

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

Факультет безопасности информационных технологий

КУРСОВАЯ РАБОТА

По дисциплине:


“Инженерно-технические средства защиты информации”

На тему:

**“Проектирование инженерно-технической системы защиты информации на
предприятии. Вариант 115”**

Выполнил(а):

Ильменская Д.Е.,
студентка группы N34511


(подпись)

Проверил преподаватель:

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

(подпись).


Отметка о выполнении:

Санкт-Петербург

2023

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент	Ильменская Д. Е.
	(Фамилия И.О.)
Факультет	Факультет безопасности информационных технологий
Группа	N34511
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 115
Задание	Разработка комплекса 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.
Руководитель	
	(Подпись, дата)
Студент	
	(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Ильменская Дарья Евгеньевна
(Фамилия И.О.)

Факультет Факультет безопасности информационных технологий

Группа N34511

Направление (специальность) 10.03.01 (Технология защиты информации)

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 115

№ п/ п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Разработка и утверждение задания и календарного плана на курсовую работу	07.10.2022	09.10.2022	
2	Анализ теоретической составляющей	01.12.2022	01.12.2022	
3	Разработка комплекса инженерно-технической защиты информации в помещении	05.12.2022	05.12.2022	
4	Защита курсовой работы	19.12.2022	19.12.2022	

Руководитель _____
(Подпись, дата)

Студент  _____
(Подпись, дата)

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

АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ

Студент	Ильменская Дарья Евгеньевна
	(Фамилия И.О.)
Факультет	Факультет безопасности информационных технологий
Группа	Н34511
Направление (специальность)	10.03.01 (Технология защиты информации)
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 115

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

1. Цель и задачи работы:

- ☐ Предложены студентом
☐ Сформулированы при участии студента
☒ Определены руководителем

2. Характер работы

- ☐ Расчет ☒ Конструирование
☐ Моделирование ☐ Другое

3. Содержание работы

Курсовая работа включает:

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)

Оглавление

Введение.....	5
Анализ каналов утечки информации.....	6
Руководящие документы.....	9
Анализ защищаемых помещений.....	11
Описание помещений.....	12
Анализ возможных утечек информации.....	13
Выбор средств защиты информации.....	13
Анализ рынка технических средств.....	15
Устройства для перекрытия акустического и виброакустического каналов утечки информации.....	15
Защита от утечек по оптическому каналу.....	17
Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации.....	17
Защита от ПЭМИН.....	17
Описание расстановки технических средств.....	18
Заключение.....	19
Список литературы.....	20

Введение

Деятельность любого современного предприятия основана на обладании и управлении информацией. В связи с этим защита информации становится предметом пристального внимания, так как повсеместно внедряемые технологии и компоненты без соответствующих предосторожностей быстро становятся источниками проблем.

Средства защиты информации (СЗИ) обеспечивают защиту информации в информационных системах, по сути, представляющих собой совокупность хранимой в базах данных информации, информационных технологий, обеспечивающих ее обработку, и технических средств. Они позволяют предотвратить несанкционированный доступ злоумышленника к ресурсам и данным предприятия, тем самым снизив риск несанкционированных утечки, утраты, искажения, уничтожения, копирования и блокирования информации и, как следствие, нанесения экономического, репутационного или других видов ущерба предприятию. Разработка эффективного комплекса мер для выполнения данной задачи является одной из наиболее актуальных современных проблем. Технические средства защиты информации являются важной частью комплекса мер по обеспечению режима конфиденциальности на предприятии.

В данной работе рассмотрен процесс разработки комплекса инженерно-технической защиты информации, составляющей государственную тайну с уровнем «секретно» на объекте информатизации. Защищаемый объект состоит из одиннадцати помещений и представляет собой офис предприятия с кабинетом директора/переговорной/приемной, кабинетами, серверной, санузелом и общей зоной.

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.

Анализ каналов утечки информации

Утечка — это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена. Утечка информации может осуществляться по различным каналам. Каналом утечки информации называют канал коммуникации, позволяющий процессу передавать информацию путем, нарушающим безопасность системы.

Существует три формы утечки информации:

- разглашение информации;
- несанкционированный доступ к информации;
- утечка информации по техническим каналам.

Технический канал утечки информации (ТКУИ) - совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Утечка (информации) по техническому каналу - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Структура технического канала утечки информации изображена на рисунке 1.

