

**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»

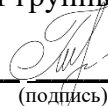
На тему:

«Проектирование инженерно-технической системы защиты информации на предприятии.

Вариант 94»

Выполнил:

Николаев Глеб Витальевич, студент группы N34501



(подпись)

Проверил:

Попов Илья Юрьевич, к.т.н, 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	Николаев Глеб Витальевич
	(Фамилия И.О.)
Факультет	Безопасности Информационных Технологий
Группа	N34501
Направление (специальность)	10.03.01. - Технологии защиты информации
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ Университета ИТМО
	(Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической системы защиты информации на предприятии
Задание	Проанализировать всевозможные каналы утечки данных в помещении, провести анализ рынка технических средств защиты информации разных категорий, разработать схему расстановки выбранных технических средств в защищаемом помещении

Краткие методические указания

Рекомендуемая литература

Руководитель	Попов Илья Юрьевич	
		(Подпись, дата)
Студент	Николаев Глеб Витальевич	
		(Подпись, дата)

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»
ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

Студент Николаев Глеб Витальевич

(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34501

Направление (специальность) 10.03.01. - Технологии защиты информации

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

(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	Разработка и согласование ТЗ	24.10.2023	24.10.2023	
2	Анализ источников Информации	26.10.2023	26.10.2023	
3	Работа над курсовой работой	04.11.2023	04.11.2023	
4	Оформление отчета по курсовой работе	06.11.2023	06.11.2023	
5	Защиты курсовой работы	09.12.2023	25.12.2023	

Руководитель Попов Илья Юрьевич

(Подпись, дата)

Студент Николаев Глеб Витальевич

(Подпись, дата)

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

Студент	Николев Глеб Витальевич
	(Фамилия И.О.)
Факультет	Безопасности Информационных Технологий
Группа	N34501
Направление (специальность)	10.03.01. - Технологии защиты информации
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ Университета ИТМО
	(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 данной работы – разработать инженерно-техническую систему защиты информации на на предприятии, обеспечивающую надежную защиту информации от утечки повреждения или несанкционированного доступа

**2. Характер
работы**

- ☐ Расчет ☐ Конструирование
☒ Моделирование ☐ Другое

3. Содержание работы

В данной курсовой работе рассмотрена схема организации, проанализированы потенциальные каналы утечки информации, проанализирован рынок технических средств защиты информации, выбраны оптимальные и создана схема расположения выбранных средств защиты информации на схеме предприятия

4. Выводы

В результате работы был произведен комплексный анализ возможных технических каналов утечки информации в предложенных помещениях, предложены меры пассивной и активной защиты информации.

Руководитель	Попов Илья Юрьевич
	(Подпись, дата)
Студент	Николев Глеб Витальевич
	(Подпись, дата)

СОДЕРЖАНИЕ

Введение	2
2 Анализ защищаемой организации	3
2.1 Организационная структура предприятия	3
2.2 Информационные потоки	3
3 Обоснование защиты информации	6
4 Анализ защищаемых помещений	7
4.1 Схема помещения	7
4.2 Описание помещений	9
4.3 Анализ возможных каналов утечки информации	10
5 Анализ рынка технических средств	11
5.1 Выбор средств защиты	11
5.2 Защита от утечки информации по акустическим и виброакустическим каналам	12
5.3 Защита от утечек информации по электрическим акустоэлектрическим и электромагнитным каналам	13
5.4 Защита от утечек информации по оптическим каналам	13
6 Описание расстановки технических средств	14
Заключение	17
Список использованных источников	18

ВВЕДЕНИЕ

Защита информации в информационных системах играет ключевую роль в обеспечении безопасности предприятий. Эта защита охватывает не только хранимую в базах данных информацию, но и технологии, обеспечивающие ее обработку, а также различные технические средства. Основная цель заключается в предотвращении несанкционированного доступа к данным и ресурсам предприятия, с целью снизить риски утечки, утраты, искажения, уничтожения, копирования и блокирования информации. Это в свою очередь помогает предотвратить экономический, репутационный или другие виды ущерба. Разработка эффективных мер по обеспечению безопасности информации является важным вопросом, особенно при рассмотрении государственных объектов с уровнем конфиденциальности "совершенно секретно". Процесс создания комплекса инженерно-технической защиты этой информации на объекте информатизации требует системного подхода.

