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 системы защиты от утечки информации по различным каналам»

Выполнил:
студент группы N34532
Груздев Ярослав Вячеславович

_____

Проверил преподаватель:
к.т.н., доцент ФБИТ
Попов И.Ю.

_____

Отметка о выполнении:

_____

Санкт-Петербург
2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент Груздев Ярослав Вячеславович

(фамилия И.О.)

Факультет Безопасность Информационных Технологий

Группа N34532

Направление (специальность) 11.03.03 (Конструирование и технология электронных средств2020)

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

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

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Разработка комплекса инженерно-технической защиты информации в помещении

Задание Разработка комплекса инженерно-технической защиты информации в помещении

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

Содержание пояснительной записки
1. Введение.
2. Анализ технических каналов утечки информации.
3. Руководящие документы
4. Анализ защищаемых помещений
5. Анализ рынка технических средств
6. Описание расстановки технических средств
7. Заключение
8. Список литературы

Рекомендуемая литература
1. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010.- 436

Руководитель

(Подпись, дата)

Студент

(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Груздев Ярослав Вячеславович

(фамилия И.О.)

Факультет Безопасность Информационных Технологий

Группа N34532

Направление (специальность) 11.03.03 (Конструирование и технология электронных средств2020)

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

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

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Разработка комплекса инженерно-технической защиты информации в помещении

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Разработка и утверждение задания и календарного плана на курсовую работу	01.10.2023		
2	Анализ источников	01.11.2023		
3	Разработка комплекса инженерно-технической защиты информации в заданном помещении	15.11.2023		
4	Представление выполненной курсовой работы	19.12.2023		

Руководитель

(Подпись, дата)

Студент

(Подпись, дата)

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

АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ

Студент Груздев Ярослав Вячеславович

(фамилия И.О.)

Факультет Безопасность Информационных Технологий

Группа N34532

Направление (специальность) 11.03.03 (Конструирование и технология электронных средств2020)

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

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

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Разработка комплекса инженерно-технической защиты информации в помещении

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

Цель и задачи работы Целью работы является повышение защищенности рассматриваемого помещения. Задачами является анализ Защищаемого помещения, оценка каналов утечки информации и выбор мер пассивной и активной защиты информации.

Характер работы Конструирование

Содержание работы

1. Введение.
2. Анализ технических каналов утечки информации.
3. Руководящие документы
4. Анализ защищаемых помещений
5. Анализ рынка технических средств
6. Описание расстановки технических средств
7. Заключение
8. Список литературы

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

(Подпись, дата)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Цель работы

Разработка эффективного комплекса инженерно-технической защиты информации в помещении.

Задачи

- Анализ возможных каналов утечки информации и уровней риска
- Разработка стратегий для минимизации рисков утечки данных
- Оценка и выбор соответствующих технических средств защиты информации
- Подробное изучение защищаемых помещений и определение требований к их обеспечению безопасности

ОСНОВНАЯ ЧАСТЬ

1 Анализ защищаемой организации

1.1 Общее описание

Наименование организации: ООО “АрхФеникс”

Область деятельности: экспериментальные разработки в области ИТ.

Компания специализируется на B2B-сегменте, предоставляя услуги по разработке программного обеспечения для других организаций. За счет объединения людей с творческим подходом в одном рабочем пространстве организация получает преимущество в разработке новых решений.

Руководство компании приняло решение о расширении бизнеса за счет вовлечения в проекты B2G. В частности, связанных со сведениями, составляющими государственную тайну уровня “секретно”. В связи с этим возникла необходимость оснащения арендованного офисного пространства современными средствами технической защиты информации.

1.2 Информационные потоки

Разработка разбита на небольшие группы, каждая из которых работает над отдельным проектом. Заказчик и проектная группа общаются через посредников из отдела продаж - специалистов по связям. Таким образом уменьшается распространенность сведений конфиденциального характера и улучшается взаимопонимание.

Кроме непосредственно разработки имеются: отдел информационной безопасности, инфраструктурный отдел, отдел HR, финансовый отдел.

Большая часть отделов не имеет доступа к государственной тайне - с ней работают отдел продаж, группы разработки и отдел информационной безопасности.

