

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ

УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«УНИВЕРСИТЕТ ИТМО»

Факультет безопасности информационных технологий

КУРСОВАЯ РАБОТА

по дисциплине:

«Инженерно-технические средства защиты информации»

на тему:

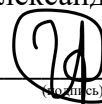
«Проектирование инженерно-технической защиты информации на предприятии»

Вариант 68

Выполнила:

Студент группы N34491

Ивахненко Александра Андреевна



(подпись)

Проверил:

к.т.н., доцент ФБИТ

Попов Илья Юрьевич

(подпись)

(отметка о выполнении)

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент Ивахненко Александра Андреевна
(Фамилия И.О.)
Факультет Безопасности Информационных Технологий
Группа №34491
Направление (специальность) Комплексные системы 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 защиты информации на предприятии
Задание Проектирование 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, 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 Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010.- 436 с

Руководитель Попов Илья Юрьевич
(Подпись, дата)
Студент Ивахненко Александра Андреевна 20.12.2023
(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОГО ПРОЕКТА (РАБОТЫ)

Студент Ивахненко Александра Андреевна
(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34491

Направление (специальность) Комплексные системы защиты информации

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

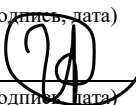
Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической защиты информации на предприятии

Задание Проектирование инженерно-технической защиты информации на предприятии

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Разработка и утверждение задания и календарного плана на курсовую работу	27.09.2023	11.10.2023	
2	Анализ теоретической составляющей	18.10.2023	1.11.2023	
3	Разработка комплекса инженерно-технической защиты информации в заданном помещении	22.11.2023	6.12.2023	
4	Представление выполненной курсовой работы	20.12.2023	20.12.2023	

Руководитель Попов Илья Юрьевич
(Подпись, дата)

Студент Ивахненко Александра Андреевна  20.12.2023
(Подпись, дата)

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

АННОТАЦИЯ НА КУРСОВОЙ ПРОЕКТ (РАБОТУ)

Студент Ивахненко Александра Андреевна
(Фамилия И.О.)
Факультет Безопасности Информационных Технологий
Группа N34491
Направление (специальность) Комплексные системы 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 защиты информации на предприятии
Задание Проектирование инженерно-технической защиты информации на предприятии

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

1. Цель и задачи работы ☐ Предложены студентом ☐ Сформулированы при участии студента
☒ Определены руководителем

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 ☐ Расчет ☒ Конструирование
☐ Моделирование ☐ Другое _____

3. 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

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 Попов Илья Юрьевич

Студент Ивахненко Александра Андреевна

(Подпись, дата)

(Подпись, дата)

20.12.2023

СОДЕРЖАНИЕ

Цель работы	6
Задачи работы	6
Введение	7
1 Анализ технических каналов утечки информации.....	8
2 Нормативно-правовая база	8
3 Анализ защищаемых помещений	14
3.1 План и описание помещения	14
3.2 Информационные потоки предприятия.....	15
3.3 Анализ возможных утечек информации.....	16
3.4 Выбор средств защиты информации.....	16
4 Анализ технических средств защиты информации	18
4.1 Требования к защите помещений.....	18
4.2 Анализ СЗИ для акустического и виброакустического каналов.....	20
4.3 Анализ СЗИ для электромагнитного, электрического каналов	23
4.4 Анализ СЗИ для ПЭМИН	26
4.5 Анализ СЗИ для визуально-оптического канала	27
5 Описание расстановки технических средств.....	28
Заключение	33
Список использованных источников.....	34

Цель работы

Повышение защищенности рассматриваемого помещения.

Задачи работы

1. Проанализировать защищаемые помещения.
2. Изучить нормативно-правовую базу.
3. Оценить каналы утечки информации.
4. Проанализировать средства защиты информации.
5. Разработать систему защиты информации на основе выбранных средств.

Введение

Конфиденциальная информация, циркулирующая на предприятии, играет важную роль в его функционировании. Под конфиденциальной информацией понимают документированную информацию, доступ к которой ограничен законодательством Российской Федерации. Это могут быть сведения, которые составляют коммерческую тайну предприятия, персональные данные сотрудников или клиентов, служебная информация и др. Соответственно, эти данные могут стать объектом интереса злоумышленников. Поэтому необходимо создавать условия, при которых возможность утечки конфиденциальной информации будет минимизирована.

