

**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:

Пимашин Егор Николаевич, студент группы N34501

 _____
(подпись)

Проверил:

Попов Илья Юрьевич,
кандидат технических наук, доцент ФБИТ

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент Пимашин Егор Николаевич

(Фамилия И.О.)

Факультет Факультет Безопасности Информационных Технологий

Группа N34501

Направление (специальность) Технологии защиты информации

Руководитель Попов Илья Юрьевич, доцент ФБИТ, кандидат технических наук

(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической защиты информации на предприятии

Задание Разработать системы инженерно-технической защиты информации на предприятии

Краткие методические указания:

Объект исследований курсовой работы ограничивается заданным помещением.

Содержание пояснительной записки Введение: краткое введение в курсовую работу

Организационная структура предприятия: описание структуры предприятия

Обоснование защиты информации: описание угроз и каналов утечки информации

Анализ защищаемых помещений: анализ помещений на предмет возможных утечек

Анализ рынка технических средств: сравнительный анализ рынка ИТСЗИ

Описание расстановки технических средств: описание расстановки ИТСЗИ

Заключение: выводы к курсовой работе

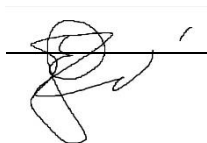
Руководитель

(Подпись, дата)

Студент

21.10.2023

(Подпись, дата)



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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Пимашин Егор Николаевич

(Фамилия И.О.)

Факультет Факультет Безопасности Информационных Технологий

Группа N34501

Направление (специальность) Технологии защиты информации

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

(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Анализ теоретической составляющей	27.09.2023	27.09.2023	
2	Написание введения и основной части	15.10.2023	27.09.2023	
3	Разработка комплекса инженерно-технической защиты информации в заданном помещении	15.11.2023	10.10.2023	
4	Оформление курсовой работы	20.11.2023	20.10.2023	

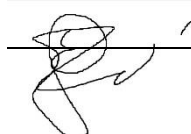
Руководитель

(Подпись, дата)

Студент

21.10.2023

(Подпись, дата)



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

Студент Пимашин Егор Николаевич

(Фамилия И.О.)

Факультет Факультет Безопасности Информационных Технологий

Группа N34501

Направление (специальность) Технологии защиты информации

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

(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

**1. Цель и задачи
работы**

☐ Предложены студентом

☐ Сформулированы при участии студента

☒ Определены руководителем

Цель курсовой работы: Повышение защищенности рассматриваемого помещения.

Задачи курсовой работы:

- анализ защищаемого помещения;
- оценка каналов утечки информации;
- выбор мер пассивной и активной защиты информации.

**2. Характер
работы**

☐ Расчет

☒ Конструирование

☐ Моделирование

Другое: _____

3. Содержание работы

Введение

Организационная структура предприятия.

Обоснование защиты информации.

Анализ защищаемых помещений.

Анализ рынка технических средств.

Описание расстановки технических средств.

Заключение.

Список литературы

4. Выводы

В результате была предложена защита от утечек информации по оптическому, акустическому, виброакустическому, электромагнитному каналам, обеспечена защита от ПЭМИН.

Итоговая цена системы защиты информации составляет 1 145 260 рублей.

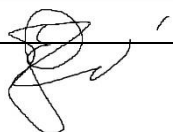
Руководитель _____

(Подпись, дата)

Студент _____

21.10.2023

(Подпись, дата)



«21» октября 2023 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	7
1. ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ	8
1.1 Общие сведения о защищаемой организации	8
1.2 Информационные потоки	9
2. ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ.....	11
3. АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ	12
3.1 Схема помещения.....	12
3.2 Описание помещений.....	13
3.3 Анализ возможных каналов утечки информации	14
3.3.1 Оптический канал	14
3.3.2 Акустический, виброакустический каналы	15
3.3.3 Электромагнитный канал	15
3.3.4 Закладные устройства	15
3.3.5 Материально-вещественный канал	15
4. АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ	16
4.1 Оптический канал.....	16
4.2 Акустический, виброакустический канал.....	16
4.3 Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам.....	18
4.4 Защита от ПЭМИН.....	19
4.5 Защита от утечки информации через закладные устройства.....	20
4.6 Защита от утечки информации по материально-вещественному каналу...	21
5. ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ	22
ВЫВОД.....	25
СПИСОК ИСТОЧНИКОВ	26

ВВЕДЕНИЕ

Цель курсовой работы:

Повышение защищенности рассматриваемого помещения.

