

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

Факультет безопасности информационных технологий

КУРСОВАЯ РАБОТА

По дисциплине:

***«Инженерно-технические средства защиты
информации»***

На тему:

**«Проектирование инженерно-технической системы защиты информации на
предприятии»**

Вариант 32

Выполнил(а):

Малыхина Екатерина
Евгеньевна, студент группы
N34471



Проверил преподаватель:

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

Отметка о выполнении:

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент Малыхина Е.Е.

(Фамилия И.О.)

Факультет Безопасности информационных технологий

Группа N34471

Направление (специальность) Информационная безопасность

Руководитель Попов И. Ю., доцент, к. т. н.

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

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии

Задание Цель: Спроектировать инженерно-техническую систему защиты информации для предприятия;

Задачи: 1) Произвести исследование организации, ее структуры и обрабатываемой информации; 2)

Обосновать разработку системы для защиты информации 3) Изучить план предприятия;

4) Проанализировать рынок инженерно-технических средств защиты информации;

5) Разработать итоговую инженерно-техническую систему защиты информации.

Краткие методические указания

Содержание пояснительной записки

Рекомендуемая литература

Руководитель

(Подпись, дата)

Студент

24 октября 2023

(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Малыхина Е.Е.

(Фамилия И.О.)

Факультет Безопасности информационных технологий

Группа N34471

Направление (специальность) Информационная безопасность

Руководитель Попов И. Ю., доцент, к. т. н.

(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	Исследование организации и обрабатываемой информации	31.10.23	31.10.23	
2	Выявление обоснования для разработки инженерно-техническую систему защиты информации	07.11.23	07.11.23	
3	Изучение плана предприятия	14.11.23	14.11.23	
4	Анализ рынка инженерно-технических средств защиты информации	28.11.23	28.11.23	
5	Разработка итоговой инженерно-технической системы защиты информации	12.12.23	12.12.23	

Руководитель _____

(Подпись, дата)

Студент _____

12 декабря 2023

(Подпись, дата)

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

Студент	Малыхина Е.Е. (Фамилия И.О.)
Факультет	Безопасности информационных технологий
Группа	N34471
Направление (специальность)	Информационная безопасность
Руководитель	Попов И. Ю., доцент, к. т. н. (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

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 работы

1. Обследование организации

2. Обоснование защиты информации

3. Обследования плана предприятия

4. Анализ рынка

5. Разработка инженерно-технической системы защиты информации

6. Выводы

7. Список литературы

4. Выводы

В результате выполнения работы был разработан проект инженерно-технической системы защиты информации.

Руководитель

(Подпись, дата)

Студент

27 октября 2023

(Подпись, дата)

«27» октября 2023 г.

СОДЕРЖАНИЕ

Введение	6
1. Обследование предприятия.....	7
2. Обоснование защиты информации.....	9
3. Обследование плана предприятия.....	13
4. Анализ рынка.....	16
4.1 Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам	16
4.2 Защита от утечки информации по (вибро-) акустическим каналам	18
4.4 Защита от ПЭМИН	20
4.4 Защита от утечек информации по оптическим каналам	22
5. Разработка инженерно-технической системы защиты информации	23
Заключение.....	25
Список литературы.....	26

ВВЕДЕНИЕ

Средства защиты информации — это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки, НСД и обеспечения безопасности защищаемой информации.

В данной курсовой работе разработан комплекс инженерно-технической защиты информации, составляющей государственную тайну (с грифом «секретно»). Система защиты создается для офиса, состоящего из девяти помещений, в трех из которых обрабатывается государственная тайна (кабинет директора, переговорная комната, первый отдел).

В работе проведен анализ технических каналов утечки информации, анализ требований к организации защиты РСП, рассмотрены различные средства технической защиты информации и выделены подходящие из них, а также разработана схема монтирования и установки выбранных средств для защиты информации.

1. ОБСЛЕДОВАНИЕ ПРЕДПРИЯТИЯ

Было проведено исследование предприятия с целью разработки системы защиты информации.

Наименование организации: "Платинум"

Область деятельности: разведка и разработка месторождений платины, металлов платиновой группы и природных алмазов.