Одним из способов перехвата информации выделенного помещения без проникновения в пределы контролируемой зоны объекта является перехват информации по техническим каналам утечки.

В данной работе рассмотрен процесс разработки комплекса инженерно-технической защиты информации, составляющей служебную тайну с уровнем «секретно» на объекте информатизации.

Объектом исследования являются защищаемые помещения.

Предметом исследования является безопасность информации ограниченного доступа, циркулирующей внутри помещения.

1 Анализ технических каналов утечки информации

Утечка - бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

Канал утечки информации – совокупность источника информации, материального носителя или среды распространения несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя. Одним из основных свойств канала является месторасположение средства выделения информации из сигнала или носителя, которое может быть в пределах контролируемой зоны, охватывающей систему, или вне ее.

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

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

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

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

Таким образом, описание ТКУИ должно включать в себя:

- источник угрозы (приемник информативного сигнала);
- среда передачи информационного сигнала;
- источник (носитель) информации.



Рисунок 1 – Структура технического канала утечки информации

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

- визуально-оптические;
- электромагнитные;
- акустические;
- материально-вещественные.

1. Визуально-оптические каналы утечки.

В зависимости от условий наблюдения обычно используются соответствующие технические средства, в том числе: оптика (бинокли, подзорные трубы, телескопы, монокуляры), телекамеры, приборы ночного видения, тепловизоры и т. п. Для документирования результатов наблюдения

проводится съемка объектов с помощью фотографических и телевизионных средств, соответствующих условиям съемки. Для снятия копий документов используются электронные и специальные (закамуфлированные) фотоаппараты. Для дистанционного съема видовой информации используют видеозакладки.

2. Электромагнитные каналы утечки.

Каждое электрическое (электронное) устройство является источником магнитных и электромагнитных полей широкого спектра, характер которых определяется назначением и схемными решениями, мощностью устройства, материалами, из которых оно изготовлено, и его конструкцией.

3. Акустические каналы утечки.

Акустический канал утечки информации реализуется в следующем:

- подслушивание разговоров на открытой местности и в помещениях, находясь рядом или используя направленные микрофоны (бывают параболические, трубчатые или плоские). Направленность 2-5 градусов, средняя дальность действия наиболее распространенных — трубчатых составляет около 100 метров. При хороших климатических условиях на открытой местности параболический направленный микрофон может работать на расстояние до 1 км;
- негласная запись разговоров на диктофон или магнитофон (в том числе цифровые диктофоны, активизирующиеся голосом);
- подслушивание разговоров с использованием выносных микрофонов (дальность действия радиомикрофонов 50-200 метров без ретрансляторов).

4. Материально-вещественные каналы утечки.

Утечка информации производится путем несанкционированного распространения за пределы контролируемой зоны вещественных носителей с

защищаемой информацией. Но данный вид утечек не рассматривается в курсовой работе.

2 Нормативно-правовая база

Основными документами в области защиты информации являются:

1. Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера».
3. Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
4. Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации».
5. Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) «О сертификации средств защиты информации».
6. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
7. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
8. СТР-К. Специальные требования и рекомендации по технической защите конфиденциальной информации.
9. Методика сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров.
10. Временные методики сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров по требованиям безопасности информации.
11. Временный порядок аттестации объектов информатизации по требованиям безопасности информации.
12. РД. Защита от несанкционированного доступа к информации. Термины и определения.

13. РД. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.

14. РД. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.

15. РД. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники.

16. Требования по содержанию и функционированию нотариальной конторы, обеспечению надлежащих условий для приема нотариусом обратившихся за совершением нотариальных действий лиц.

17. Требования по содержанию и функционированию нотариальной конторы, обеспечению надлежащих условий для приема нотариусом обратившихся за совершением нотариальных действий лиц.

18. РД. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации.

19. РД. Защита информации. Специальные защитные знаки. Классификация и общие требования.

