

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

Факультет безопасности информационных технологий

Дисциплина:

«Инженерно-технические средства защиты информации»

ОТЧЕТ ПО КУРСОВОЙ РАБОТЕ

«Проектирование системы защиты от утечки информации по различным каналам»

Выполнил:

студент группы N34461

Чувашова Виктория

Александровна



Проверил:

Попов Илья Юрьевич, доцент ФБИТ

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023г.

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

Студент	<u>Чувашова Виктория Александровна</u> (Фамилия И.О)
Факультет	<u>Безопасность информационных технологий</u>
Группа	<u>Н34461</u>
Направление (специальность)	<u>10.03.01 (Технологии защиты информации 2019)</u>
Руководитель	<u>Попов Илья Юрьевич</u> (Фамилия И.О)
Дисциплина	<u>Инженерно-технические средства защиты информации</u>
Наименование темы	<u>Проектирование системы защиты от утечки информации по различным каналам</u>
Задание	<u>Разработка системы инженерно-технической защиты информации в помещении</u>

Краткие методические указания

Содержание пояснительной записки

Пояснительная записка включает разделы – введение, анализ технических каналов утечки информации, перечень управляющих документов, анализ защищаемых помещений и технических средств защиты информации разных категорий, разработка схем расстановки выбранных технических средств в защищаемом помещении.

Рекомендуемая литература

Руководитель	<hr/>
	(Подпись, дата)
Студент	<hr/>
	(Подпись, дата)

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

Студент Чувашова Виктория Александровна
(Фамилия И.О)

Факультет Безопасность информационных технологий

Группа N34461

Направление (специальность) 10.03.01 (Технологии защиты информации 2019)

Руководитель Попов Илья Юрьевич
(Фамилия И.О)

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.	Создание плана КР	10.10.2023	10.10.2023	
2.	Анализ информации	28.11.2023	28.11.2023	
3.	Написание курсовой работы	01.12.2023	01.12.2023	
4.	Защита курсовой работы	19.12.2023	19.12.2023	

Руководитель _____
(Подпись, дата)

Студент _____
(Подпись, дата)

Студент	Чувашова Виктория Александровна (Фамилия И.О)
Факультет	Безопасность информационных технологий
Группа	N34461
Направление (специальность)	10.03.01 (Технологии защиты информации 2019)
Руководитель	Попов Илья Юрьевич (Фамилия И.О)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование системы защиты от утечки информации по различным каналам

1. Цель и задачи работы	Повышение уровня защиты информации от утечек.
2. Характер работы	Отчетная курсовая работа
3. Содержание работы	Анализ защищаемого помещения, оценка каналов утечки информации, выбор средств и методов защиты информации.
4. Вывод	По итогам проделанной работы была разработана система инженерно-технической защиты информации от утечек, повышающей защищенность информации, обрабатываемой в организации.

4

СОДЕРЖАНИЕ

Введение	6
1 Анализ технических каналов утечки информации	7
2 Перечень управляющих документов	10
3 Анализ защищаемых помещений	12
3.1 Сведения об организации	12
3.2 Описание помещения	13
3.3 Анализ возможных утечек информации	15
3.4 Анализ возможных утечек информации	15
4 Анализ технических средств защиты информации	16
4.1 Устройства для перекрытия акустического и виброакустического канала утечки информации	16
4.2 Устройства для перекрытия электрического и акустоэлектрического каналов утечки информации	17
4.3 Защита от утечек по каналу побочных электромагнитных излучений (ПЭМИН)	19
4.4 Защита от утечек по оптическому каналу	19
5 Описание расстановки технических средств	20
Заключение	23
Список использованной литературы	24

ВВЕДЕНИЕ

Средства защиты информации обеспечивают защиту информации в информационных системах, позволяют предотвратить несанкционированный доступ злоумышленника к ресурсам и данным предприятия, тем самым снизив риск несанкционированных утечки, утраты, искажения, уничтожения, копирования и блокирования информации и 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 5 помещений и представляет собой кабинет директора, переговорную, офисное помещение для сотрудников, компьютерный зал и свободная зона.

По ходу работы произведен анализ технических каналов утечки информации, приведен перечень управляющих документов, анализ защищаемых помещений с точки зрения возможных утечек информации и требуемых для защиты технических средств, анализ рынка технических средств защиты информации разных категорий и разработка схем расстановки выбранных технических средств в защищаемом помещении.

