицию в современном мире, где защита приватности и неприкосновенности данных является критически важной для бизнес-операций. Это исследование сосредоточено на разработке комплексного подхода к инженерно-техническому обеспечению безопасности информации, особенно для данных, классифицированных как государственная тайна с уровнем "секретно" в рамках информационных систем.

Основной упор делается на анализ возможных технических каналов утечки информации, представление списка нормативных документов и тщательный осмотр помещений, требующих защиты. Это позволяет выявить возможные угрозы и формулировать специфические требования к средствам защиты информации. Анализ рынка технических средств защиты информации разных категорий, а также разработка планов размещения этих устройств в защищаемых зонах являются важными шагами в создании эффективной системы безопасности.

Эти меры направлены не только на предотвращение несанкционированного доступа, но и на снижение рисков потери, утечки или искажения критически важной информации. В дополнение к техническим аспектам, исследование также включает анализ управленческих процессов и документации, подчеркивая комплексный подход к обеспечению информационной безопасности.

1 АНАЛИЗ ЗАЩИЩАЕМОЙ ОРГАНИЗАЦИИ

1.1 Общее описание

Наименование организации: ООО "Araka"

Область деятельности: разработка новых технологий в сфере биоинженерии.

Организация "Araka" специализируется на B2B-сегменте, предлагая услуги по разработке передовых технологий в области биоинженерии. Компания объединяет специалистов с инновационным и творческим мышлением, что позволяет реализовывать уникальные проекты и решения, находящиеся на стыке биологии, медицины и инженерии.

С учетом растущего интереса государственных структур к передовым технологиям в области биоинженерии, руководство "Araka" решило расширить свою деятельность, включая B2G-проекты, особенно в сегменте, касающемся разработки и исследования биотехнологических решений, затрагивающих аспекты государственной тайны уровня "секретно". Это включает в себя установку высокотехнологичных систем безопасности для защиты чувствительных данных и интеллектуальной собственности.

1.2 Информационные потоки

Организационная структура и информационные потоки:

Генеральный директор является центральным узлом организации, к которому напрямую подсоединены руководители ключевых отделов: отдел информационной безопасности (ИБ), отдел разработки, финансовый отдел и отдел кадров.

Отдел информационной безопасности обеспечивает защиту информации и имеет дело с конфиденциальными данными. Работники ИБ общаются с руководителем отдела и генеральным директором.

Отдел разработки разбит на малые группы, каждая из которых занимается отдельным проектом. Потоки информации движутся от генерального директора к руководителю отдела разработки и далее к каждой проектной группе.

Финансовый отдел управляет финансовыми потоками и взаимодействует с внешними организациями, такими как банки, налоговая служба, пенсионный фонд, военкомат и т.д.

Информация о финансах течет от и к генеральному директору, а также во внешние организации.

Отдел кадров отвечает за найм и управление персоналом. Информация о сотрудниках течет от руководителя отдела к генеральному директору.

Работа с государственной тайной:

Менеджеры по продажам и в отделе разработки являются ключевыми участниками в работе с информацией, составляющей государственную тайну. Они действуют как посредники между заказчиками и проектными группами, уменьшая тем самым распространение конфиденциальной информации и улучшая взаимопонимание сторон.

Отдел информационной безопасности обеспечивает защиту информации, включая государственную тайну, через разработку и внедрение соответствующих мер и процедур.

Финансовый отдел имеет ограниченный доступ к конфиденциальной информации, связанной с финансированием проектов, которые включают работу с государственной тайной.

Информационные потоки:

Государственный заказ: Обсуждение заказа и предоставление продукта на тестирование идут через менеджера по продажам и отдел разработки, где информация о статусе тестирования обратно сообщается менеджеру.

Внутренняя работа компании: Финансовый отдел предоставляет смету на разработку и выделяет средства на разработку. Отдел кадров отвечает за найм сотрудников, а отдел информационной безопасности — за обеспечение безопасности всех отделов.

В данной структуре информация строго контролируется и передается по необходимости, с особым вниманием к сведениям, составляющим государственную тайну.