В данной работе рассмотрены различные аспекты этого процесса, начиная с анализа потенциальных технических каналов утечки информации и заканчивая разработкой схем расстановки выбранных технических средств в защищаемых помещениях.

Данная работа включает в себя анализ защищаемых помещений, перечень управляющих документов, а также обзор рынка технических средств защиты информации различных категорий. В результате проведенного исследования разрабатываются рекомендации по использованию технических средств для эффективной защиты информации на предприятии.

1 АНАЛИЗ ЗАЩИЩАЕМОЙ ОРГАНИЗАЦИИ

1.1 Организационная структура предприятия

Предприятие представляет собой объект, обрабатывающий как материальные, так и информационные потоки. Организационная архитектура предприятия представляет собой формальную систему, определяющую, как осуществляется управление и координация разнообразных функциональных направлений, подразделений и индивидуумов в рамках организации. Схема организационной структуры защищенной компании изображена на рисунке 1, демонстрируя ее внутренний механизм и взаимодействие составляющих частей.

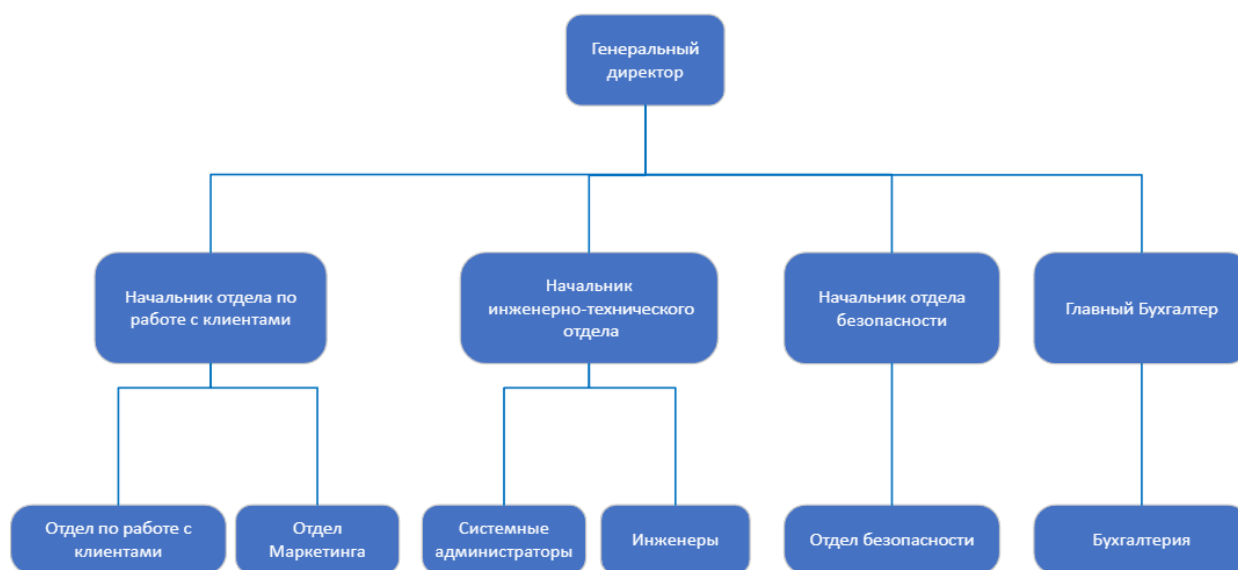


Рисунок 1 – Организационная структура предприятия

1.2 Информационные потоки

Информационные потоки представляют собой важный компонент системы передачи данных в организации или процессе. Графическое представление информационных потоков помогает визуализировать и описать обмен информацией между различными участниками системы, а также выявлять и анализировать все этапы передачи и обработки информации. Это позволяет идентифицировать узкие места и потенциальные проблемы в потоке данных, а также оптимизировать процессы коммуникации и обработки информации.

На рисунке 2 представлена схема информационных потоков предприятия. Значение обозначений схемы представлено в таблице 1.

К информации, передающейся по открытым потокам, относятся налоговые сведения и финансовая отчетность.