1 АНАЛИЗ ТЕХНИЧЕСКИХ 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.

Причины утечек информации:

- использование ошибочных форм защиты информации, их нарушение или жеполное несоблюдение;
- малейшие отступления от правил работы с критически важными документами, техникой, продукцией и прочими конфиденциальными материалами.

Формы утечки информации:

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

Согласно теме данной работы рассмотрим только утечку 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.

На рисунке 1 представлена схема структуры технического канала утечки информации. На вход ТКУИ поступает информация в виде первичного сигнала, представляющего собой носитель с информацией от её источника.

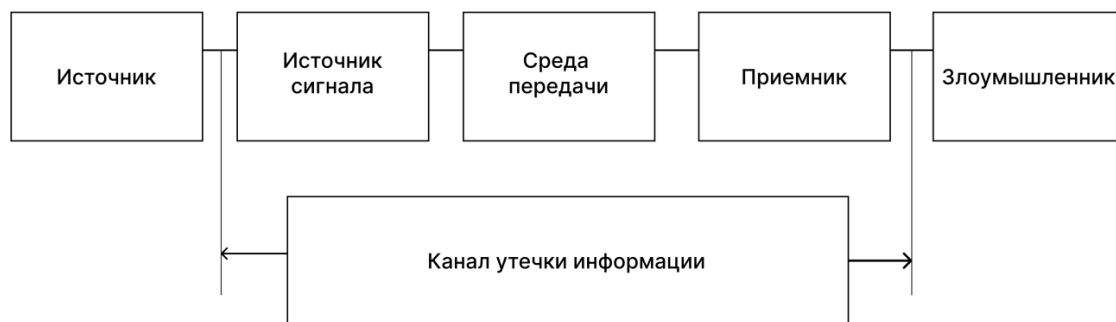


Рисунок 1 – Схема технического канала утечки информации

Источники сигнала:

- 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.

Полученная информация преобразуется в форму, обеспечивающую запись ее на носитель информации, соответствующий среде распространения.

Среда распространения сигнала – физическая среда, по которой информативный сигнал может распространяться и регистрироваться приемником, характеризующаяся набором физических параметров, определяющих условия перемещения сигнала.

Приемник после этого снимает информацию с носителя, обрабатывает полученный сигнал и преобразует информацию в форму сигнала, доступную получателю.

По физической природе носителя и виду канала связи ТКУИ делятся на:

- оптические;
- радиоэлектронные;
- электрические;
- электромагнитные;
- индукционные;
- акустические;
- акустоэлектрические;
- виброакустические;

- материально-вещественные.

Носителем информации в оптическом и визуально-оптическом канале является электромагнитное поле. Снятие информации возможно с помощью наблюдения через подсмотренное в окно или приоткрытую дверь. В качестве защиты от утечки информации следует снизить освещенность защищаемого объекта и его отражательные свойства, использовать различные пространственные ограждения (экраны, шторы, темные стекла), применять специальную маскировку и средства сокрытия защищаемых объектов (сетки, краски, укрытия).

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

В электромагнитном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток (поток электронов), распространяющийся по металлическим проводам. Способом защиты от утечки информации по электромагнитным каналам считается экранирование аппаратуры и ее элементов. Электростатическое, магнитостатическое и электромагнитное экранирование позволяет предохранить объект от воздействия и электромагнитных, и акустических сигналов. Таким образом, обеспечивает надежную защиту информации от утечки по ПЭМИН.

Материально-вещественные каналы также нуждаются в защите, так как различные материальные носители могут содержать в себе важнейшую секретную информацию. Для защиты материально-вещественных каналов от утечки информации разрабатывается целый комплекс организационных мер.

К основным причинам образования ТКУИ относятся:

- несовершенство элементной базы;
- несовершенство схемных решений;
- эксплуатационный износ;
- злоумышленные действия.

Показатели ТКУИ, позволяющие оценить риск утечки информации:

- пропускная способность ТКУИ;
- длина ТКУИ;
- относительная информативность ТКУИ.