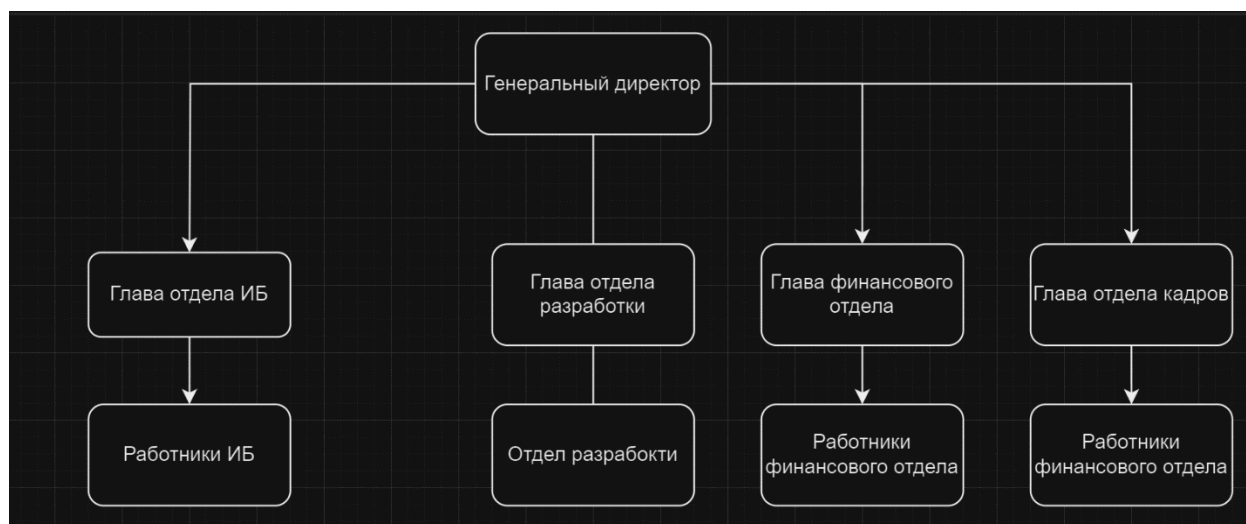


Рисунок 1 – Структура организации

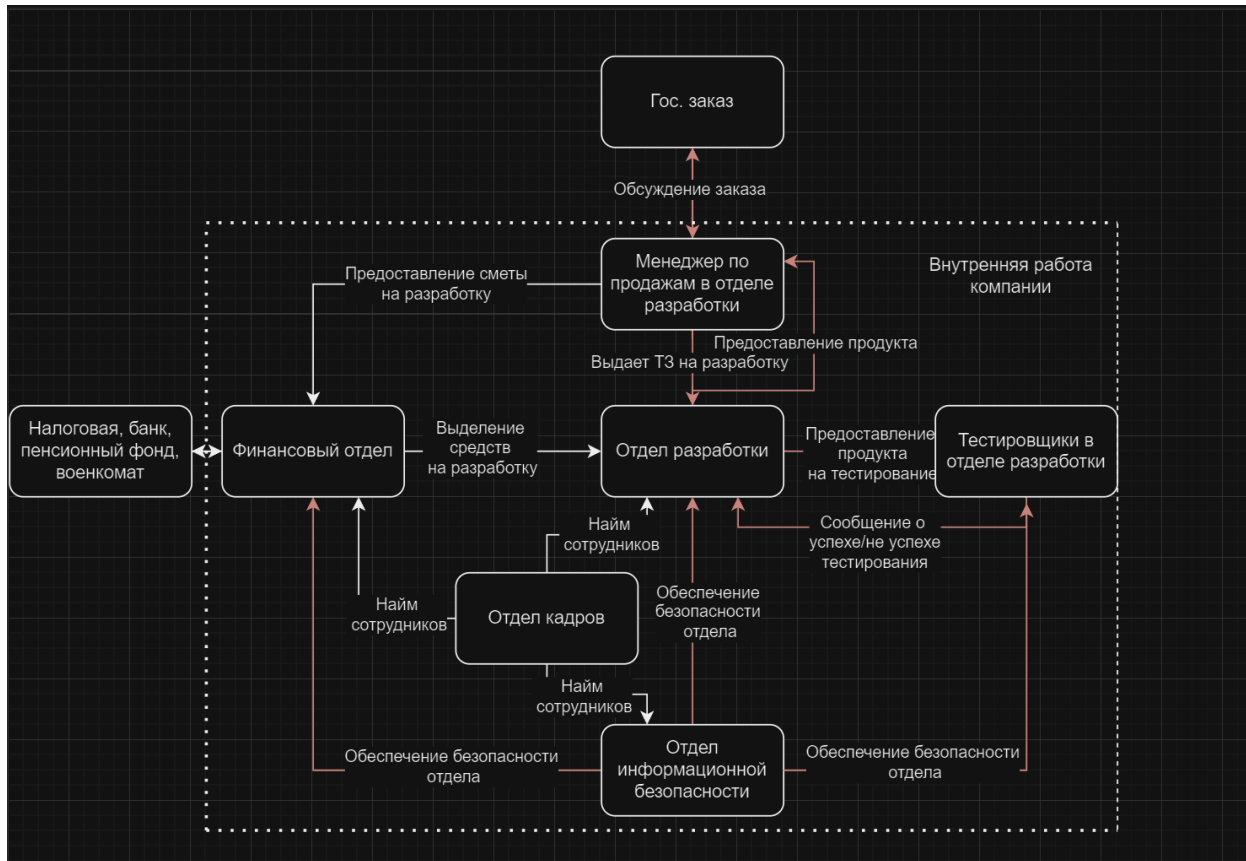


Рисунок 2 – информационные потоки организации

1.3 Защищаемое помещение


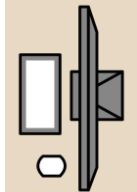


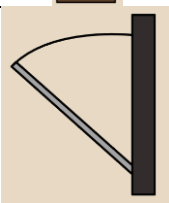


Офис организации, располагается на 14 этаже Бизнес-центра. Напротив северных и южных окон, располагаются другие офисные здания. Стены сделаны из железобетона толщиной не менее 10 см. Над и под офисом расположены другие арендуемые офисы, футкорд и спортзал соответственно.

Доступ в офис контролируется через продвинутую систему управления доступом, что гарантирует безопасность и конфиденциальность проводимых работ. В помещение могут войти только сотрудники компании, что обеспечивает дополнительный уровень защиты информации.

В офисе предусмотрены следующие функциональные зоны:

Open-space зона (позиция 1 на плане) пролегает через весь офис, обеспечивая легкий доступ ко всем рабочим зонам, а также является местом для работы отдела разработки.

Таблица 1 – описание элементов, изображенных на плане.

Фото	Наименование
	Стул
	АРМ
	Стол
	Шкаф
	Дверь
	Сервер
	Окно