К защищаемой информации, передающейся по закрытым потокам, относятся персональные данные клиентов и сотрудников, служебная тайна, коммерческая тайна, сведения о разработках,

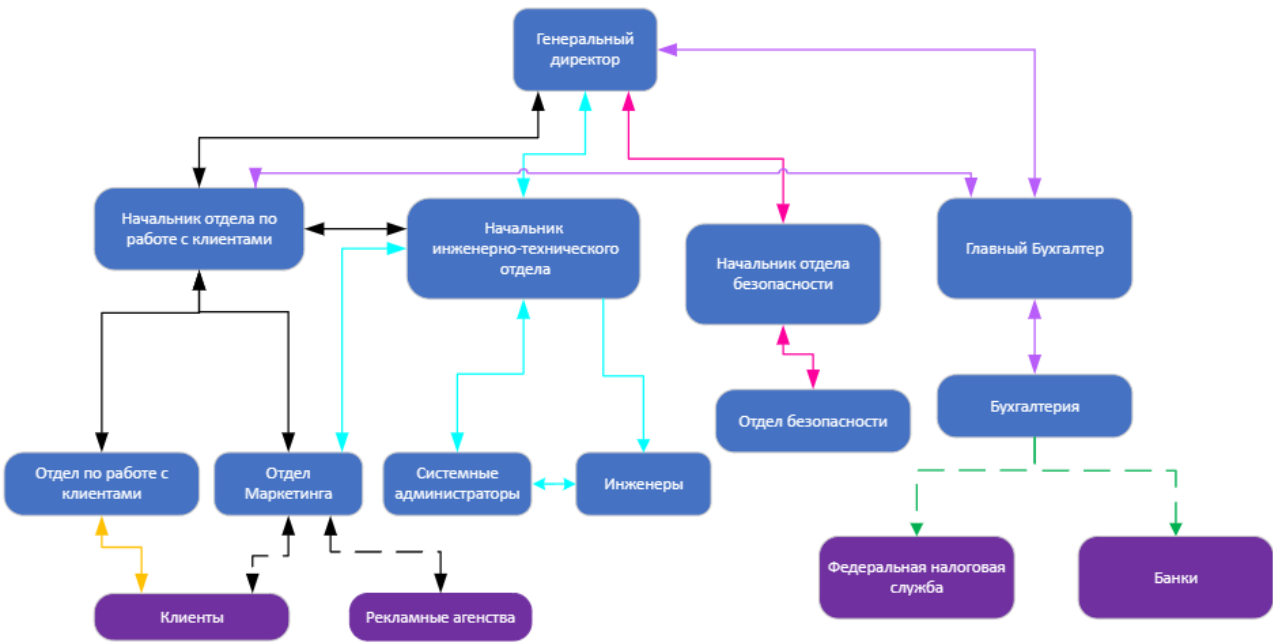


Рисунок 2 – Информационные потоки предприятия

Таблица 1 – Обозначения на рисунке 2

Обозначение	Значение
	Закрытая финансовая информация
	Информация об инцидентах безопасности
	Закрытая информация о разработках
	Закрытая информация
	Информация о клиентах
	Открытая информация
	Открытая финансовая информация

Обозначение	Значение
Клиенты	Внешний субъект информационного объекта
Генеральный директор	Внутренний субъект информационного объекта

2 ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Разрабатываемая система обеспечения безопасности информации предназначена для защиты информации, состоящей государственную тайну уровня "совершенно секретно". В соответствии с требованиями "Типовыми нормами и правилами проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними", утвержденными Межведомственной комиссией по защите государственной тайны (21.01.2011 № 199), обеспечение безопасности данных помещений должно соответствовать следующим критериям:

