

**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

Выполнила:

студентка группы N34511

Голубева И. В.



Проверил:

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	Голубева Ирина Владимировна (фамилия И.О.)
Факультет	Безопасность Информационных Технологий
Группа	N34511
Направление (специальность)	10.03.01 (Технологии защиты информации 2020)
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 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. 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.: НИЦ «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	Голубева Ирина Владимировна
	(фамилия И.О.)
Факультет	Безопасность Информационных Технологий
Группа	N34511
Направление (специальность)	10.03.01 (Технологии защиты информации 2020)
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	01.12.2023		


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

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

Студент	Голубева Ирина Владимировна <hr/> (фамилия И.О.)
Факультет	Безопасность Информационных Технологий <hr/>
Группа	N34511 <hr/>
Направление (специальность)	10.03.01 (Технологии защиты информации 2020) <hr/>
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ <hr/> (Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации <hr/>
Наименование темы	Разработка комплекса инженерно-технической защиты информации в помещении <hr/>

**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	<ol style="list-style-type: none"> 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	<hr/> (Подпись, дата)
Студент	 <hr/> (Подпись, дата)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	5
1 АНАЛИЗ ЗАЩИЩАЕМОЙ ОРГАНИЗАЦИИ	6
1.1 Основная информация об организации	6
1.2 Информационные потоки.....	6
1.3 Защищаемое помещение	8
1.4. Качественная оценка угроз.....	16
1.4.1. Оптический канал	16
1.4.2. Акустический и виброакустический каналы	17
1.4.3. Электромагнитный и электрический канал.....	17
1.4.4. Материально-вещественный канал	18
1.4.5. Закладные устройства.....	18
2. АНАЛИЗ РУКОВОДЯЩИХ ДОКУМЕНТОВ	20
2.1. Перечень руководящих документов	20
3. ВЫБОР ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ	21
3.1. Оптический канал	21
3.1.1. Окна.....	21
3.1.2. Двери	21
3.2. Акустический и виброакустический канал	21
3.3. Электромагнитный канал.....	22
3.3.1. Активная защита от ПЭМИН	22
3.4. Защита от закладных устройств	23
3.4.1. Обнаружение закладных устройств.....	23
4. РАЗМЕЩЕНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ	24
ЗАКЛЮЧЕНИЕ	25
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	26

ВВЕДЕНИЕ

Цель работы: повышение защищенности рассматриваемого помещения.

Задачи:

1. Анализ Защищаемого помещения;
2. Оценка каналов утечки информации;
3. Выбор мер пассивной и активной защиты информации

1 АНАЛИЗ ЗАЩИЩАЕМОЙ ОРГАНИЗАЦИИ

1.1 Основная информация об организации

Защищаемое предприятие осуществляет свою деятельность в области права и фактически является частной юридической консультацией.

Клиентами организации являются как частные клиенты, так и крупные организации производства, финансов; научно-исследовательские кооперативы. Совокупность данных факторов подразумевает получение юридической консультацией доступа к необходимым для построения линии защиты данным таким, как:

1. Персональные данные клиентов
2. Аналитические данные представляемой организации
3. Коммерческая документация организации

Поскольку юридическая консультация является частным предприятием, существует также соответствующий список документации о самой защищаемой организации, включающий в себя персональные данные сотрудников, аналитические данные рынка и конкурентов, финансовые отчетные документы.

С подписанием нового контракта и во избежание нежелательных утечек информации по крупному судебному процессу, руководителем организации было принято решение о применении мер, направленных на укрепление существующей защиты предоставляемой информации.

1.2 Информационные потоки

Система взаимодействия и передачи информации осуществляется классическим для данной организации способом: первоначально руководитель организации (генеральный юрисконсульт) принимает потенциального клиента и в ходе беседы принимает решение о подписании или отказе от контракта на предоставление юридических услуг.

Также, работа над новым делом может быть предложена и реализована руководителем одного из отделов. Однако, в таком случае руководитель организации проводит первичную работу с клиентом и только впоследствии передает дело коллегам.

Проведение работы над каждым проектом может быть произведено как руководителем, так и рядовым сотрудником в зависимости от степени ценности клиента, сложности дела, а также уровня и спецификации профессиональных навыков сотрудника. Решение о назначении консультанта, оператора или правозащитника на каждое отдельное дело принимается лично генеральным юрисконсультом.

После заключения контракта между клиентом и организацией, работу по данному делу передают под руководство одного из сотрудников. При необходимости в дальнейшем к участию в проекте могут привлечены другие сотрудники организации, в качестве консультантов или помощников юриста.

При рассмотрении дела в суде юрист также взаимодействует с сотрудниками правоохранительных и судебных органов. В случае возникновения конфликта сторон и благоприятном стечении обстоятельств, возможно взаимодействие юриста организации с оппонентом клиента и/или его правозащитником.

Внутренние конфиденциальные данные организации циркулируют между отделами секретариата, финансов, информационной безопасности и архива. Руководитель организации осуществляет контроль и регуляцию работы отделов посредством передачи указаний в отдел секретариата, изучения отчетности, а также, в исключительных случаях, путем личной проверки и организации совещания в рассматриваемом отделе.

