

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

Факультет безопасности информационных технологий

КУРСОВАЯ РАБОТА

По дисциплине:

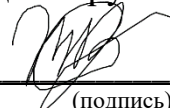
«Инженерно-технические средства защиты информации»

На тему:

«Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 133»

Выполнил:

Жестков В. А., студент группы N34521



(подпись)

Проверил:

Попов Илья Юрьевич

к.т.н., доцент ФБИТ

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023 г.

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

Студент	Жестков Владислав Андреевич
	(Фамилия И.О.)
Факультет	Безопасности Информационных Технологий
Группа	N34521
Направление (специальность)	Эксплуатация транспортно-технологических машин и комплексов
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ
	(Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 133
Задание	Проектирование инженерно-технической системы защиты информации на предприятии.
	Вариант 133

Краткие методические указания

Рекомендуемая литература

Руководитель

Студент



(Подпись, дата)

(Подпись, дата)

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

Студент Жестков Владислав Андреевич
(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34521

Направление (специальность) Эксплуатация транспортно-технологических машин и комплексов


Руководитель Попов Илья Юрьевич, к.т.н., доцент ФБИТ
(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 133

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Разработка и утверждение задания и календарного плана на курсовую работу	08.11.2023	08.11.2023	
2	Создание плана КР	08.11.2023	08.11.2023	
3	Анализ теоретической составляющей	13.11.2023	13.11.2023	
4	Разработка комплекса инженерно-технической защиты информации в заданном помещении	20.11.2023	20.11.2023	
5	Представление выполненной курсовой работы	18.12.2023	18.12.2023	

Руководитель _____
(Подпись, дата)

Студент  _____
(Подпись, дата)

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

Студент	Жестков Владислав Андреевич
	(Фамилия И.О.)
Факультет	Безопасности Информационных Технологий
Группа	N34521
Направление (специальность)	Эксплуатация транспортно-технологических машин и комплексов
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ
	(Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 133

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

**1. Цель и задачи
работы**

☐ Предложены студентом ☐ Сформулированы при участии студента
☒ Определены руководителем

Целью данной 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

☐ Расчет ☒ Конструирование
☐ Моделирование ☐ Другое

3. Содержание работы

В ходе курсовой работы будут выполнены анализы технических каналов утечки информации, защищаемых
помещений и рынка технических средств, будут рассмотрены руководящие документы, будет произведено
описание расстановки технических средств.

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

Студент



(Подпись, дата)

(Подпись, дата)

« ____ » _____ 20 ____ г

Содержание

ВВЕДЕНИЕ.....	2
1. Анализ технических каналов утечки информации	4
1.1 Технические каналы утечки информации при передаче ее по каналам связи.....	4
1.2 Технические каналы утечки речевой информации	5
1.3 Технические каналы утечки видовой информации	5
2. Руководящие документы.....	5
3. Анализ защищаемых помещений	8
4. Анализ технических средства защиты информации	15
4.1 Устройства противодействия утечке информации по акустическому и виброакустическому каналам	16
4.2 Устройства противодействия утечке информации по оптическому каналу.....	18
4.3 Устройства противодействия утечке по электромагнитным и электрическим каналам.....	19
5. Описание расстановки технических средств	21
ВЫВОДЫ.....	22
СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ.....	24

ВВЕДЕНИЕ

В настоящее время работа любого современного предприятия связана с обработкой большого количества информации. Защита этого объема информации – одно из самых важных и быстроразвивающихся направлений в любой крупной компании, так как современные внедряемые технологии и компоненты без соответствующей безопасности – наиболее возможный источник проблем.

Чтобы организовать эффективную систему предотвращения утечки информации, необходимо понимать потенциальные и реальные угрозы технического проникновения на предприятие, теоретические каналы для несанкционированного доступа и утечки информации. Правильное определение всех потенциальных угрозы на начальном этапе, в последствии поможет выбрать оптимальные меры и средства защиты.

В данной работе будет рассмотрен процесс проектирование инженерно-технической системы защиты на информации на предприятии. Защищаемая информация включает в себя государственную тайну с уровнем «секретно». Защищаемый объект полностью занимает второй этаж торгового центра и состоит из следующих помещений:

- Две переговорные
- Два рабочих кабинета
- Холл
- Администрация
- Комната персонала
- Кладовая
- Уборная
- Кабинет директора

Далее мы проведем анализ технических каналов утечки, приведем перечень руководящих документов, проведем анализ защищаемых помещений

и анализ технических средств защиты информации, в конце будет представлена схема расстановки технических средств.

1. АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

В данной курсовой работе будет рассматриваться только утечка информации по техническим каналам. Под техническим каналом утечки информации понимают совокупность объекта разведки, технического средства разведки и физической среды, в которой распространяется информационный сигнал.

В зависимости от физической природы сигналы распространяются в определенных физических средах. Средой распространения могут быть газовые (воздушные), жидкостные (водные) и твердые среды. К таким средам относятся воздушное пространство, конструкции зданий, соединительные линии и токопроводящие элементы, грунт и т. п.

Особенности технических каналов утечки информации определяются физической природой информационных сигналов и характеристиками среды распространения сигналов утекаемой информации. Ниже приведены некоторые особенности технических каналов утечки информации.

1.1 Технические каналы утечки информации при передаче ее по каналам связи

1. Электромагнитные каналы: электромагнитные излучения передатчиков связи, модулированные информационным сигналом (прослушивание радиотелефонов, сотовых телефонов, радиорелейных линий связи).
2. Электрические каналы: подключение к линиям связи.
3. Индукционный канал: эффект возникновения вокруг высокочастотного кабеля электромагнитного поля при прохождении информационных сигналов.

4. Паразитные связи: паразитные емкостные, индуктивные и резистивные связи и наводки близко расположенных друг от друга линий передачи информации.

1.2 Технические каналы утечки речевой информации

1. Акустические каналы: среда распространения – воздух.
2. Виброакустические каналы: среда распространения – ограждающие строительные конструкции.
3. Параметрические каналы: результат воздействия акустического поля на элементы схем, что приводит к модуляции высокочастотного сигнала информационным.
4. Акустоэлектрические каналы: преобразование акустических сигналов в электрические.
5. Оптико-электронный (лазерный) канал: облучение лазерным лучом вибрирующих поверхностей.

1.3 Технические каналы утечки видовой информации

1. Наблюдение за объектами. Для наблюдения днем применяются оптические приборы и телевизионные камеры. Для наблюдения ночью – приборы ночного видения, тепловизоры, телевизионные камеры.
2. Съёмка объектов. Для съёмки объектов используются телевизионные и фотографические средства. Для съёмки объектов днем с близкого расстояния применяются портативные камуфлированные фотоаппараты и телекамеры, совмещенные с устройствами видеозаписи.

2. РУКОВОДЯЩИЕ ДОКУМЕНТЫ

Далее представлены основные документы в области защиты информации и противодействию технической разведке:

1. Законы Российской Федерации:

- «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.
- «О федеральных органах правительственной связи и информации» от 19 февраля 1993 г. №4524–1.
- «О связи» от 16 февраля 1995 г. №15-ФЗ.
- «Об участии в международном информационном обмене» от 4 июля 1996 г. №85-ФЗ.
- «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ.
- «О персональных данных» от 27 июля 2006 г. № 152-ФЗ.

2. Указы Президента Российской Федерации:

- «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.
- «Об утверждении Доктрины информационной безопасности Российской Федерации» от 05.12.2016 №646.

3. Постановления Правительства Российской Федерации:

- «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» от 15 апреля 1995 г.

№333.

- «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 4 сентября 1995 г. №870.
- «Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам» от 2 августа 1997 г. №973.
- «О сертификации средств защиты информации» от 26 июня 1995 г, №608.
- «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г. № 1119.

4. Решения Гостехкомиссии России:

- «Основы концепции защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам» от 16 ноября 1993 г. № 6.
- «О типовых требованиях к содержанию и порядку разработки руководства по защите информации от технических разведок и от ее утечки по техническим каналам на объекте» от 3 октября 1995 г. № 42.
- «Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР)» от 23 мая 1997 г. № 55.
- «О защите информации при вхождении России в международную информационную систему «Интернет» от 21 октября 1997 г. № 61.

5. Руководящие и нормативно-методические документы Гостехкомиссии России:

- РД. СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации. Решение Председателя Гостехкомиссии России от 25 июля 1997 г.

- РД. Защита информации Специальные защитные знаки. Классификация и общие требования. Решение Председателя Гостехкомиссии России от 25 июля 1997г.
- Нормативно-методические документы по противодействию средствам иностранной гидроакустической разведки. Решение Гостехкомиссии России от 16 ноября 1993 г. № 7.
- Нормативно-методические документы по противодействию радиационной разведке. Решение Гостехкомиссии России от 15 ноября 1994 г. № 25.

3. АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

Наименование организации: ООО «Деньжата»

Область деятельности: бухгалтерия

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

Основные информационные процессы:

1. Публикация предложения услуг
2. Предоставление пользователям инструментов для заказа услуг и создания учётной записи на сайте
3. Техническая поддержка при оказании услуги
4. Предоставление консультаций пользователям
5. Удаление данных по завершении сотрудничества
6. Ведение бухгалтерского учёта организации, взаимодействие внутренних отделов с бухгалтерией
7. Хранение, обработка, передача, утилизация персональных данных пользователей

Основные информационные потоки:

1. Открытые потоки: взаимодействие с отделом клиентского управления (служба поддержки, отдел по работе с ключевыми клиентами, отдел

предоставления услуг), взаимодействие с отделом маркетинга, взаимодействие со службой контроля качества.

2. Закрытые потоки: взаимодействие с финансовым отделом, взаимодействие с отделом технического управления (дежурная служба, отдел информационной безопасности, отдел системного администрирования).

Информация ограниченного доступа:

1. Персональные данные сотрудников
2. Персональные данные клиентов
3. Техническая информация
4. Коммерческая тайна

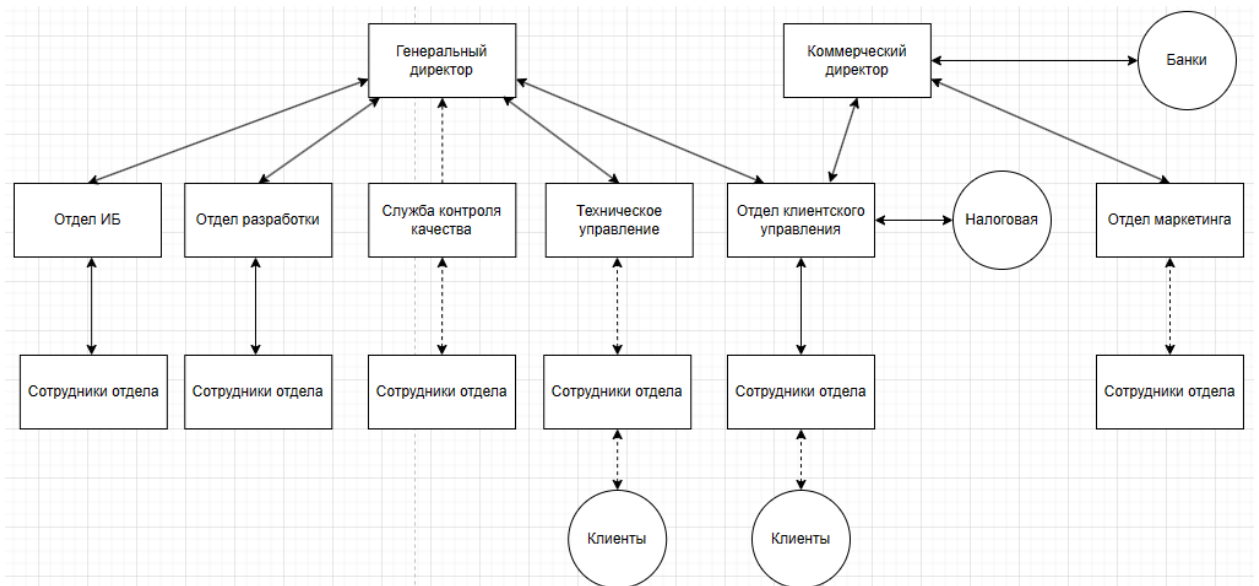


Рисунок 1 – Основные информационные потоки

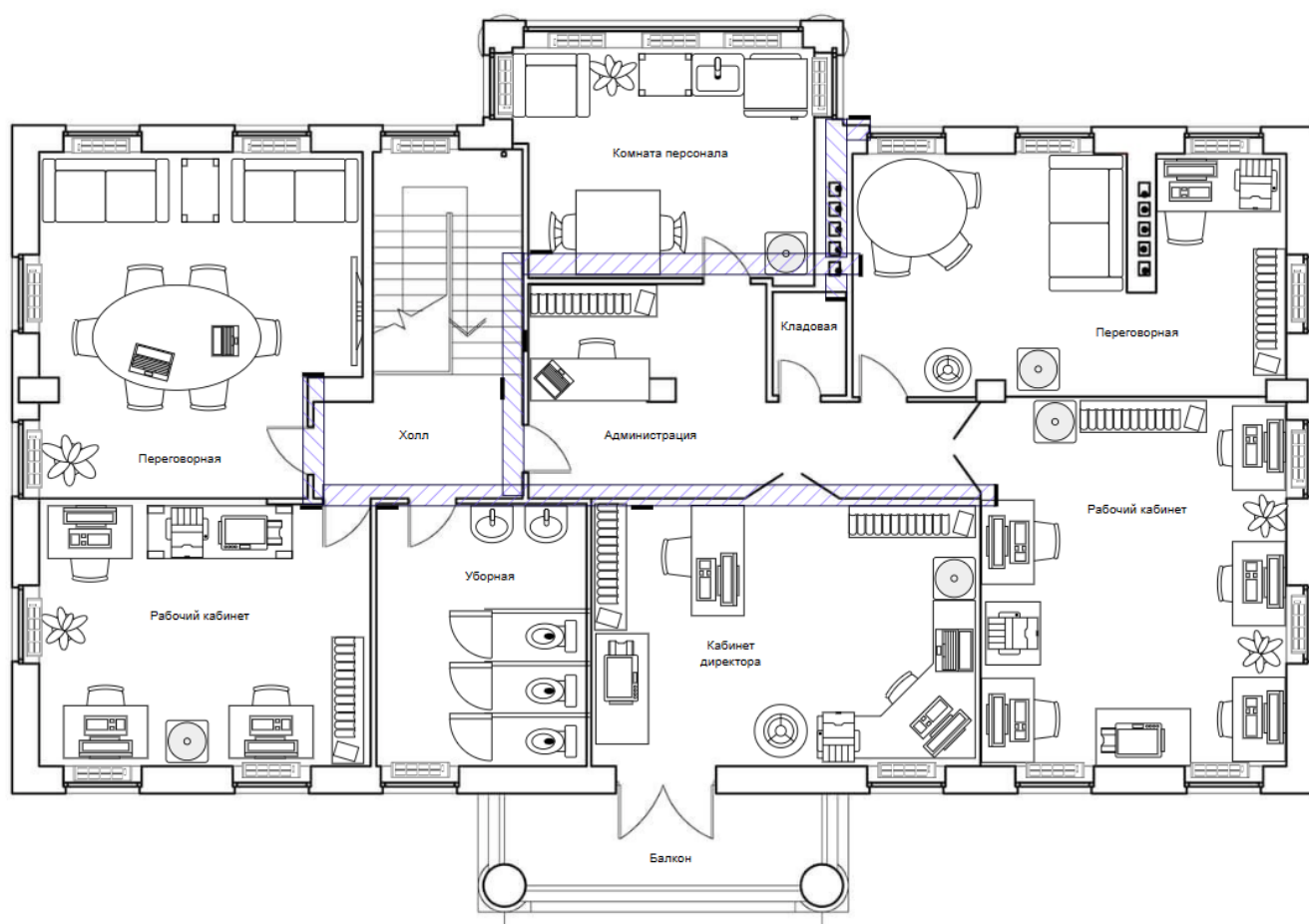

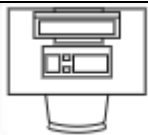







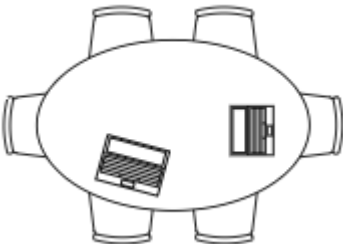









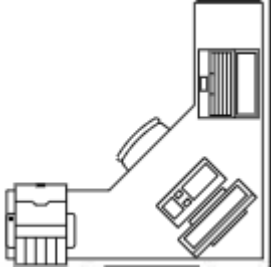


Рисунок 2 – План помещения

Обозначение	Описание
	Цветок
	Рабочее место с компьютером
	Диван
	Столик
	Телевизор

	Принтер
	Сканер + принтер
	Стеллаж с книгами
	Батарея
	Стол со стульями
	Дверь
	Кулер
	Раковина
	Унитаз
	Ноутбук
	Напольная лампа
	Холодильник
	Раковина
	Вентиляция (черная полоса – выход вентиляции)

	Угловое рабочее место
---	-----------------------

Помещения, требующие защиты:

- Переговорная со столом на 6 мест: 37,5 кв.м.
- Переговорная со столом на 3 места: 35,9 кв.м.
- Кабинет на 3 сотрудника: 34,5 кв.м.
- Кабинет на 5 сотрудников: 40,3 кв.м.
- Кабинет директора: 37,2 кв.м.

Для ведения переговоров предназначено два помещения (большая и малая переговорные). В малой переговорной находятся: стол, 3 стула, диван, лампа, кулер, стеллаж, компьютерный стол, компьютерное кресло, компьютер, принтер, 3 розетки, 4 батареи центрального отопления. В большой переговорной находятся: стол, 6 стульев, 2 ноутбука, 2 дивана, столик, телевизор, растение, 4 батареи центрального отопления, 3 розетки.