1. В помещениях для работы с государственной тайной и хранилищах секретных документов предусматривается использование усиленных дверей, обеспечивающих надежное закрытие. Двери обшиваются металлическим листом толщиной не менее 2 мм с обеих сторон, внутри применяется звукоизоляционный материал. Толщина двери должна составлять не менее 4 см. Дверь устанавливается на металлический каркас.
2. Обязательно предусмотрено противопожарное перекрытие между блоком режимных помещений и остальными зонами здания.
3. В соответствии с требованиями безопасности режимных помещений, если окна комнат и хранилищ находятся рядом с водостоками, эвакуационными лестницами, крышами соседних зданий, на первом или последнем этаже, каждое окно оборудуется выдвижными ставнями или створками с металлической решеткой, крепящейся к железным конструкциям оконного проема в стене.
4. Все режимные помещения оснащаются системой аварийного освещения.
5. Оборудование помещений для работы с государственной тайной соответствует требованиям технической безопасности. Все устройства, периферийные устройства и программное обеспечение проходят сертификацию и соответствуют стандартам ФСТЭК для оборудования в защищенных помещениях.
6. Перед вводом в эксплуатацию необходимо провести проверку выделенных и других режимных помещений на наличие "жучков" и других средств несанкционированного доступа к информации. Подобные проверки следует проводить периодически с целью исключения возможности утечки данных.

3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

3.1 Схема помещения

Перед началом проектирования инженерно-технической защиты важно подробно изучить план помещений и меблировку предприятия (рисунок 3). Анализ помещения офисного типа на рисунке 3 сопровождается описанием обозначений в таблице 2. Этот этап анализа позволяет эффективно разместить технические средства защиты, учитывая структуру объекта и особенности помещений.

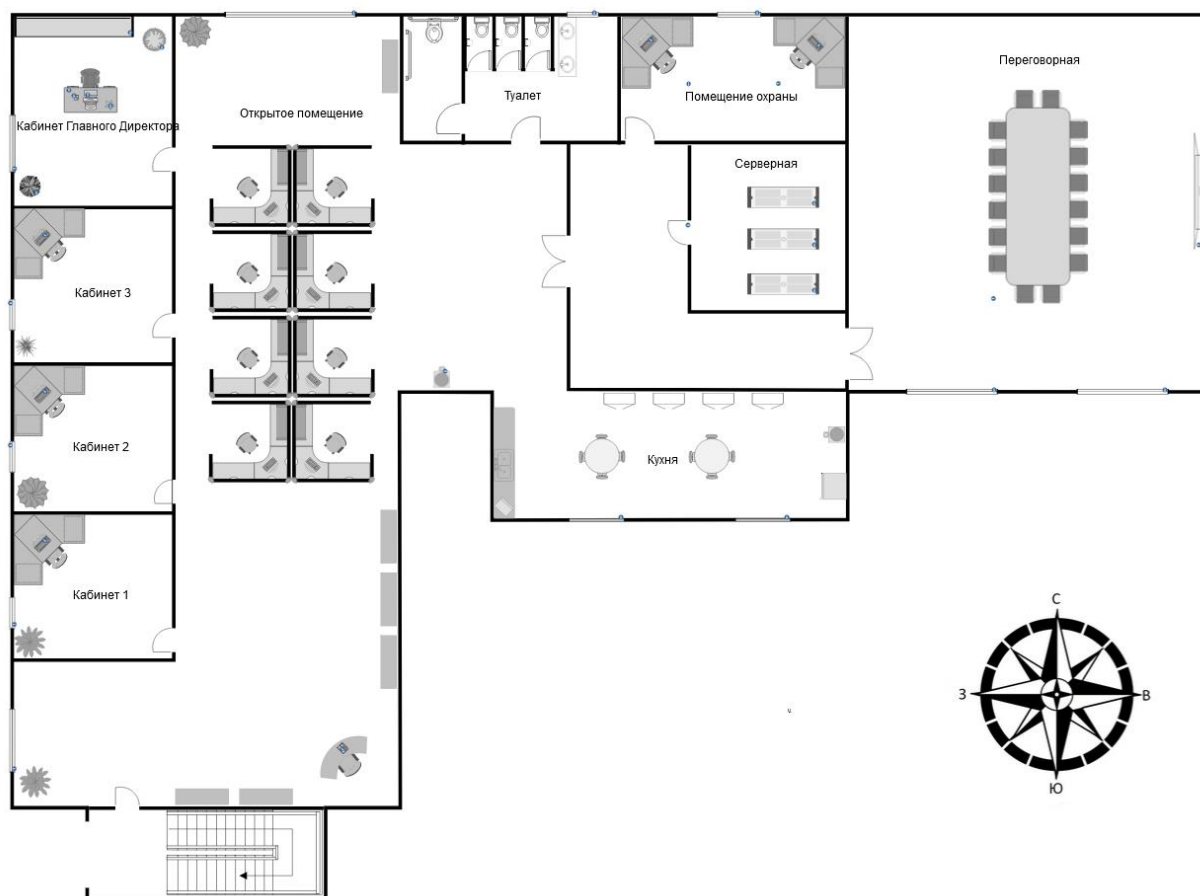
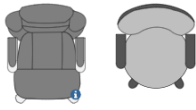