Таким образом, первично информация о клиенте поступает в организацию путем личной беседы клиента и руководителя организации. После заключения контракта клиент перенаправляется к юристу, назначенному на это дело, и продолжает работу с ним, предоставляя любую необходимую информацию в устном или письменном виде по запросу правозащитника. Предоставляемая информация защищена адвокатской тайной и относится к категории конфиденциальной информации согласно Указу Президента РФ от 06.03.1997 №188 (3) и Федеральному Закону от 31.05.2002 №63-ФЗ (4).



Рисунок 1 - Схема информационных потоков в организации

1.3 Защищаемое помещение

Защищаемое помещение находится на четвертом этаже десятиэтажного офисного комплекса и занимает половину этажа. Офисы 3, 4 и 11, а также кухня оборудованы высокими оконными проемами и выходят на северо-запад. Напротив здания находится небольшой офисный центр в пять этажей. Помещения 1, 2, 7 и уборные граничат с широким холлом, объединяющим защищаемую организацию с соседними офисами.

На первом этаже здания располагается пропускной пункт, осуществляющий процесс допуска/недопуска посетителей. Пункт оборудован стандартной системой СКУД и видеонаблюдения.

Основная работа с конфиденциальными данными осуществляется в помещениях 1, 2, 3, 7 и 11 (офис руководителя, архив, финансовый отдел, переговорная, общий офис).

На рисунках 2-7 представлен подробный план помещений организации.