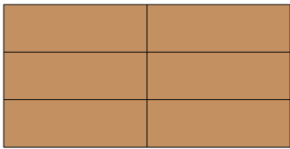
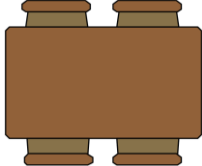
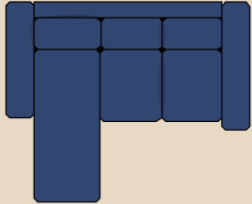

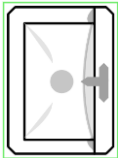
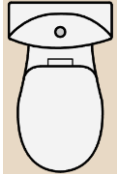


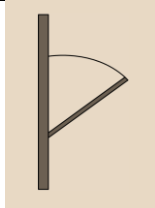
	Стол для переговоров
	Обеденный стол
	Диван
	Кухня
	Раковина
	Унитаз
	Большое окно
	Диван
	Входная дверь

Таблица 2 – Список комнат и их площадь

Номер комнаты	Название комнаты	Площадь комнаты, м2
1	Орг-спасе зона	106
2	Переговорная	37,4
3	Комната отдыха	27,6
4	Туалет	11,9
5	Кабинет генерального директора	21,5

6	Кабинет HR-отдела	12,5
7	Кабинет финансового отдела	12,5
8	Кабинет отдела ИБ	14,1
9	Серверная	6,26

Зона open-space содержит 40 розеток, двадцать рабочих мест, четыре окна с батареями.

В каждом туалете имеется унитаз и раковина.

В серверной находятся четыре серверных стойки, четыре розетки, выход вентиляции. Серверная отделена от зоны open-space стеной и дверью.

Переговорная содержит четыре розетки, маркерную доску, офисные кресла, выход вентиляции.

В кабинетах HR и финансового отдела находиться шесть розеток, 3 АРМ, окно с батареей отопления, выход вентиляции в каждой из комнат.