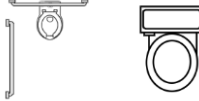

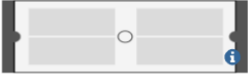
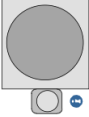
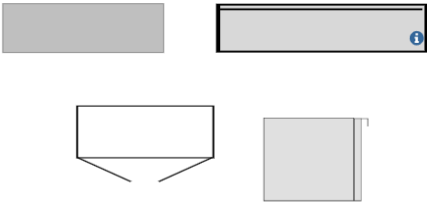
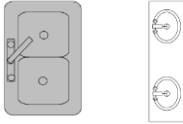



Рисунок 3 – План защищаемого помещения

Таблица 2 – Описание обозначений

Обозначение	Описание
	Офисные стулья
	Стол

Обозначение	Описание
	Кухонный стол со стульями
	Стол для переговоров со стульями
	Растения
	Персональные компьютеры
	Кабинка
	Телефон
	Туалеты
	СВЧ-печь
	Серверная стойка
	Куллер
	Шкафы
	Раковины
	Телевизор

3.2 Описание помещений

На плане обозначены 8 комнат, из них подлежат защите помещения под номерами 1,2,11:

1. Кабинет Главного Директора, 4,5м х 3,5м (15,75 м²)
2. Кабинет 1, 3,5м х 3,5м (12,25 м²)
3. Кабинет 2, 3,5м х 3,5м (12,25 м²)
4. Кабинет 3, 3,5м х 3,5м (12,25 м²)
5. Открытое помещение, 9,5м х 3,5м + 15м х 11,5м + 4м х 5м (225,75 м²)
6. Кухня, 3м х 8м (24 м²)
7. Туалет, 3м х 5м (15 м²)
8. Помещение охраны, 3м х 5м (15 м²)
9. Коридор, 5,5м х 2,5 м + 2м х 4м (21,75 м²)
10. Серверная, 3,5м х 4м (14 м²)
11. Переговорная, 8м х 9м (72 м²)

В кабинете главного директора расположены: стол, стул, три растения, шкаф, Персональный компьютер, телефон, три розетки и

В каждом из кабинетов 1-3 расположены по доному стулу, одному угловому столу, одному растеную, в каждом кабинете по три розетки и одно окно.

В открытом помещении расположены: 8 кабинок со стулом, угловым столом, стулом, персональный компьютер в каждой, 7 шкафов, один полукруглый стол, один стул, один телефон, один куллер и два окна. В открытом помещении 14 розеток.

В кухне расположены: 2 кухонных стола и 8 стульев, 5 шкафов, одна раковина, кухонный стол, одна СВЧ-печь, один куллер и два окна. Кухня оснащена четырьмя розетками.

В серверном помещении расположено 3 серверных стойки, в помещении 16 розеток.

В переговорной расположен переговорный стол с 16 стульями и телевизор, в помещении 6 розеток и два окна.

В помещении охраны расположено: два угловых стола, два персональных компьютера и два стула. Комната оснащена четырьмя розетками и одним окном.

Коридор соединяет переговорную, серверную, помещение охраны и открытое пространство.

Офис находится на втором этаже, вход в офис находится на южной стороне. Окна западной стороны выходят на улицу, окна северной стороны также выходят на улицу, окна южной стороны выходят во внутренний двор. Окна помещения не имеют смежности с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и другими элементами, которые могли бы использоваться посторонними лицами для доступа в помещение. Стены и внутренние перегородки здания выполнены из железобетона и имеют толщину не менее 16 см.