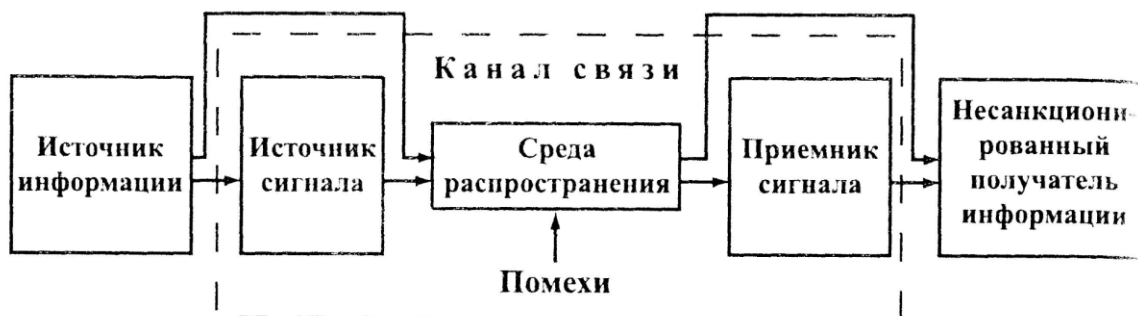


Рисунок 1 - Структура технического канала утечки информации

На вход канала поступает информация в виде первичного сигнала. Первичный сигнал представляет собой носитель с информацией от ее источника или с выхода предыдущего канала. В качестве источника сигнала могут быть:

- объект наблюдения, отражающий электромагнитные и акустические волны;
- объект наблюдения, излучающий собственные (тепловые) электромагнитные волны в оптическом и радиодиапазонах;
- передатчик функционального канала связи;
- закладное устройство;
- источник опасного сигнала;
- источник акустических волн, модулированных информацией.

Так как информация от источника поступает на вход канала на языке источника (в виде буквенно-цифрового текста, символов, знаков, звуков, сигналов и т. д.), то передатчик производит преобразование этой формы представления информации в форму, обеспечивающую запись ее на носитель информации, соответствующий среде распространения. В общем случае он выполняет следующие функции:

- создает поля или электрический ток, которые переносят информацию;

- производит запись информации на носитель;
- усиливает мощность сигнала (носителя с информацией);
- обеспечивает передачу сигнала в среду распространения в заданном секторе пространства.

Среда распространения сигнала - физическая среда, по которой информативный сигнал может распространяться и регистрироваться приемником. Она характеризуется набором физических параметров, определяющих условия перемещения сигнала. Основными параметрами, которые надо учитывать при описании среды распространения, являются:

- физические препятствия для субъектов и материальных тел;
- мера ослабления сигнала на единицу длины;
- частотная характеристика;
- вид и мощность помех для сигнала.

Среда может быть однородная и неоднородная. Однородная - вода, воздух, металл и т.п. Неоднородная среда образуется за счет перехода сигнала из одной среды в другую, например, акустоэлектрические преобразования.

Приемник выполняет функцию, обратную функции передатчика. Он производит:

- выбор носителя с нужной получателю информацией;
- усиление принятого сигнала до значений, обеспечивающих съем информации;
- съем информации с носителя;
- преобразование информации в форму сигнала, доступную получателю (человеку, техническому устройству), и усиление сигналов до значений, необходимых для безошибочного их восприятия.

