

**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 88»**

Выполнил(а):

Студент группы N34501 Иванов Никита Андреевич



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	Иванов Никита Андреевич
	(Фамилия И.О.)
Факультет	Безопасности информационных технологий
Группа	N34501
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 системы инженерно-технической защиты информации на предприятии

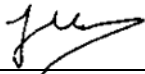
Краткие методические указания

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

Содержание пояснительной записки

1. Введение.
2. Организационная структура предприятия.
3. Обоснование защиты информации.
4. Анализ защищаемых помещений.
5. Анализ рынка технических средств.
6. Описание расстановки технических средств.
7. Заключение.
8. Список литературы.

Рекомендуемая литература

Руководитель		(Подпись, дата)
Студент		17.12.2023
		(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Иванов Никита Андреевич
(Фамилия И.О.)

Факультет Безопасности информационных технологий

Группа N34501

Направление (специальность) Информационная безопасность

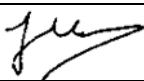
Руководитель Попов И. Ю., доцент, к. т. н.
(Фамилия И.О., должность, ученое звание, степень)

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	09.11.23	10.11.23	
2	Выявление обоснования для разработки инженерно-техническую систему защиты информации	13.11.23	14.11.23	
3	Изучение плана предприятия	15.11.23	17.11.23	
4	Анализ рынка инженерно-технических средств защиты информации	10.12.23	15.12.23	
5	Разработка итоговой инженерно-технической системы защиты информации	16.12.23	17.12.23	

Руководитель _____
(Подпись, дата)

Студент  17.12.2023
(Подпись, дата)

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

АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ

Студент Иванов Никита Андреевич

(Фамилия И.О.)

Факультет Безопасности информационных технологий

Группа N34501

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

☐ 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 _____

Содержание работы

1. Введение.

2. Исследование предприятия.

3. Обоснование защиты информации.

4. Анализ защищаемых помещений.

5. Анализ рынка технических средств.

6. Описание расстановки технических средств.

7. Заключение.

8. 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 _____

17.12.2023

(Подпись, дата)

«_____» _____ 20____ г

СОДЕРЖАНИЕ

Введение	6
1 Исследование предприятия.....	7
2 Обоснование защиты информации	9
3 Исследование плана предприятия.....	14
3.1 Анализ каналов утечки.....	17
4 Анализ рынка	19
4.1 Защита от утечки информации по электрическим и электромагнитным каналам ...	19
4.2 Защита от утечки информации по акустическим и виброакустическим каналам	21
4.3 Защита от утечек информации по оптическим каналам	22
5 Разработка инженерно-технической системы защиты информации.....	23
Заключение.....	25

ВВЕДЕНИЕ

Цель работы – разработать инженерно-техническую систему защиты информации на предприятии, обеспечивающую надежную защиту сведений, составляющих государственную тайну.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Исследовать организационную структуру предприятия.
2. Обосновать необходимость защиты информации.
3. Провести анализ защищаемых помещений, возможные каналы утечки;
4. Проанализировать рынок инженерно-технических средств защиты информации;
5. Спроектировать систему защиты информации на основе выбранных средств.