3.3 Анализ возможных каналов утечки информации

В каждом помещении имеются маршруты для нежелательного выхода информации. Утечка может происходить по электромагнитным и электрическим каналам, то есть с применением компьютеров или розеток. Также захват данных может производиться по визуальному каналу, с использованием незащищенных окон и дверей. Еще одним каналом, является виброакустический канал, снятие данных по такому каналу возможно при помощи твердых поверхностей, таких как стены или отопительные батареи. Декоративные элементы могут использоваться для скрытой установке закладных устройств, захватывающих информацию через оптический или акустические каналы.

4 АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ

4.1 Выбор средств защиты

Для обеспечения надежной защиты от несанкционированного доступа и предотвращения утечки конфиденциальной информации, соответствующей типа государственной тайны с уровнем “совершенно секретно”, необходимо оснащение защищаемых помещений специальными средствами и устройствами, перечисленными в таблице 3. Это обеспечит высокий уровень комплексной безопасности защищаемой информации.

Таблица 3 – Источники и средства защиты каналов утечки

Каналы	Источники	Пассивная защита	Активная защита
Виброционный, виброакустический	Батареи отопления, твердые поверхности в помещениях	Изоляция поверхностей при помощи дополнительной обшивки, наличие тамбура	Вибрационные извещатели
Визуально-оптический	Двери, окна	Средства для подавления отраженного света, доводчики на дверях	Маскирующие средства, преграждения от отраженного света.
Акустический, акустоэлектрический	Окна, двери, электрические сети, вводка, вентиляция	Фильтры для цепей электропитания, акустические экраны, звукоизоляция	Акустические извещатели
Электромагнитный, электрический	Розетки, проводка, любые электрические приборы	Фильтры для цепей электропитания, экранирование металлом для подавления шума	Системы защиты от электромагнитных помех, электромагнитные защитные экраны

4.2 Защита от утечки информации по акустическим и виброакустическим каналам

Для пассивной защиты от акустических и виброакустических утечек будут использоваться следующие средства:

- Усиленные двери со звукоизоляцией;
- Тамбурное помещения перед переговорной;
- Дополнительная отделка звукоизолирующими материалами.

Для активной защиты будет использоваться система виброакустического зашумления. 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. Список рассмотренных систем представлен в таблице 4.

Таблица 4 – Активная защита от утечек информации по акустическим и виброакустическим каналам

Модель	Характеристики	Цена, руб
Соната-АВ	Диапазон частот: 175 – 11200 Гц 6 независимых шумовых канала 8 часов непрерывной работы Максимальное количество излучателей – 239 Потребляемая мощность 40 Вт	44 200
Вуаль	Диапазон частот 90 – 11200 Гц 3 шумовых канала 24 часа непрерывной работы Максимальное количество излучателей – 60 Потребляемая мощность 20 Вт	44 730
ЛГШ-404	175 – 11200 Гц 2 шумовых канала Круглосуточная непрерывная работа Максимальное количество излучателей – 40 Потребляемая мощность 25 Вт	35 100

В результате сравнения была выбрана система Вуаль. Она имеет наиболее широкий диапазон частот, Достаточно долгий период непрерывной работы, достаточное количество излучателей и минимальную потребляемую мощность. Система имеет возможность дистанционной настройки.

4.3 Защита от утечек информации по электрическим акустоэлектрическим и электромагнитным каналам

Для пассивной защиты от электрических акустоэлектрических и электромагнитных утечек будут использоваться фильтры цепей электропитания и экранирование металлическим материалом

Для активной защиты будет использоваться система белого шума в сети, которая будет маскировать колебания, вызванные звуковыми волнами или работой электронных устройств (таблица 5)

Таблица 5 – Средства активной защиты от утечек по электрическим каналам

Модель	Характеристики	Цена, руб
ЛГШ-513	Диапазон частот 10 кГц – 1800 МГц Потребляемая мощность 60 Вт Уровень Шума от -18 дБ(мкА/м*√кГц) до 50 дБ(мкВ/м*√кГц) Круглосуточная непрерывная работа	39 000
ПОКРОВ	Диапазон частот 0,01 – 6000 МГц Потребляемая мощность 15 Вт	32 800
ГШ-111Б	10 кГц – 1800 МГц Уровень Шума от 0 до -30 дБ	33 000

В качестве средства защиты от ПЭМИН был выбран ПОКРОВ, поскольку он имеет широкий диапазон частот, низкую потребляемую мощность и самую низкую цену из рассмотренных.