Кроме заказчиков, организация взаимодействует с банком, налоговой, пенсионным фондом, военкоматом и прочими организациями.

Иерархическая структура представлена на рисунке 1. Схема информационных потоков представлена на рисунке 2.

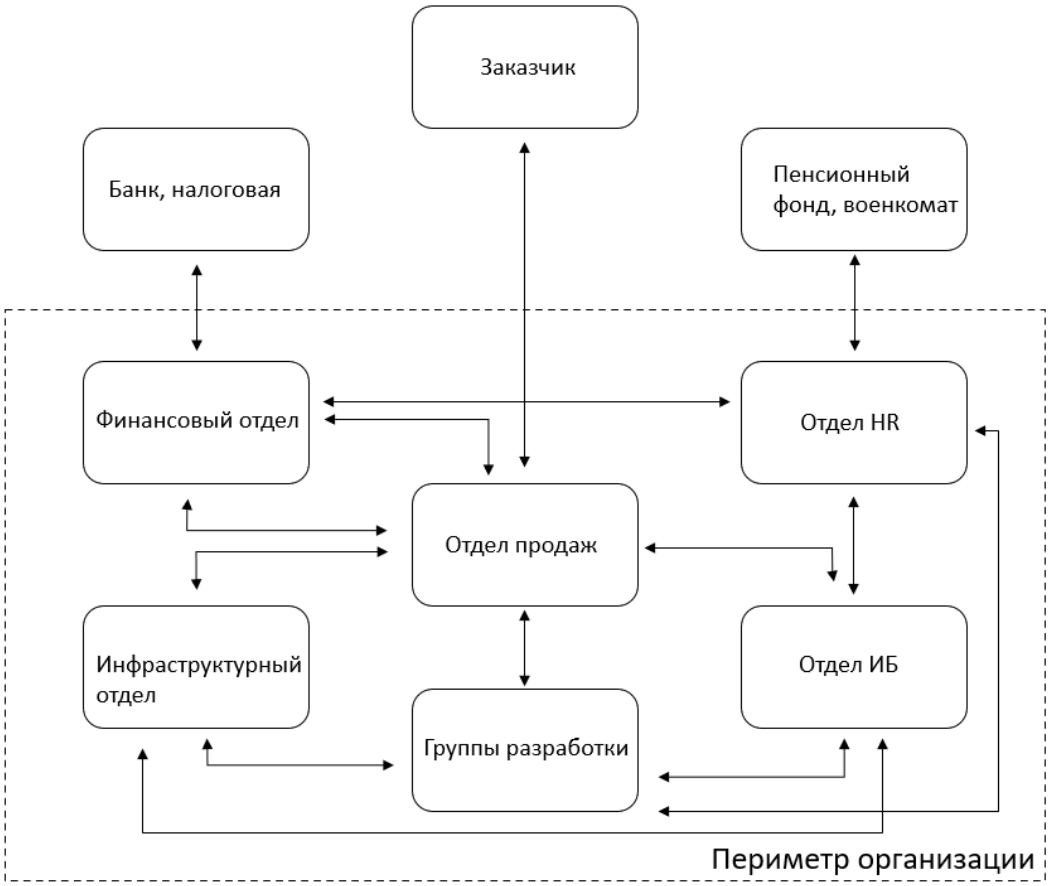

Рисунок 1 - Схема информационных потоков в организации

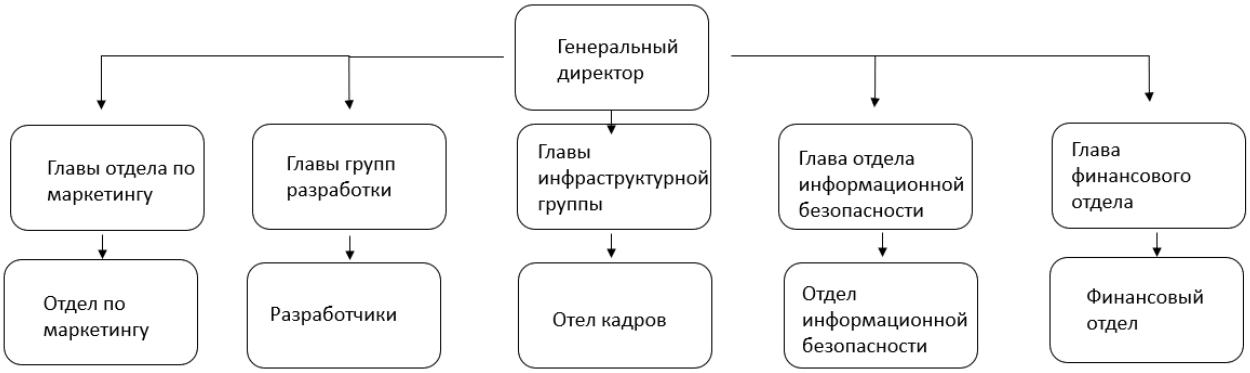

Рисунок 2 – Иерархическая структура

1.3 Защищаемое помещение

Помещение расположено на третьем этаже пятиэтажного здания. Здание располагается на охраняемой территории отдельно от остальных. Окна располагаются вдали от пожарных и эвакуационных лестниц на северной и восточной сторонах. Около окон нет пристроек, выступов, балконов и других элементов, при помощи которых посторонние лица могли бы проникнуть в помещение. Напротив расположены другие офисные здания. 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.