В кабинете директора находится одно рабочее место, одно окно с батареей отопления, сейф, шкаф, диван.

В отделе ИБ находиться шесть розеток, 3 АРМ, выход вентиляции.

В комнате отдыха находиться кухня, диван, 2 обеденных стола, телевизор и окно с батареей.

1.4 Качественная оценка угроз

Для обеспечения защиты информации в организации, работающей с государственной тайной, необходимо учитывать различные каналы возможной утечки информации. Приведем подробный анализ уязвимостей:

1.4.1 Оптический канал

Офисные помещения с видом на улицу и окна, выходящие на соседние здания, могут быть уязвимы для наблюдения через оптические приборы. Это включает в себя возможность использования высокотехнологичных телескопов и биноклей для наблюдения за действиями сотрудников внутри помещений, что может привести к утечке визуальной информации.

Для предотвращения этого рода утечек информации, окна должны быть оборудованы специальными шторами или светонепроницаемым стеклом. Также возможно использование антиотражающего покрытия на стеклах, чтобы затруднить использование лазерных микрофонов для считывания вибраций стекол.

1.4.2 Акустический и виброакустический каналы

Акустическая утечка может происходить через окна, стены и системы вентиляции. Специализированные устройства, такие как направленные микрофоны, могут использоваться для прослушивания из внешних источников. Чтобы минимизировать риск, необходимо применять звукоизолирующие материалы и антивибрационные системы, а также регулярные проверки вентиляционных систем на наличие несанкционированного проникновения.

Отопительные системы также могут стать источником утечки акустической информации. Для снижения риска рекомендуется использование теплоизоляционных материалов, а также регулярный осмотр и техническое обслуживание системы отопления.

1.4.3 Электромагнитный канал

Компьютеры и другое электронное оборудование излучают электромагнитные поля, которые могут быть перехвачены специализированным оборудованием. Использование экранированных кабелей, фильтров и защищенных линий электропередач может существенно снизить риск утечки через этот канал.

Ethernet-кабели и другие проводные сети должны быть защищены через использование шифрования и физической защиты кабельных каналов, чтобы предотвратить возможность подключения к сети несанкционированных устройств.

1.4.4 Закладные устройства

Помещение может содержать множество потенциальных укрытий для закладных устройств. Регулярные инспекции и использование технических средств обнаружения, включая нелинейные локаторы и специализированные сканеры, позволят своевременно обнаружить и нейтрализовать любые скрытые устройства.

1.4.5 Материально-вещественный канал

Этот канал связан с физическим перемещением материалов, содержащих конфиденциальную информацию. Хотя он не рассматривается в рамках данного анализа, важно обеспечить должный уровень контроля за материалами и документацией, а также использование средств уничтожения информации (измельчителей, дегауссеров) для предотвращения утечки через этот канал.

2 ПЕРЕЧЕНЬ РУКОВОДЯЩИХ ДОКУМЕНТОВ

При разработке комплекса защиты информации будем руководствоваться следующими документами:

- Закон “О государственной тайне”;
- Федеральный Закон №149 - “Об информации, информационных технологиях и защите информации”;
- Указ Президента РФ от 30.11.1995 №1203 "Об утверждении Перечня сведений, отнесенных к государственной тайне";
- Постановление Правительства РФ от 15 апреля 1995 г. №333 “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 06.02.2010 N 63 (ред. от 29.10.2022) "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне";
- Постановление Правительства РФ от 26 июня 1995 г, №608 “О сертификации средств защиты информации”;
- ГОСТ Р ИСО/МЭК 27001-2021 “Системы менеджмента информационной безопасности. Требования”;
- ГОСТ Р ИСО/МЭК 27002-2021 “Свод норм и правил менеджмента информационной безопасности”;
- ГОСТ Р ИСО/МЭК 27033-2011 “Безопасность сетей”.

3 ВЫБОР СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

3.1 Оптический канал

3.1.1 Шторы

Таблица 3 – Расчет стоимости установки штор

Наименование товара / работы / услуги	Количество, шт.	Цена, руб. (ориентировочно)	Сумма, руб. (ориентировочно)
Bali Blackout Roller Shades	10	5 700	57 000
Установка	1	3 000	3 000
ИТОГО по варианту 1			60 000
Home Decorators Collection Blackout Roller Shade	10	5 200	52 000
Установка	1	3 000	3 000
ИТОГО по варианту 2			55 000

Вариант 1: **Bali Blackout Roller Shades** получили множество положительных отзывов от покупателей за их надежность и качество затемнения, что делает их подходящим выбором для офисных помещений, требующих уровня конфиденциальности. Цена за штуку ориентировочно составляет 5 700 рублей, что приводит к общей стоимости в 60 000 рублей включая установку.