4.4 Защита от утечек информации по оптическим каналам

Для предотвращения утечки информации через оптические каналы будут установлены жалюзи на окна и доводчики на двери

5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

На основе анализа рынка приведенного в главе 4, выбранные средства защиты информации включают в себя:

- Генератор акустических и виброакустических помех “ВУАЛЬ”, с которым будут использоваться: оконные вибропреобразователи ВПО-ВЛ-34х9, Вибропреобразователи для стен ВПС-ВЛ-39х32, вибропреобразователь для труб ВПТ-ВЛ-46х17 и акустические преобразователи ПА-ВЛ

- Устройство защиты объектов информатизации от утечки информации - ПЭМИН “ПОКРОВ”

- Жалюзи на 4 окна

- 3 звукоизолирующие двери

- размыкатели Ethernet “СОНАТА-ВК4.3” и размыкатель слаботочной линии “СОНАТА-ВК4.2”

Для оценки необходимого количества компонентов были учтены спецификации акустических и вибропреобразователей. Оценка стоимости выбранных средств представлена в таблице 6.

Таблица 6 – Оценка стоимости выбранных средств защиты

Наименование средства	Количество, у.е.	Цена за штуку, руб	Общая стоимость, руб
Генератор “ВУАЛЬ”	3	44 730	134 190
Оконный вибропреобразователь ВПО-ВЛ-34х9	7	2 243	15 701
Вибропреобразователь ВПС-ВЛ- 34х9	32	2 760	88 320
Вибропреобразователь ВПТ-ВЛ- 46х17	8	2 760	22 080
Акустический преобразователь ПА-ВЛ	4	3 000	12 000
ПОКРОВ	4	32 800	131 200
Звукоизолирующая усиленная дверь	3	60 000	180 000

Наименование средства	Количество, у.е.	Цена за штуку, руб	Общая стоимость, руб
Жалюзи blackout	4	3 000	12 000
СОНАТА-ВК4.3	3	6 000	18 000
СОНАТА-ВК4.2	3	6 000	18 000
Доводчик дверей	3	2 000	6 000