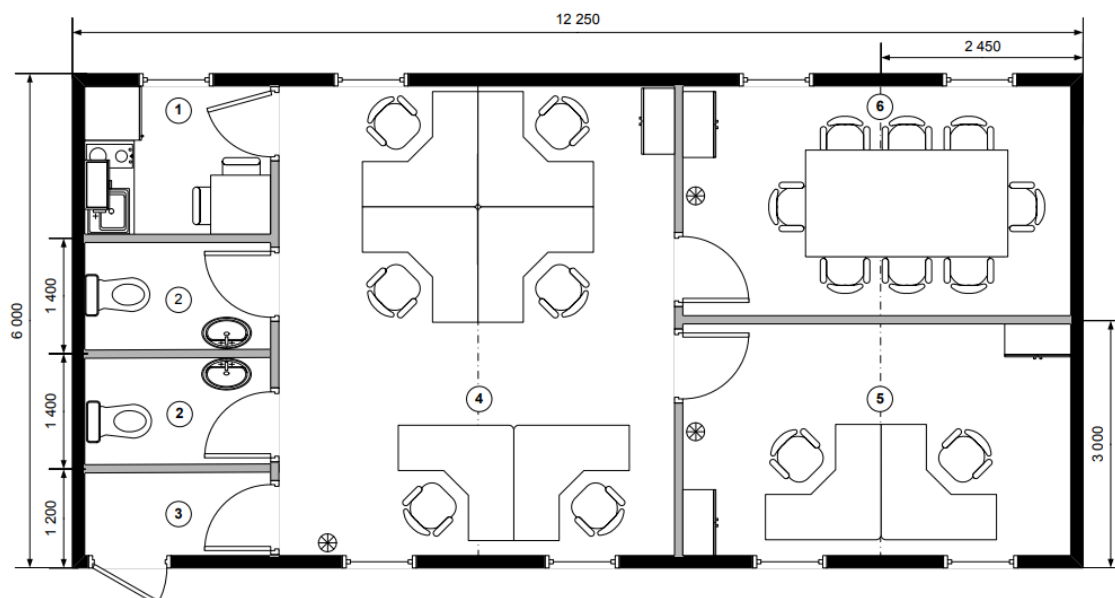
20. РД. Гостехкомиссии России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей.

21. РД. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам.

3 Анализ защищаемых помещений

3.1 План и описание помещений

Проведем анализ защищаемых помещений. На рисунке 2 представлен план с учетом мебелировки.



Наименование	Площадь, м²	Наименование	Площадь, м²
1. Кухня, комната отдыха	4,9	4. Кабинет	29,4
2. Санузел	3,4	5. Кабинет	14,7
3. Тамбур	2,9	6. Зал совещаний	14,7

Рисунок 2 – План защищаемого помещения

Защите подлежат следующие помещения:

- 1) Кабинет директора (5): 4,9 м * 3 м (14,7 м²);
- 2) Зал совещаний (6): 4,9 м * 3 м (14,7 м²);
- 3) Компьютерный зал (4): 4,9 м * 6 м (29,4 м²);
- 4) Кухня, комната отдыха (1): 4,9 м * 6 м (29,4 м²).

В кабинете директора находится 2 стола, 2 стула, 1 шкаф, 1 сейф, ПК, телефон. Помещение оснащено батареями центрального отопления, 2 окнами и 3 розетками.

В переговорной находится стол, 8 стульев, проектор и доска для проектора, часы и шкаф. Помещение оснащено батареями центрального

отопления, 2 окнами и 4 розетками.

В компьютерном зале находятся 6 столов, 6 стульев, 6 ПК. Помещение оснащено 3 окнами, батареями центрального отопления и 5 розетками.

На кухне (зона отдыха) находится холодильник, плита, стол, 2 кресла. Помещение оснащено окном, батареей центрального отопления, раковиной и 2 розетки.

Помещение расположено на первом этаже многоэтажного здания, окна выходят в закрытый контролируемый двор. Окна не соседствуют с пожарными и эвакуационными лестницами и элементами, с которых в помещения могут проникнуть внешние нарушители, крышами пристроек, выступами на стенах, балконами и прочими элементами, с которых в помещения могут проникнуть посторонние лица.

Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см, высотой 3 м.

3.2 Информационные потоки предприятия

На схеме информационных потоков (рисунок 3) пунктиром обозначены открытые потоки, сплошной линией – закрытые.

Открытые информационные потоки:

Взаимодействие с внешним предприятием – налоговой.

Закрытые информационные потоки:

Взаимодействие работников нотариальной конторы между собой, взаимодействие нотариуса и секретарей с клиентами, банковские операции.



Рисунок 3 – Схема информационных потоков предприятия

3.3 Анализ возможных утечек информации

В помещениях предприятия такие элементы, как шкафы и часы, куда можно спрятать закладное устройство. Практически в каждом помещении есть розетки и электрические приборы, поэтому есть возможность снятия информации с электрического и электромагнитного каналов. Окна в помещениях не защищены, поэтому актуальны визуально-оптический, акустический, виброакустический, вибрационный канал утечки информации.

