

**Министерство науки и высшего образования Российской Федерации
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 защиты
информации на предприятии**

Выполнил:

**Креславский Михаэль
N34501**



Проверил преподаватель:

**Попов И. Ю., к.т.н, доцент
ФБИТ**

Отметка о выполнении:

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент	Креславский Михаэль
	(Фамилия И.О.)
Факультет	Безопасность информационных технологий
Группа	
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
Задание	Разработать систему инженерно-технической защиты информации на предприятии


Краткие методические указания

- Курсовая работа выполняется в рамках изучения дисциплины «Инженерно-технические средства защиты информации».
- Порядок выполнения и защиты курсовой работы представлен в методических указаниях, размещенных на коммуникационной площадке дисциплины.
- Объект исследований курсовой работы ограничивается заданным помещением.

Содержание пояснительной записки

- Введение.
- Организационная структура предприятия.
- Обоснование защиты информации.
- Анализ защищаемых помещений.
- Анализ рынка технических средств.
- Описание расстановки технических средств.
- Заключение.
- Список литературы.

Рекомендуемая литература

Руководитель		(Подпись, дата)
Студент		18.12.2023
		(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Креславский Михаэль

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа

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

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируема я	Фактически я	
1	Разработка и утверждение задания и календарного плана на курсовую работу	13.11.2023	13.11.2023	
2	Анализ теоретической составляющей	25.11.2023	25.11.2023	
3	Разработка комплекса инженерно-технической защиты информации в заданном помещении	03.12.2023	04.12.2023	
4	Представление выполненной курсовой работы	18.12.2023	18.12.2023	

Руководитель

(Подпись, дата)

Студент



18.12.2023

(Подпись, дата)

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

Студент	Креславский Михаэль
	(Фамилия И.О.)
Факультет	Безопасность информационных технологий
Группа	
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

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

1. Цель и задачи работы

Предложены студентом при участии студента	<input checked="" type="checkbox"/> Сформулированы
	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

2. Характер работы

Расчет	<input type="checkbox"/>	<input type="checkbox"/>	Конструирование Другое Проектирование
Моделирование	<input checked="" type="checkbox"/>	<input type="checkbox"/>	


Содержание работы

- Введение.
- Организационная структура предприятия.
- Обоснование защиты информации.
- Анализ защищаемых помещений.
- Анализ рынка технических средств.
- Описание расстановки технических средств.
- Заключение.
- Список литературы.

3. 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  18.12.2023

(Подпись, дата)

«__» _____ 20__ г

СОДЕРЖАНИЕ

Введение	7
1 Организационная структура предприятия	8
1.1 Информационные потоки	8
1.2 Структура информационных потоков на предприятии	8
2 Обоснование защиты информации	9
3 Анализ защищаемых помещений	10
3.1 Схема помещения	10
4 Анализ рынка технических средств	12
4.1 Выбор средств защиты	12
4.2 Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам	13
4.3 Защита от утечки информации по (вибро-) акустическим каналам	15
4.4 Защита от ПЭМИН	17
4.5 Защита от утечек информации по оптическим каналам	19
5 Описание расстановки технических средств	20
Заключение	24
Список использованных источников	25

ВВЕДЕНИЕ

Средства защиты информации представляют собой разнообразные технические средства, включая инженерные, электрические, электронные и оптические устройства, используемые для решения задач по обеспечению безопасности и предотвращению утечки защищенной информации. Они нужны для обеспечения безопасности и конфиденциальности информации, защиты от несанкционированного доступа, утечки данных. Разработка комплексных мер информационно-технической защиты информации в организации является неотъемлемой частью обеспечения безопасности организации в целом.

В данной работе рассмотрен процесс разработки информационно-технической защиты информации в организации, которая работает с государственной тайной. Работа состоит из пяти разделов:

- анализ технических каналов утечки информации;
- составление перечня управляющих документов;
- проведения анализа защищаемых помещений с учетом возможных утечек информации и необходимости обеспечения защиты технических средств;
- обзор рынка различных технических средств защиты информации;
- разработка схем размещения выбранных технических средств в защищаемых помещениях.

1 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

1.1 Информационные потоки

Информационный поток в организации – это совокупность передаваемых внутри предприятия сообщений, которые необходимы для управления подразделениями и контроля деятельности сотрудников.