Вариант 2: **Home Decorators Collection Blackout Roller Shade** также являются конкурентоспособным выбором, предлагая хорошее соотношение цены и качества с ценой около 5 200 рублей за штуку. Общая стоимость с установкой будет приблизительно 55 000 рублей.

Исходя из ценового анализа и учета положительных отзывов, вариант 1 (Bali Blackout Roller Shades) может быть предпочтительнее, несмотря на несколько более высокую стоимость, т.к. отзывы покупателей подчеркивают их высокое качество и надежность, что является критически важным для обеспечения конфиденциальности в офисе.

3.1.2 Доводчики на двери

Таблица 4 – Расчет стоимости установки доводчиков

Наименование товара / работы / услуги	Количество, шт.	Цена, руб.	Сумма, руб.
Доводчик дверной Dormakaba	10	4 000	40 000
Доводчик дверной Geze	10	6 000	60 000

Доводчик дверной NORA-M	10	3 145	31 450
Установка	1	5 000	5 000
ИТОГО Dormakaba			45 000
ИТОГО Geze			65 000
ИТОГО NORA-M			36 450

Доводчик дверной Dormakaba - известный бренд, предлагает качественные модели, цены варьируются от 483 до 44 505 рублей в зависимости от модели и характеристик.

Доводчик дверной Geze - другой немецкий бренд, известный своими надежными решениями в области доводчиков, цены на сайте не указаны, но известно, что они обычно находятся в высоком ценовом сегменте.

Доводчик дверной NORA-M - отечественный производитель, предлагает морозостойкие и противопожарные модели, цена одной из моделей - 3 144.9 рубля.

Нам важен баланс цены и качества, поэтому мы рассматриваем NORA-M.

3.2 Акустический и виброакустический канал

3.2.1 Излучатели виброакустических помех

Таблица 5 – Сравнение излучателей виброакустических помех

Наименование	Возможности	Стоимость, руб.
ЛГШ-404	<ul style="list-style-type: none"> Учет времени работы Контроль и защита органов регулировки уровня выходного шумового сигнала Проводное дистанционное управление и контроль Диапазон частот: 175 - 11 200 Гц Круглосуточная непрерывная работа Средний срок службы: 7 лет 	136 000
Генератор виброакустических помех КЕДР-А	<ul style="list-style-type: none"> Цифровое автономное (защищённое паролем) управление и контроль за настройками системы с выводом информации на встроенный жидкокристаллический экран. встроенного счётчика суммарного времени наработки генерации помех с регистрацией значений в защищённой энергонезависимой памяти. Система контроля и индикации нормального режима работы или возникновения аварийной ситуации в элементах системы (визуальная, звуковая) 	28 000

	<p>позволяет получать информацию о функционировании системы в режиме реального времени.</p> <ul style="list-style-type: none"> Наличие 3-х статистически независимых каналов генерации «белого» шума (два виброакустических и один акустический) и наличие 7-полосного октавного эквалайзера в каждом канале. Наличие канала виброакустического зашумления корпуса генератора, для предотвращения утечки информации за счет микрофонного эффекта 	
SI-3002	<ul style="list-style-type: none"> Автоматическое программирование 	29 000

В качестве приоритетной системы был выбран генератор виброакустических помех КЕДР-А

Особенности: Цифровое автономное управление, встроенный жидкокристаллический экран, счётчик суммарного времени работы, система контроля и индикации, три независимых канала генерации шума, 7-полосный октавный эквалайзер, канал зашумления корпуса генератора.

Преимущества: Обеспечивает высокий уровень безопасности и контроля, multifunctionality и подходит для защиты от утечки информации.

3.2.2 Пассивная звукоизоляция

Многие компании предлагают услугу отделки помещения пассивной звукоизоляцией. Пассивная звукоизоляция необходима в двух помещениях - комнате генерального директора и переговорной. Расчет стоимости представлен в таблице 6.