Задачи курсовой работы:

- анализ защищаемого помещения;
- оценка каналов утечки информации;
- выбор мер пассивной и активной защиты информации.

В современном информационном обществе вопросы обеспечения безопасности и защиты конфиденциальной информации становятся все более актуальными и приобретают важное значение для предприятий любого масштаба. В условиях активного цифрового развития и расширения использования информационных технологий возникает необходимость эффективной защиты конфиденциальных данных от внешних угроз, кибератак, а также внутренних утечек информации.

Основное внимание уделяется разработке комплекса мероприятий, направленных на минимизацию уязвимостей информационных систем и созданию эффективной системы защиты данных.

В работе будут рассмотрены основные аспекты проектирования системы защиты информации на предприятии, включая анализ угроз информационной безопасности, выбор и реализацию соответствующих технических средств защиты, разработку политики безопасности, обучение персонала и многое другое.

Исследование планируется провести на основе анализа существующих методов защиты информации, нормативно-правовой базы в области информационной безопасности, а также на основе изучения передовых практик в данной области. Результаты и рекомендации, представленные в данной работе, будут иметь практическую значимость для предприятий, стремящихся обеспечить надежную защиту своей конфиденциальной информации.

1. ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

1.1 Общие сведения о защищаемой организации

Наименование организации: НАО “ММФ”.

Область деятельности: Инвестиционная деятельность.

Цели для защиты: Основные информационные процессы и потоки в организации, включая описание информации ограниченного доступа, пароли от тёплых и холодных крипто-кошельков, *коммерческая тайна, персональные данные* клиентов и работников, *сведения о сущности изобретения, государственная тайна.*

Прибыль (месячная/годовая), расходы, стоимость информационных активов:

1. Прибыль:

1.1.месячная: плавающая, от убытка в 9 597 940 рублей до прибыли в 23 981 370 рублей;

1.2.годовая: плавающая, от прибыли в 9 597 940 рублей до прибыли в 191 958 800 рублей;

2. Расходы:

2.1.общий фонд оплаты труда: 38 391 760 рублей;

2.2.коммунальные платежи: 1 597 940 рублей;

2.3.лицензионное ПО: 4 798 970 рублей;

2.4.расходы первой необходимости: 9 597 940 рублей;

3. Стоимость информационных активов

3.1.стоимость криптовалютных активов на холодных кошельках: 966 000 000 рублей;

3.2.стоимость криптовалютных активов на тёплых кошельках: 96 600 000 рублей;

3.3.стоимость криптовалютных активов на аккаунтах трейдеров 193 200 000 рублей;

3.4.стоимость **персональных данных** клиентов: штраф (60–500 тысяч рублей)
+ репутационные потери;

3.5.стоимость потери коммерческой тайны: до 20% убытка по открытым инвестициям на холодных кошельках - 193 200 000 рублей;

3.6.стоимость потери сведений о сущности изобретения оценивается в количество инвестиций, вложенных в разработку этого изобретения. То есть, заработная плата сотрудников, которые занимаются разработкой, стоимость ПО для разработки, упущенная выгода. Это всё невозможно оценить без знания количества времени, которое ушло на разработку.

Персонал организации 55 человек:

1. Генеральный директор;
2. Зам. Директора;
3. Бухгалтер;
4. Юрист;
5. Специалист по информационной безопасности;
6. Технический администратор;
7. Старший риск-менеджер;
8. Риск-менеджер;
9. HR;
- 10.Специалист по переговорам;
- 11.Тимлидер;
- 12.Старший трейдер;
- 13.Алгоритмические трейдеры (13–25);
- 14.Трейдеры (26–55).

1.2 Информационные потоки

Информационные потоки представляют собой жизненно важный элемент для эффективной работы любой организации. Они являются основным каналом передачи данных, знаний и коммуникации между подразделениями, сотрудниками и внешними стейкхолдерами. Рассмотрение информационных потоков в контексте организации позволяет увидеть важность эффективного управления информацией для достижения целей и обеспечения конкурентоспособности.