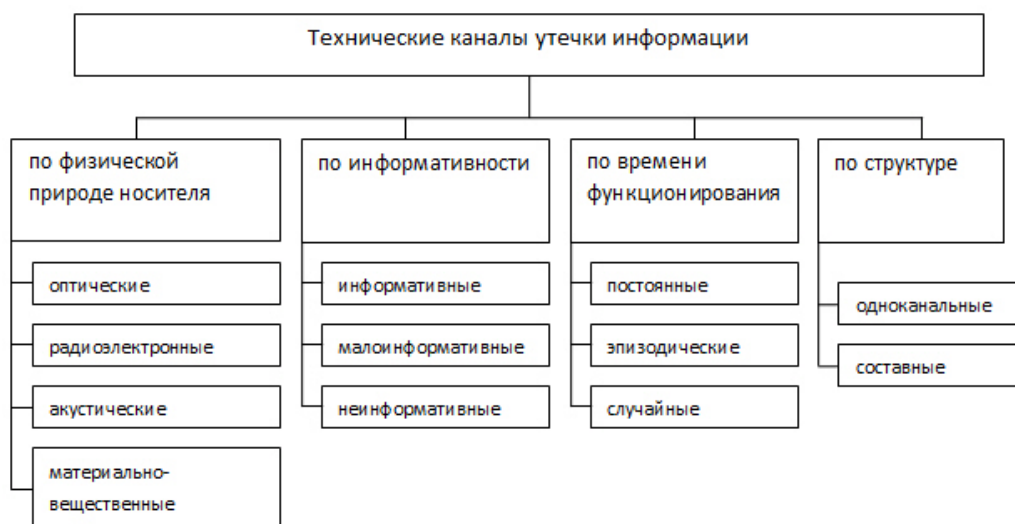


Рисунок 2 - Классификация технических каналов утечки информации

Основным признаком для классификации технических каналов утечки информации является физическая природа носителя. По этому признаку ТКУИ делятся на:

- оптические;
- радиоэлектронные;

- акустические;
- материально-вещественные.

Носителем информации в оптическом канале является электромагнитное поле (фотоны). Оптический диапазон подразделяется на:

- дальний инфракрасный поддиапазон 100 - 10 мкм (3 - 300 ТГц);
- средний и ближний инфракрасный поддиапазон 10 - 0,76 мкм (30 - 400 ТГц);
- видимый диапазон (сине-зелёно-красный) 0,76 - 0,4 мкм (400 - 750 ТГц).

В радиоэлектронном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток (поток электронов), распространяющийся по металлическим проводам. Диапазон частот радиоэлектронного канала занимает полосу частот от десятков ГГц до звукового. Он подразделяется на:

- низкочастотный 10 - 1 км (30 - 300 кГц);
- среднечастотный 1 км - 100 м (300 кГц - 3 МГц);
- высокочастотный 100 - 10 м (3 - 30 МГц);
- ультравысокочастотный 10 - 1 м (30 - 300 МГц);
- и т.д. до сверхвысокочастотного 3 - 30 ГГц (10 - 1 см).

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

- инфразвуковой диапазон 1500 - 75 м (1 - 20 Гц);
- нижний звуковой 150 - 5 м (1 - 300 Гц);
- звуковой 5 - 0,2 м (300 - 16000 Гц);
- ультразвуковой < 0,2 м (> 16000 Гц) и до 4 МГц.

В материально-вещественном канале утечка информации производится путем несанкционированного распространения за пределы контролируемой зоны вещественных носителей с защищаемой информацией. В качестве вещественных носителей чаще всего выступают черновики документов и использованная копировальная бумага.

Каналы утечки информации можно также классифицировать по информативности на информативные, малоинформативные и неинформативные. Информативность канала оценивается ценностью информации, которая передается по каналу.

По времени проявления каналы делятся на постоянные, периодические и эпизодические. В постоянном канале утечка информации носит достаточно регулярный характер. К эпизодическим каналам относятся каналы, утечка информации в которых имеет случайный разовый характер.

Руководящие документы

Основными документами в области защиты информации являются:

- Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера».
- Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
- Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации».
- Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне».
- Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) «О сертификации средств защиты информации».
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
- Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Закон РФ «О государственной тайне» от 21.07.1993 N 5485-1.
- МЕЖВЕДОМСТВЕННАЯ КОМИССИЯ ПО ЗАЩИТЕ ГОСУДАРСТВЕННОЙ ТАЙНЫ РЕШЕНИЕ № 199 от 21.01.2011г. "О Типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними".

Также на сайте ФСТЭК существует отдельный раздел, содержащий специальные нормативно-технические документы ФСТЭК России – нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации:

- 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.
- Временные методики сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров по требованиям безопасности информации.
- Временный порядок аттестации объектов информатизации по требованиям безопасности информации.
- 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.
- Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники.
- Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации.
- Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования.
- Руководящий документ Гостехкомиссии России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей.
- Руководящий документ. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам.