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

3.4 Выбор средств защиты информации

Для обеспечения комплексной безопасности согласно типу конфиденциальной информации (служебная тайна) требуется оснастить помещение средствам защиты, приведенными в таблице 1.

Таблица 1 – Активная и пассивная защита информации

Каналы	Источники	Пассивная защита	Активная защита
Электромагнитный, электрический	Розетки во всех помещениях, ПК, линии связи, электрические приборы	Фильтры для сетей электропитания, экранирующие материалы	Устройства электромагнитного зашумления
Вибрационный, виброакустический	Стены, потолки, полы, трубы водоснабжения, канализации, батареи центрального отопления	Изоляция стен, дверей в виде дополнительных обшивок	Устройства вибрационного зашумления
Акустический	Окна, двери, электрические сети, проводка, розетки	Звукоизоляция, фильтры для сетей электропитания, доводчики	Устройства акустического зашумления
Визуально-оптический	Окна, двери	Жалюзи на окнах, доводчики	Бликующие устройства

4 Анализ технических средств защиты информации

4.1 Требования к защите помещений

В соответствии с заданием курсовой работы предприятие работает с информацией 3 степени секретности или с информацией, представляющей служебную тайну с грифом «секретно».

Организация и проведение работ по технической защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, при ее обработке техническими средствами определяются специальными требованиями и рекомендациями по технической защите конфиденциальной информации.

Основные требования и рекомендации по защите информации, циркулирующей в защищаемых помещениях:

1) Защищаемые помещения (ЗП) должны размещаться в пределах контролируемой зоны (КЗ). При этом рекомендуется размещать их на удалении от границ контролируемой зоны, обеспечивающем эффективную защиту, ограждающие конструкции (стены, полы, потолки) не должны являться смежными с помещениями других учреждений (предприятий). Не рекомендуется располагать защищаемые помещения на первых этажах зданий. Для исключения просмотра текстовой и графической конфиденциальной информации через окна помещения рекомендуется оборудовать их шторами (жалюзи).

2) Специальная проверка ЗП и установленного в нем оборудования с целью выявления возможно внедренных в них электронных устройств перехвата информации "закладок" проводится, при необходимости, по решению руководителя предприятия.

3) Во время проведения конфиденциальных мероприятий запрещается использование в ЗП радиотелефонов, оконечных устройств сотовой, пейджинговой и транкинговой связи, переносных магнитофонов и других средств аудио и видеозаписи. При установке в ЗП телефонных и

факсимильных аппаратов с автоответчиком или спикерфоном, а также аппаратов с автоматическим определителем номера, следует отключать их из сети на время проведения этих мероприятий.

4) Для исключения возможности утечки информации за счет электроакустического преобразования рекомендуется использовать в ЗП в качестве оконечных устройств телефонной связи, имеющих прямой выход в городскую АТС, телефонные аппараты (ТА), прошедшие специальные исследования, либо оборудовать их сертифицированными средствами защиты информации от утечки за счет электроакустического преобразования.

5) Системы пожарной и охранной сигнализации ЗП должны строиться только по проводной схеме сбора информации (связи с пультом) и, как правило, размещаться в пределах одной с ЗП контролируемой зоне. В качестве оконечных устройств пожарной и охранной сигнализации в ЗП рекомендуется использовать изделия, сертифицированные по требованиям безопасности информации, или образцы средств, прошедшие специальные исследования и имеющие предписание на эксплуатацию.

6) Звукоизоляция ограждающих конструкций ЗП, их систем вентиляции и кондиционирования должна обеспечивать отсутствие возможности прослушивания ведущихся в нем разговоров из-за пределов ЗП. Проверка достаточности звукоизоляции осуществляется аттестационной комиссией путем подтверждения отсутствия возможности разборчивого прослушивания вне ЗП разговоров, ведущихся в нем. При этом уровень тестового речевого сигнала должен быть не ниже используемого во время штатного режима эксплуатации помещения. Для обеспечения необходимого уровня звукоизоляции помещений рекомендуется оборудование дверных проемов тамбурами с двойными дверями, установка дополнительных рам в оконных проемах, уплотнительных прокладок в дверных и оконных притворах и применение шумопоглотителей на выходах вентиляционных каналов. Если предложенными выше методами не удастся обеспечить необходимую акустическую защиту, следует применять организационно-режимные меры,

ограничивая на период проведения конфиденциальных мероприятий доступ посторонних лиц в места возможного прослушивания разговоров, ведущихся в ЗП.