1 ИССЛЕДОВАНИЕ 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

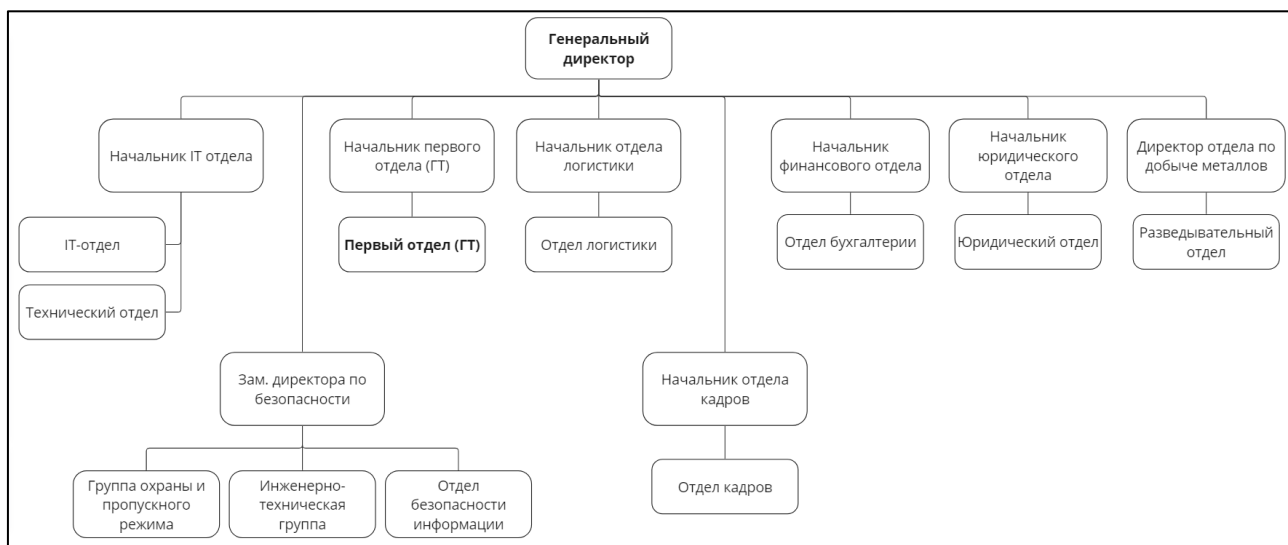


Рисунок 1 - Структура организации

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;
- Отчеты логистики и продаж;

- Иная коммерческая тайна;
- ПДн сотрудников;
- Информация о разведке и месторождениях металлов платиновой группы, платины, алмазов (гостайна (ГТ)).

Информационные потоки предприятия представлены на рисунке 2.

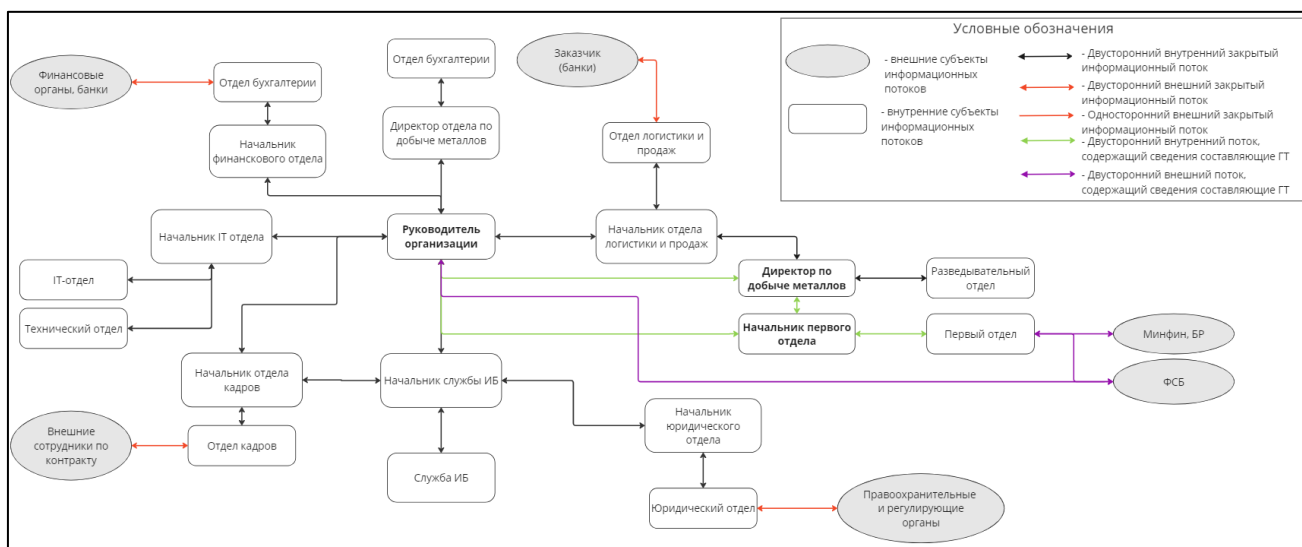


Рисунок 2 - Информационные потоки в организации

2 ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

На основе данных, полученных в предыдущем разделе, был проведен анализ нормативной базы, с целью выявления обоснований защиты информации. Поскольку на предприятии осуществляется поток сведений, относящихся к государственной тайне под грифом «секретно», основной упор с точки зрения обоснования защиты информации будет в области защиты гостайны.