Анализ защищаемых помещений



Рисунок 2 - План помещений до установки ТСЗИ

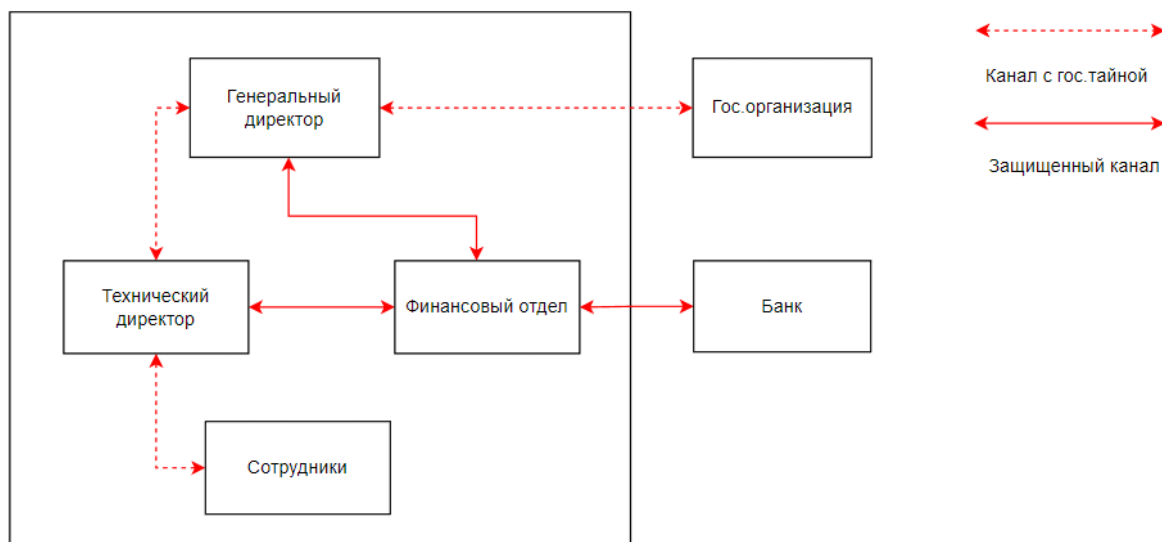



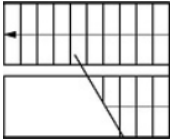
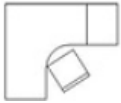
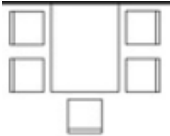









Рисунок 3 - Информационные потоки

По защищенным каналам передается информация, которая не связана с государственной тайной, то есть различные необходимые закупки и другие финансовые вопросы.

По каналу с государственной. тайной передается информация, которая связана с проектом, который выполняется для заказчика - государственная организация.

Таблица 1 - Легенда плана защищаемого помещения

Обозначения	Описание
	Стена
	Окно
	Дверь
	Лестница
	Рабочее место
	Обеденный стол
	Стол для переговоров
	Проектор
	Книжный шкаф
	Раковина
	Унитаз
	Диван
	Шкаф с документами

Описание помещений

1. Коридор + лестничная клетка - 67 м²
2. Кабинет - 18,7 м²
3. Кабинет - 17,8 м²

4. Кабинет - 12,2 м²
5. Кабинет - 12,2 м²
6. Переговорная - 35,5 м²
7. Приемная - 17,8 м²
8. Комната отдыха - 11 м²
9. Кабинет директора- 11 м²
10. Кухня - 26 м²
11. Санузел - 10,5 м²
12. Архив - 14,5 м²

Для ведения переговоров выделено обособленное помещение, в котором помимо стола и стульев имеется проектор. В помещении есть 5 окон и 5 розеток.

Для работы организации выделено несколько кабинетов под номерами 2-5. Всего 6 рабочих мест, каждое из которых обеспечено персональными компьютерами. Помимо этого, имеется 7 окон и 8 розеток.

Для работы директора организации выделено три помещения: приемная, кабинет директора и комната отдыха. В них присутствует 4 окна, 2 рабочих персональных места, 6 розеток, диван, журнальный столик и 3 шкафа для документов.

Для организации досуга работников имеется комната с залом и кухней. В ней есть 2 окна, 5 розеток и 2 стола.

Также имеется комната для хранения документов, называемая архивом. В ней есть 4 шкафа для документов, 1 компьютер для быстрого поиска нужного документа, 1 розетка.

Помещение расположено на втором этаже малоэтажного здания, окна выходят в закрытый контролируемый двор. Помещения занимают весь этаж здания, который не используется сотрудниками при выполнении служебных обязанностей, не связанных с доступом к государственной тайне. Все окна имеют с внутренней стороны шторы, плотно закрывающие видимость снаружи. Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см.

Анализ возможных утечек информации

В некоторых помещениях есть шкафы, в которых можно спрятать закладные устройства. В каждом помещении имеются розетки, а значит, актуальны электрического и электромагнитного каналов утечки информации.

Также есть угроза снятия информации по вибрационному, оптическому, акустическому, виброакустическому, акустоэлектрическому каналам.