2 ПЕРЕЧЕНЬ УПРАВЛЯЮЩИХ ДОКУМЕНТОВ

Основными документами в области защиты информации являются:

- ФЗ 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»;
- ПП РФ от 26.06.1995 N 608 (ред. от 21.04.2010) «О сертификации средств защиты информации»;
- ФЗ от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- ПП 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";
- 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 НСД. Термины и определения;
- Руководящий документ. СВТ. Защита от НСД. Показатели защищенности от несанкционированного доступа к информации;
- Руководящий документ. Автоматизированные системы. Защита от НСД. 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 Гостехкомиссии России. Защита от НСД. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей;
- Руководящий документ. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам.

3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

3.1 Сведения об организации

В данной работе рассмотрен процесс разработки комплекса инженерно-технической защиты информации, составляющей третий тип – уровень «секретно». Защищаемый объект состоит из шести помещений и представляет собой офис организации с кабинетом директора, переговорной, зоной отдыха, бухгалтерия, офисное помещение для сотрудников и компьютерный зал.

Информационные потоки организации представлены на рисунке 2, красными стрелками обозначены закрытые потоки, в которых передается информация ограниченного доступа, а зелеными – открытые потоки. Закрытые потоки в схеме разделены на информацию конфиденциального характера – красная пунктирная линия, информацию с грифом «секретно» - красная сплошная линия.

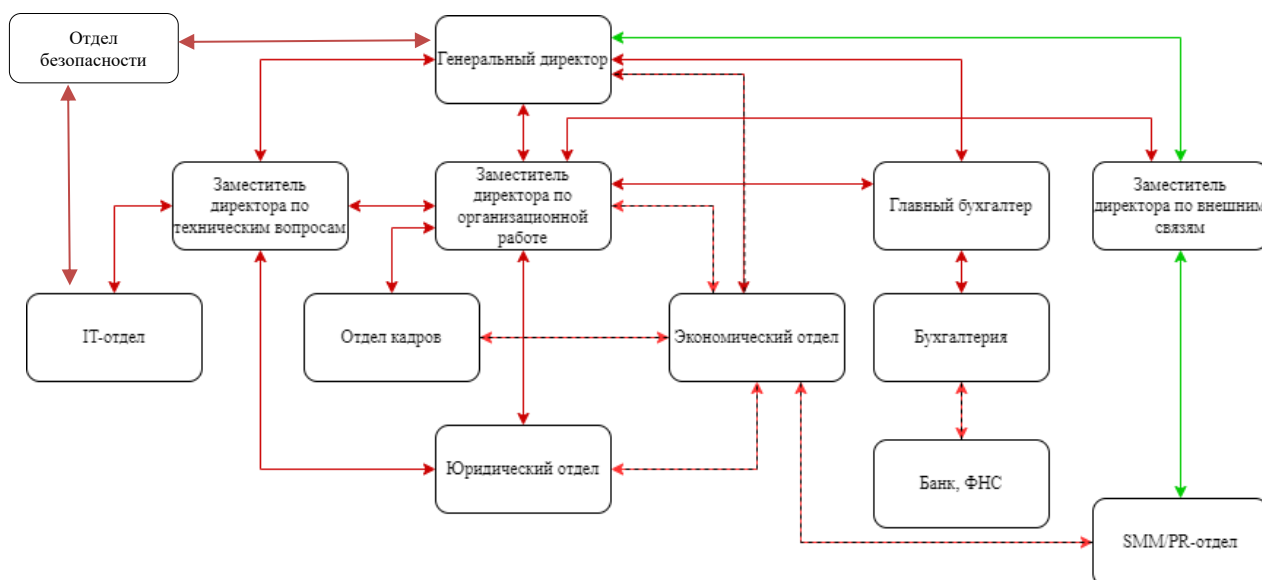


Рисунок 2 – Информационные потоки организации

Открытые потоки проходят между SMM/PR-отделом, заместителем директора по внешним связям и генеральным директором. Данные в этом случае не нуждаются в сокрытии.

Внутренние закрытые потоки проходят внутри предприятия между сотрудниками. Внешние закрытые потоки проходят между бухгалтером и банком.

Закрытые потоки с передаваемой информацией с грифом секретно передаются между юридическим отделом, экономическим отделом, отделом кадров, заместителем директора по организационной работе и генеральным директором.