Так как основной защищаемой информацией для организации "Платинум" является информация, составляющая государственную тайну, то в первую очередь 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." и 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:

6. 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;
7. 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);

б) 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 ИССЛЕДОВАНИЕ 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. Описание обозначений представлено в таблице 1.

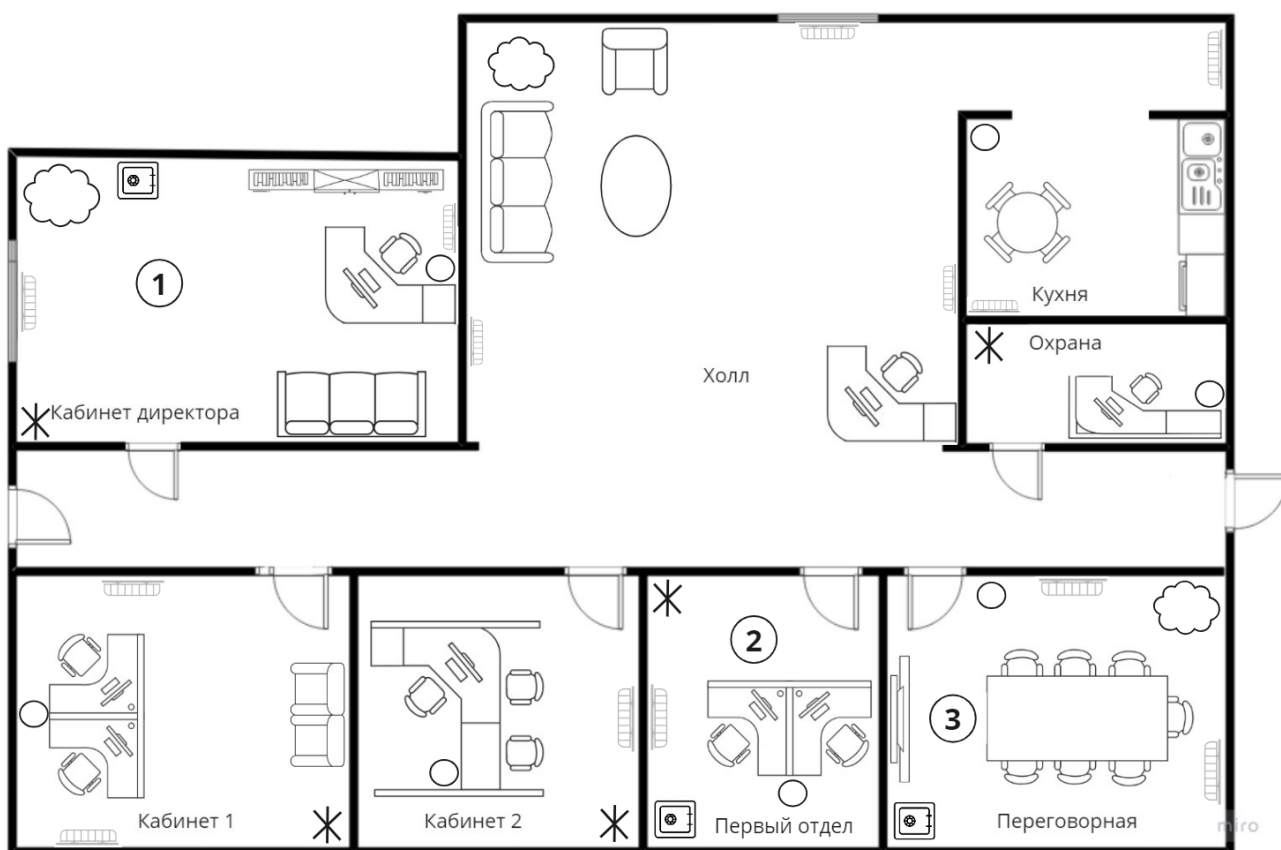



Рисунок 3 - План помещения предприятия

Таблица 1 – Описание обозначений

Обозначение	Описание	Обозначение	Описание
	Кресло		Комнатное растение
	Офисный стул		Компьютер
	Журнальный столик		Дисплей для презентаций