Содержание информационного потока классифицируются по передаваемой информации:

- управленческий: управленческие решения, приказы, распоряжения по всем административным подразделениям, руководящим работникам;
- экономический: вся информация о хозяйственной деятельности, экономических показателях и т. д.;
- финансовый: финансовые показатели, расчетная и бухгалтерская информация, а также иные данные, относимые к финансам предприятия;
- формализованный: любые данные, передаваемые в рамках действующих регламентов на периодической основе;
- отчетный: сведения передаваемые по итогам работы подразделений, отдельных специалистов и т. д., представленные в виде отчетов;
- юридический: сведения правового характера, контракты, претензии, рекламации и т. д.;
- технологический – все сведения, касающиеся технологических компонентов по основной деятельности предприятия.

Также информационные потоки можно классифицировать по степени открытости:

- открытые информационные потоки (доступны сотрудникам и другим заинтересованным сторонам в пределах предприятия без специальных ограничений);
- закрытые информационные потоки (содержат конфиденциальную, чувствительную информацию, которая требует высокого уровня защиты).

Информационные потоки охватывают перемещение приказов, распоряжений, отчетов, плановых документов, показателей работы, договоры, оперативную информацию, текущую переписку и т. д.

1.2 Структура информационных потоков на предприятии

Организация производит антивирусное ПО. Организация продает ПО как обычным пользователям, так и пишет ПО для ФСБ. Следовательно, на предприятии циркулирует гос. тайна.

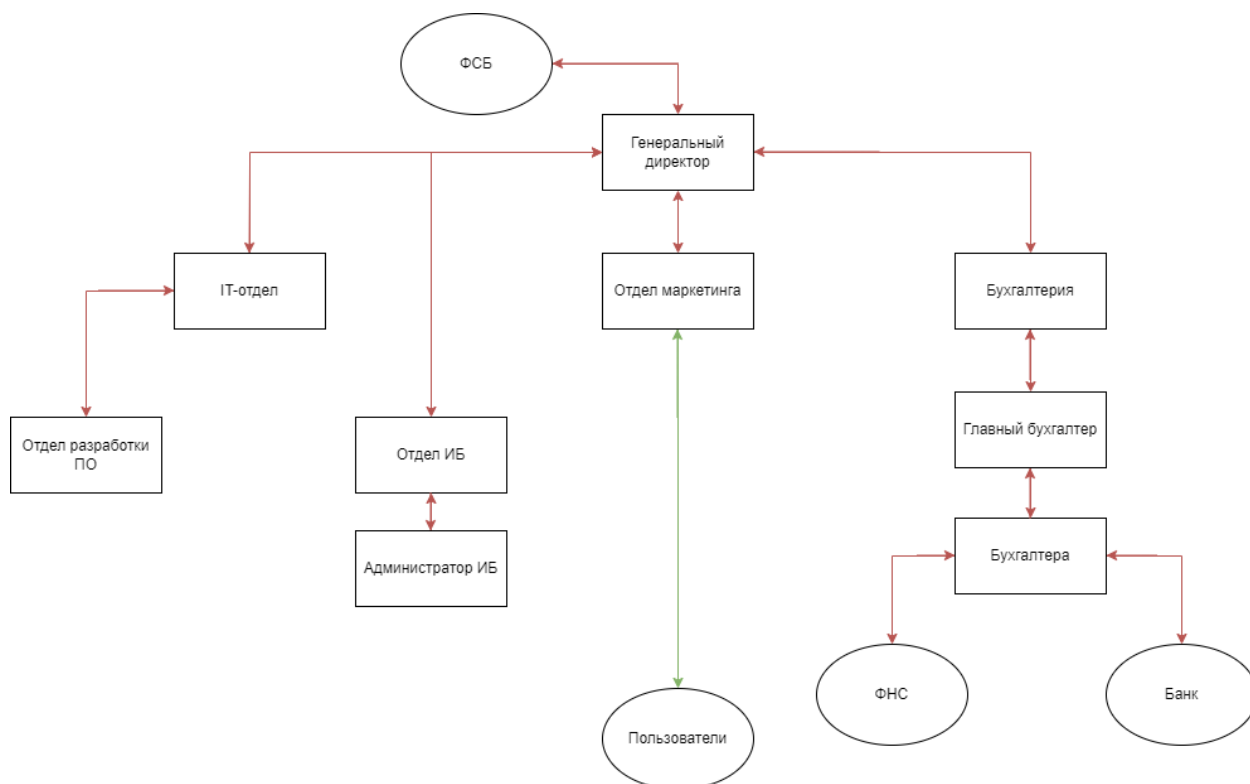


Рисунок 1 – Схема информационных потоков на предприятии

2 ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Организация сотрудничает с ФСБ, поэтому она в том числе работает с государственной тайной уровня «совершенно секретно». Разрабатывая систему защиты будем опираться на следующий документ: Решение Межведомственной комиссии по защите государственной тайны от 21 января 2011 г. N 199 "О Типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними". Необходимо выполнить следующие требования для обеспечения безопасности режимно-секретного подразделения(РСП):