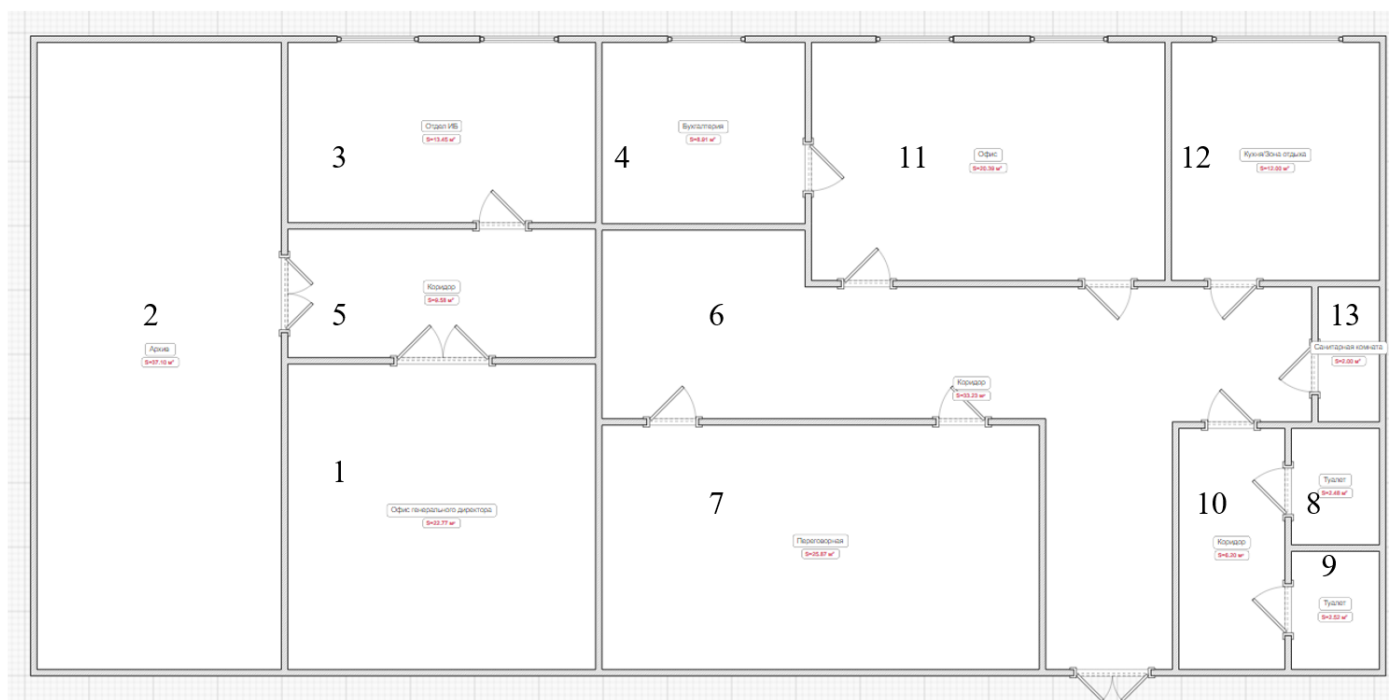


Рисунок 2 – Общий план помещений

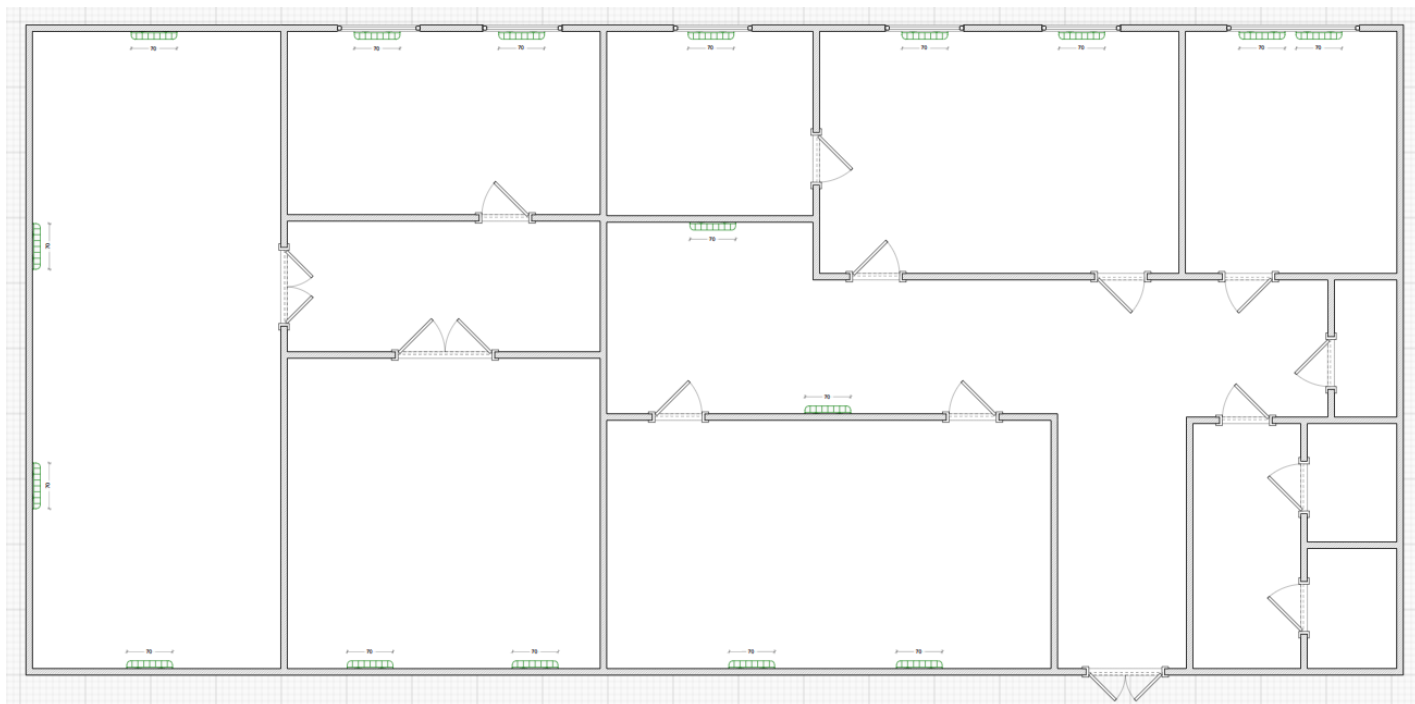


Рисунок 3 – Схема расположения радиаторов

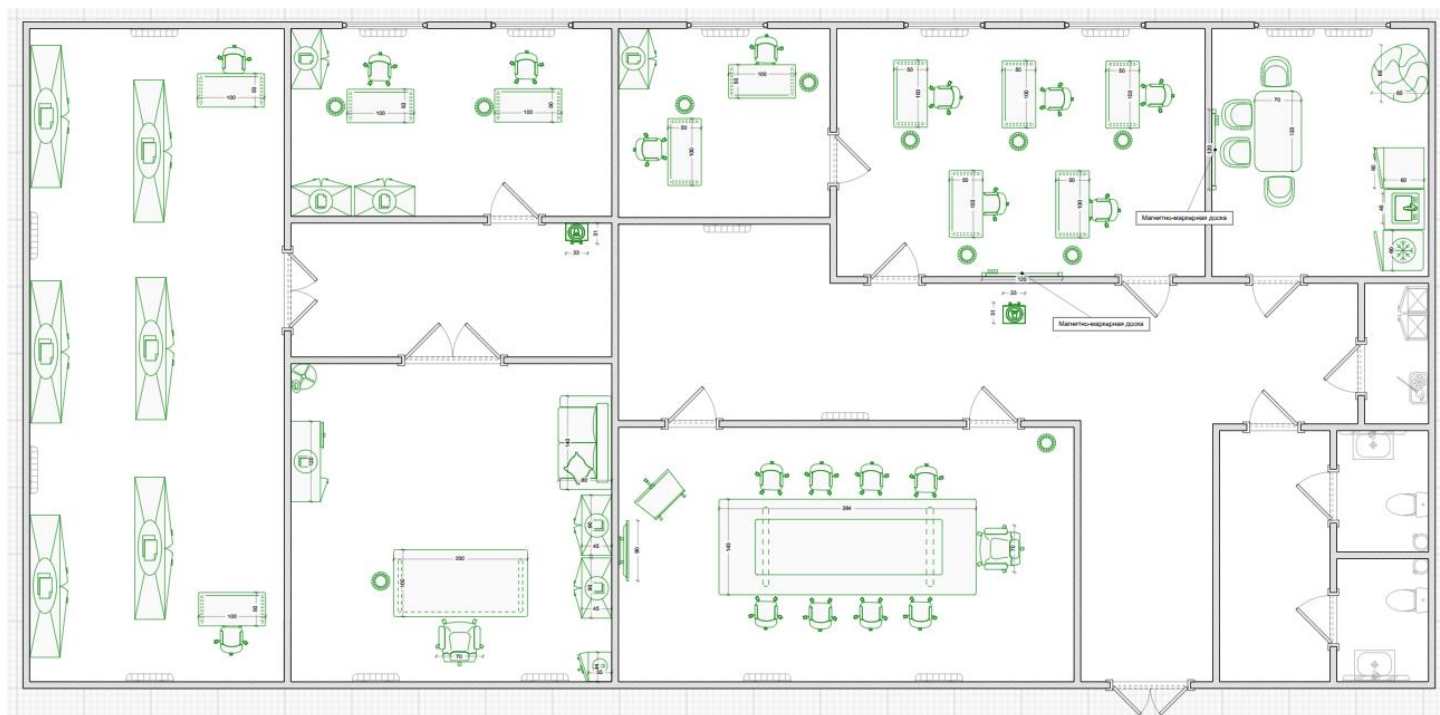