Обозначение	Описание	Обозначение	Описание
	Диван		Сейф
	Шкаф		Рабочий стол с тумбочкой
	Радиатор отопления		Кухонная раковина с микроволновой печью
	Кухонный стол со стульями		Холодильник
	Стол переговоров со стульями		Сдвоенный рабочий стол
	Урна		Окно
	Вешалка		Дверь

В помещениях, помеченными номерами 1, 2, 3, производится обработка сведений составляющих гостайну. Легенда:

1) Холл - общее пространство, за рабочим столом сидит администратор, он принимает новоприбывших посетителей и сопровождает их до нужных общедоступных помещений. Также здесь находится зона для посетителей с диваном, креслом, столиком, комнатным растением, окном, двумя радиаторами отопления;

2) Кабинет охраны (11 м²) – здесь находятся стол с тумбочкой, компьютер, стул, вешалка, урна, дверь. Оснащено шестью розетками и вентиляционным люком на потолке;

3) Кухня (16 м²) – кухонный стол со стульями, холодильник, урна, кухонная раковина с микроволновой печью, радиатор отопления. Оснащено четырьмя розетками и вентиляционным люком на потолке;

4) Кабинет директора (25 м²) – вешалка для одежды, диван, стол с тумбочкой, стул, урна, компьютер, комнатное растение, сейф, окно, дверь, два радиатора отопления. Оснащено тремя розетками и вентиляционным люком на потолке. Здесь может обрабатываться гостайна;

5) Кабинет 1 (18 м²) – два кресла, два компьютера, вешалка, урна, сдвоенный рабочий стол, два стула, дверь, два радиатора отопления. Оснащено тремя розетками и вентиляционным люком на потолке;

6) Кабинет 2 (16 м²) – три стула, стол с тумбочкой, вешалка, урна, дверь, компьютер, радиатор отопления. Оснащено четырьмя розетками и вентиляционным люком на потолке;

7) Первый отдел (14 м²) – сейф, дверь, два компьютера, вешалка, урна, сдвоенный рабочий стол, два стула, дверь, радиатор отопления. Оснащено четырьмя розетками и вентиляционным люком на потолке. Здесь может обрабатываться гостайна;

8) Переговорная (20 м²) – вешалка, стол со стульями для переговоров, дисплей для презентаций, комнатное растение, урна, сейф, два радиатора отопления. Оснащено четырьмя розетками и вентиляционным люком на потолке. Здесь может обрабатываться гостайна.

Организация арендует офис на седьмом этаже девятиэтажного здания. Стены здания и внутренние перегородки железобетонные, толщиной не менее 13 см. Окна не соседствуют с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и прочими элементами, с которых в помещения могут проникнуть посторонние лица.

3.1 Анализ каналов утечки

В каждом помещении существуют потенциальные пути для нежелательной утечки информации, связанные с электромагнитными и электрическими утечками информации, то есть с использованием компьютеров и розеток. Потенциальные каналы утечки информации – это пути распространения информации, при передаче по которым существует вероятность перехвата информации. 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.

Возможные каналы утечки, источники утечки, а также средства активной и пассивной защиты на предприятии представлены в таблице 2.

Таблица 2 – Каналы утечки и защита

Канал утечки	Источники	Пассивная защита	Активная защита
Визуально-оптический	Окна, двери	Защитные экраны и фильтры для сетей электропитания, доводчики дверей, жалюзи, блэкаут шторы	-
Электромагнитный, электрический	Розетки, компьютеры, любые	Фильтры для цепей электропитания, экранирование	Системы линейного и пространственного

	электрические приборы	металлическим материалом	зашумления
Акустический Электроакустический	Стены, двери, окна, электрические сигналы, вентиляция	Звукоизоляция помещений, акустические экраны, фильтры для цепей электропитания	Устройства акустического зашумления
Вибрационный, Виброакустический	Любые твердые поверхности в помещении, например, радиаторы отопления	Изоляция помещений за счет использования антивибрационных материалов	Устройства вибрационного зашумления

4 АНАЛИЗ РЫНКА

По итогам анализа предыдущих разделов, для обеспечения комплексной безопасности в предприятии с обработкой сведений, составляющих государственную тайну уровня «секретно» требуется оснастить выделенные помещения средствами инженерно-технической защиты.