- помещения РСП нежелательно размещать на первом и последнем этаже. Допустимо оборудовать РСП на первом этаже в случае, когда окна помещений выходят в закрытый контролируемый двор;
- окна помещений режимно-секретного отдела, а также помещений, используемых для хранения носителей гостайны, по возможности не должны соседствовать с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и прочими элементами, с которых в помещения могут проникнуть посторонние лица;
- режимные помещения рекомендуется группировать и размещать в «непроходной» части здания, которая редко используется сотрудниками при выполнении

служебных обязанностей, не связанных с доступом к государственной тайне;

- стены или перегородки между обычными и защищенными помещениями должны быть бетонными, железобетонными или металлическими с толщиной стен — от 10 см, или кирпичными с толщиной стен от 12 см;

- в помещениях для работы с гостайной 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;

- оборудование помещений для работы с гостайной по требованиям технической безопасности, вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемым к оснащению защищенных и выделенных помещений. 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;

- для предотвращения доступа посторонних лиц в режимные помещения требуется установить замки. Для более надежной защиты можно устанавливать кодовые и электронные замки, а также автоматические турникеты;

- помещения, где хранятся секретные документы и носители гостайны, оборудуются охранной и аварийной сигнализацией, которая выводится на пульт дежурного по организации, на пульт караульного помещения, а также на пульт централизованной службы наблюдения за сигнализацией.

3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

3.1 Схема помещения

Прежде чем устанавливать технические средства защиты, проведем анализ защищаемого помещения.