Информация ограниченного доступа:

1. Персональные данные сотрудников – является информационным активом, представлены в электронной форме, владельцем является руководитель службы безопасности, отдел информационной безопасности;

2. Персональные данные клиентов - является информационным активом, представлены в электронной форме, владельцем являются сотрудники отдела по работе с клиентами с необходимым уровнем доступа;

3. Конфигурация ПО клиентов - является информационным активом, представлена в электронной форме, владельцем являются сотрудники IT-отдела;

4. Техническая информация (логины, пароли, данной локальной сети и т. д.) – является информационным активом, представлены в электронной форме, владельцем являются сотрудники IT-отдела с необходимым уровнем доступа;

5. Коммерческая тайна (данные о производстве) – представлен в электронной форме, владельцем является владелец Организации;

6. Финансовые данные, данные о состоянии счетов, доходов и расходов – являются информационным активом, представлены в электронной форме, владельцем является главный бухгалтер.

3.2 Описание помещения

На рисунке 3 представлен план защищаемого помещения. В таблице 1 представлена легенда плана защищаемого помещения.

Помещение состоит из 6 комнат:

1. Кабинет директора - 10.31 м²;
2. Офисное помещение - 19.51 м²;
3. Компьютерный зал - 11.06 м²;
4. Переговорная - 13.29 м²;
5. Свободная зона - 9.3 м²;
6. Бухгалтерия - 7.9 м².

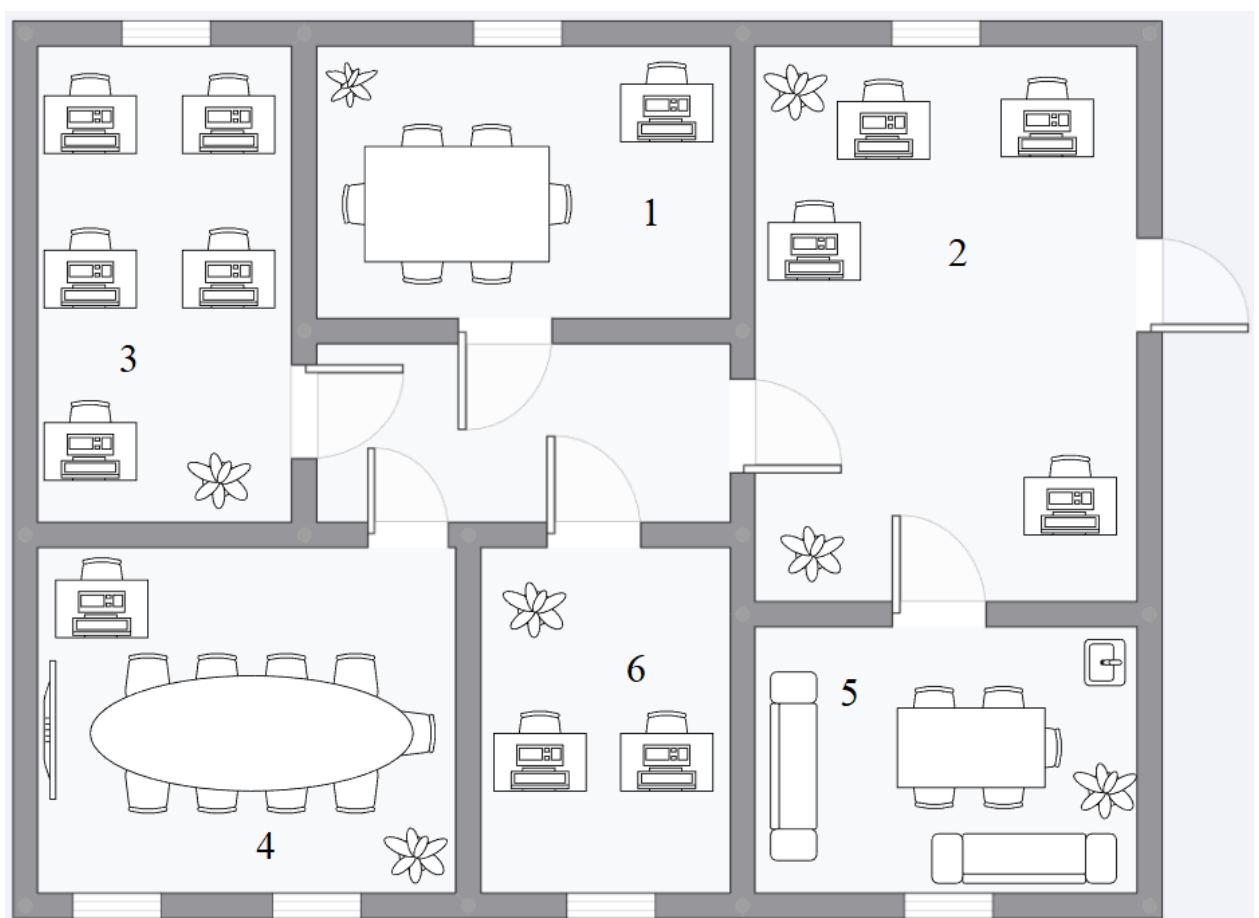
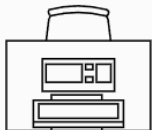
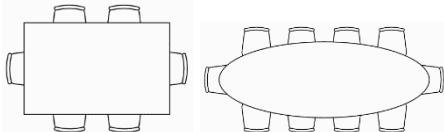