4.1 Защита от утечки информации по электрическим и электромагнитным каналам

Пассивная защита включает себя размещение размыкателей и фильтров в электропитании.

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 3.

Таблица 3 – Активная защита от утечек информации по электрическим и электромагнитным каналам

Модель	Характеристики	Особенности	Цена, руб.
Генератор шума ЛГШ-513	Диапазон частот 10 кГц – 1800 МГц. Не более 45 ВА. Нарботка на отказ 6000 часов.	Генератор шума по цепям электропитания, заземления и ПЭМИН	39 000
Генератор шума Соната-РС3	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
Соната-РС1	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	16 520
Генератор шума ЛГШ-221	Диапазон частот 10 кГц – 400 МГц. Мощность, потребляемая от сети не более 45 ВА.	Сетевой генератор шума. Возможность управления устройством с помощью пульта ДУ.	36 400

На основании анализа, проведенного в таблице 3, был выбран генератор шума «ЛГШ-513». За отличную цену данный генератор шума предлагает широкий диапазон частот, защиту по целям электропитания, заземления и ПЭМИН.

Предложения по защите слаботочных линий, линий связи, Ethernet линий представлена в таблице 4.

Таблица 4 – Защита слаботочных линий и линий связи

Модель	Характеристики	Особенности	Цена, руб.
Соната-ВК 4.1 (в составе Соната АВ-4Б)	Частота - 150 Гц - 10 МГц. Интервал давления - 30–60 дБ.	Размыкатель аналоговых телефонных линий + Соната-ИП4.4 (36 000 руб.). Потребляет не более 60 мА и может работать непрерывно до 8 часов.	6 000
Соната-ВК 4.2 (в составе Соната АВ-4Б)	Частота - 150 Гц - 10 МГц. Интервал давления - 30–60 дБ.	Размыкатель линий оповещения и сигнализации + Соната-ИП4.4 (36 000 руб.). Потребляет не более 60 мА и может работать непрерывно до 8 часов.	6 000
Соната-ВК 4.3 (в составе Соната АВ-4Б)	Частота - 150 Гц - 10 МГц. Интервал давления - 30–60 дБ.	Размыкатель компьютерных сетей + Соната-ИП4.4 (36 000 руб.). Потребляет не более 60 мА и может работать непрерывно до 8 часов.	6 000
ЛУР 2 (В составе ЛГШ-404)	Частота – 175 Гц – 11.2 МГц	Размыкатель слаботочных линий питания	5 590
ЛУР 4 (В составе ЛГШ-404)	Частота – 175 Гц – 11.2 МГц	Размыкатель слаботочных линий Телефон	5 590
ЛУР 8 (В составе ЛГШ-404)	Частота – 175 Гц – 11.2 МГц	Размыкатель слаботочных линий Ethernet	5 590

В качестве защиты слаботочных линий и линий связи были выбрали Соната-ВК 4.1, Соната-ВК 4.2, Соната-ВК 4.3. Данные приборы за счет

акустоэлектрических преобразований позволяют защищать систему от утечек по всевозможным физическим линиям связи. Входят в состав системы Соната АВ-4Б, которая используется в системе. В качестве защиты линий 220 В был выбран сетевой фильтр Соната-ФС10.1.

4.2 Защита от утечки информации по акустическим и виброакустическим каналам

Пассивные меры безопасности включают от утечки по акустическим и виброакустическим каналам заключается в себя установку усиленных дверей. Для обеспечения звукоизоляции переговорной комнаты и кабинета руководителя используются специальные материалы для звукоизоляции стен.

Для обеспечения безопасности помещения, в котором обрабатывается информация, отнесенная к категории «секретно», активные меры безопасности представляют собой систему виброакустической маскировки.