Для работы сотрудников предназначено также два помещения (большой и малый кабинеты). В малом кабинете расположено: 4 стола, 3 компьютера, 3 кресла, растение, стеллаж, кулер, принтер, сканер, 3 батареи центрального отопления, 5 розеток. В большом кабинете расположено: 7 столов, 5 компьютеров, 5 кресел, кулер, стеллаж, принтер, сканер, 2 растения, 4 батареи центрального отопления, 6 розеток.

В кабинете директора: 3 стола, 2 кресла, 2 компьютера, 2 стеллажа, кулер, лампа, сканер, принтер, 4 розетки, 1 батарея центрального отопления.

Помещение расположено на 2 этаже двухэтажного торгового центра, окна выходят на улицу. Окна не соседствуют с пожарными и эвакуационными

лестницами, крышами пристроек. Помещения занимают всю площадь второго этажа здания. Из кабинета директора есть выход на балкон. Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см.

В помещениях присутствуют декоративные элементы, например растение, кулер или диван, в которых можно спрятать закладное устройство. В каждом помещении имеются розетки, а значит, актуальны электрического и электромагнитного каналов утечки информации. Также есть угроза снятия информации по вибрационному и оптическому каналам, а также акустическому, виброакустическому, акустоэлектрическому. Материально-вещественный канал утечки информации регулируется строгой политикой компании в отношении физических носителей информации, и в рамках курсовой работы не рассматривается.

Для обеспечения комплексной безопасности согласно типу конфиденциальной информации – государственная тайна типа «секретно» требуется оснастить помещение средствами защиты, приведенными в таблице 1.

Таблица 1. Активная и пассивная защита информации

Каналы	Источники	Пассивная защита	Активная защита
акустический акустоэлектрический	Проводка, двери, окна	Сетевые фильтры, звукоизоляция кабинета директора и переговорной	Акустическое зашумление
вибрационный виброакустический	Батареи и трубы, стены, пол, окна, двери	Изолирующие звук и вибрацию материалы стен	Вибрационное зашумление
оптический	Окна, двери	Жалюзи/шторы на окнах, доводчики на двери	Блокирующие обзор устройства

электромагнитный электрический	АРМ, ноутбуки, бытовые приборы, телевизоры, розетки	Сетевые фильтры	Электромагнитное зашумление
-----------------------------------	---	-----------------	--------------------------------

4. АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

В задании на курсовую работу нам было необходимо создать систему защиты информации, которая будет работать с информацией, содержащей государственную тайну. Таким образом, 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.

4.1 Устройства противодействия утечке информации по акустическому и виброакустическому каналам

Пассивная защита представляет собой:

- Усиленные двери
- Сетевые фильтры
- Изолирующие звук и вибрацию материалы стен

Активная защита представляет собой систему виброакустического зашумления. Для защиты помещения для работы с государственной тайной уровня «секретно» рассматриваются технические средства активной защиты информации для объектов информатизации категории не ниже 1Б. Ниже в таблице 2 приведен сравнительный анализ подходящих средства активной защиты помещений по виброакустическому и акустическому каналам.

Таблица 2. Сравнительный анализ средств активной защиты

Устройство	Характеристики	Предназначение	Цена, руб
Портативный генератор акустического шума ЛГШ-303	Диапазон рабочих частот 180 ÷ 11 300 Гц	Изделие предназначено для защиты речевой информации от перехвата по прямому акустическому каналу.	15 600
Генератор акустического шума ЛГШ-304	Диапазон рабочих частот 175 ÷ 11 200 Гц	Сертификат ФСТЭК РОССИИ по 2 классу защиты; может устанавливаться в ВП до 2 категории	25 220
SI-3030 Виброакустический шумогенератор	Спектр шумовой помехи 125 Гц - 6,3 кГц	Предназначен для защиты помещений от прослушивания через строительные элементы конструкции.	28 500