7) Для снижения вероятности перехвата информации по виброакустическому каналу следует организационно-режимными мерами исключить возможность установки посторонних (нештатных) предметов на внешней стороне ограждающих конструкций ЗП и выходящих из них инженерных коммуникаций (систем отопления, вентиляции, кондиционирования). Для снижения уровня виброакустического сигнала рекомендуется расположенные в ЗП элементы инженерно-технических систем отопления, вентиляции оборудовать звукоизолирующими экранами.

8) В случае, если указанные выше меры защиты информации от утечки по акустическому и виброакустическому каналам недостаточны или нецелесообразны, рекомендуется применять метод активного акустического или виброакустического маскирующего зашумления. Для этой цели должны применяться сертифицированные средства активной защиты.

9) Передача конфиденциальной речевой информации по открытым проводным каналам связи, выходящим за пределы КЗ, и радиоканалам должна быть исключена. При необходимости передачи конфиденциальной информации следует использовать защищенные линии связи (например, защищенные волоконно-оптические), устройства скремблирования или криптографической защиты. Используемые средства защиты информации должны быть сертифицированы по требованиям безопасности информации.

4.2 Анализ СЗИ для акустического и виброакустического каналов

Пассивная защита представляет собой: усиленные двери звукоизоляционные Rw Prima M900, стоимостью 27 150 рублей.

Активная защита представляет собой систему виброакустического зашумления. Для защиты помещения для работы со служебной тайной уровня «секретно» рассматриваются технические средства активной защиты

информации для объектов информатизации категории не ниже не ниже 3Б соответствии с РД Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации". Ниже в таблице 2 приведен сравнительный анализ подходящих средства активной защиты помещений по виброакустическому каналу.

Таблица 2 – Сравнительный анализ средств активной защиты для виброакустического канала

Модель	Цена, руб.	Назначение	Описание	Особенности
SI-3030	28 500	Предназначен для защиты помещений от прослушивания через строительные элементы конструкции. Принцип действия прибора основан на маскировании спектра речи шумовой помехой, излучаемой в стены, перекрытия, окна, воздухов.	Спектр шумовой помехи: 125 Гц – 6,3 кГц	Время работы не ограничено.
ШОРОХ-5Л	21 500	Предназначена для защиты акустической речевой информации, циркулирующей в помещениях от утечки по акустическим, вибрационным, виброакустическим каналам, а также за счёт акустоэлектрических преобразований в линиях компьютерных сетей и телефонии, слаботочных и электропитания, отходящих от технических средств.	Диапазон частот 80–11300 Гц	Успешно прошла сертификацию ФСТЭК и разрешена для использования в выделенных помещениях всех категорий.

Модель	Цена, руб.	Назначение	Описание	Особенности
СОНАТА АВ-4Б	44 200	“Соната-АВ” модель 4Б является комплексом защиты от утечки информации по различным каналам. Производство изделия Соната-АВ” модель 4Б сертифицировано. Сертификат ФСТЭК. “Соната-АВ” модель 4Б построена по принципу "единый источник электропитания + генераторы-электроакустические преобразователи (излучатели)". Благодаря этому построению проявляется высокая стойкость защиты информации.	Диапазон воспроизводимого шумового сигнала 175–11200 Гц	<p>Есть возможность подключения к одному питающему шлейфу. Это делает легче процесс проектирования и монтажа</p> <p>Индивидуальная регулировка интегрального уровня и корректировка спектра каждого генератора улучшает действие системы</p>
БУБЕН- УЛЬТРА МАКС	52 797	Предназначен для полного или частичного подавления полезного звукового сигнала при попытке записи на записывающие устройства, специальные технические средства, выносные микрофоны посредством генерации трех типов помех	До 48 ультразвуковых излучателей	<p>Самое большое количество подключаемых излучателей – до 192 шт при подключении четырех основных блоков.</p> <p>Четыре канала усилителя низкой частоты (далее УНЧ) для вывода речеподобной помехи.</p> <p>Возможность вывода речеподобной помехи на трансляционные громкоговорители, акустические излучатели разных типов,</p>

Модель	Цена, руб.	Назначение	Описание	Особенности
				пьезоэлектрический и электромагнитный виброакустический излучатель.