Рисунок 4 – План помещения с мебелью

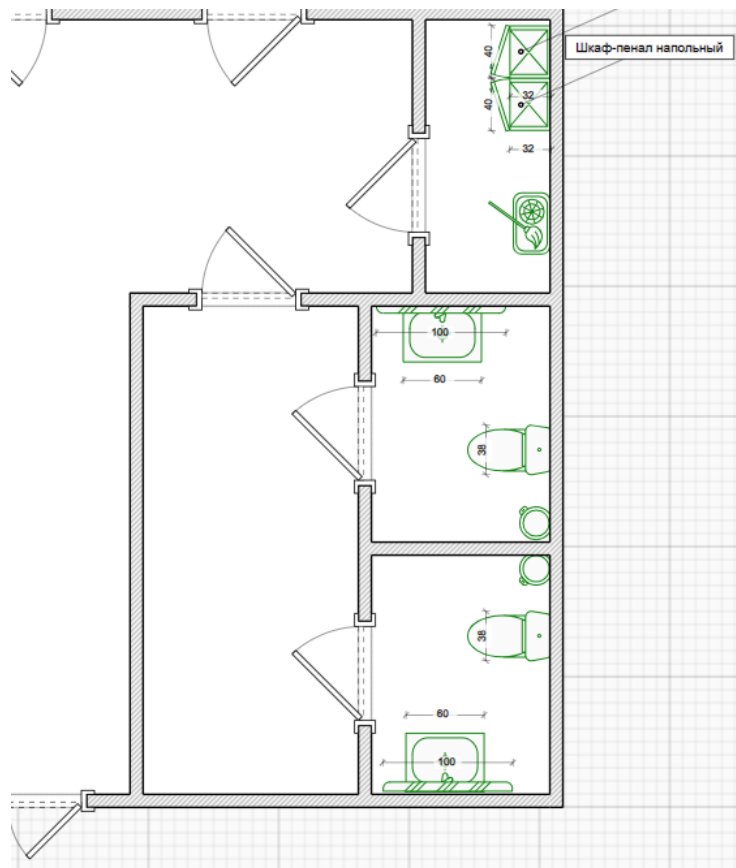


Рисунок 5 – Схема расположения сантехники

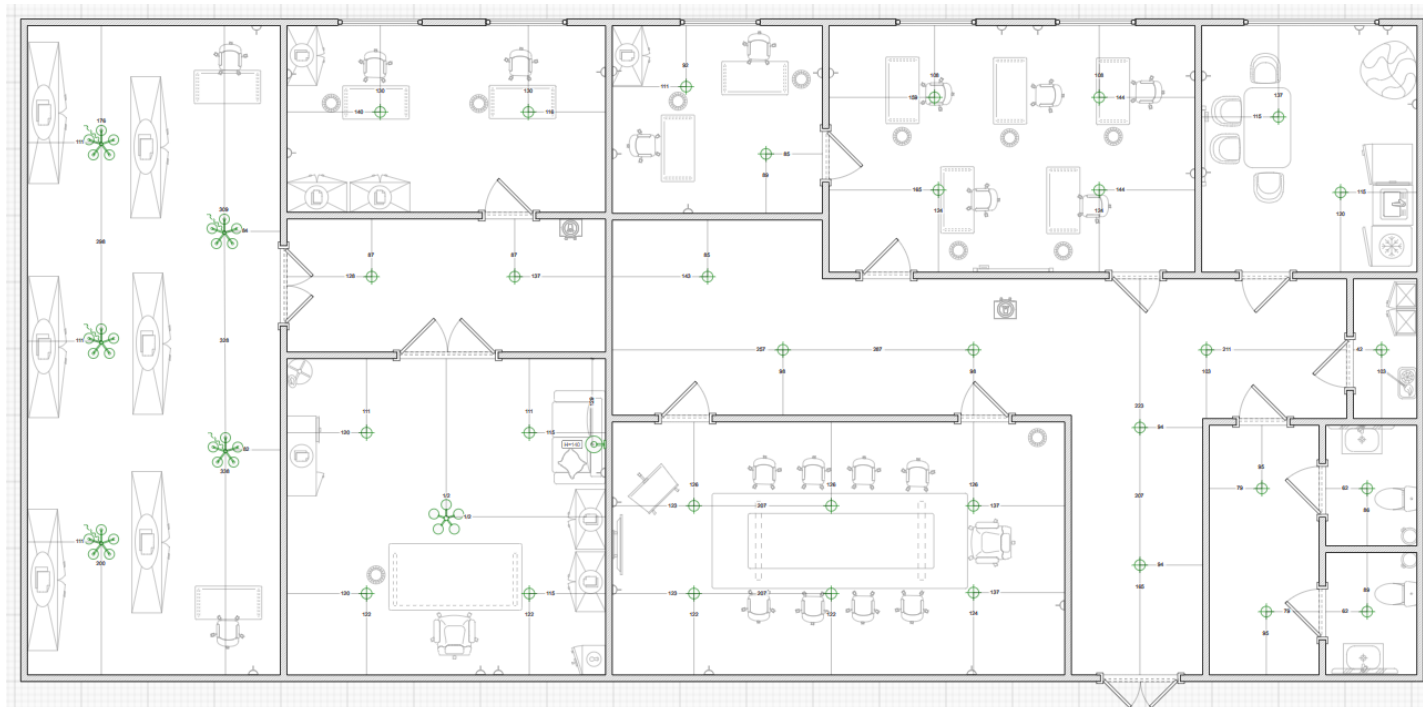