Таблица 6 – Расчет стоимости пассивной звукоизоляции

Наименование	Площадь, м ²	Цена, руб./м ²	Сумма, руб.
Система звукоизоляции пола (плавающая стяжка) «Стандарт 1»	56	1 140	63 840
Каркасная система звукоизоляции потолка «Базовая»	56	4 780	267 680

Каркасная система звуко- изоляции стен «Базовая»	56	4 245	237 720
Наименование	Количество, шт.	Цена, руб.	Сумма, руб.
Дверь звукоизоляционная Rw 42dB Prima M900	2	34 050	68 100
ИТОГО			637 340

3.3 Электромагнитный канал

3.3.1 ПЭВМ

Таблица 7 – Сравнение комплексов ПЭВМ

Наименование	Возможности	Количество, шт.	Стоимость, руб.
ПЭВМ на Core-i7	Процессор: intel i7 2.90 ГГц Память: 32 GB Жесткий диск: SSD 960 Gb Операционная система: Windows 10 / Linux SE Монитор: Dell 23.8 Дополнительное: высокоскоростной интернет, продвинутое программное обеспечение для разработки МДЗ: ПАК «Соболь 4» / Dallas Lock СЗИ от НСД: Secret net Studio 8 / Dallas Lock Антивирус (ФСТЭК): Dr.web	20	220 000
Офисная ПЭВМ на Core-i5	Процессор: intel i5 2.90 ГГц Память: 16 GB Жесткий диск: SSD 480 Gb Операционная система: Windows 10 Монитор: Dell 23.8 Дополнительное: офисный пакет программ, антивирус МДЗ: ПАК «Соболь 4» / Dallas Lock СЗИ от НСД: Secret net Studio 8 / Dallas Lock Антивирус (ФСТЭК): Dr.web	4	160 000
Бюджетная ПЭВМ для на Core-i3	Процессор: intel i3 3.3 ГГц Память: 8 GB Жесткий диск: HDD 500 Gb Операционная система: Windows 10	6	120 000

	Монитор: 21.5 Дополнительное: базовый пакет офисных программ, антивирус МДЗ: ПАК «Соболь 4» / Dallas Lock СЗИ от НСД: Secret net Studio 8 / Dallas Lock Антивирус (ФСТЭК): Dr.web		
--	---	--	--

Идеальный выбор для разработки ПО: ПЭВМ на Core-i7 с высокой производительностью и большим объемом оперативной и дисковой памяти для выполнения ресурсоемких задач и запуска виртуальных машин. Она будет предоставлена разработчикам в Open-space

Идеальный выбор для офисной работы: Офисная ПЭВМ на Core-i5 предоставляет хорошее соотношение цены и производительности, обеспечивая достаточную мощность для выполнения повседневных офисных задач и некоторых специализированных программ. Будет предоставлена работникам ИБ и генеральному директору компании.

Бюджетный вариант: ПЭВМ на Core-i3 подойдет для несложных офисных задач, таких как работа с текстовыми документами, таблицами, электронной почтой и интернет-серфингом. Жесткий диск HDD предложит достаточное пространство для хранения документов, но будет медленнее SSD. Будет предоставлено отделу финансов и HR-отделу.

3.3.2 Защита от ПЭМИН

Таблица 8 – Сравнение средств активной защиты от ПЭМИН

Устройство	Характеристики	Диапазон частот	Цена (руб.)
------------	----------------	-----------------	-------------

Генератор шума ПУЛЬСАР	<p>Имеет диапазоны частот от 10 кГц до 6 ГГц.</p> <p>Оборудован 2 съемными антеннами, счетчиком наработки.</p> <p>Индикаторы нормального режима работы (диод) и аварийного режима (свет и звук).</p> <p>Имеет защиту регулятора уровня выходного шумового сигнала от нелегального доступа (и сигнализирует об этом)</p> <p>Соответствует требованиям документа «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России) – по 2 классу защиты.</p> <p>Можно применять в выделенных помещениях до 2 категории включительно.</p>	10 кГц – 6 ГГц	24 525
ГЕНЕРАТОР ШУМА ЛГШ-501	<p>Оснащено визуальной системой индикации нормального режима работы и визуально звуковой системой индикации аварийного режима.</p> <p>Оснащено счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы Изделия в режиме формирования маскирующих помех.</p> <p>Обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним.</p> <p>Имеет возможность подключения проводного пульта дистанционного управления.</p>	-	29 900
Генератор шума ЛГШ-503	<p>Генератор белого шума ЛГШ-503 соответствует требованиям документа «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, 2014) – по 2 классу защиты.</p>	10 кГц – 1800 МГц	44 200

После проведенного анализа был выбран генератор шума ГЕНЕРАТОР ШУМА ЛГШ- 501 из-за соотношения цены и качество и хорошими отзывами потребителей.