По результатам анализа была выбрана система **СОНАТА АВ-4Б**, стоимость которой равна 44 200 рублей. Улучшенная аппаратная настройка элементов модели 4Б позволяет связывать источник электропитания с другими для обмена информацией. Это дает возможность:

- Создать систему автоматического контроля всех элементов;
- Снизить время на конфигурирование и тестирование системы;
- Изменить настройки генераторов и построить гибкую систему виброакустической защиты;
- Уменьшить затраты благодаря использованию единой линии связи и электропитания.

4.3 Анализ СЗИ для электромагнитного, электрического каналов

Пассивная защита представляет собой фильтры для сетей электропитания во всех помещениях.

Активная защита основывается на установке систем пространственного зашумления, использующие помехи типа "белый шум", то есть излучающие широкополосный шумовой сигнал (как правило, с равномерно распределенным энергетическим спектром во всем рабочем диапазоне частот), существенно превышающий уровни побочных электромагнитных излучений.

Таблица 3 – Активная защита от утечек по электрическим каналам

Модель	Цена, руб.	Назначение	Описание	Сертификация
ФИЛЬТР ФП-6	50 556	Фильтр ФП-6 предотвращает утечки информации по цепям электропитания, а также защищает средства оргтехники от внешних помех.	Фильтр сетевой помехоподавляющий	ФП-6 ослабляет любые сигналы в диапазоне 0,01–1800 МГц с эффективностью 60 дБ и, соответственно, не пропускают информативные сигналы, возникающие при работе средств оргтехники
Генератор шума ЛГШ-501	29 900	Предназначен для использования в целях защиты информации, содержащей сведения, составляющие государственную тайну и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет побочных электромагнитных излучений и наводок путем формирования маскирующих шумоподобных помех.	Генератор шума по цепям электропитания, заземления и ПЭМИН	Изделие «ЛГШ-501» соответствует требованиям документа «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, 2014)
ГЕНЕРАТОР ШУМА СОНАТА РС2	23 600	Предназначен для активной защиты объектов ВТ (объектов вычислительной техники) или, другими словами, переговорных помещений от утечки информации через линии электропитания	Устройства для защиты линий электропитания, заземления от утечки информации	Отличается от прибора Соната РС-1 только наличием модуля ИК-управления, что позволяет дистанционное включение прибора с пульта

Модель	Цена, руб.	Назначение	Описание	Сертификация
		и заземления.		управления. Тогда как Соната РС-1 включается только в розетку
ГЕНЕРАТОР ШУМА СОНАТА-РС3	32 400	Предназначено для подключения к 3-проводной сети (энергосеть с проводом заземления);	Устройство для активной защиты информации от утечки по сети электропитания	<ul style="list-style-type: none"> — возможность регулирования уровня излучаемых электромагнитных шумов; — возможность блокировки прибора от несанкционированного доступа; — световой и звуковой индикаторы работы и контроля уровня излучения; — совместимость с проводными пультами ДУ линейки СОНАТА.

В результате анализа был выбран генератор шума **Соната-РС2**, стоимость которого равна 23 600 рублей (приемлемая цена), а фирма производителя совпадает с виброакустической защитой.

Другие преимущества:

- диапазон частот для "Соната-РС2" – до 2 ГГц;
- в изделии "Соната-РС2" возможна регулировка уровня шума в 3

частотных полосах;

- в изделии "Соната-РС2" предусмотрена возможность удаленного управления, как в случае автономного использования (непосредственно Пультом ДУ ИК 2х-кнопочным), так и в случае использования в составе комплекса ТСЗИ.

4.4 Анализ СЗИ для ПЭМИН

Для реализации активной защиты от ПЭМИН было выбрано устройство **Соната-РЗ**, стоимостью 97 200 рублей. Устройство совместимо со средством защиты Соната АВ-4Б, которое выбрано для виброакустической защиты.

Другие преимущества:

- комбинированный характер защиты (электромагнитное излучение + шумовое напряжения в линии электропитания и заземления);
- наличие регулятора интегрального уровня формируемых электромагнитного поля шума и шумовых напряжений;
- возможность, в случае необходимости, дополнительного повышения уровня излучаемого электромагнитного поля шума в диапазоне частот 0,01...200 МГц за счет применения опционально поставляемой дополнительной антенны;
- встроенная система контроля интегрального уровня излучения со световой индикацией и звуковой сигнализацией;
- возможность удаленного управления изделием как в случае автономного использования, так и в случае использования в составе комплекса ТСЗИ;
- наличие счетчика наработки в режиме "Излучение".