Схема организации представлена на рисунке 1

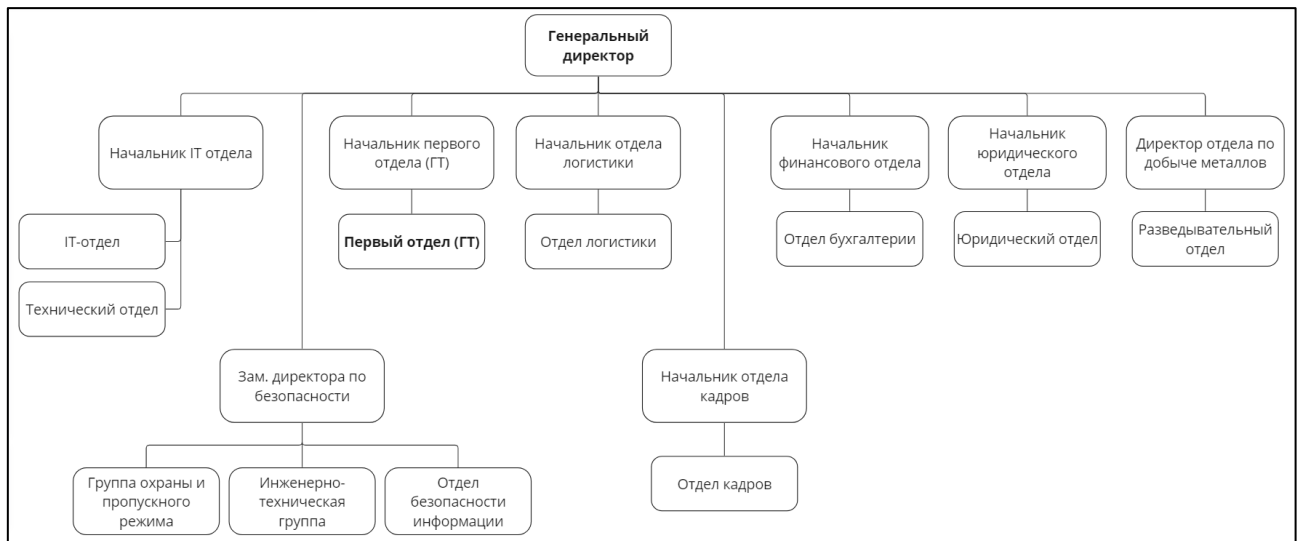


Рисунок 1 - Структура организации

Информационные потоки представляют собой ключевую составляющую системы передачи данных в организации или процессе. Схема информационных потоков позволяет визуализировать и описать обмен информацией между различными участниками системы. Она помогает выявить и проанализировать все этапы передачи и обработки информации, идентифицировать узкие места и возможные проблемы в потоке данных, а также оптимизировать процессы коммуникации и обработки информации.

Основные информационные процессы и потоки в организации, включая описание информации ограниченного доступа:

- Финансовая отчетность;
- Отчетность по обеспечению ЗГТ;
- Детали логистики и продаж;
- ПДн сотрудников;
- Информация о разведке и месторождениях металлов платиновой группы, платины, алмазов (ГТ).

Информационные потоки предприятия представлены на рисунке 2.