"ANG-2200" - генератор шума	Диапазон акустического шума 250 Гц...5 кГц	Генератор шума для акустического зашумления помещения и его защиты от утечки информации по виброканалам (250...5000 Гц). Сертификат Гостехкомиссии.	18 000
«БУБЕН» - генератор акустической помехи	Диапазон рабочих частот 400...18000 Гц	Используется для защиты конфиденциальных переговоров по принципу создания акустических помех. Вид помех: речеподобная, "белый шум".	15 000
SpyLock Jack - устройство блокирования утечки информации по акустическому каналу	Подходит для iPhone, Samsung и других аппаратов. Разъем 3.5 mm.	Устройство предназначено для защиты речевой информации путем блокирования микрофонов и динамиков мобильного телефона на механическом и программном уровне.	15 000
Фотон-М - устройство защиты оптоволоконной линии от утечки акустической информации	Скорость передачи данных в сетях по технологии Ethernet до 100 Мбит/с	Устройство защиты акустической речевой информации от утечки по волоконно-оптической линии связи (ВОЛС).	395 000
Антенна 3 ГГц пассивная двухкомпонентная ПА-111		Антенна ПА-111 позволяет формировать в пространстве как магнитную (в диапазоне от 0,01 до 30 МГц), так и электрическую (в диапазоне от 0,01 до 3000 МГц) составляющие электромагнитного поля шума. Конструкция предусматривает возможность установки на ней генераторов ГШ-111У или ГШ-111П системы «Шифон» и возможность крепления на вертикальные поверхности (стены).	
Упрощенный вариант генератора ГШ-111У	В комплект поставки входит генератор ГШ-111У и ПО конфигуратора системы / Дополнительно к генератору можно приобрести: Антенна 6 ГГц активная АА-6000, Антенна 3 ГГц пассивная двухкомпонентная ПА-111	Упрощенный вариант генератора шума без кнопочной клавиатуры и ЖКИ. Управление, регулировка и контроль осуществляются только через компьютер по сети Ethernet.	75 000
Буран-2	Диапазон рабочих частот не менее 180–11200 Гц	Система акустических и виброакустических помех «Буран-2» является средством активной акустической и вибрационной защиты акустической речевой информации, соответствует требованиям ФСБ России к разработке, производству, сертификации и эксплуатации технических средств защиты особо важных и выделенных помещений	81 000

		органов государственной власти по виброакустическому каналу утечки речевой информации и может использоваться для защиты акустической речевой информации, содержащей сведения, составляющие государственную тайну, циркулирующей в выделенных помещениях до 2 категории включительно.	
Система активной акустической и вибрационной защиты акустической речевой информации "Соната-АВ" модель 4Б	Диапазон частот до 2 ГГц, диапазон регулировки	Генератор шума. Регулировка уровня шума в 3 частотных полосах. Индикация нормального/аварийного режима работы. Большой комплект.	23 000
БУБЕН-УЛЬТРА (Исп. «ЛЮСТРА») - подавитель диктофонов и микрофонов увеличенной мощности, встроенный в подвесной динамик системы оповещения.	24 ультразвуковых излучателя	Самый мощный прибор из представленных на рынке! Ультразвуковая помеха не слышима. Повышенная дальность подавления за счёт «know how» производителя. Два вида сложной помехи: сложная ультразвуковая помеха. Крепиться к потолку над столом переговоров. Имеет возможность регулировки по высоте.	65 000

В результате анализа была выбрана Система активной акустической и вибрационной защиты акустической речевой информации "Соната-АВ" модель 4Б. Данный выбор обоснован небольшой ценой устройства, и большим комплектом (Генераторы-акустоизлучатели – СА-4Б, СА-4Б1; Генератор-вибровозбудитель – СВ-4Б Размыкатель телефонной линии – Соната-ВК4.1; Размыкатель слаботочной линии – Соната-ВК4.2; Размыкатель линии Ethernet – Соната-ВК4.3 и т. д.).

4.2 Устройства противодействия утечке информации по оптическому каналу.

Для обеспечения защиты помещения от визуального наблюдения, необходимо установить на окно жалюзи или шторы. Были выбраны blackout шторы, так как они выглядят симпатичнее, чем жалюзи.

4.3 Устройства противодействия утечке по электромагнитным и электрическим каналам

Пассивная защита основывается на установке фильтров для сетей электропитания во всех помещениях. Активная защита основывается на создании в сети белого шума, который скрывает колебания, порождаемые воздействием звуковой волны или работающей электрической техникой. Устройства активной защиты представлены в Таблице 3.