4.5 Анализ СЗИ для оптического канала

Для обеспечения защиты информации по оптическому каналу необходимо установить шторы на окна – Штора рулонная блэкаут «Штрих» 100x175 см 2 008 рублей / штука.

5 Описание расстановки технических средств

В ходе анализа в 4 пункте работы были выбраны следующие средства защиты информации:

- Виброакустическая защита «Соната АВ-4Б»;
- Генератор шума «Соната РС2»;
- Средство активной защиты информации от ПЭМИН «Соната-РЗ»;
- Шторы рулонные блэкаут «Штрих»;
- Двери звукоизоляционные Rw Prima M900.

В состав комплекса "Соната-АВ" модель 4Б входят:

- 1) Пульт управления "Соната-ДУ4.3";
- 2) Генераторы-акустоизлучатели "СА-4Б";
- 3) Генераторы-вибровозбудители "СВ-4Б";
- 4) Блок электропитания и управления "Соната-ИП4.3";
- 5) Генераторный блок "Соната-АВ-4Л";
- 6) Вибровозбудитель "Соната-СП-4Л";
- 7) Размыкатель телефонной линии "Соната-ВК4.1"
- 8) Размыкатель слаботочной линии "Соната-ВК4.2"
- 9) Размыкатель линии Ethernet "Соната-ВК4.3"

Рекомендации по определению количества и мест установки акустоизлучателей и вибровозбудителей:

Оптимальное количество акустоизлучателей и вибровозбудителей для каждого помещения определяется такими факторами, как его звукоизолирующие свойства, конфигурация, материалы ограждающих поверхностей, расположение помещения, уровень шумового фона и т.п. Весьма существенными могут быть ограничения, обусловленные жесткими требованиями к сохранению дизайна помещения. При этом аттестация помещения возможна только после измерения уровня его защищенности и

приведения показателей в соответствие с нормативными требованиями. Указанные факторы и обстоятельства делают невозможным точное теоретическое предсказание оптимального количества и мест установки акустоизлучателей и вибровозбудителей в каждом конкретном случае.

В то же время, в ходе решения таких задач, как предпроектная подготовка, составление сметы по спецоборудованию объектов и т.п., возникает потребность в быстрой предварительной оценке необходимого количества элементов аппаратуры виброакустической защиты.

Ориентировочное количество вибровозбудителей "СВ-4Б" может быть определено исходя 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;
- окна - один на окно (при установке на оконный переплет);
- двери - один на дверь (при установке на верхнюю перекладину дверной коробки);
- трубы систем.

Ориентировочное количество акустоизлучателей "СА-4Б" может быть определено исходя из следующих норм:

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

Также будет установлено 3 звукоизоляционные двери (в зал совещаний, кабинет директора и компьютерный зал) и 8 рулонных штор блэкаут (на каждое окно)