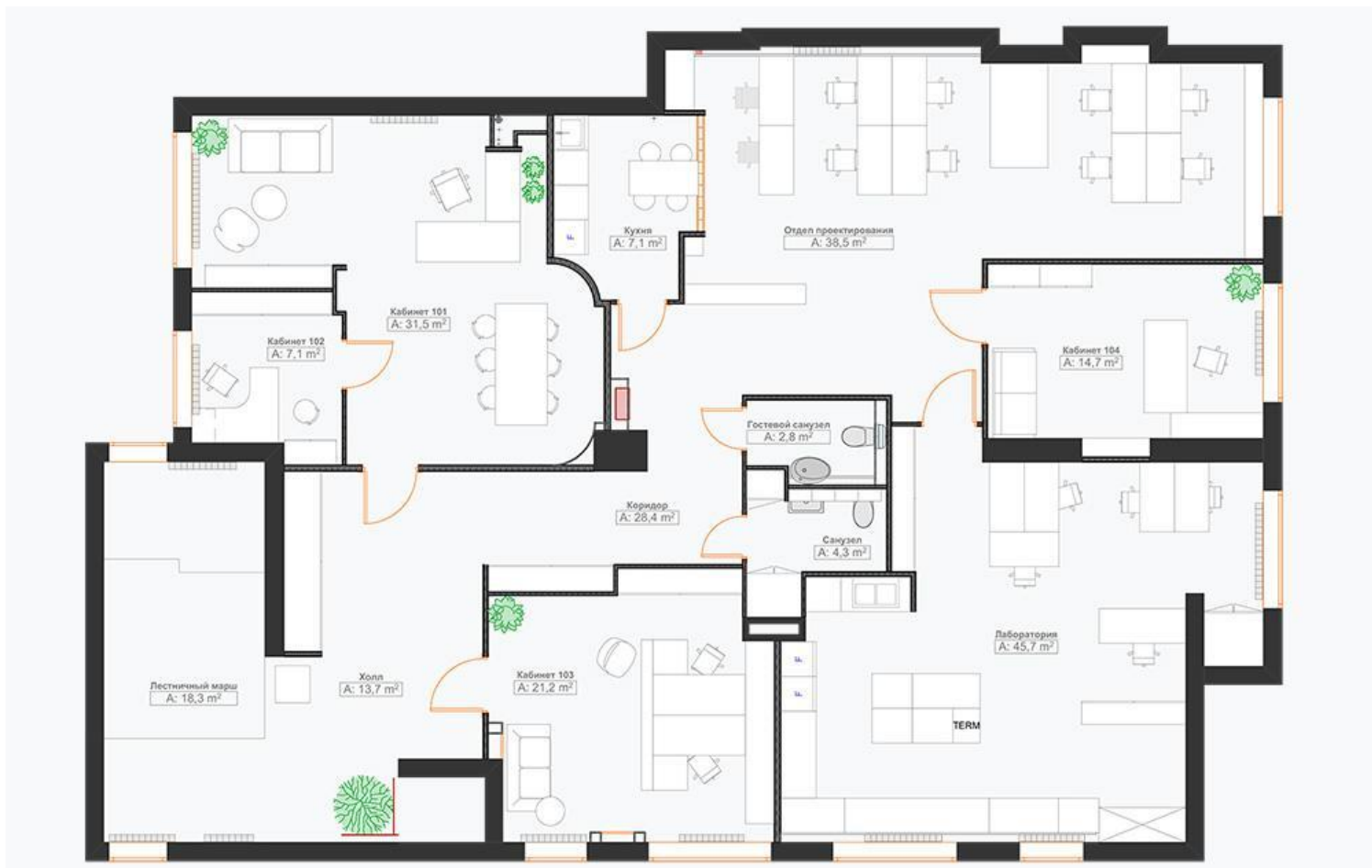

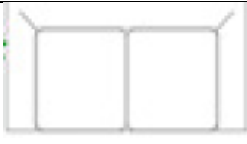


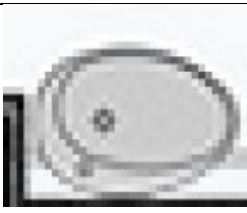

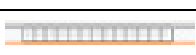



Рисунок 2 – План защищаемого помещения

Таблица 1 – Описание обозначений

Изображение предмета	Описание
	Офисный стол
	Журнальный столик
	Кухонный стол с табуретками

Продолжение таблицы 1

	Кресло
	Диван
	Кресло(округлое)
	Шкаф
	Раковина
	Унитаз
	Батарея
	Комнатные растения

4 АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ

4.1 Выбор средств защиты

Для обеспечения высокого уровня комплексной безопасности информации, которая

отнесена к категории «совершенно секретно» в зависимости от её типа, требуется оснащение помещения специальными средствами и устройствами, перечисленными в таблице 2. Это позволит обеспечить надежную защиту от несанкционированного доступа и утечки такой конфиденциальной информации.

Таблица 2 – Активная и пассивная защита информации

Каналы	Источники	Активная защита	Пассивная защита
Акустический Электроакустический	Стены, двери, окна, электрические сигналы	Устройства акустического зашумления	Защитные экраны и фильтры для сетей электропитания, изоляция особо важных помещений
Виброакустический	Стекла, стены и иные твердые поверхности	Устройства вибрационного зашумления	Изоляция переговорной, использование антивибрационных материалов и звукозащитных экранов
Визуально- оптический	Окна и стеклянные поверхности, двери	Жалюзи, бликующие устройства	Защитные экраны и фильтры для сетей электропитания
Электрический Электромагнитный	Компьютеры, сервера, бытовая техника, розетки	Устройства электромагнитного зашумления	Защитные экраны и фильтры для сетей электропитания

4.2 Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам

Пассивная защита в данном контексте включает в себя установку фильтров в электропитании всех помещений, направленных на минимизацию возможных электромагнитных и электрических утечек информации.

Система активной защиты основана на использовании белого шума в сети. Эта система генерирует постоянный фоновый шум, который маскирует колебания, возникающие от звуковых волн или работы электронных устройств. Для более детального

анализа представлены модели устройств и их характеристики в таблице 3. Эти меры активной защиты направлены на обеспечение дополнительного уровня безопасности и предотвращение возможных технических каналов утечки информации в защищаемых помещениях.

Таблица 3 – Активная защита от утечек информации по электрическим каналам

Модель	Цена, руб.	Характеристики	Особенности
ФП-6	50 556	Ток нагрузки – 20 А. Уровень шума/затухания – 60 дБ. Напряжение – при постоянном токе - 500 В / при переменном токе с частотой 50 Гц - 220 В / при переменном токе с частотой 400 Гц - 115 В. Частотный диапазон – 0,01 - 1800 МГц. Количество фаз – 1. Тип соединения – экранированный кабель (2 шт) в комплекте.	Фильтр ФП-6 предотвращает утечки информации по цепям электропитания, а также защищает средства оргтехники от внешних помех. 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. Сертификат ФСТЭК.
Генератор шума СОНАТА-РСЗ	32 400	Ток нагрузки – сеть ~220 В +10%/-15%, 50 Гц. Напряжение – 220 В. Количество фаз – 1. Потребляемая мощность 10 Вт.	Устройство для активной защиты информации от утечки по сети электропитания. Предназначено для подключения к 3-проводной сети. Звуковая и световая индикация работы. Сертифицировано ФСТЭК.