Рисунок 6 – Схема расположения светильников и розеток

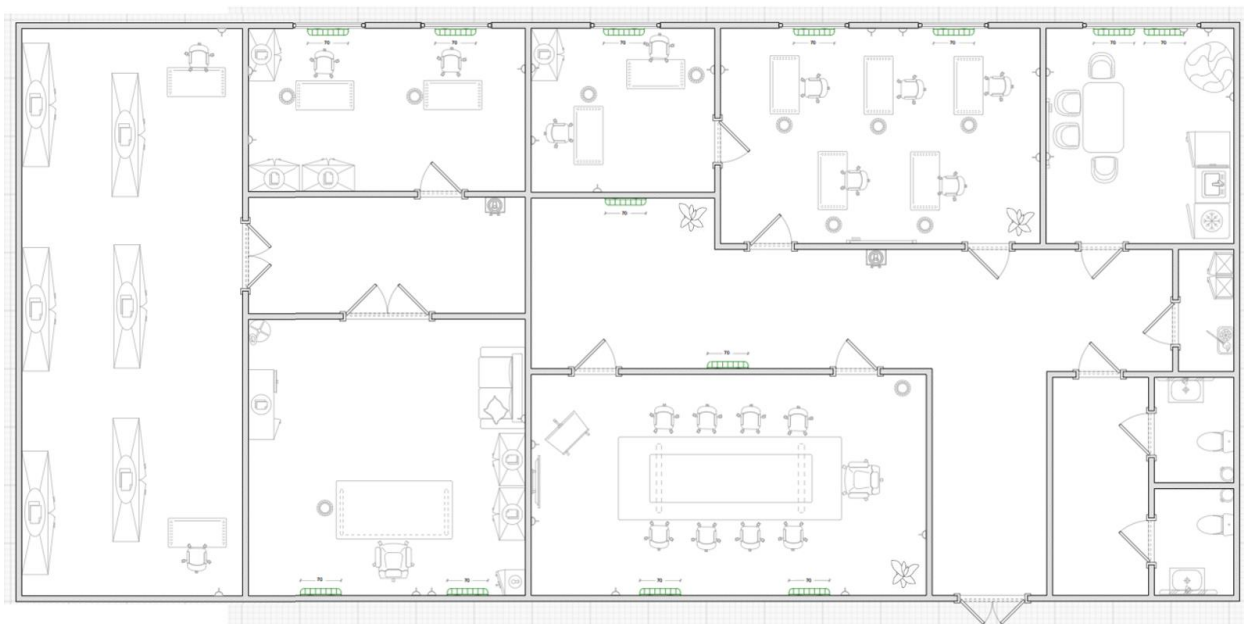



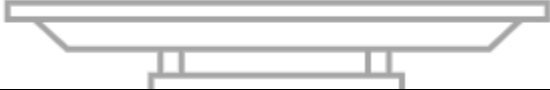
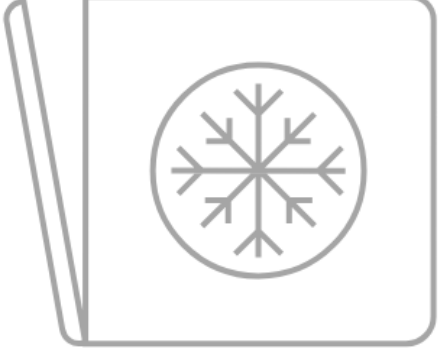