Арендуемое помещение состоит из:

— Внутреннего коридора,
— Туалетов,
— Складов,
— Серверной,
— Переговорной,
— Open-space зоны,
— Комнаты для ведения закрытых разработок.

Основная работа со сведениями, составляющими государственную тайну будет осуществляться в комнате для ведения закрытых разработок. Также время от времени в переговорной будут проводиться совещания, связанные с данными разработками.

На рисунке 3 представлен план защищаемого помещения и описание элементов, изображенных на плане. Список комнат приведены в таблице 1.

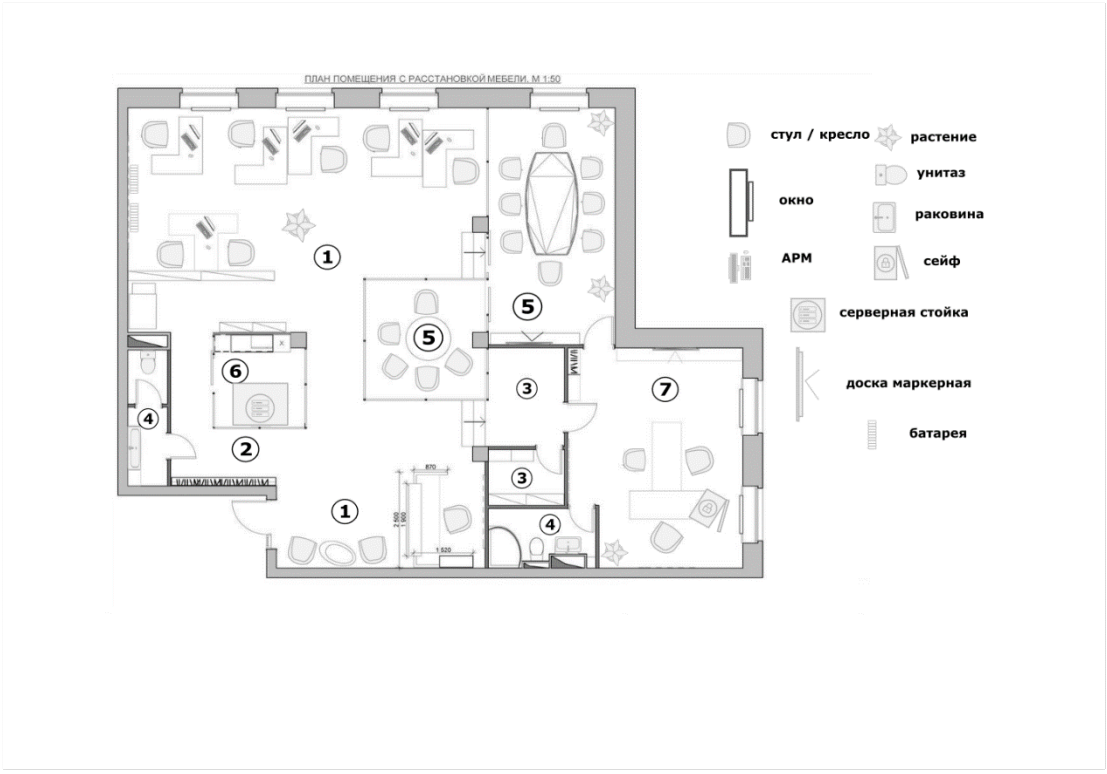

Рисунок 3 - План помещения

Таблица 1 - Комнаты на плане

Номер	**Название**	**Площадь, м^2**
1	Зона open-space	70
2	Внутренний коридор	12
3	Склад	9
4	Туалеты	8
5	Переговорная	31
6	Серверная	6
7	Комната для ведения закрытых разработок	24