Продолжение таблицы 3

Модель	Цена, руб.	Характеристики	Особенности
ФСПК-40	59 800	Ток нагрузки – 40 А. Уровень шума/затухания – защита информации от утечки за счет побочных электромагнитных наводок на линии электропитания по 2 классу защиты. Напряжение 220/380 В. Частотный диапазон – 0,15–1000 МГц. Количество фаз – 1. Тип соединения – подключение к цепям электропитания с 2 проводами (ноль и фаза, без заземления).	Устройство защиты речевой информации от утечки по электросети. Два фильтруемых провода (ноль, фаза). Подавление помех, побочных излучений, наводок в диапазоне 0,15–1000 МГц. Напряжение питающей сети 220/380 В, частота – 50Гц. Класс электробезопасности – I (ГОСТ Р 12.1.019–2009 ССБТ). Сертифицировано ФСТЭК.

На основании анализа, проведенного в таблице 4, был выбран генератор шума Соната РС3. Оптимальный вариант, так как устройством возможно управлять дистанционно посредством проводного пульта, а также у устройство есть сертификат от ФСТЭК.

4.3 Защита от утечки информации по (вибро-) акустическим каналам

Пассивные меры безопасности охватывают установку тамбурной зоны перед переговорной комнатой и усиление дверей для дополнительной защиты. Для обеспечения звукоизоляции переговорной комнаты и офиса руководителя применяются специализированные материалы, способствующие снижению звуковой проницаемости стен и, таким образом, повышению конфиденциальности обсуждаемой информации.

Активные меры безопасности включают в себя систему виброакустической

маскировки. Для обеспечения безопасности помещения, где обрабатывается информация с уровнем секретности "совершенно секретно", рассматриваются технические средства активной защиты информации, соответствующие категории не ниже 1Б (таблица 4). Эти меры направлены на предотвращение возможных технических каналов утечки информации, обеспечивая дополнительный уровень безопасности в защищаемых помещениях.

Таблица 4 – Активная защита от утечек информации по (вибро-)акустическим каналам

Модель	Цена, руб.	Характеристики	Особенности
Генератор шума ЛГШ-303	15 600	Диапазон частот акустической помехи – 180–11300 Гц. Средняя наработка на отказ – не менее 5000 ч. Средний срок службы – 5 лет. Время автономной работы – до 5 часов.	Мобильно и предназначено для работы в помещениях, (автомобилях) и других местах не требующих стационарных средств защиты информации по прямому акустическому каналу. В непрерывном режиме изделие работает до пяти часов при температуре окружающей среды от плюс 1 до плюс 40 °С, относительная влажность не более 80 %(при температуре + 25 °С).
Шорох 5Л	21 500	Диапазон регулировки уровня шумового сигнала в полосе октавных фильтров, не менее 18 дБ. Диапазон регулировки общего уровня шумового сигнала, не менее 30 дБ. Частота переменного напряжения электропитания 50±2 Гц. Потребляемая мощность при полной нагрузке, не более 130 ВА.	Система «Шорох-5Л» относится к средствам активной акустической и вибрационной защиты информации 1-го класса тип «Б». Система представляет собой комплекс устройств, состоящий из блока питания и управления «БПУ-1» с активными вибровозбудителями «ПЭД-8А» и активными акустическими излучателями «АИ-8А/Н» и «АИ-8А/Мини».

Продолжение таблицы 4

Модель	Цена, руб.	Характеристики	Особенности
Соната АВ-4Б	44 200	Диапазон воспроизводимого шумового сигнала 175–11200 Гц. Выходное напряжение В $12,5 \pm 0,5$. Электропитание сеть ~220 В/50 Гц.	Комплект состоит из блоков электропитания и управления, генераторов-акустоизлучателей, генераторов-вибровозбудителей, размыкателя телефонной линии, размыкателя слаботочной линии, размыкателя линии Ethernet, пульта управления, блоков сопряжения из внешних устройств. Технического средства защиты речевой информации от утечки по оптико-электронному (лазерному) каналу и прочих аксессуаров.