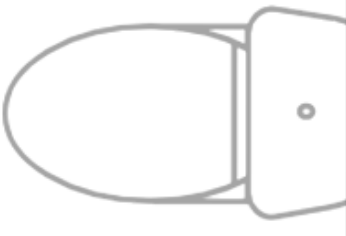


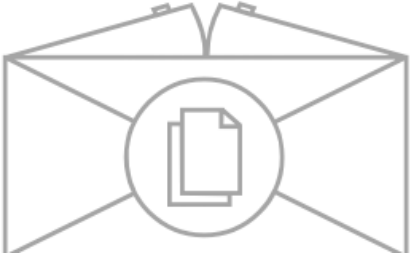
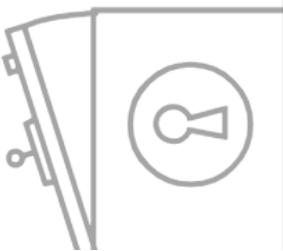

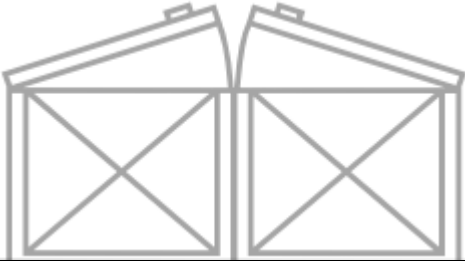
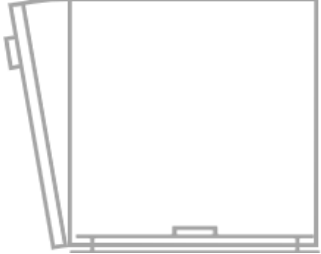
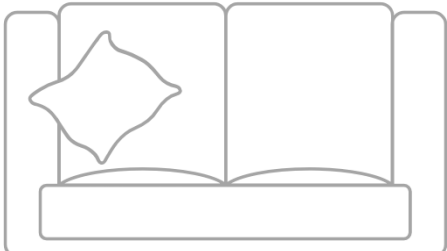


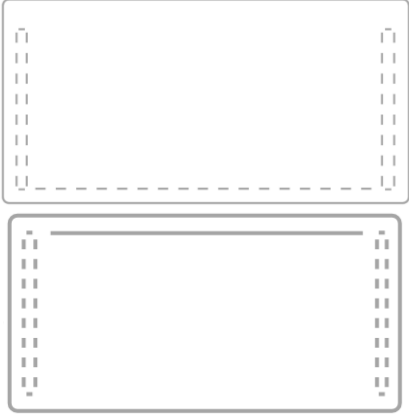


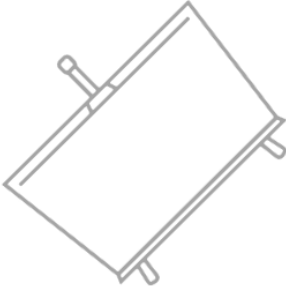



Рисунок 7 - План помещения






Таблица 1 – Условные обозначения

Символ	Описание
	Обычная межкомнатная дверь
	Окно
	Двустворчатые входные двери
	Радиатор
	Розетка стандартная, 220В

	Светильник точечный, встраиваемый
	Люстра подвесная потолочная
	Светильник настенный
	Телевизор на кронштейне
	Холодильник
	Раковина кухонная
	Раковина бытовая
	Унитаз
	Офисное кресло

	Стул обеденный
	Шкаф для документов
	Сейф
	Офисная тумба
	Шкаф напольный
	Тумба кухонная напольная
	Диван

	<p>Рабочий стол</p>
	<p>Стол для переговоров</p>
	<p>Стол обеденный</p>
	<p>Флипчарт</p>
	<p>Маркерная доска</p>
	<p>Зеркало настенное</p>
	<p>Кресло-мешок</p>

	Кулер
	Растение живое в горшке
	Вешалка для одежды напольная
	Санитарные принадлежности
	Урна

Основной коридор содержит кулер, два радиатора и живое комнатное растение. В кабинете руководителя располагаются офисные стол и стул, два шкафа для документов, сейф, диван, урна, два радиатора, комод, вешалка для верхней одежды и секретер.

В архиве расположено пять шкафов с документацией и два рабочих места с доступом к электронному хранилищу.

В каждом туалете имеется унитаз, раковина, мусорное ведро и зеркало. Уборные соединены с основным коридором посредством другого коридора.

В финансовом отделе находятся два рабочих места, столы и шкафы для хранения документации, два мусорных ведра и две розетки, два окна, два радиатора.

В коридоре, объединяющем кабинет руководителя, архив и финансовый отдел стоит кулер и комнатное растение.

В отделе ИБ расположены два рабочих места, розетки под них, две урны, шкаф для документации и розетка. Вход и выход в кабинет осуществляется только через общий офис.

Переговорная содержит пять розеток, флипчарт, телевизор, кресла, стол и выход вентиляции.

Общий офис содержит пять полноценных рабочих мест, пять розеток, два окна и маркерную доску.

На кухне стол на 4 персоны, варочная панель, микроволновка, раковина и холодильник. Также, кресло-мешок, два радиатора под окнами и четыре розетки.

Также, в офисе имеется санитарная комната, используемая для хранения бытовых инструментов, моющих средств и других приспособлений для уборки.

1.4. Качественная оценка угроз

В контексте защиты с использованием технических средств защиты информации следует рассмотреть потенциальные каналы утечки информации.