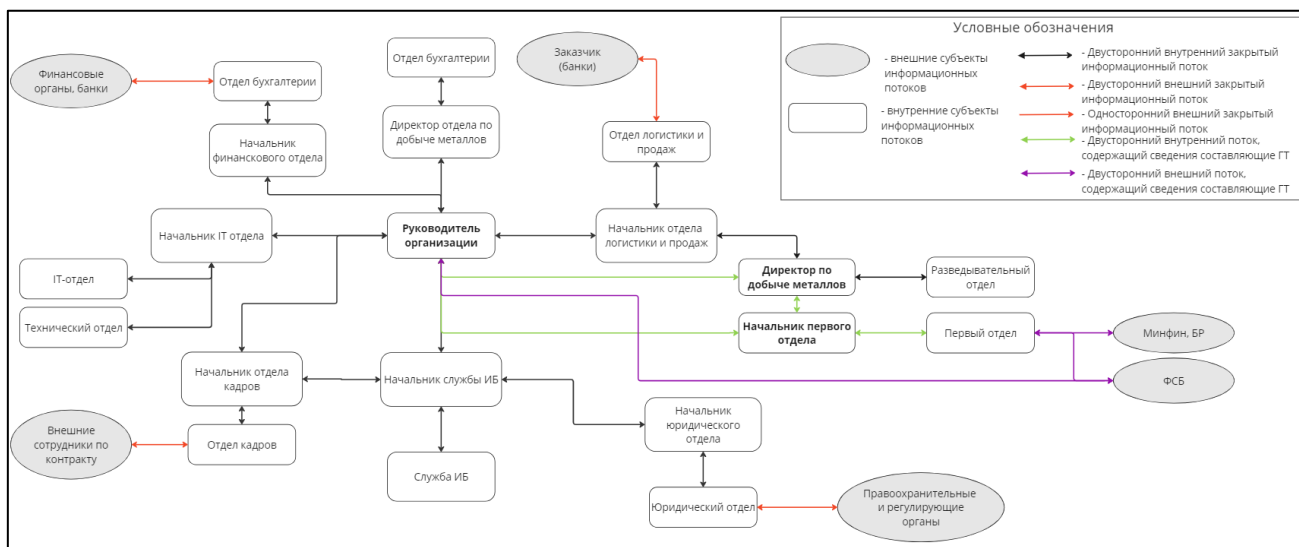


Рисунок 2 - Информационные потоки в организации

2. ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

На основе данных, полученных в предыдущем разделе, я провела анализ нормативной базы, с целью выявления обоснований защиты информации.

Так как основной защищаемой информацией для организации "Платина" является информация, составляющая государственную тайну, то опираться следует на

- закон РФ "О государственной тайне" от 21.07.1993 N 5485-1,
- Постановление Правительства РФ от 15.04.1995 N 333 "О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны."

- Постановление Совета Министров – Правительства РФ от 15 сентября 1993 г. № 912-51 "О государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам".

Согласно закону РФ "О государственной тайне" от 21.07.1993 N 5485-1, статье 5, государственную тайну составляют: ...

2) сведения в области экономики, науки и техники:

о запасах платины, металлов платиновой группы, природных алмазов в Государственном фонде драгоценных металлов и драгоценных камней Российской Федерации, Центральном банке Российской Федерации, а также об объемах запасов в недрах, добычи, производства и потребления стратегических видов полезных ископаемых Российской Федерации (по списку, определяемому Правительством Российской Федерации);

Согласно закону РФ "О государственной тайне" от 21.07.1993 N 5485-1, статье 27, допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, осуществляется путем получения ими в порядке, устанавливаемом Правительством Российской Федерации, лицензий на проведение работ со сведениями соответствующей степени секретности.

Лицензия на проведение работ с использованием сведений, составляющих государственную тайну, выдается предприятию, учреждению, организации при выполнении ими следующих условий: наличие у них сертифицированных средств защиты информации.

Согласно закону РФ "О государственной тайне" от 21.07.1993 N 5485-1, статье 28, средства защиты информации должны иметь сертификат, удостоверяющий их соответствие

требованиям по защите сведений соответствующей степени секретности.

Согласно Постановлению Правительства РФ от 15.04.1995 N 333, пункту 7, лицензии выдаются на основании результатов специальных экспертиз предприятий и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну (далее именуются - руководители предприятий), и при выполнении следующих условий:

соблюдение требований законодательных и иных нормативных актов Российской Федерации по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;

наличие на предприятии средств защиты информации, имеющих сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Согласно Постановлению Правительства РФ от 15.04.1995 N 333, пункту 10, специальная экспертиза предприятия проводится путем проверки выполнения требований нормативно-методических документов по режиму секретности, противодействию иностранным техническим разведкам и защите информации от утечки по техническим каналам, а также соблюдения других условий, необходимых для получения лицензии.

Согласно Постановлению Совета Министров – Правительства РФ от 15 сентября 1993 г. № 912-51, статье 1, пункту 4, защита информации осуществляется путем выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения, по противодействию иностранным техническим разведкам, а также путем проведения специальных работ, порядок организации и выполнения которых определяется Советом Министров – Правительством Российской Федерации.