3.4 Защита от закладных устройств





Таблица 8 - Сравнение комплексов для обнаружения закладных устройств



Наименование	Возможности	Стоимость, руб.
Подавитель "UltraSonic-ШАЙБА-50-GSM"	<p>Круговое распространение ультразвуковых помех на 360 градусов. Благодаря распространению ультразвукового излучения во все стороны достигается максимальный эффект защиты от аудиозаписи.</p> <p>Ультразвуковая помеха. Подавитель оснащен 48 ультразвуковыми излучателями, которые напрямую воздействуют на мембрану микрофона записывающего устройства, что не позволяет произвести запись разговора.</p> <p>Блокировка 10-ти частот беспроводной связи.</p>	52 000
Блокиратор "Завеса-12СТН"	<p>Блокируемые стандарты сотовой связи:</p> <ul style="list-style-type: none"> • GSM 900 / 1800; E-GSM; • 3G; 3G+; • 4G+; 4G-LTE; 4G-LTE 800; • DECT; • UMTS; • WCDMA. <p>Особенности:</p> <p>Блокиратор подавляет 14 стандартов связи, которые используются с целью организации каналов утечки информации, спутниковым слежением за автомобилями и грузами, имеет высокую выходную мощность и рассчитан на круглосуточную эксплуатацию.</p> <p>Блокиратор оснащен защищенными от внешних воздействий, встроенными в корпус высокоэффективными малогабаритными антеннами.</p> <p>Блокиратор рассчитан на работу от бортовой сети автомобиля (12 Вольт) или на работу от сети 220 Вольт.</p> <p>Завеса 12 СТН имеет профессиональную надежность и рассчитана на непрерывную длительную работу. Допускается круглосуточная эксплуатация блокиратора при соблюдении мер температурного режима и вентиляции.</p> <p>Гарантийный срок эксплуатации 1 год.</p>	111 409

Было выбрано средство подавления сигналов Блокиратор "Завеса 12СТН" – Из-за длительности работы и надежности

4 РАЗМЕЩЕНИЕ СРЕДСТВ ЗАЩИТЫ

Средство защиты	Установка	Условное обозначение	Количество
Шторы Bali Blackout Roller Shades	У окон		8
Доводчики на двери NORA-M	Один на каждый вентиляционный канал или дверной тамбур; один на каждые 8...12 м³ надпотолочного пространства или др. пустот		7
«КЕДР-А» генератор-вибровозбудитель (двери, окна, батареи)	Один на каждое окно сто шторами и по одному на двери в переговорную и кабинет генерального директора		10
«КЕДР-А» генератор-вибровозбудитель (пол, потолок)	Один на каждые 15...25 м² перекрытия		16
«КЕДР-А» генератор-вибровозбудитель (стены)	На каждую стену, ведущую наружу, каждый 5 метров		17

«КЕДР-А» генератор-вибровозбудитель (Вентиляция)	Один на каждую вертикаль (отдельную трубу) вида коммуникаций		5
Пассивная звукоизоляция	Комплекс мероприятий принятый в кабинете генерального директора и переговорке		2
Защита от ПЭМИН ГЕНЕРАТОР ШУМА ЛГШ- 501	Устанавливается в переговорной, кабинете генерального директора и отдела информационной безопасности		3
Подавитель сигналов блокиратор“Завеса 12СТН”	Устанавливается в потенциально опасных для закладки кабинетах(переговорка, кабинет ИБ, кабинет генерального директора)		3

Размыкатель Ethernet	в розетку, подключение к 3-проводной сети (энергосеть с проводом заземления)		
Размыкатель слаботочной линии	Подключена к системе электропитания согласно рекомендациям производителя		