Рисунок 3 – План защищаемого помещения

Таблица 1 – Описание условных обозначений

Условное обозначение	Описание
	Окно

	Стол с персональным компьютером
	Стол для переговоров
	Проектор
	Растение
	Раковина
	Диван

Описание данных в помещениях:

1. Кабинет директора: 1 окно, 1 рабочее место с персональным компьютером, 3 розетки, стол для переговоров на 6 человек, 1 горшок с цветами;
2. Офисное помещение: 1 окно, 4 рабочих места с персональным компьютером, 10 розеток, 2 горшка с цветами;
3. Компьютерный зал: 1 окно, 5 рабочих мест с персональным компьютером, 12 розеток, 1 горшок с цветами;
4. Переговорная: 2 окна, 1 рабочее место с персональным компьютером, 4 розетки, стол для переговоров на 9 человек, проектор, 1 горшок с цветами;
5. Свободная зона: 1 окно, стол на 5 человек, 3 розетки, 2 дивана, раковина, 1 горшок с цветами;
6. Бухгалтерия: 1 окно, 2 рабочих места с персональным компьютером, 5 розеток, 1 горшок с цветами.

Помещение расположено на втором этаже офисного здания, окна выходят в закрытый контролируемый двор. Имеется только один вход и выход. Для всех окон используются решетки с внешней стороны, а с внутренней - жалюзи, плотно закрывающие видимость снаружи.

3.3 Анализ возможных утечек информации

Неправомерный доступ к конфиденциальной информации и информации, составляющей государственную тайну, может осуществляться злоумышленником путем прослушивания разговоров через окна, двери, стены, а также с помощью использования закладных устройств в декоративных элементах помещения. В помещениях есть электрические розетки и персональные компьютеры, которые могут быть использованы для перехвата передаваемой информации.

Таким образом, на объекте актуальны акустические, акустоэлектрические, виброакустические, визуально-оптические, электромагнитные и электрические каналы утечки информации. Материально-вещественный канал утечки информации регулируется организационно-правовыми методами организации.

3.4 Анализ возможных утечек информации

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

Таблица 2 – Средства защиты информации

Технические каналы утечки информации	Источники	Пассивные средства защиты	Активные средства защиты
Акустический, акустоэлектрический	Окна, двери, электрические провода, кабели	Звукоизоляция	Устройства акустического зашумления
Виброакустический	Твердые поверхности помещения	Звукоизоляция	Устройства виброакустического зашумления
Визуально-оптический	Окна, двери	Жалюзи на окнах, доводчики на дверях	Блокирующие устройства
Электрический, электромагнитный	ПК, электрические приборы, розетки	Сетевые фильтры	Устройства электромагнитного зашумления

4 АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Требования к режимным помещениям и их оборудованию содержатся в Решении Межведомственной комиссии по защите государственной тайны №199 от 21.01.2011г. "О типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними".