Внутренний коридор содержит незначительное количество мебели.

На складе расположено несколько полок и коробки с различным оборудованием и материалами.

В каждом туалете имеется унитаз, раковина, мусорное ведро, шкаф и розетка.

В серверной находятся две серверных стойки, две розетки, выход вентиляции.

Серверная отделена от зоны open-space стеклянной стеной и дверью.

Переговорная содержит две розетки, маркерную доску, кресла, окно, два растения.

Зона open-space содержит четыре розетки, семь рабочих мест, сейф для документов, три шкафа для оборудования и документов, кулер, холодильник, диван, мусорное ведро, растение в горшке, три окна с батареями отопления и выход вентиляции.

В комнате для ведения закрытых разработок расположены четыре розетки, серверная стойка, маркерная доска, растение в горшке, сейф документов, кулер, три рабочих места, вентиляция и два окна.

1.4. Качественная оценка угроз

1.4.1. Оптический канал

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

1.4.2. 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.

1.4.3. 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.

1.4.4. Закладные устройства

В помещении располагаются декоративные элементы, в которые могут быть подложены закладные устройства. Возможно размещение закладных устройств в стенах, либо их маскировка под розетки, светильники, выключатели.

1.4.5. Материально-вещественный канал

Материально-вещественный канал утечки информации может присутствовать. В рамках курсовой работы данный канал не рассматривается.

2. Анализ руководящих документов

2.1. Перечень руководящих документов

При разработке комплекса защиты информации будем руководствоваться следующими документами:

- Закон “О государственной тайне”;
- Федеральный Закон №149 - “Об информации, информационных технологиях и защите информации”;
- Указ Президента РФ от 30.11.1995 №1203 "Об утверждении Перечня сведений, отнесенных к государственной тайне";
- Постановление Правительства РФ от 15 апреля 1995 г. №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 Правительства РФ от 06.02.2010 N 63 (ред. от 29.10.2022) "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне";
- Постановление Правительства РФ от 26 июня 1995 г, №608 “О сертификации средств защиты информации”;
- ГОСТ Р ИСО/МЭК 27001-2021 “Системы менеджмента информационной безопасности. Требования”;
- ГОСТ Р ИСО/МЭК 27002-2021 “Свод норм и правил менеджмента информационной безопасности”;
- ГОСТ Р ИСО/МЭК 27033-2011 “Безопасность сетей”.

2.2. Требования к составу мер защиты

Для получения лицензии на работу с государственной тайной степени “секретно” необходимо выполнить следующие требования:

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

кирпичными с толщиной стен от 12 см;

- Все режимные помещения оборудуются аварийным освещением;
- Вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемым к оснащению защищенных и выделенных помещений.

3. Выбор средств защиты информации

3.1. Оптический канал

3.1.1. Шторы

В качестве средства защиты информации от утечек по оптическому каналу через окна достаточно использовать любые плотные офисные шторы. В таблице 2 представлен расчет стоимости решения.

Таблица 2 - Расчет стоимости установки штор

Наименование товара / работы / услуги	Количество, шт.	Цена, руб.	Сумма, руб.
Рулонная штора “Blackout”	6	900	5 400
Установка	1	2 000	2 000
ИТОГО			7 400

3.1.2. Доводчики

Для защиты от утечек по оптическому каналу через двери используются доводчики. В таблице 3 представлен расчет стоимости.