Информационные потоки играют решающую роль в повседневной деятельности предприятия. Они представляют собой механизм передачи, обработки и анализа информации, который влияет на принятие решений на всех уровнях управления. Эффективные информационные потоки способствуют оперативности, точности и своевременности передачи информации между различными структурными подразделениями организации. Типы информационных потоков в организациях:

- Внутренние информационные потоки: это информация, передаваемая внутри организации между различными отделами, сотрудниками и уровнями управления. Внутренние потоки могут быть формальными (например, отчеты, инструкции, приказы) и неформальными (устные обсуждения, электронные сообщения).
- Внешние информационные потоки: они представляют собой обмен информацией между организацией и внешней средой, такой как клиенты, поставщики, партнеры, регуляторы. Эти потоки включают в себя заказы, отчетность, рекламные материалы и другую коммуникацию с внешними стейкхолдерами.

На рисунке 1 представлены информационные потоки организации «ММФ»

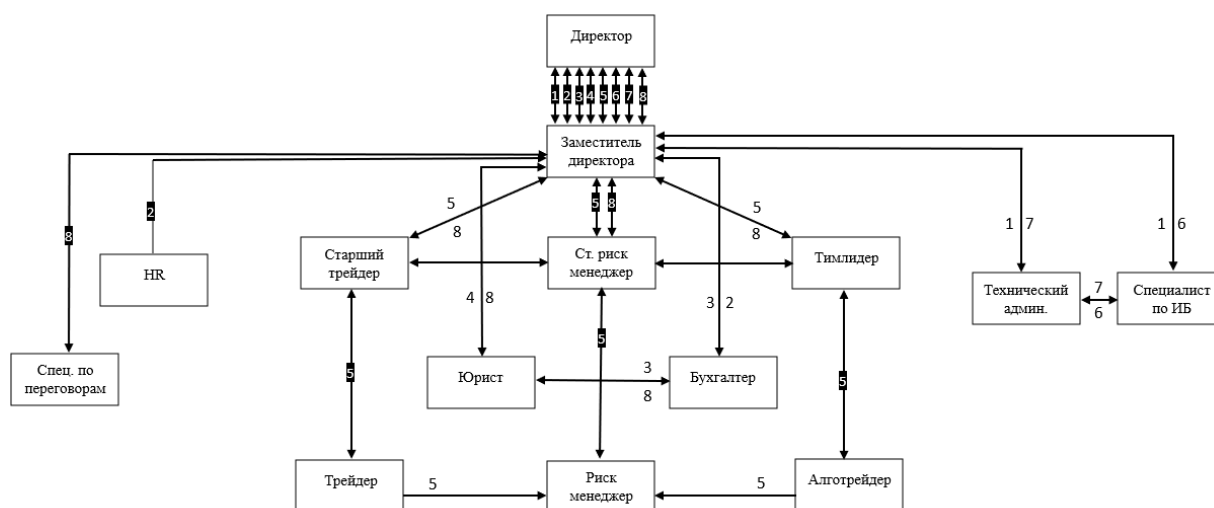


Рисунок 1 – схема информационных потоков организации



Рисунок 2 – схема внешних информационных потоков

2. ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Согласно заданию на курсовую работу, создаваемая система защиты информации предназначена для информации, составляющей государственную тайну уровня «совершенно секретно». Согласно требованиям «Типовых норм и правил проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними», утвержденных Решением Межведомственной комиссии по защите государственной тайны от 21.01.2011 N 199, защита рассматриваемых помещений должна удовлетворять следующим критериям:

1. В помещениях для работы с государственной тайной и хранилищах секретных документов устанавливаются усиленные двери, обеспечивающие надежное закрытие. Двери с двух сторон обшиваются металлическим листом не менее 2 мм толщиной, внутри — звукоизоляционный материал, сама дверь должна иметь толщину не менее 4 см. Дверь устанавливается на металлический каркас.
2. Обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании.
3. По требованиям безопасности режимных помещений, если окна комнат и хранилищ находятся рядом с водостоком, эвакуационной лестницей, крышами стоящих вблизи зданий, на первом или последнем этаже, каждое окно оборудуется выдвижными ставнями или створками с металлической решеткой, которая крепится к железным конструкциям оконного проема в стене.
4. Все режимные помещения оборудуются аварийным освещением.