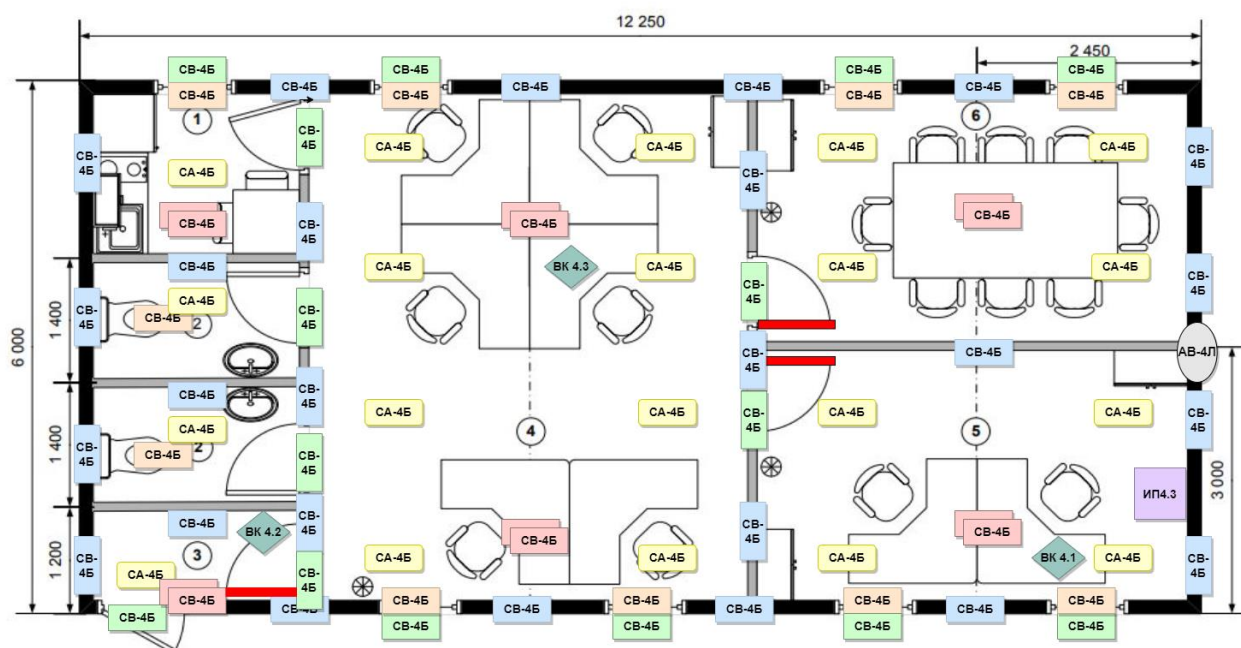
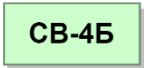
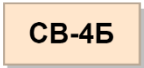








Рисунок 4 – План помещения с расстановкой устройств

Таблица 4 – Смета и условные обозначения

СЗИ	Условное обозначение	Цена за штуку, руб.	Количество, шт.	Конечная стоимость, руб.
Пульт управления "Соната-ДУ4.3"	-	7 680	1	7 680
Генераторы-акустоизлучатели "СА-4Б"	<div style="border: 1px solid black; background-color: yellow; padding: 2px; display: inline-block;">СА-4Б</div>	7 440	16	119 040
Генераторы-вибровозбудители "СВ-4Б"	Стены: <div style="border: 1px solid black; background-color: lightblue; padding: 2px; display: inline-block;">СВ-4Б</div> Потолок, пол: <div style="border: 1px solid black; background-color: pink; padding: 2px; display: inline-block;">СВ-4Б</div> Окна, двери:	7 440	$26 + 12 + 8 + 8 = 54$	401 760

СЗИ	Условное обозначение	Цена за штуку, руб.	Количество, шт.	Конечная стоимость, руб.
	 Трубы систем: 			
Блок электропитания и управления "Соната-ИП4.3"		21 600	1	21 600
Генераторный блок "Соната-АВ-4Л"		10 320	1	10 320
Вибровозбудитель "Соната-СП-4Л"	Входят в СВ-4Б на окнах	840	8	6 720
Размыкатель "Соната-ВК4.1"		6 000	1	6 000
Размыкатель "Соната-ВК4.2"		6 000	1	6 000
Размыкатель "Соната-ВК4.3"		6 000	1	6 000
Генератор шума "Соната РС2"	Входит в ИП4.3	23 600	1	23 600
СЗИ от ПЭМИН "Соната-РЗ"	Входит в ИП4.3	97 200	1	97 200

СЗИ	Условное обозначение	Цена за штуку, руб.	Количество, шт.	Конечная стоимость, руб.
Шторы рулонные блэкаут «Штрих»	На каждом окне	2 008	8	16 064
Двери звукоизоляцион ные Rw Prima M900		27 150	3	81 450
Итог:	803 434 рублей			

Заключение

В ходе выполнения курсовой работы был произведен разбор теоретического материала по техническим каналам утечек и мерам защиты от них. В соответствии с вариантом были проанализированы защищаемые помещения и изучена нормативно-правовую базу. После оценки каналов утечки информации и анализа средств защиты информации была разработана система защиты информации на основе выбранных средств. Итоговый комплекс СЗИ был оценен в 803 434 рубля.

Список использованных источников

1. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010.- 436 с.
2. Трунова, А. А. Анализ каналов утечки конфиденциальной информации в 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: 20.12.2022).
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. НПО «Анна» / [Электронный ресурс] // Npoanna: [сайт]. — URL: <http://www.npoanna.ru/> (дата обращения: 20.12.2022).
5. Детектор Системс» / [Электронный ресурс] // Detsys: [сайт]. — URL: <https://detsys.ru/> (дата обращения: 20.12.2022).