Согласно Постановлению Совета Министров – Правительства РФ от 15 сентября 1993 г. № 912-51, статье 1, пункту 9, проведение любых мероприятий и работ с использованием сведений, отнесенных к государственной или служебной тайне, без принятия необходимых мер по защите информации не допускается.

Согласно Постановлению Совета Министров – Правительства РФ от 15 сентября 1993 г. № 912-51, статье 2, пункту 19, предприятия, имеющие намерения заниматься деятельностью в области защиты информации, должны получить соответствующую лицензию на определенной вид этой деятельности. Лицензии выдаются Государственной

технической комиссией при Президенте Российской Федерации и другими лицензирующими органами в соответствии со своей компетенцией по представлению органа государственной власти.

Согласно Постановлению Совета Министров – Правительства РФ от 15 сентября 1993 г. № 912-51, статье 3, пункту 26, защита информации осуществляется путем:

...

2) предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами, а также электроакустических преобразований;

...

5) выявления возможно внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств);

6) предотвращения перехвата техническими средствами речевой информации из помещений и объектов.

Предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, а также электроакустических преобразований достигается применением защищенных технических средств, аппаратных средств защиты, средств активного противодействия, экранированием зданий или отдельных помещений, установлением контролируемой зоны вокруг средств информатизации и другими организационными и техническими мерами.

Выявление возможно внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств) достигается проведением специальных проверок по выявлению этих устройств.

Предотвращение перехвата техническими средствами речевой информации из помещений и объектов достигается применением специальных средств защиты, проектными решениями, обеспечивающими звукоизоляцию помещений, выявлением специальных устройств подслушивания и другими организационными и режимными мероприятиями.

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 эта же, каждое окно оборудуется выдвижными ставнями или створками с металлической решеткой, которая крепится к железным конструкциям оконного проема в стене.

4. Все режимные помещения оборудуются аварийным освещением.

5. Оборудование помещений для работы с государственной тайной по требованиям технической безопасности, вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемым к оснащению защищенных и выделенных помещений.

6. Перед началом эксплуатации необходимо проверить выделенные и иные режимные помещения проверить на предмет наличия «жучков» и иных средств несанкционированного получения информации. В дальнейшем такие проверки желательно проводить периодически, чтобы исключить возможность утечки.

3. ОБСЛЕДОВАНИЕ ПЛАНА ПРЕДПРИЯТИЯ


В этом разделе представлен результат анализа плана помещения предприятия. Целью анализа являлась идентификация защищаемых помещений и выявление возможных каналов утечки. План помещения предприятия представлен на рисунке 3.

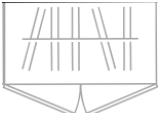
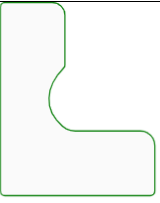


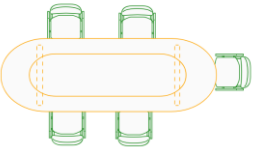
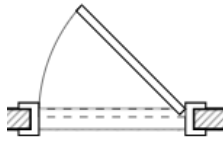




Рисунок 3 - План помещения предприятия

Организация снимает офис в бизнес-центре класса А, поэтому собственной охраны нет.

Таблица 1 – Описание обозначений

Обозначение	Описание	Обозначение	Описание
	Кресло		Комнатное растение
	Офисный стул		Сейф
	Журнальный столик		Рабочий стол
	Диван		Кулер

Обозначение	Описание	Обозначение	Описание
	Шкаф		Угловой рабочий стол
	Радиатор отопления		Окно
	Стол переговоров со стульями		Дверь
	Урна		Вешалка

Описание комнат офисного помещения:

1. Общий туалет
2. Кабинет ИТ-отдела, здесь находится электрический щиток и специалисты по настройке всех технических средств;
3. Кабинет отдела кадров
4. Кабинет отдела логистики
5. Коридор с вестибюлем, общее пространство, за стойкой находится администратор
6. Кабинет юридического и бухгалтерского отделов
7. Кабинет генерального отдела, рядом находится начальник первого отдела и начальник отдела логистики (в помещении обрабатывается гостайна)
8. Переговорная (гостайна)
9. Кабинет первого отдела (гостайна)

В каждом помещении существуют потенциальные пути для нежелательной утечки информации, связанные с электромагнитными и электрическими утечками информации, то есть с использованием компьютеров и розеток. Вентиляционные люки и декоративные элементы, такие как комнатные растения, могут использоваться для установки закладных устройств, которые могут использоваться для передачи информации через акустический канал.