Таблица 3 - Расчет стоимости установки доводчиков

Наименование товара / работы / услуги	Количество, шт.	Цена, руб.	Сумма, руб.
Доводчик дверной “БУЛАТ ULTIMATE”	10	1 300	13 000
Установка	1	3 000	3 000
ИТОГО			16 000

3.2. Акустический, виброакустический канал

3.2.1. Пассивная звукоизоляция

Многие компании предлагают услугу отделки помещения пассивной звукоизоляцией. Цена зависит от площади комнат и высоты потолков. Пассивная звукоизоляция необходима в двух помещениях - комнате для ведения закрытых разработок и переговорной. Расчет стоимости представлен в таблице 4.

Таблица 4 - Расчет стоимости пассивной звукоизоляции

Наименование	**Площадь, м^2**	**Цена, руб./м^2**	**Сумма, руб.**
Звукоизоляция пола с установкой	160	4 500	720 000
Звукоизоляция потолка с отделкой	160	3 700	592 000
Звукоизоляция стен с отделкой	116	4 100	475 600
Наименование	**Количество, шт.**	**Цена, руб.**	**Сумма, руб.**
Звукоизолирующие двери с установкой	4	60 000	240 000
ИТОГО			2 027 600

3.2.2. Излучатели виброакустических помех

В таблице 5 приведено сравнение вариантов излучателей виброакустических помех. Стоимость указана с учетом комплектации, необходимой для защиты трех помещений.

Таблица 5 - Сравнение излучателей виброакустических помех

Наименование	**Возможности**	**Стоимость, руб.**
ЛГШ-404	● Учет времени работы ● Контроль и защита органов регулировки уровня выходного шумового сигнала ● Проводное дистанционное управление и контроль ● Диапазон частот: 175 - 11 200 Гц ● Круглосуточная непрерывная работа ● Средний срок службы: 7 лет	136 000
КАМЕРТОН-5	● Диапазон частот: 90 - 11 200 Гц ● Круглосуточная непрерывная работа	92 000
Буран	● Частотная коррекция спектра помехового сигнала ● Мониторинг уровня нагрузки каналов ● Учет времени работы ● Защита от несанкционированного изменения настроек ● Диапазон частот: 100 - 11 200 Гц ● Непрерывная работа до 24 часов	89 800

В результате сравнения характеристик трех устройств, выбор был сделан в пользу ЛГШ-404. Решение обусловлено его способностью контролировать и регулировать уровень выходного шумового сигнала, что является важным фактором для использования устройства в местах, находящихся в непосредственной близости от помещений, эксплуатируемых другими организациями.

3.3. Электромагнитный канал

3.3.1. Активная защита от ПЭМИН

В таблице 6 приведено сравнение средств активной защиты от ПЭМИН. Стоимость указана с учетом комплектации, необходимой для защиты двух помещений.

Таблица 6 - Сравнение средств активной защиты от ПЭМИН

Наименование	**Возможности**	**Стоимость, руб.**
Соната-Р3.1	● Регулировка мощности ● Удаленное управление ● Время непрерывной работы: 8 часов ● Гарантия: 2 года	2 * 33 000
Пульсар	● Защита от несанкционированного изменения настроек ● Учет времени работы	2 * 19 000
Гамма-ГШ18	● Учет времени работы ● Защита от несанкционированного изменения настроек ● Время непрерывной работы: не ограничено ● Срок службы: от 10 лет ● Гарантия: 3 года	2 * 29 400

По результатам сравнения был выбран “Гамма-ГШ18” как наиболее надёжный.

3.3.2. ПЭВМ в защищенном исполнении

В таблице 7 приведено сравнение комплексов ПЭВМ. Стоимость указана с расчетом на 5 рабочих мест, которые необходимо обеспечить для ведения закрытых разработок.

Таблица 7 - Сравнение комплексов ПЭВМ

Наименование	Возможности	Стоимость, руб.
ЛИС-40НС	● Процессор: Intel Core i5 / i7 ● Оперативная память: DDR4 от 8 ГБ ● Постоянная память: SSD от 256 ГБ, HDD от 500 ГБ ● Операционная система: по выбору	5 * 188 500
ЛИС-40.1	● Процессор: Intel Core i3-10110U ● Оперативная память: DDR4 8 ГБ ● Постоянная память: HDD 1 ТБ	5 * 230 000
Гамма МБ-16-01	● Процессор: Intel Bay Trail J1900 ● Оперативная память: DDR3 4 ГБ ● Постоянная память: HDD 320 ГБ ● Операционная система: Free DOS	5 * 280 000

На данный момент единственным подходящим для ведения современной разработки ПЭВМ является “ЛИС-40НС”. Будем использовать его.