Исходя из анализа, представленного в таблице 5, было принято решение о выборе системы Соната АВ-4Б. По сравнению с альтернативными системами, предназначенными для защиты от утечек информации через акустические и вибрационные каналы, данная система считается наиболее востребованной и получила множество положительных отзывов.

4.4 Защита от ПЭМИН

ПЭМИН – побочные электромагнитные излучения и наводки. Вариант защиты компьютерной информации методом зашумления (радиомаскировки) предполагает использование генераторов шума в помещении, где установлены средства обработки конфиденциальной информации. Зашумление обеспечивается типами генераторов, представленными в таблице 5.

Таблица 5 – Активная защита от ПЭМИН

Модель	Цена, руб.	Характеристики	Особенности
СОНАТА-РЗ.1	33 120	Наличие регулировки уровня шума. Диапазон частот – соответствует требованиям документа "Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок" (ФСТЭК России, 2014) - по 2 классу защиты. Электропитание – сеть 220 В +10%/-15%, 50 Гц. Мощность – 10 Вт. Режим работы – продолжительность непрерывной работы не менее 8 ч.	Техническое средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок типа (класса) АБ(2). Соответствует современным требованиям. Может устанавливаться в выделенных помещениях до 1-й категории включительно, в том числе оборудованных системами звукоусиления речи, без применения дополнительных мер защиты информации. Сертификат ФСТЭК 3539.
Генератор шума ГНОМ-3М	57 200	Диапазон частот 10 кГц - 1800 МГц. Уровень шума от -26 дБ (мкА/м*√кГц) до 50 дБ(мкВ/м*√кГц). Мощность – 45 Вт.	Предназначен для активной защиты информации, обрабатываемой на электронно-вычислительной технике. Имеет 4 выхода для подключения к цепям электропитания и к антенным контурам. Прост в эксплуатации и не требует дополнительных настроек. Имеет сертификат ФСТЭК.

Продолжение таблицы 5

Модель	Цена, руб.	Характеристики	Особенности
Генератор шума ЛГШ-501	29 900	<p>Присутствует регулировка уровня шума, диапазон регулировки уровня выходного шумового сигнала не менее 20 дБ. Диапазон частот – 0,01–1800 МГц. Уровень шума – от -28 дБ(мкА/м*√кГц) до 57 дБ(мкВ/м*√кГц). Электропитание – однофазная сеть переменного тока 187 В-242 В. Мощность – не более 45 ВА. Режим работы – круглосуточно.</p>	<p>Оснащено визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима. Оснащено счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы Изделия в режиме формирования маскирующих помех. Обеспечивает защиту органов регулировки уровня выходного шумового сигнала от несанкционированного изменения и обнаружение несанкционированного доступа к ним.</p>

В качестве средства активной защиты от ПЭМИН был выбран генератор шума Соната-РЗ.1. Этот выбор обоснован соответствию требованиям к документам ФСТЭК, а также наличие возможности, в случае необходимости, дополнительного повышения уровня излучаемого электромагнитного поля шума в диапазоне частот 0,01...200 МГц за счет применения опционально поставляемой дополнительной антенны ВЕЕР.

4.5 Защита от утечек информации по оптическим каналам

Для предотвращения возможности использования оптического канала для утечки информации можно воспользоваться следующими средствами:

- шторы;
- жалюзи;

- тонированные пленки на стеклах.

Среди предложенных вариантов защиты от оптического канала утечки информации использование жалюзи выделяется как наиболее эффективное решение. Жалюзи не только препятствуют визуальному наблюдению, но также успешно защищают от солнечных лучей. При выборе таких средств важно учитывать их адаптивность к конкретным потребностям и особенностям окружающей среды, чтобы обеспечить максимальный уровень безопасности.

5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

В предыдущей главе был проанализирован рынок инженерно-технических средств и были выбраны лучшие средства защиты информации из них, которые включает в себя:

- сетевой генератор шума «Соната-РС3»;
- система виброакустической защиты «Соната АВ-4Б»;
- генератор шума «Соната-РЗ.1» от ПЭМИН
- жалюзи на одиннадцать окон;
- три усиленные двери с толщиной 4 мм, обшитые металлическим листом не менее 2 мм, внутри – звукоизоляционный материал.

Для каждого помещения оптимальное количество акустоизлучателей и вибровозбудителей зависит от различных факторов, таких как звукоизоляция, форма, материалы стен, местоположение, уровень фонового шума и другие подобные аспекты.