Существуют также риски утечки информации через оптические каналы, например, из-за незакрытых окон и незащищенных дверей. Важно учитывать также виброакустический канал, который может быть использован для передачи информации из-за наличия твердых

поверхностей, таких как стены или батареи отопления.

Вещественно-материальный канал утечки информации возможен ввиду наличия вещественных носителей информации, однако он не учитывается в данной работе, поскольку он не перекрывается техническими средствами защиты и регламентируется внутренней политикой безопасности организации.

Таблица 1 – Источники утечек

Канал	Источник	Пассивная защита	Активная защита
Акустический/ виброакустический	Окна, двери, стены	Звукоизоляция рабочих помещений, использование двойных окон	Устройства акустического зашумления
Электрический/ акустоэлектрический	Компьютерная техника, телефоны	Использование фильтров	Линейные генераторы шума
Оптический	Окна и двери	Запторивание окон, установка доводчиков на двери	-
Электрический/ электромагнитный	Компьютеры, кабели, проводка	-	Устройства линейного и пространственного зашумления

Пассивные средства защиты направлены на ослабление информативных сигналов. Такими средствами являются шторы, жалюзи, средства вибро- и звукоизоляции.

Активные средства защиты генерируют помехи, искажающие информативные сигналы и мешающие работе прослушивающих устройств. Такими средствами являются комплексные устройства, генерирующие сигналы в разных диапазонах частот.

4. АНАЛИЗ РЫНКА

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 4.1. Это позволит обеспечить надежную защиту от несанкционированного доступа и утечки такой конфиденциальной информации.

Таблица 4.1 – Активная и пассивная защита информации

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

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

Пассивная защита включает себя размещение фильтров в электропитании всех

помещений.

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 4.2.

Таблица 4.2 – Активная защита от утечек информации по электрическим каналам

Модель	Производитель	Характеристики	Цена, руб.
Соната-РС3	Соната	Работа от сети ~220 В +10%/-15%, 50 Гц. Потребляемая мощность – 10Вт. Продолжительность работы не менее 8 часов. Звуковая и световая индикация работы. Возможно дистанционное управление посредством проводного пульта.	32 400
ЛГШ-221	Лаборатория ПППШ	Сетевой генератор шума. Устройство оснащено световым и звуковым индикаторами работы. Возможность управления устройством с помощью пульта ДУ.	36 400
Соната-РС1	Соната	Диапазон частот до 1 ГГц, регулировка уровня шума в 1 частотной полосе. Напряжение 220 В. Возможность локального проводного управления в случае использования в составе комплекса ТСЗИ (встроенный модуль Rebus)	16 520
Генератор шума Покров	Институт Радиоэлектронных Систем	Диапазон частот 10 кГц – 6000 МГц. Мощность 15 Вт. Нарботка на отказ 5000 часов. Централизованное управление и контроль по Ethernet (для исполнения 2), для	32 800

Модель	Производитель	Характеристики	Цена, руб.
		применения в системах пространственного зашумления. Независимая регулировка уровней электромагнитного поля шумового сигнала и шумового сигнала в линии электропитания и заземления.	

На основании анализа, проведенного в таблице 4.1, был выбран генератор шума Соната-РС3. Оптимальный вариант по соотношению цена и качество позволяют установить достаточное количество подобных устройств в помещениях.

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

Пассивные меры безопасности включают в себя создание тамбурной зоны перед переговорной комнатой и установку усиленных дверей. Для обеспечения звукоизоляции переговорной комнаты и кабинета руководителя используются специальные материалы для звукоизоляции стен.

Активные меры безопасности представляют собой систему виброакустической маскировки. Для обеспечения безопасности помещения, в котором обрабатывается информация, отнесенная к категории «совершенно секретно», рассматриваются технические средства активной защиты информации для объектов информатизации, имеющих категорию не ниже 1Б.