Материально-вещественный канал утечки информации регулируется строгой политикой компании в отношении физических носителей информации, и в рамках курсовой работы не рассматривается.

Выбор средств защиты информации

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

Таблица 2 - Активная и пассивная защита информации

Каналы	Источники	Пассивная защита	Активная защита
Вибрационный и виброакустический	Твердые поверхности	Изолирующие звук и вибрацию обшивки стен	Устройства вибрационного шумления
Оптический	Окна, двери	Шторы, доводчики для плотного закрывания дверей	Бликующие устройства
Электромагнитный и электрический	розетки, АРМ, бытовая техника	Фильтры для сетей электропитания	Устройства электромагнитного шумления
Акустический и акустоэлектрический	Окна, Двери, электрические сети, проводка	Звукоизоляция, фильтры для сетей электропитания	Устройства акустического шумления

Анализ рынка технических средств

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.

Устройства для перекрытия акустического и виброакустического каналов утечки информации

Пассивная защита представляет собой:

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

Активная защита представляет собой систему виброакустического шумления. Для защиты помещения для работы со служебной тайной уровня “секретно” рассматриваются средства активной защиты не ниже 3 класса защищенности.

Таблица 3 - Сравнительный анализ средств активной защиты

Наименование	Характеристики	Примечание
ЛГШ-404	Диапазон рабочих частот - 175...11200 Гц Потребляемая мощность - 25 Вт Электропитание - 220 В, 50 Гц Размеры - 188x160x60 мм Кол-во подключаемых излучателей - 20	Соответствует требованиям по 2-му классу защиты
Шорох-5Л	Диапазон рабочих частот - 80 ... 11300 Гц Потребляемая мощность - не более 130 Вт Электропитание - 220 В, 50 Гц Размеры - 222 x 225 x 52 мм Кол-во подключаемых излучателей - 35	Соответствует 1-ому классу защищенности
"Соната-АВ" модель 4Б	Диапазон рабочих частот - 175 – 11 200 Гц Потребляемая мощность - не более 40 Вт Электропитание - 220 В, 50 Гц Размеры - 45x75x120 мм	Соответствует требованиям по 1-му классу защиты

Таким образом, по результатам анализа выбрана система постановки виброакустических помех ЛГШ-404. Выбрано именно эта система, так как она соответствует требованиям к грифу “Секретно” и обладает наилучшими характеристиками по диапазону рабочих частот, интервалу уровня регулировки звукового давления, а также меньшими габаритными размерами, что будет удобнее при установке системы.

Состав системы:

- Изделие «ЛГШ-404» - генератор шума
- Вибровозбудитель «ЛВП-10» - для установки на стены, трубы и окна
- Акустический излучатель «ЛВП-2а» - для возбуждения маскирующих акустических помех
- Виброэкран «ЛИСТ-1» - для защиты от наблюдения и акустических микрофонов
- Размыкатель «ЛУР» - для размыкания слаботочных линий

Общая стоимость системы:

- Генераторный блок «ЛГШ-404» - 35100 руб./шт
- Вибровозбудитель «ЛВП-10» - 5200 руб./шт
- Акустический излучатель «ЛВП-2а» - 3700 руб./шт
- Размыкатель слаботочных линий питания «ЛУР-2» - 5600 руб./шт

Защита от утечек по оптическому каналу

Обеспечение защиты помещения по оптическим каналам будет осуществлено с помощью штор, которые уже были установлены в помещении.

Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации

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

Активная защита основывается на создании в сети белого шума, который скрывает колебания порождаемые воздействием звуковой волны или работающей электрической техникой.

Таблица 4 - Активная защита от утечек по электрическим каналам

Наименование	Характеристики	Примечание
SEL SP-44	Диапазон частот 10 кГц – 400 МГц, Диапазон регулировки уровня шума - не менее 20 Дб	Соответствует требованиям по 1-му классу защиты
Соната-РС2	Диапазон частот - до 2 ГГц Диапазон регулировки уровня шума - Не менее 35 дБ	Соответствует требованиям по 1-му классу защиты
ЛГШ-513	Диапазон частот - 0,01 до 1800 МГц Диапазон регулировки уровня шума - Не более 20 дБ	Соответствует требованиям по 2-му классу защиты

По результатам анализа, было выбрано средство защиты ЛГШ-513, так как оно имеет наиболее широкий спектр и защищает от электрического, электромагнитного каналов, а также ПЭМИН.