3.4. Защита от закладных устройств

3.4.1. Обнаружение закладных устройств

В таблице 8 приведено сравнение комплексов для обнаружения закладных устройств. Стоимость указана с учетом полной необходимой комплектации.

Таблица 8 - Сравнение комплексов для обнаружения закладных устройств

Наименование	Возможности	Стоимость, руб.
Крона-М6	● Сканирование радиоэфира, проводных коммуникаций и инфракрасного диапазона ● Обнаружение кратковременных сигналов, шумоподобных сигналов ● Контроль работы аппаратуры подавления ● Автономная работа: до 4 часов	1 360 000
ST131.S "ПИРАНЬЯ II"	● Сканирование радиоэфира, проводных коммуникаций и инфракрасного диапазона ● Контроль работы систем защиты виброакустического подавления	543 600
ST-167 "Бетта"	● Простейший поиск источников радиосигнала. Избирательный прием сигнала ● Постоянный мониторинг с созданием базы данных событий. Работа по расписанию	96 000

Был выбран комплекс ST131.S "ПИРАНЬЯ II" как наиболее многофункциональный.

3.4.2. Подавление сигнала закладных устройств

В таблице 9 представлено сравнение средств подавления сигналов закладных устройств.

Таблица 9 - Сравнение средств подавления сигналов закладных устройств

Наименование	**Возможности**	**Стоимость, руб.**
Блокиратор сотовой связи ЛГШ-716	● Блокировка сотовой связи, Bluetooth, WiFi 2.4 ГГц ● Время постоянной работы: не ограничено ● Срок службы: 10 лет	89 700
Блокиратор стандартов Wi-Fi, Bluetooth ЛГШ-702	● Блокировка Bluetooth, WiFi 2.4 ГГц ● Время постоянной работы: не ограничено ● Срок службы: 10 лет	61 100
ЛГШ-725	● Блокировка сотовой связи, Bluetooth, WiFi 2.4 и 5 ГГц ● Независимая регулировка мощности по каждому диапазону ● Дистанционное управление ● Время постоянной работы: не ограничено ● Срок службы: 10 лет	247 000

Было выбрано средство подавления сигналов “ЛГШ-725” - независимая настройка мощности по каждому диапазону важна при использовании системы вблизи помещений, контролируемых другими организациями.

3.4.2. Подавление микрофонов

В таблице 10 представлено сравнение средств подавления микрофонов.

Таблица 10 - Сравнение средств подавления микрофонов

Наименование	**Возможности**	**Стоимость, руб.**
Бубен-Ультра	● Три типа помех: ультразвуковой диапазон, сложная звуковая помеха, речеподобная помеха ● Возможность автономной работы: до 6 часов ● Радиус подавления: до 5 м ● Различные варианты маскировки	2*48 000
BugHunter DAudio bda-5	● Три типа помех: два вида ультразвука, акустическая помеха ● Радиус подавления: до 10 м ● Дистанционное управление	1*145 600
BugHunter DAudio bda-3 Voices	● Ультразвуковой диапазон ● Автономная работа ● Радиус подавления: до 3 м ● Дистанционное управление	2*68 900

Был сделан выбор в пользу средства “Бубен-Ультра” и его маскированного исполнения под систему оповещения.

4. Размещение средств защиты

На рисунке 4 изображены условные обозначения устанавливаемого оборудования и план размещения оборудования.