Таблица 5 – Активная защита от утечек информации по акустическим и виброакустическим каналам

Модель	Характеристики	Особенности	Цена, руб.
ЛГШ-404	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.	35 100
Соната АВ-4Б	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.	44 200
Шорох 5Л	Максимальное количество излучателей – 40. Электропитание 220	Сетевой генератор шума. Устройство оснащено световым и звуковым индикаторами работы.	21 500

Модель	Характеристики	Особенности	Цена, руб.
	(+10% - 15%) В (есть возможность работы системы от источника питания 12В).		
SEL SP-157 Шагрень	Диапазон воспроизводимого шумового сигнала 90–11200 Гц. Максимальное количество излучателей – 64. Электропитание 220В/50Гц.	Защита паролем настроек системы. Отсчёт времени наработки генерации шума по каждому каналу с выводом на экран.	47 400

В качестве системы защиты от (вибро-)акустических утечек была выбрана «Соната АВ-4Б». У данной системы большое количество положительных отзывов. «Соната АВ-4Б» является использование принципа «единый источник электропитания + генераторы-электроакустические преобразователи (излучатели)», что обеспечивает высокую степень надежности в защите информации.

4.3 Защита от утечек информации по оптическим каналам

Для обеспечения защиты помещения от возможной фото-видеосъемки или визуального наблюдения следует установить на окна блэкаут-шторы. Также воспользоваться доводчиками для дверей.

5 РАЗРАБОТКА ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

По результатам анализа предыдущих разделов и согласно документации выбранных приборов был разработан план помещения предприятия «Платинум» с инженерно-техническими средствами для защиты информации от возможных утечек на рисунке 4.










Рисунок 4 - План помещения с инженерно-техническими средствами защиты информации

В таблице 6 представлены условные обозначения средств защиты их итоговое количество и стоимость.

Таблица 6 – Обозначения устройств, количество и цена

Средство защиты	Обозначение	Кол-во	Цена, руб.
Генератор шума ЛГШ-513	ГШ	3	117 000
Сетевой фильтр Соната-ФС10.1	СФ	1	50 400
Размыкатель слаботочной линии Соната ВК 4.1	РСЛ	3	18 000

Средство защиты	Обозначение	Кол-во	Цена, руб.
Размыкатель телефонной линии Соната ВК 4.2		3	18 000
Размыкатель линии Ethernet Соната ВК 4.3		4	24 000
Пульт управления Соната-ИП4.3		2	72 000
Генератор-вибровозбудитель Соната СА-4Б		20	148 800
Генератор-акустоизлучатель СА-4Б		6	44 640
Штора-блэкаут		2	7 000
Дверь звукоизоляционная 36 dB		3	97 460
Итого			597 300

Итого, на систему инженерно-технической защиты информации на предприятии с обработкой гостайны было потрачено 597 300 рублей.

ЗАКЛЮЧЕНИЕ

В результате выполнения курсового проекта мной была разработана инженерно-техническая система защиты информации предприятия, которые занимается разведкой и разработкой месторождений платины, металлов платиновой группы и природных алмазов «Платинум», на данном предприятии обрабатывается гостайна грифа «секретно». Для достижения цели 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. По итогу был предложен план организации с инженерно-техническими средствами защиты информации. Общая стоимость предложенных средств защиты составила 578 700 рублей.

СПИСОК ЛИТЕРАТУРЫ

1. Закон Российской Федерации "О государственной тайне" от 21.07.1993 № 5485–1 // Официальный интернет-портал правовой информации
2. 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
3. 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
4. Кармановский, Н. С. Организационно-правовое и методическое обеспечение информационной безопасности : учебное пособие / Н. С. Кармановский, О. В. Михайличенко, С. В. Савков. — Санкт-Петербург : НИУ ИТМО, 2013. — 148 с. — Текст : электронный — URL: <https://e.lanbook.com/book/43579> (дата обращения: 10.12.2023).
5. Detector Systems: Системы комплексной безопасности [Электронный ресурс]. – URL: <https://detsys.ru/> (дата обращения: 16.12.2023).