Согласно информации на официальном веб-сайте производителя НПО «АННА» для выбранной системы виброакустической защиты, предварительную оценку необходимого количества вибровозбудителей «Соната СВ-4Б» можно провести, руководствуясь следующими стандартами:

- 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 водо- (тепло- и газо-) снабжения - один на каждую вертикаль (отдельную трубу) вида коммуникаций.

Предварительная оценка необходимого количества акустоизлучателей «Соната СВ-4Б» может быть выполнена из следующих норм:

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

В таблице 6 содержится список мер защиты, предназначенных для применения во всех помещениях, а также конечная стоимость.

Таблица 6 – Необходимое оборудование

Меры защиты	Цена, руб.	Количество, шт.	Итоговая стоимость
Сетевой генератор шума «Соната-РС3»	32 400	1	32 400
Генератор шума «Соната-Р3.1»	33 120	3	99 360
Блок электропитания и управления «Соната-ИП4.3»	21 600	1	21 600
Генератор-акустоизлучатель «Соната СА-4Б1»	3 540	14	49 560
Генератор-вибровозбудитель «Соната СА-4Б»	7 440	77	572 880
Размыкатель телефонной линии «Соната ВК4.1»	6 000	2	12 000
Размыкатель слаботочной линии «Соната ВК4.2»	6 000	1	6 000
Размыкатель линии «Ethernet» «Соната ВК4.1»	6 000	1	6 000
Пульт управления «Соната-ДУ 4.3»	7 680	1	7 680
Шторы-плиссе Blackout	4 900	11	53 900
Усиленные звукоизолирующие двери «Ultimatum Next ПВХ»	83 619	3	250 857
Итого			

В трех помещениях установлены усиленные звукоизолирующие двери, как показано на рисунке 5. На каждом окне установлены шторы. Системы «Соната СА-4Б1» и «Соната СВ-4Б» размещены в соответствии с указаниями производителя. «Соната-РС3» и «Соната-Р3.1» находятся рядом с «Соната-ИП4.3» и подключены к ней. Все выключатели установлены в соответствии с рекомендациями производителя. В таблице 7 приведены

описание обозначений устройств.