Защита от ПЭМИН

Для реализации активной защиты от ПЭМИН было выбрано устройство ЛГШ-513. Данный выбор обоснован тем, что устройство имеет возможность подключения проводного дистанционного управления и контроля, в качестве которого может использоваться программно-аппаратный комплекс «Паутина».

Описание расстановки технических средств

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

- Система постановки виброакустических и акустических помех ЛГШ-404;
- Генератор шума ЛГШ-513;
- Усиленные двери (4 мм+), обшитые металлом (2 мм+) со звукоизолирующей прокладкой на металлическом каркасе – 4 шт., в переговорную, приемную, кабинет директора и архив.

Крепеж вибровозбудителя ЛВП-10:

- Для элементов строительных конструкций:

Радиус действия одного вибровозбудителя зависит от материала строительных конструкций и составляет ориентировочно 1,5 м.

- Для инженерных коммуникаций:

Крепление выполняется на каждый независимый участок инженерно-технических коммуникаций (например, водопровод и т.д.).

- Для стекол оконных блоков:

Для каждой оконной секции требуется установка вибровозбудителя, радиус действия одного вибровозбудителя составляет ориентировочно 2 м.

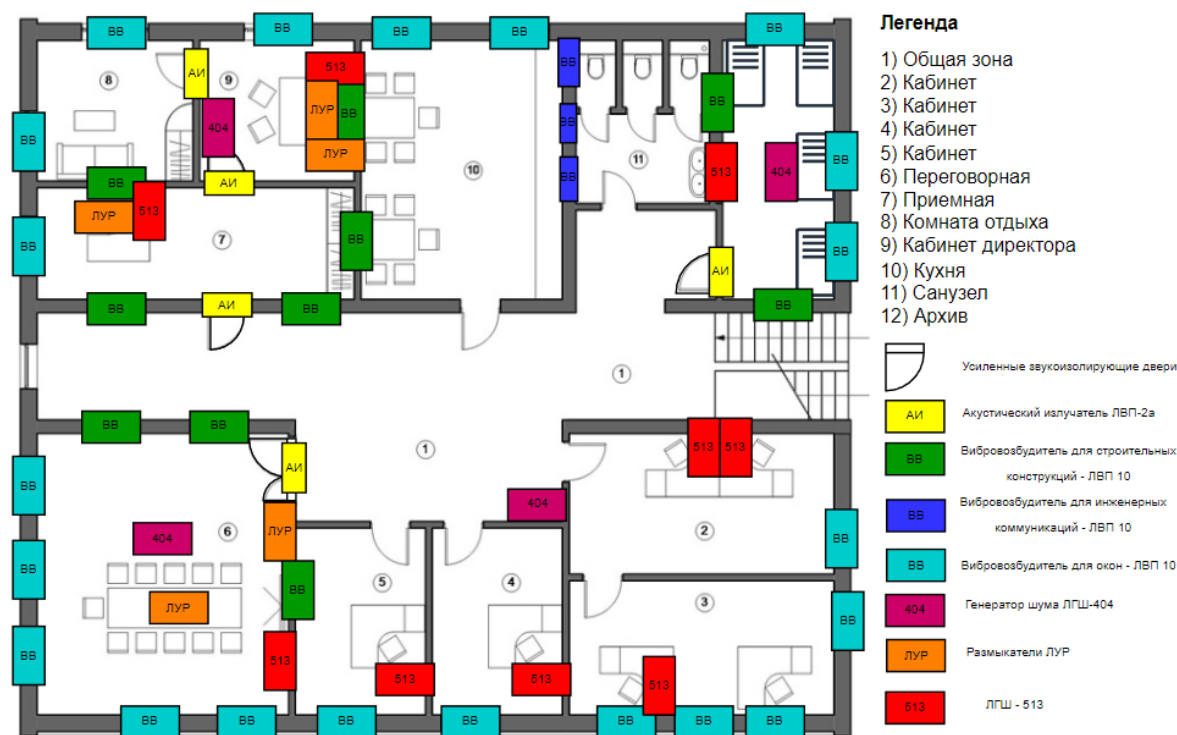


Рисунок 4 - План помещений с ТСЗИ

Заключение

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.

Список литературы

1. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012. - 416 с. - экз.
2. Скрипник Д. Техническая защита информации. [Интернет-ресурс] URL: <https://intuit.ru/studies/courses/3649/891/info> (дата обращения: 26.12.2022)