Таблица 3. Сравнительный анализ средств активной защиты

Устройство	Характеристики	Предназначение	Цена, руб
SEL SP-44 Устройство защиты цепей электросети и заземления	Спектральная плотность напряженности электрического поля шума 0,01–1 МГц 90 дБ / 1–10 МГц 70 дБ / 10 - 100 МГц 50 дБ / 100 - 300 МГц 35 дБ	Генератор зашумления электросети 220 В и цепи заземления	24 000
ФСП-1Ф-7А Фильтр сетевой помехоподавляющий	Напряжение питания 220В	ФСП-1Ф-7А Фильтр сетевой помехоподавляющий	15 300
Фильтр сетевой помехоподавляющий ФСПК-40	Напряжение питания 220/380 В \pm 10%, 50 Гц	Фильтр сетевой помехоподавляющий ФСПК-40-220-99-УХЛ4 предназначен для защиты информации от утечки за счет побочных электромагнитных наводок на линии электропитания. В общем случае защитное устройство может применяться как сетевой фильтр для улучшения параметров качества сети.	70 500
"СОНАТА-ФС10.1"	Защищаемая линия электропитания Однофазная, номинальное напряжение 220 В, частота 50 Гц	ТСЗИ "Соната-ФС10.1" (далее – Изделие) предназначено для защиты информации, содержащей сведения, составляющие государственную тайну, и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет побочных электромагнитных наводок информативного сигнала на линии электропитания напряжением 220 В с частотой 50 Гц.	32 400
Фильтр сетевой помехоподавляющий ФСПК-200	Напряжение питания 220/380 В \pm 10%, 50 Гц	Фильтр сетевой помехоподавляющий ФСПК-200-0,22/0,38-91-УХЛ4 предназначен для защиты информации от утечки за счет побочных электромагнитных наводок на линии электропитания. В общем случае защитное устройство может применяться как сетевой	315 000

		фильтр для улучшения параметров качества сети.	
ЛРЧФ-100-1Ф	Диапазон рабочих частот 0,15–40 000 МГц	Изделие «ЛРЧФ-100-1Ф» предназначено для исключения или затруднения получения иностранной радио-, радиотехнической разведкой охраняемых параметров образцов вооружения и военной техники (ВиВТ) на технологических рабочих местах путем ограничения электромагнитной энергии опасного сигнала внутри замкнутых экранов в линиях электропитания напряжением до 380 В. Изделие «ЛРЧФ-100-1Ф» является пассивным техническим средством противодействия иностранной радио-, радиотехнической разведке.	83 200







По результатам анализа была выбрана система "СОНАТА-ФС10.1". Кроме того, что она является наиболее популярным решением для этого класса защиты (отмечена как «хит продаж» на нескольких сайтах-агрегаторах), она сочетает в себе умеренную стоимость с большим диапазоном. Так же был выбран сетевой фильтр ФСПК-40 за счет его возможности улучшения качества сети.




5. ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

Согласно информации, приведенной в 4 главе, выбранные средства защиты включают в себя:

- Усиленные двери (4 мм+), обшитые металлом (2 мм+) со звукоизолирующей прокладкой на металлическом каркасе – 9 шт., в переговорные, кабинет директора, рабочие кабинеты.
- Blackout шторы на 16 окон.
- Генератор акустической помехи "Соната-АВ" модель 4Б
- "СОНАТА-ФС10.1"
- ФСПК-40 Фильтр сетевой помехоподавляющий
- РАЗМЫКАТЕЛЬ СОНАТА-ВК 4.1 для защиты телефонной линии

Таблица 4. Смета

Устройство	Цена, руб	Кол-во	Обозначение	Стоимость, руб
Blackout шторы	4500	16	-	72 000
Усиленные звукоизолирующие двери Ultimatum PP	75 283	9		677547
Генератор-акустоизлучатель «СА-4Б1»	7440	10		74400
Генератор-вибровозбудитель «СА-4Б1» (окна)	7440	16		119040
Генератор-вибровозбудитель «СА-4Б1» (двери)	7440	6		44640
Генератор-вибровозбудитель «СА-4Б1» (стены)	7440	27		193440
Генератор-вибровозбудитель «СА-4Б1» (пол, потолок)	7440	10		74400

Размыкатель соната-вк 4.1 для защиты телефонной линии	6000	1		6000
"СОНАТА-ФС10.1"	32 400	5		162000
ФСПК-40 Фильтр сетевой помехоподавляющий	70 500	1		70500
Итого	1331967			