Для степени секретно должны быть соблюдены следующие требования:

- в помещениях устанавливаются усиленные двери, обеспечивающие надежное закрытие и звукоизоляцию. Двери с двух сторон обшиваются металлическим листом не менее 2 мм толщиной, внутри - звукоизоляционный материал, сама дверь должна иметь толщину не менее 4,5 см.;
- по требованиям безопасности режимных помещений, если окна в комнатах и хранилищах 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;
- оборудование помещений, вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемым к оснащению защищенных и выделенных помещений;
- обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании;
- все режимные помещения оборудуются аварийным освещением;
- перед началом эксплуатации необходимо проверить выделенные и иные режимные помещения проверить на предмет наличия «жучков» и иных средств несанкционированного получения информации.

4.1 Устройства для перекрытия акустического и виброакустического канала утечки информации

Пассивная защита обеспечивается установкой усиленных дверей, обеспечивающих надежное закрытие и звукоизоляцию, отделкой переговорной комнаты и директорского кабинета, используя материалы со звукоизолирующими свойствами.

Активная защита обеспечивается устройствами виброакустического зашумления. Устройства должны быть сертифицированы для защиты выделенных помещений не ниже 3 категории, что соответствует обработке в помещениях информации, составляющей государственную тайну уровня «секретно». Рассмотренные устройства приведены в таблице 3.

Таблица 3 – Средства активной защиты информации акустического и виброакустического канала

Наименование	Описание	Цена, руб.
«Соната-АВ» модель 4Б	Диапазон частот: 175-11200 Гц Количество каналов: 1 Количество логических каналов: 239 Высокая стойкость защиты информации. Есть возможность подключения к одному питающему шлейфу, что делает легче процесс проектирования и монтажа. Индивидуальная регулировка интегрального уровня и корректировка спектра каждого генератора улучшает действие системы. Имеет сертификат соответствия ФСТЭК.	44 200
ЛГШ-404	Диапазон частот: 175-11200 Гц Количество каналов: 2 Предусмотрена возможность регулировки уровня шумового сигнала и частотной коррекции сигнала для каждого выхода в отдельности, а также возможность дистанционного включения и выключения при помощи проводного пульта дистанционного управления. Имеет сертификат соответствия ФСТЭК.	35 100
«БУРАН»	Диапазон частот: 100-11200 Гц Количество каналов: 3 Вывод информации о состоянии работы системы на жидкокристаллический индикатор. Оптимальное использование мощности каналов за счет мониторинга уровня их нагрузки. Возможность дистанционного включения системы по проводному каналу. Имеет сертификат соответствия ФСТЭК.	50 000

По результатам анализа в качестве средства виброакустической защиты был выбран система «Соната-АВ» модель 4Б. Данная модель имеет наиболее широкий диапазон частоты умеренную стоимость.

4.2 Устройства для перекрытия электрического и акустоэлектрического каналов утечки информации

Пассивная защита обеспечивается фильтрации для сетей электропитания во всех помещениях.

Активная защита заключается в создании и передаче по каналам связи белого шума, не позволяющий выделить из перехваченного сигнала полезную информацию. Рассмотренные устройства приведены в таблице 4.

Таблица 4 – Средства активной защиты информации электрического канала

Наименование	Описание	Цена, руб.
ЛГШ-503	<p>Диапазон частот: 0.01–1800 МГц.</p> <p>Система представляет собой генератор шума по цепям электропитания, заземления и ПЭМИН. Обеспечивает защиту информации от утечки по каналам ПЭМИН путем создания на границе контролируемой зоны широкополосной шумовой электромагнитной помехи, которая зашумляет побочные излучения защищаемого объекта.</p> <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 суммарное время работы 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>	44 200
СОНАТА-РСЗ	<p>Диапазон частот: 0.01-2000 МГц</p> <p>Предназначены для защиты объектов вычислительной техники от утечки информации за счет наводок на линии электропитания и заземления.</p> <p>Обеспечивает формирование не синфазных токов и синфазных и паразитных составляющих шумового напряжения во всех проводниках.</p>	32 400
ЛГШ-513	<p>Диапазон частот: 0.009-1800 МГц</p> <p>Система представляет собой генератор шума по цепям электропитания, заземления и ПЭМИН. Обеспечивает защиту информации от утечки за счет побочных электромагнитных излучений и наводок путем формирования маскирующих шумоподобных помех.</p> <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 суммарное время работы в режиме формирования маскирующих помех.</p>	39 000

	Обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним.	
--	---	--

По результатам анализа в качестве средства защиты было выбрано ЛГШ-513, так как оно имеет приемлемую цену и наиболее широкий диапазон частот и защищает от электрического, электромагнитного каналов, а также ПЭМИН.