5. Оборудование помещений для работы с государственной тайной по требованиям технической безопасности, вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемым к оснащению защищенных и выделенных помещений.
6. Перед началом эксплуатации необходимо проверить выделенные и иные режимные помещения проверить на предмет наличия «жучков» и иных средств несанкционированного получения информации. В дальнейшем такие проверке желательно проводить периодически, чтобы исключить возможность утечки.

Основными документами в области защиты информации, составляющей государственную тайну, являются:

- Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне»;
- 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".

3. АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

3.1 Схема помещения

Необходимо провести анализ защищаемого помещения, чтобы разместить технические средства защиты на объекте. План помещения предприятия офисного типа представлен на рисунке 3. На рисунке 4 представлены описание обозначений, изображенных на плане.



Рисунок 3 – план защищаемого помещения



Рисунок 4 – условные обозначения на плане помещения

3.2 Описание помещений

На рассматриваемом предприятии в рамках курсовой работы имеются следующие помещения, подлежащие инженерно-технической защите:

- кабинет директора (12,9 м²);
- переговорная комната (25,2 м²);

- Кабинет Юриста (12,2 м²);
- Кабинет администратора ИБ и технического администратора (12,3 м²);
- Бухгалтерия (12,3 м²);
- Кабинет заместителя директора (12,3 м²);
- главный холл (82,4 м²).

Офис организации, в котором планируется вести работу с государственной тайной, расположен на третьем этаже 15-этажного офисного здания. На южной стене расположены окна, выходящие на улицу. Напротив, расположены другие офисные здания.

Западная и восточная стены граничат с другими арендуемыми офисами. Северная стена связывает офис с техническими помещениями. Над и под защищаемым помещением также расположены арендуемые офисы. Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см.

Доступы к помещениям здания ограничен системой контроля и управления доступом. Допуск в общие помещения имеют все арендаторы и обслуживающий персонал, доступ к офису имеют только сотрудники организации-арендатора.

Главный холл содержит 33 рабочих места, которые включают кресло и рабочий стол, два горшка с растением, 3 нерабочих стола, барная стойка, два шкафа и 1 стеллаж.

В кабинете Юриста расположено 2 рабочих места и 2 тумбочки.

В кабинете АИБ и технического администратора расположено 2 рабочих места и дополнительный серверный ПК, где находится управление всеми системами безопасности.

В кабинете бухгалтера, замдиректора и генерального директора находятся по одному рабочему месту и дополнительному столу.

В переговорной находится стол, 8 кресел, 3 тумбочки и горшок с комнатным растением.

3.3 Анализ возможных каналов утечки информации

3.3.1 Оптический канал

Возможен частичный просмотр помещения со стороны улицы. Возможен просмотр помещения из соседних зданий с использованием оптических приборов.

3.3.2 Акустический, виброакустический каналы

Помещение расположено на третьем этаже напротив высотного здания. Окна выходят на улицу. Возможно прослушивание со стороны улицы или соседнего дома с использованием направленных микрофонов. Возможен съем речевой информации с оконных стекол с помощью лазера.

Во всех комнатах, где идёт работа с секретными сведениями, имеется вентиляция.

Возможно прослушивание через вентиляцию с использованием стетоскопов, спускаемых микрофонов.

В комнате, где ведутся закрытые разработки, имеются батареи отопления.

Возможно прослушивание через систему отопления с использованием стетоскопов.

3.3.3 Электромагнитный канал

В каждой комнате имеются розетки. Возможен съем информации через систему электропитания.

Из проводных каналов связи за пределы помещения выходит только ethernet кабель общего шлюза. Возможны съем и навязывание информации на этом канале связи.

Работа с секретными сведениями ведется с использованием компьютеров.

Возможно прослушивание паразитных электромагнитных полей, восстановление из них информации.

3.3.4 Закладные устройства

В помещении имеется множество мест, где можно спрятать закладное устройство: цветочные горшки, шкафы и полки с оборудованием, мусорные корзины.

Возможно размещение закладных устройств в стенах, либо их маскировка под розетки, светильники, выключатели.

3.3.5 Материально-вещественный канал

Материально-вещественный канал утечки информации присутствует. И угроза утечки по этому каналу нивелируется использованием СКУДа

4. АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ

4.1 Оптический канал

В качестве средства защиты информации от утечек по оптическому каналу через окна необходимо использовать смарт плёнку для переговорного помещения и одностороннюю зеркальную плёнку на все окна.