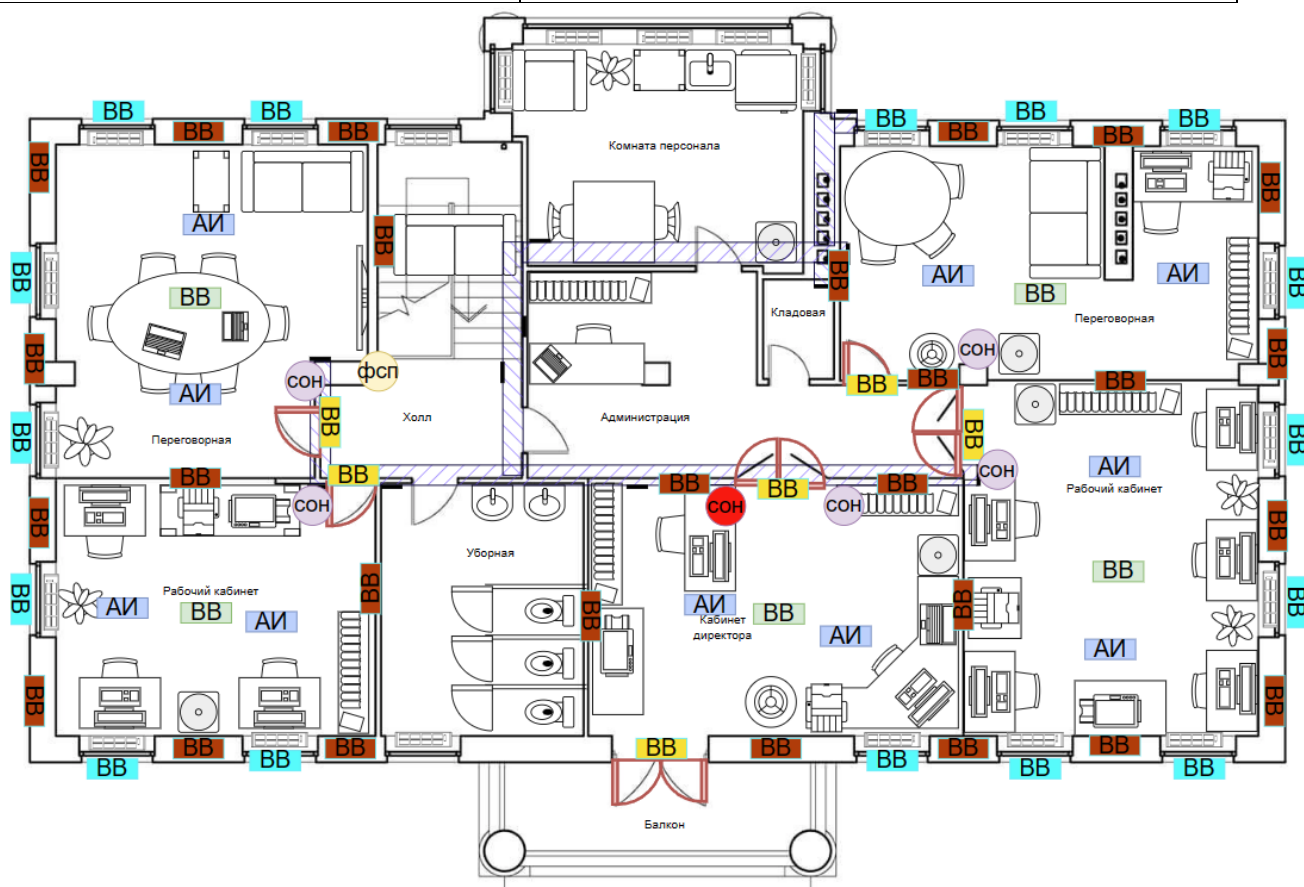


Рисунок 3 – Схема расстановки устройств

ВЫВОДЫ

В ходе данной работы был произведен теоретический обзор существующих каналов утечки информации, анализ потенциальных каналов

утечки информации в защищаемом помещении и описаны необходимые меры их защиты. Был проанализирован рынок существующих технических средств для противодействия рассматриваемым каналам утечки информации и выбраны подходящие для нашего объекта. Был разработан план установки и произведен расчет сметы затрат. В результате была предложена защита от утечек информации по акустическому, виброакустическому, оптическому, акустоэлектрическому, электрическому, электромагнитному, оптико-электронному техническим каналам защиты информации.

Итоговая стоимость системы защиты: 1331967 руб.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Скрипник Д. Техническая защита информации. [Интернет-ресурс] URL: <https://intuit.ru/studies/courses/3649/891/info>
2. Требования к режимным помещениям и их оборудованию // Компания КАСЛ-ЦЛС Прогресс URL: <https://licenziya-fsb.com/trebovaniya-k-rezhimnym-pomeshheniyam>
3. Закон Российской Федерации "О государственной тайне" от 21.07.1993 № 5485-1
4. Каторин Ю. Ф., Разумовский А. В., Спивак А. И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012. - 416 с. - экз.