Согласно физическим свойствам носителя и характеру канала связи технические средства коммуникации и информации делятся на следующие категории:

1. Оптические
2. Акустические и виброакустические
3. Электрические
4. Электромагнитные
5. Радиоэлектронные
6. Индукционные
7. Материально-вещественные

Рассмотрим возможные каналы утечки информации в соответствии с каждым из перечисленных каналов связи.

1.4.1. Оптический канал

В данном случае утечка данных осуществима при помощи оптических датчиков, улавливающих световые излучения в различном диапазоне. Чаще используются датчики видимого диапазона, однако, не исключено использование и инфракрасных датчиков.

Злоумышленники нередко прибегают к использованию высокоточной аппаратуры, позволяющей масштабировать изображение и менять угол обзора, улавливая даже наименее доступный оптический сигнал, тем самым используя уязвимость максимально эффективно.

Для ведения фотосъемки используются портативные устройства повышенного уровня точности, что позволяет оперативно и эффективно произвести перехват

внушительного объема данных с использованием оптического канала.

Для получения видеозаписи доступного визуально помещения организации достаточно использовать те же портативные камеры, оборудованные высокоточными телеобъективами.

Также, использование оптического канала утечки информации может быть осуществлено при помощи инфракрасного излучения, улавливаемого специализированным оборудованием.

Утечки через оптический канал возможны, так как офисы находятся на внешней стороне здания и оборудованы окнами, следовательно, вероятен просмотр помещения из окон соседних зданий или с улицы.

1.4.2. Акустический и виброакустический каналы

Акустические и виброакустические колебания обладают свойством распространяться в окружающей источник среде. Тогда, при возникновении сигнала такого рода, окружающие его препятствия в зависимости от их наличия и материала, из которого они изготовлены, способны пропускать или задерживать излучаемый источником сигнал.

Отличие виброакустических колебаний от акустических заключается в свойстве распространения сигнала в окружающей среде. Акустические колебания, как правило, отражаются и перенаправляются при столкновении с препятствием. Однако, некоторые материалы способны «поглощать акустический сигнал», преобразовывая его в виброакустический и передавая звуковую волну посредством колебания частиц с различной частотой.

Поскольку офис не оснащен дополнительной звукоизоляцией, а толщина стен средняя (порядка 7-ми сантиметров), существует вероятность утечки информации из соседнего здания путем считывания колебаний при помощи микрофонов или лазера.

В переговорной комнате и офисах имеется вентиляция и радиаторы, следовательно, возможно прослушивание через общую систему отопления или вентиляции.

1.4.3. Электромагнитный и электрический канал

Использование электромагнитного канала связи подразумевает перехват информации, передаваемой посредством радиосвязи, спутниковой связи, а также проводной аппаратуры, подключённой к сети.

Особенно вероятна уязвимость данного канала связи в случае наличия на

предприятию электронно-вычислительных машин (персональных и/или корпоративных устройств).

В процессе работы и при нормальном функционировании персональные компьютеры сотрудников излучают побочное электромагнитное излучение, которое может быть использовано злоумышленниками в целях нарушения информационной безопасности организации.

Проводной канал связи также можно считать уязвимостью системы. Кража конфиденциальных данных осуществляется посредством подключения специализированной аппаратуры к проводным линиям связи с целью получения информации о системе и подключенных в ней устройствах.

Таким образом, следует считать возможным съём информации через систему электропитания, так как каждое помещение оборудовано элементами электропитания и подключено к сети.

Из проводных каналов связи за пределы помещения выходит только Ethernet-кабель общего шлюза, что также может быть использовано злоумышленниками для съёма информации при помощи электромагнитного канала связи.

1.4.4. Материально-вещественный канал

Материально-вещественный канал утечки информации реализуется при обнаружении злоумышленниками объектов, относящихся к категории конфиденциальных данных, за пределами предприятия.

К таким объектам могут относиться черновые записи сотрудников, заметки, записные книжки, образцы-прототипы разрабатываемых устройств или программного обеспечения, хранящегося на съёмных носителях.

1.4.5. Закладные устройства

Также, следует учитывать вероятность проникновения нарушителей информационной безопасности непосредственно на территорию организации с целью хищения засекреченных данных.

В таком случае злоумышленник может использовать уязвимости как в техническом, так и в программном комплексах защиты. Для получения несанкционированного доступа к конфиденциальным данным путем установления закладного устройства нарушитель будет заинтересован в поиске подходящего для инсталляции места, находящегося вблизи от источника необходимой ему информации.

К подходящим точкам для установки закладного устройства относятся:

1. Элементы декора (картины, статуэтки, журнальные столики и т.д.)
2. Довольно часто используются полки шкафа, искусственные или даже живые комнатные растения.
3. Труднодоступные места (внутренняя поверхность рабочего стола,)
4. Открытые линии электропередач, либо зашитые кабель-каналом
5. Розетки, светильники, факсы и проводные телефоны.