4.3 Защита от утечек по каналу побочных электромагнитных излучений (ПЭМИН)

Средством защиты от ПЭМИН было выбрано ЛГШ-513. Изделие «ЛГШ-513» соответствует требованиям документа «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок» – по 2 классу защиты.

4.4 Защита от утечек по оптическому каналу

Для обеспечения защиты помещения от утечки по оптическим каналам необходимо установить жалюзи на окна, а также используются доводчики для плотного закрывания дверей. Для данной организации было решено установить жалюзи на все окна в помещении, а также установить доводчики на двери.

5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

Выбранные средства защиты информации включают в себя:

- усиленные двери (переговорная, кабинет директора);
- жалюзи на 7 окон;
- «Соната-АВ» модель 4Б;
- генератор шума «ЛГШ-513».

Таблица 5 – Состав изделия «Соната-АВ» модель 4Б

Базовый элемент	Тип базового элемента
Блок электропитания и управления	"Соната-ИП4.3"
Генератор-акустоизлучатель	"СА-4Б"
Генератор-вибровозбудитель	"СВ-4Б"
Размыкатель телефонной линии	"Соната-ВК4.1"
Размыкатель слаботочной линии	"Соната-ВК4.2"
Размыкатель линии Ethernet	"Соната-ВК4.3"
Пульт управления	"Соната-ДУ4.3"
Блок сопряжения с внешними устройствами	"Соната-СК4.2"

Необходимое количество генераторов-вибровозбудителей "СВ-4Б" можно предварительно оценить из следующих норм:

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

Необходимое количество генераторов-акустоизлучателей "СА-4Б"/"СА4Б1" можно предварительно оценить из следующих норм:

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

Итоговая стоимость выбранных средств защиты информации приведена в таблице 6.

Таблица 6 – Оценка итоговой стоимости средств защиты информации

Базовый элемент	Цена, руб./1 шт.	Количество	Стоимость, руб.
Блок электропитания и управления "Соната-ИП4.3"	21 600	1	21 600
Генератор-акустоизлучатель "СА-4Б"	7 440	9	66 960
Генератор-вибровозбудитель "СВ-4Б"	7 440	14	104 160
Размыкатель телефонной линии "Соната-ВК4.1"	6 000	1	6 000
Размыкатель слаботочной линии "Соната-ВК4.2"	6 000	1	6 000
Размыкатель линии Ethernet "Соната-ВК4.3"	6 000	2	12 000
Пульт управления "Соната-ДУ4.3"	7 680	1	7 680
Блок сопряжения с внешними устройствами "Соната-СК4.2"	13 440	1	13 440
«ЛГШ-513»	39 000	2	78 000
Жалюзи Blackout	1 200	7	8 400
Усиленные двери Torex Super Omega PRO PP	45 000	2	90 000
		ИТОГО	390 264