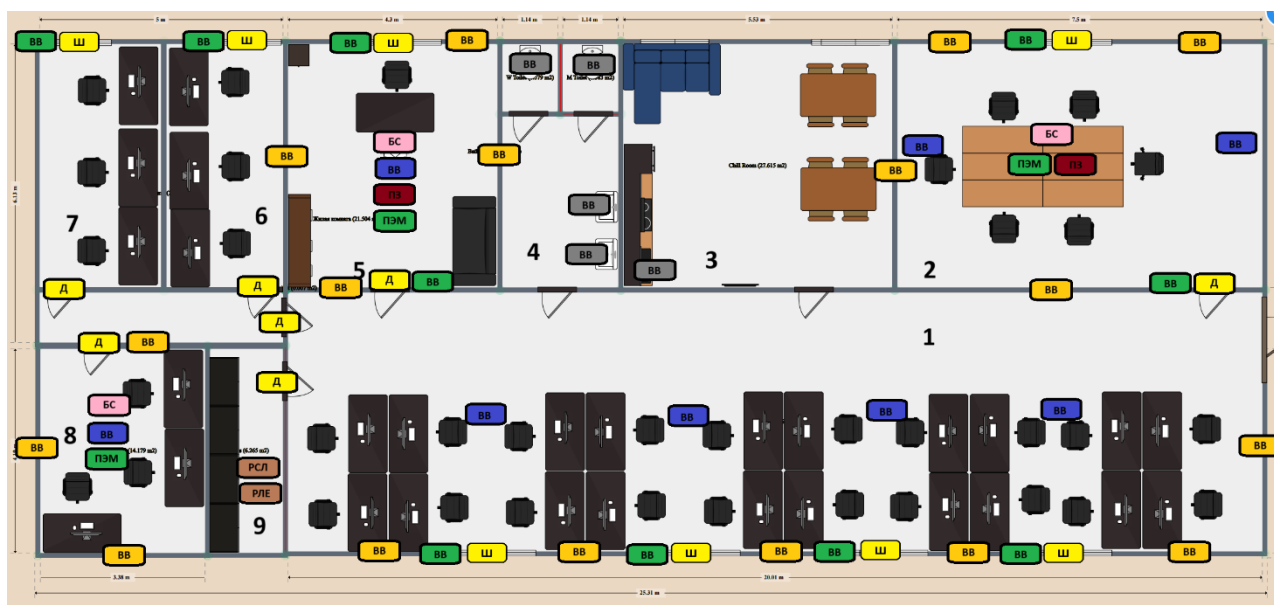


Рисунок 4 - план размещения технических средств защиты информации

ЗАКЛЮЧЕНИЕ

В рамках курсового проекта был выполнен ряд мероприятий для повышения уровня защищённости помещения. Изначально был создан план помещения, который лег в основу всех дальнейших действий по обеспечению безопасности.

Далее последовал глубокий анализ литературных источников по информационной безопасности, в ходе которого были рассмотрены потенциальные пути утечки конфиденциальных данных. С учётом этого анализа были определены необходимые защитные меры.

Разнообразные методы и инструменты защиты от утечек информации, включая новейшие технологии, прошли тщательное исследование. Этот этап исследования способствовал подбору наилучших средств защиты, с учётом их взаимодействия и совместимости.

Финальной частью работы стало составление детализированного плана установки выбранных мер защиты, как пассивных, так и активных, принимая во внимание специфику помещения и строгие критерии безопасности. Подготовленный план лег в основу создания эффективной системы обеспечения информационной безопасности в исследуемом объекте.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Кармановский Н.С., Михайличенко О.В., Савков С.В.. Организационно-правовое и методическое обеспечение информационной безопасности. Учебное пособие – Санкт-Петербург: НИУ ИТМО, 2013. - 151 с. – экз.
2. Трунова, А. А. Анализ каналов утечки конфиденциальной информации информационных системах предприятий / А. А. Трунова. — Текст: непосредственный // Молодой ученый. — 2016. — №3 (107). — С. 69–72. — URL: <https://moluch.ru/archive/107/25842/> (дата обращения: 19.01.2022).
3. Каторин Ю. Ф., Разумовский А. В., Спивак А. И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012. - 416 с. - экз.
4. Скрипник Д. Техническая защита информации. [Интернет-ресурс] URL: <https://intuit.ru/studies/courses/3649/891/info> (дата обращения: 15.01.2022)