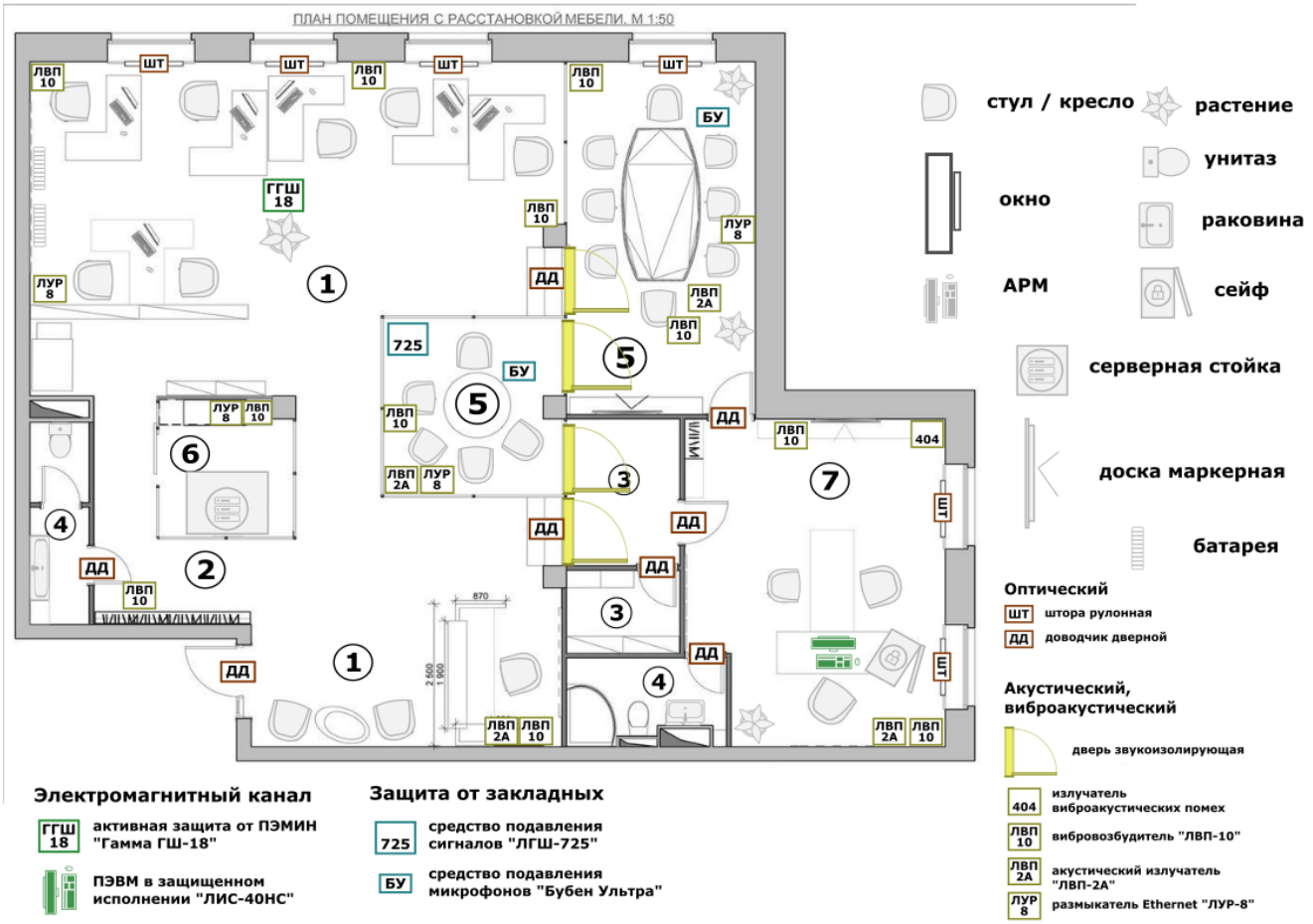

Рисунок 4 - план размещения технических средств защиты информации

ЗАКЛЮЧЕНИЕ

В рамках этой работы был проведен теоретический анализ имеющихся каналов утечки информации, исследованы потенциальные угрозы утечки информации в объекте защиты, а также разработаны рекомендации по их предотвращению. Проанализированы доступные на рынке технические средства, предназначенные для защиты от утечек информации, и подобраны подходящие варианты для рассматриваемого объекта. Был составлен план установки выбранных средств и рассчитана их общая стоимость.

В качестве итога предложена комплексная система защиты от утечек информации через оптические, акустические, виброакустические и электромагнитные каналы, включая защиту от ПЭМИН.

Итоговая цена системы защиты информации составляет 4060500 рублей.

СПИСОК ИСПОЛЬЗОВАННЫХ 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. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010.- 436

3. ArchLinux Wiki. URL: https://wiki.archlinux.org/ (дата обращения: 24.09.2023)