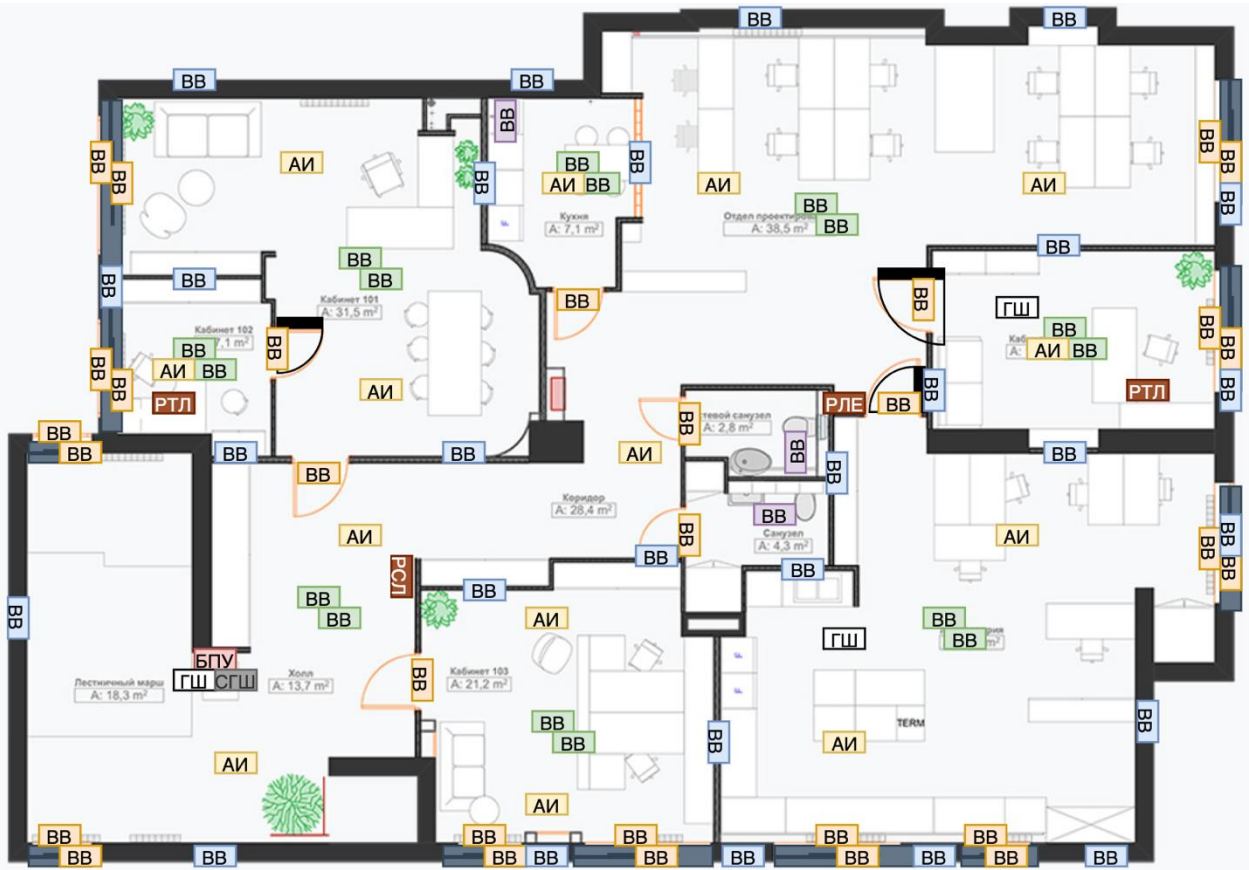


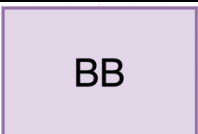
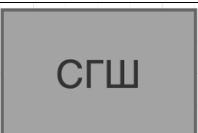




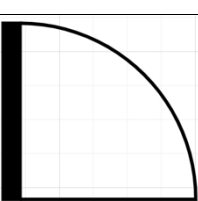



Рисунок 5 – Схема расстановки устройств

Таблица 7 – Описание обозначений устройств

Обозначение	Устройство	Количество, шт.
<div>БПУ</div>	Блок электропитания и управления «Соната-ИП4.3»	1
<div>АИ</div>	Генератор-акустоизлучатель «Соната СА-4Б1»	14
<div>ВВ</div>	Генератор-вибровозбудитель «Соната СВ-4Б» (стены)	28

Продолжение таблицы 7

Обозначение	Устройство	Количество, шт.
	Генератор-вибровозбудитель «Соната СВ-4Б» (потолок, пол)	16
	Генератор-вибровозбудитель «Соната СВ-4Б» (окна, двери, батареи)	30
	Генератор-вибровозбудитель «Соната СВ-4Б» (трубопровод)	3
	Сетевой генератор шума «Соната-РС3»	1
	Генератор шума «Соната-Р3.1»	3
	Размыкатель линии «Ethernet» «Соната-ВК4.3»	1
	Размыкатель слаботочной линии «Соната-ВК4.2»	1
	Размыкатель телефонной линии «Соната-ВК4.1»	2
	Усиленные звукоизолирующие двери «Ultimatum Next ПВХ»	3
	Шторы-плиссе BlackOut	11

ЗАКЛЮЧЕНИЕ

В рамках данной курсовой работы была проведена комплексная разработка инженерно-технической системы безопасности на предприятии. Основной акцент был сделан на анализе технических каналов утечки информации, а также разработке и внедрении эффективных средств и устройств для их перекрытия.

В ходе исследования были выделены и проанализированы различные технические каналы, представляющие потенциальные угрозы для безопасности предприятия. На основе полученных данных были разработаны мероприятия по минимизации рисков и предотвращению утечек информации.

Основываясь на полученных результатах, были предложены конкретные рекомендации по установке устройств на плане предприятия, а также проведен расчет стоимости реализации предложенных мероприятий. Это позволяет предприятию не только повысить уровень безопасности, но и рационально распределить бюджет на внедрение системы безопасности.

Инженерно-техническая система безопасности, разработанная в рамках данной работы, представляет собой комплексный и эффективный инструмент для защиты информационных ресурсов предприятия. Проведенные исследования и разработки могут служить основой для дальнейших улучшений и модернизации систем безопасности, а также применяться в других сферах бизнеса с целью обеспечения надежной защиты от угроз информационной безопасности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Титов А. А. Инженерно-техническая защита информации: учебное пособие. Томск: ТУСУР, 2010. — 195 с.
2. Хорев А. А. Техническая защита информации: учебное пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010. — 436 с.
3. Detector Systems: Системы комплексной безопасности [Электронный ресурс]. – Режим доступа: <https://detsys.ru/> (дата обращения: 01.11.2023).