Таблица 4.3 – Активная защита от утечек информации по (вибро-)акустическим каналам

Модель	Производитель	Характеристики	Цена, руб.
ЛГШ-404	Лаборатория ППШ	Электропитание 220 В/50 Гц. Максимальное количество излучателей – 40. Диапазон воспроизводимого шумового сигнала 175–11200 Гц. Вариативность количества подключаемых к генераторному блоку преобразователей. К двухканальному виброакустическому генератору шума ЛГШ-404 можно одновременно подключить до 20 ЛВП-10 и до 20 ЛВП-2А. Счетчик времени	35 100

Модель	Производитель	Характеристики	Цена, руб.
		наработки и световая индикация режима работы. Проводной пульт дистанционного управления в комплекте	
Шорох 5Л	Шорох	Максимальное количество излучателей – 40. Электропитание 220 (+10% - 15%) В (есть возможность работы системы от источника питания 12В). Количество октавных полос для регулировки уровня мощности шума – 7. Устройство оснащено световым и звуковым индикаторами работы. Возможность управления устройством с помощью пульта ДУ.	21 500
SEL SP-157 Шагренъ	Сюртель	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
Соната АВ-4Б	Соната	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.	44 200

Исходя из анализа, представленного в таблице 4.2, 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. Особенностью «Соната АВ-4Б» является использование принципа «единый источник электропитания + генераторы-электроакустические преобразователи (излучатели)», что обеспечивает высокую степень надежности в защите информации. Кроме того, усовершенствованная настройка аппаратных элементов модели 4Б позволяет интегрировать источник электропитания с другими для обмена информацией.

4.3 Защита от ПЭМИН

Таблица 4.4 – Активная защита от ПЭМИН

Модель	Производитель	Характеристики	Цена, руб.
ЛГШ 503	Лаборатория ППП	<p>Диапазон частот 10 кГц - 1800 МГц.</p> <p>Уровень шума от -26 дБ (мкА/м*$\sqrt{\text{кГц}}$) до 50 дБ(мкВ/м*$\sqrt{\text{кГц}}$).</p> <p>Мощность – 45 Вт.</p> <p>Оснащен визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа). Оснащен счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы в режиме формирования маскирующих помех.</p> <p>Прибор имеет возможность подключения проводного дистанционного управления и контроля, в качестве которого может использоваться программно-аппаратный комплекс «Паутина».</p>	44 200
Соната-Р3.1	Соната	<p>Электропитание – 220 В +10%/-15%, 50 Гц.</p> <p>Мощность – 10 Вт.</p> <p>Продолжительность непрерывной работы не менее 8 ч</p>	39 000

Модель	Производитель	Характеристики	Цена, руб.
		Обеспечивает защиту информации от утечки за счет побочных электромагнитных излучений и наводок путем излучения в окружающее пространство электромагнитного поля шума, а также наводок на линии сети электропитания и заземления путем индуцирования в них маскирующих шумовых напряжений.	
ЛГШ-513	Лаборатория ППШ	<p>Диапазон частот 10 кГц - 1800 МГц.</p> <p>Уровень шума от -18 дБ(мкА/м*√кГц) до 50 дБ(мкВ/м*√кГц).</p> <p>Мощность – не более 45 ВА.</p> <p>Режим работы – круглосуточно.</p> <p>Изделие «ЛГШ-513» оснащено визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа). Изделие «ЛГШ-513» оснащено счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы Изделия в режиме формирования маскирующих помех.</p>	33 120
Генератор шума Пульсар	Эшелон	<p>Диапазон частот 10 кГц - 6 ГГц.</p> <p>Электропитание – однофазная сеть переменного тока 187–242 В.</p> <p>Мощность – 50 ВА.</p> <p>Имеет защиту регулятора уровня выходного шумового сигнала от нелегального доступа (и сигнализирует об этом). Индикаторы нормального режима работы (диод) и аварийного режима (свет и звук).</p>	24 525

В качестве средства активной защиты от ПЭМИН был выбран генератор шума «ЛГШ-503». Этот выбор обоснован широким диапазоном частот (от 10 кГц до 1800 МГц) и

круглосуточным режимом работы. Кроме того, данный прибор поддерживает возможность подключения проводного дистанционного управления и контроля, для чего может быть использован программно-аппаратный комплекс «Паутина».