Таблица 1 – ИТСЗИ на оптический канал

Наименование средства	Достоинства	Стоимость Р
Односторонняя зеркальная пленка, 72 м ²	Закрывает обзор извне, ухудшает возможность прослушки направленным микрофоном	56 000
Смарт-плёнка, 8,1 м ²	Закрывает обзор извне, ухудшает возможность прослушки направленным микрофоном	81 290

4.2 Акустический, виброакустический канал

Для пассивной звукоизоляции мы воспользуемся услугами сторонних компаний, которые предоставляют услуги по звукоизоляции помещений. А конкретнее, необходимо провести пассивную звукоизоляцию переговорного помещения, расчёты стоимости которой можно увидеть в таблице 2.

Таблица 2 – ИТСЗИ для пассивной звукоизоляции

Наименование средства	Достоинства	Стоимость Р
Звукоизоляция пола, 25,2 м ²	Соответствует всем требованиям организации. Низкая стоимость	112 600
Звукоизоляция потолка, 25,2 м ²		98 300
Звукоизоляция стен, 51,4 м ²		252 000
Звукоизолирующие двери, х7		224 000

В таблице 3 приведён анализ рынка излучателей виброакустических помех.

Таблица 3 – Сравнение излучателей виброакустических помех

Наименование средства	Достоинства	Стоимость Р
Соната АВ-4Б	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.	44 200
Шорох 5Л	Устройство оснащено световым и звуковым индикаторами работы. Возможность управления устройством с помощью пульта ДУ.	21 500
SEL SP-157 Шагренъ	Защита паролем настроек системы. Отсчёт времени наработки генерации шума по каждому каналу с выводом на экран. Непрерывный контроль состояния системы и каждого отдельного излучателя.	47 400

В соответствии с таблицей 3 было принято решение о выборе системы «СОНАТА АВ-4Б». В сравнении с ценовым аналогом предоставляет возможность единой системы и единого управления для всех устройств ИТСЗИ «Соната».

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

Активная защита заключается в использовании системы белого шума в сети, которая создает фоновый шум, маскирующий колебания, вызванные звуковыми волнами или работой электронных устройств. Модели устройств, относительно которых будет идти дальнейший анализ, и их характеристики представлены в таблице 4.

Таблица 4 – активная защита от утечек информации по электрическим каналам.

Наименование средства	Достоинства	Стоимость Р
Соната-РСЗ	Звуковая и световая индикация работы. Возможно дистанционное управление посредством проводного пульта.	32 400
ЛГШ-221	Сетевой генератор шума. Устройство оснащено световым и звуковым индикаторами работы. Возможность управления устройством с помощью пульта ДУ.	36 400
Генератор шума Покров	Централизованное управление и контроль по Ethernet (для исполнения 2), для применения в системах пространственного зашумления. Независимая регулировка уровней	32 800

	электромагнитного поля шумового сигнала и шумового сигнала в линии электропитания и заземления.	
--	-------------------------------------------------------------------------------------------------	--

На основании анализа, проведенного в таблице 4, был выбран генератор шума «Соната-РС3». Оптимальный вариант по соотношению цена и качество позволяют установить достаточное количество подобных устройств в помещениях. Кроме того, он легко интегрируется в экосистему устройств «Соната»

4.4 Защита от ПЭМИН

Таблица 5 – активная защита от ПЭМИН

Наименование средства	Достоинства	Стоимость Р
Соната-РС.1	Просто интегрируется в экосистему «Соната». Долгое время на рынке	39 000
ЛГШ-513	Изделие «ЛГШ-513» оснащено визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа).	33 120
Генератор шума Пульсар	Имеет защиту регулятора уровня выходного шумового сигнала от нелегального доступа (и сигнализирует об этом).	24 525

	Индикаторы нормального режима работы (диод) и аварийного режима (свет и звук).	
--	--------------------------------------------------------------------------------	--

В качестве средства активной защиты от ПЭМИН был выбран генератор шума «Соната-РЗ.1». Одним из главных аргументов для выбора была лёгкая и удобная интеграция с нашим предыдущим выбором.

4.5 Защита от утечки информации через закладные устройства.