Общая стоимость затрат на ТСЗИ: 637 491 рублей

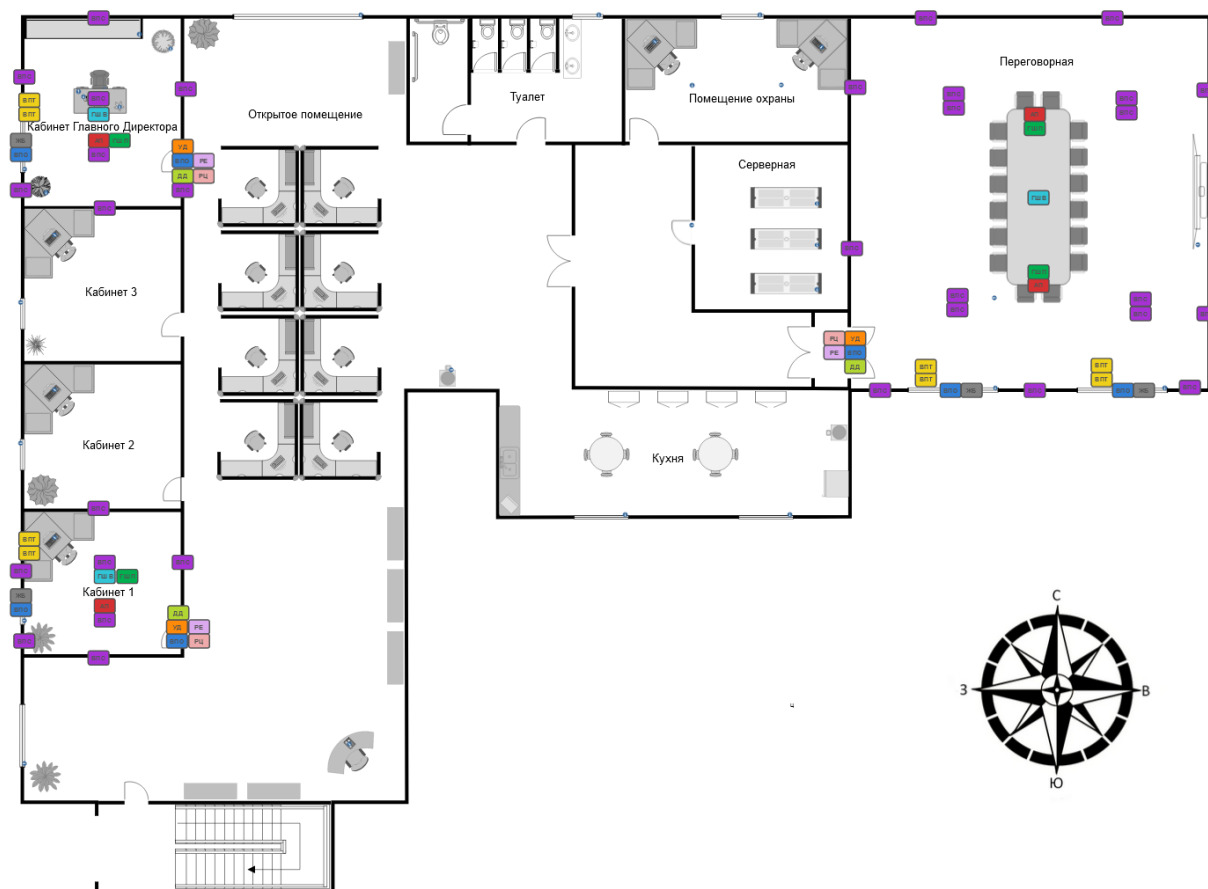









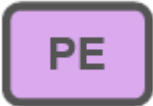



Рисунок 4 – План размещения технических средств защиты информации

Условные обозначения, используемые в рисунке 4, указаны в таблице 7.

Таблица 7 – Условные обозначения к рисунку 4

Обозначение	Средство
	Оконный вибропреобразователь ВПО-ВЛ-34х9

Обозначение	Средство
	Вибровреобразователь ВПС-ВЛ-34х9
	Вибропреобразователь ВПТ-ВЛ-46х17
	Акустический преобразователь ПА-ВЛ
	Генератор "ВУАЛЬ"
	"ПОКРОВ"
	Звукоизолирующая усиленная дверь
	Доводчик дверей
	Жалюзи blackout
	СОНАТА-БК4.3
	СОНАТА-БК4.2

ЗАКЛЮЧЕНИЕ

В ходе выполнения данной работы был проведен анализ потенциальных технических каналов утечки информации. Также была проведена детальная оценка структуры предприятия, включая подробное описание помещений и информационных каналов.

Для определения подходящих средств технической защиты информации был проведен анализ рынка существующих решений, направленных на противодействие выявленным каналам утечки. На основе этого анализа были выбраны оптимальные решения, наиболее подходящие для данного объекта.

С использованием выбранных средств был разработан план установки, а также проведен расчет финансовых затрат, которые подробно описаны в разделе 5 данной работы.

В результате проведенных мероприятий была предложена система защиты от утечек информации через различные каналы, включая акустический, виброакустический, оптический, акустоэлектрический, электрический, электромагнитный и оптико-электронный. Общие затраты на обеспечение этой защиты оцениваются в сумму 637 491 рублей, что считается обоснованным вложением для объекта, обрабатывающего и хранящего сведения, отнесенные к государственной тайне с грифом уровня «совершенно секретно».

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Рагозин, Ю. Н. Инженерно-техническая защита информации: учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург : Интермедия, 2018. — 168 с.— ISBN 978-5-4383-0161-5.
- Текст: электронный // Лань : электронно- библиотечная система. — URL: <https://e.lanbook.com/book/103203> (дата обращения: 01.12.2023). — Режим доступа: для авториз. пользователей
2. 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 // Лань : электронно- библиотечная система. — URL: <https://e.lanbook.com/book/43579> (дата обращения: 01.12.2023). — Режим доступа: для авториз. пользователей