4.4 Защита от утечек информации по оптическим каналам

Для обеспечения защиты помещения от возможной фото-видеосъемки или визуального наблюдения следует установить жалюзи на окна и также воспользоваться доводчиками для дверей.

5. РАЗРАБОТКА ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

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 «Покров»;
- система виброакустической защиты «Соната АВ-4Б»;
- генератор шума «ЛГШ-503» от ПЭМИН
- жалюзи на три окна;
- три усиленные двери.

К сетевому генератору шума Покров подключаются компьютеры в первом отделе. В АЗ и АЗ ставятся на места возможной прослушки: потолки, полы и стены, водопроводные и отопительные трубопроводы, оконные проемы помещения.

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.

Таблица 5.1 – Необходимое оборудование

Меры защиты	Цена, руб.	Количество, шт.	Итоговая стоимость
Сетевой генератор шума «Покров»	32 800	1	32 800
Генератор шума «ЛГШ-503»	44 200	2	88 400
Генератор-акустоизлучатель «Соната СА-4Б1»	3 540	6	21 240
Генератор-вибровозбудитель «Соната СА-4Б»	7 440	15	111 600
Рызмыкатель слаботочной линии «Соната ВК4.2»	6 000	1	6 000
Рызмыкатель линии «Ethernet» «Соната ВК4.1»	6 000	3	18 000
Шторы	4 900	3	14 700
Усиленные звукоизолирующие двери	83 000	3	249 000
Итого			541 740

На основе результатов анализа плана помещения предприятия и результатов анализа рынка инженерно-технических средств защиты информации была разработана инженерно-техническая система защиты информации для предприятия “Платина”. Состав и размещение инженерно-технических средств защиты информации представлен на рисунке 4.



Рисунок 4 - План помещения предприятия с инженерно-технической системой защиты информации

Легенда:

- АЗ - Система постановки акустических помех;
- ББС - Блокиратор беспроводной связи;
- ВАЗ - Система постановки виброакустических помех;
- ГШ - Генератор шума ПЭМИ;
- Р - Размыкатель Ethrnet;
- РС - Размыкатель слаботочных сетей;
- СГШ - Сетевой генератор шума;

Также на окнах в помещениях 7, 8 и 9 были установлены экраны на окна, предотвращающие утечку информации по визуально-оптическому каналу.

6. ЗАКЛЮЧЕНИЕ

В результате выполнения курсового проекта мной была разработана инженерно-техническая система защиты информации для конструкторского бюро двойного назначения, разрабатывающего гражданские коптеры и беспилотные летательные аппараты военного назначения “Платина”.

Для достижения цели мною было проведено предпроектное обследование организации и выявлены основные информационные активы, внешние и внутренние, открытые и закрытые информационные потоки, а также был обследован план помещения организации и выявлены возможные каналы утечки информации.

Также мною был проведен анализ нормативной базы, с целью выявления обоснования для защиты информации и анализ рынка инженерно-технических средств, с целью выявления наилучших предложений.

СПИСОК ЛИТЕРАТУРЫ

1. Требования к режимным помещениям и их оборудованию // Компания КАСЛ-ЦЛС Прогресс URL: <https://licenziya-fsb.com/trebovaniya-k-rezhimnym-pomeshheniyam> (дата обращения: 25.11.2023)
2. Закон Российской Федерации "О государственной тайне" от 21.07.1993 № 5485-1 // Официальный интернет-портал правовой информации
3. Постановление Правительства РФ "О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны" от 15.04.1995 № 333 // Официальный интернет-портал правовой информации
4. Постановление Совета Министров – Правительства РФ "О государственной системе защиты информации в российской федерации от иностранных технических разведок и от ее утечки по техническим каналам" от 15.09.1993 № 912-51 // Официальный интернет-портал правовой информации
5. Detector Systems. Официальный сайт. – Москва. – URL: <https://detsys.ru/> (дата обращения: 18.12.2023).
6. ЦЛС Прогресс. Требования к режимным помещениям и их оборудованию: официальный сайт. – Москва. – URL: <https://licenziya-fsb.com/trebovaniya-k-rezhimnym-pomeshheniyam> (дата обращения: 18.12.2023). – Текст: электронный.