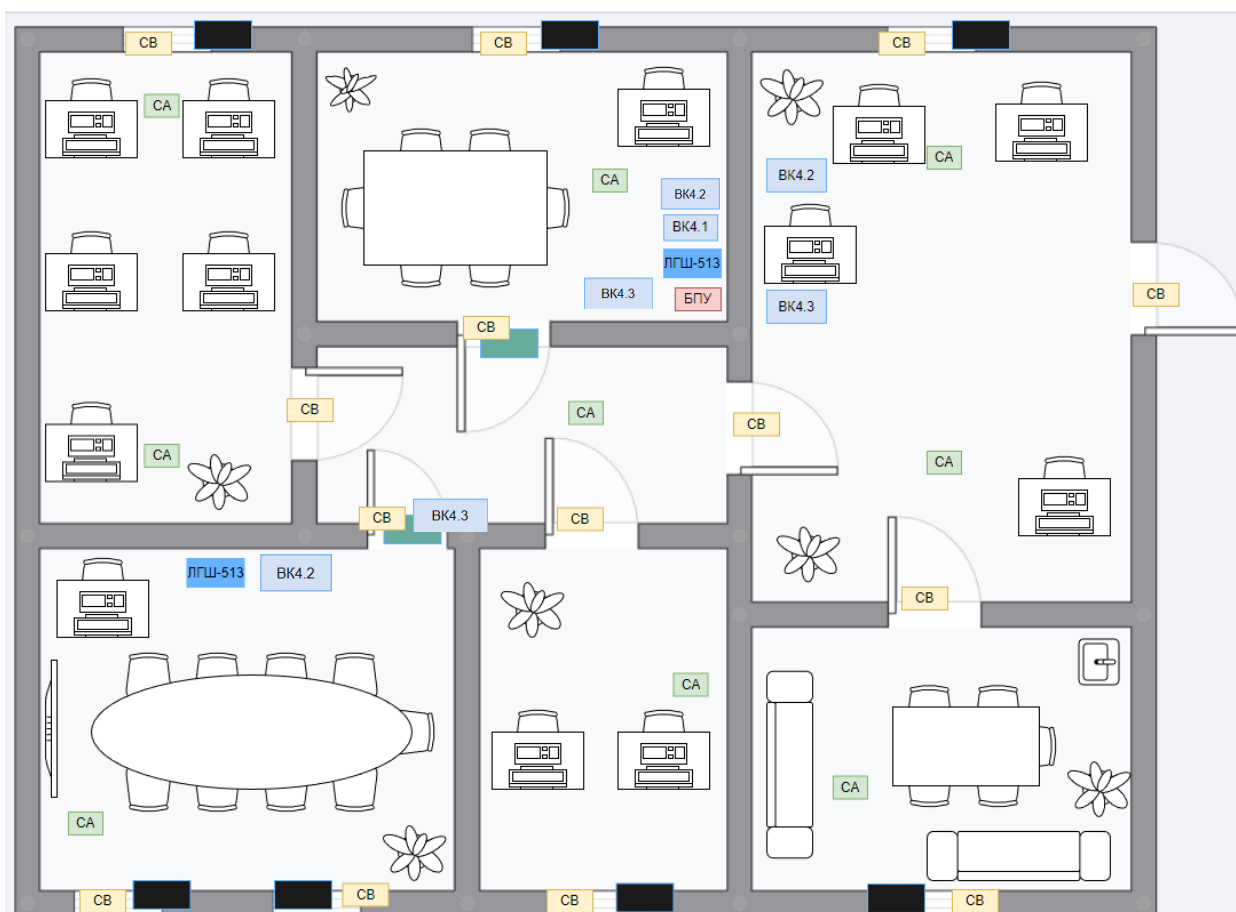


Рисунок 4 – План расстановки СЗИ

Таблица 7 – Описание условных обозначений

Условное обозначение	Описание
	Блок электропитания и управления "Соната-ИП4.3"
	Генератор-акустоизлучатель "СА-4Б"
	Генератор-вибровозбудитель "СВ-4Б"
	Размыкатель телефонной линии
	Размыкатель слаботочной линии
	Размыкатель линии Ethernet
	Генератор шума ЛГШ-513
	Усиленные двери
	Blackout жалюзи

ЗАКЛЮЧЕНИЕ

В ходе написания данной работы были проанализированы существующие каналы утечки информации, потенциальные каналы утечки информации на защищаемом объекте и описаны необходимые меры их защиты. А также проанализирован рынок существующих технических средств для противодействия рассматриваемым каналам утечки информации и выбраны наиболее подходящие для выбранного объекта. На основании выбранных средств защиты был разработан план установки и произведен расчет сметы затрат.

В результате работы была разработана система инженерно-технической защиты, предназначенная для предотвращения утечек конфиденциальной информации и информации, составляющей государственную тайну уровня «секретно», по всем актуальным каналам утечки информации. Общая стоимость всего оборудования составила 390 264 рубля.

СПИСОК ИСПОЛЬЗОВАННОЙ 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. Трунова, А. А. Анализ каналов утечки конфиденциальной информации в информационных системах предприятий / А. А. Трунова. — Текст: непосредственный // Молодой ученый. — 2016. — No 3 (107). — С. 69–72. — URL: <https://moluch.ru/archive/107/25842>.
3. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010.- 436 с.