Таблица 6 – сравнение средств для поиска закладных устройств

Наименование средства	Достоинства	Стоимость Р
SPYDER	Позволяет осуществлять поиск устройств, передающих информацию по радиоканалу, инфракрасному каналу, различным проводным линиям под напряжением до 400В, а так же позволяет оценить вероятность утечки информации по виброакустическому и акустическому каналам.	140 000
ST 600 ПИРАНЬЯ	Широкая комплектация, долгое время на рынке, множество отзывов, совместим с другими	195 000

	устройствами компании-производителя.	
ST 500 ПИРАНЬЯ	Широкая комплектация, долгое время на рынке, множество отзывов, совместим с другими устройствами компании-производителя. Множество режимов под любой режим работы закладного устройства	429 000

Таким образом, было принято решение о выборе устройства «Spyder» из-за его цены и его возможностей справляться с возможностями, которые на него возложены.

4.6 Защита от утечки информации по материально-вещественному каналу

Для обеспечения безопасности материально-вещественного канала утечки информации нужно организовать СКУД и поставить охранника, который должен осуществлять досмотр на входе в помещение.



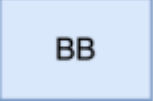

5. ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

На рисунке 5 представлена схема расположения инженерно-технических средств защиты информации, описание которых можно найти в таблице 7.



Рисунок 5 – схема расположения ИТСЗИ в офисе

Таблица 7 – количество и обозначение элементов схемы

Обозначение	Описание	Количество
	Генератор-вибровозбудитель «Соната СА-4Б1» (потолок, пол)	16
	Генератор-вибровозбудитель «Соната СВ-4Б» (окна)	21
	Генератор-вибровозбудитель «Соната СВ-4Б» (стены)	9
	Размыкатель линии «Ethernet» «Соната-ВК4.3»	1



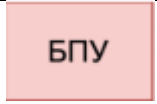

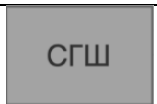
	Размыкатель телефонной линии «Соната-ВК4.1»	1
	Размыкатель слаботочной линии «Соната-ВК4.2»	2
	Генератор-акустоизлучатель «Соната СА-4Б1» (вентиляция)	8
	Блок электропитания и управления «Соната-ИП4.3»	1
	Генератор Шума Соната-РС3	1
	Сетевой генератор шума Соната-Р3.1	1

Таблица 8 – итоговая стоимость всех устройств

Меры защиты	Цена, руб	Кол-во	Итого
Блок электропитания и управления «Соната-ИП4.3»	21600	1	21 600
Генератор-акустоизлучатель «Соната СА-4Б1»	3540	8	28 320
Генератор-вибровозбудитель «Соната СА-4Б»	7440	46	342 240
Размыкатель телефонной линии «Соната ВК4.1»	6000	1	6 000

Рызмыкатель линии «Ethernet» «Соната БК4.1»	6000	1	6 000
Пульт управления «Соната-ДУ 4.3»	7680	1	7 680
SPYDER	140000	1	140 000
Звукоизолирующая дверь	65000	7	224 000
Звукоизоляция переговорного помещения	462900	1	462 900
Генератор Шума Соната-РС3	32400	1	32400
Сетевой генератор шума Соната-Р3.1	33 120	1	33 120
Итого			1 145 260

ВЫВОД

В ходе данной работы был произведен теоретический обзор существующих каналов утечки информации, анализ потенциальных каналов утечки информации в защищаемом помещении и описаны необходимые меры их защиты. Был проанализирован рынок существующих технических средств для противодействия рассматриваемым каналам утечки информации и выбраны подходящие для нашего объекта. Был разработан план установки и произведен расчет стоимости предложенных активных и пассивных средств защиты информации.

В результате была предложена защита от утечек информации по оптическому, акустическому, виброакустическому, электромагнитному каналам, обеспечена защита от ПЭМИН.

Итоговая цена системы защиты информации составляет 1 145 260 рублей.

СПИСОК ИСТОЧНИКОВ

1. Кармановский Н.С., Михайличенко О.В., Савков С.В.. Организационно-правовое и методическое обеспечение информационной безопасности. Учебное пособие – Санкт-Петербург: НИУ ИТМО, 2013. - 151 с. – экз.
2. Титов А. А. Инженерно-техническая защита информации: учебное пособие. Томск: ТУСУР, 2010. — 195 с