2. АНАЛИЗ РУКОВОДЯЩИХ ДОКУМЕНТОВ

2.1. Перечень руководящих документов

При разработке комплекса защиты информации будем руководствоваться следующими документами:

1. закон “О государственной тайне”;
2. ФЗ №149 - “Об информации, информационных технологиях и защите информации”;
3. Постановление Правительства РФ от 26 июня 1995 г, №608 “О сертификации средств защиты информации”;
4. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ
5. Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) "Об утверждении Перечня сведений конфиденциального характера"
6. Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 14.05.2020) "Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"
7. ГОСТ Р ИСО/МЭК 27001-2021 “Системы менеджмента информационной безопасности. Требования”;
8. ГОСТ Р ИСО/МЭК 27002-2021 “Свод норм и правил менеджмента информационной безопасности”;

Согласно Закону РФ от 21.07.1993 N 5485-1 (ред. от 04.08.2023) "О государственной тайне", учреждение, имеющее допуск к конфиденциальным персональным данным, обязательно соответствует ряду требований:

1. Выполнение требований нормативных документов, утверждаемых Правительством Российской Федерации, по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;
2. Наличие в их структуре подразделений по защите персональных данных и специально подготовленных сотрудников для работы по защите информации;
3. Наличие сертифицированных средств защиты информации.

3. ВЫБОР ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

3.1. Оптический канал

3.1.1. Окна

Для предотвращения утечки информации при помощи использования внешнего наблюдения за помещением через оконные проёмы следует установить жалюзи или шторы, изготовленные из любого плотного материала.

Поскольку, конструктивной разницы между предложенными вариантами нет, оптимальным выбором будет более бюджетное решение.

3.1.2. Двери

В качестве защиты от использования оптического канала для нарушения информационной безопасности организации при помощи дверей следует воспользоваться доводчиками.

3.2. Акустический и виброакустический канал

При обеспечении защиты акустического и виброакустического каналов утечки информации следует воспользоваться мерами как пассивной, так и активной защиты.

Для обеспечения пассивной шумоизоляции следует заменить установленный в переговорной телевизор на информационную доску, а также использовать дополнительные звукопоглощающие материалы в отделке стен, пола и потолка.

Поскольку в переговорной комнате нет окон, они не нуждаются в звукоизоляции, однако, входную дверь стоит заменить на звуконепроницаемую.

В качестве средств обеспечения активной звукоизоляции помещения рассмотрим несколько доступных вариантов, представленных в Таблице 2.

Таблица 2 – Генераторы шума

Характеристика	Устройство	ЛГШ-404	Соната АВ-4Б
Диапазон воспроизводимого шумового сигнала		175–11200 Гц	175–11200 Гц
Максимальное количество излучателей		40 шт	239 шт
Электропитание		220 В, 50 Гц	сеть 220В/50Гц
Удаленный мониторинг		проводной пульт ДУ или ПАК «Паутина»	Ethernet + СПО "Инспектор" для блока управления версии "Соната-ИП4.2"
Индикация		диодная + звуковая + ЖК	световая, звуковая
Наличие сертификата ФСТЭК		да	да
Время непрерывной работы		круглосуточно	8 ч

Условия эксплуатации	от 1 до 40 °С, относительная влажность воздуха не более 80 % при 25 °С	от +5 до +40 °С, влажность до 80 % при температуре +25 °С
Стоимость	35 100 РУБ	44 200 РУБ

Был сделан выбор в пользу ЛГШ-404, так как функционал системы оптимален в рамках защиты данного объекта, а использование системы СонатаАВ-4Б является избыточным. Также, можно воспользоваться виброизлучателем ВД-120 для обеспечения защиты системы отопления.

3.3. Электромагнитный канал

3.3.1. Активная защита от ПЭМИН

Таблица 3 – Генераторы шума

Характеристика	Устройство	ГАММА ГШ-18	Покров
Диапазон частот		от 0,009 до 6000 МГц	0,01–6000 МГц
Электропитание		однофазная сеть переменного тока с напряжением от 187 до 242 В и частотой (50 ± 0,5) Гц	выполнен в виде сетевого удлинителя с 5 розетками типа F
Мощность		максимальная – не более 50 Вт	15 Вт
Время непрерывной работы		с перерывом 10 мин после каждых 8 ч непрерывной работы	круглосуточно
Условия эксплуатации		от 5 до 45 °С; относительная влажность воздуха – не более 90 % при 30 °С	от + 5°С ... + 40°С
Индикация		светодиодная + звуковая	светодиоды
Управление		аттенюатор ОПЦИЯ - пульт ДУ	Ethernet
Наличие сертификата ФСТЭК		да	да
Стоимость		29 400 РУБ	32 800 РУБ

По результатам сравнения был выбран “Гамма-ГШ18” как оптимальный с учетом надёжности и доступности устройства.

3.4. Защита от закладных устройств

3.4.1. Обнаружение закладных устройств

Таблица 4 - Устройства для обнаружения закладных устройств

Функционал	Устройство	ST 600 ПИРАНЬЯ	ST131.S ПИРАНЬЯ П
Детектор магнитного поля		да	да
Диапазон частот		0,04–30 кГц	0,01–125 кГц
Трассировка кабелей		да	да
Источник питания		3,7 В	4 аккумулятора 16650
Стоимость		195 000 РУБ	543 600 РУБ

В итоге сравнения было принято решение в пользу устройства ST 600 ПИРАНЬЯ, так как в рамках обеспечения безопасности юридической консультации функционала данного устройства будет достаточно (определение радиомикрофонов, скрытых видеокамер, мобильных телефонов и т. д.)

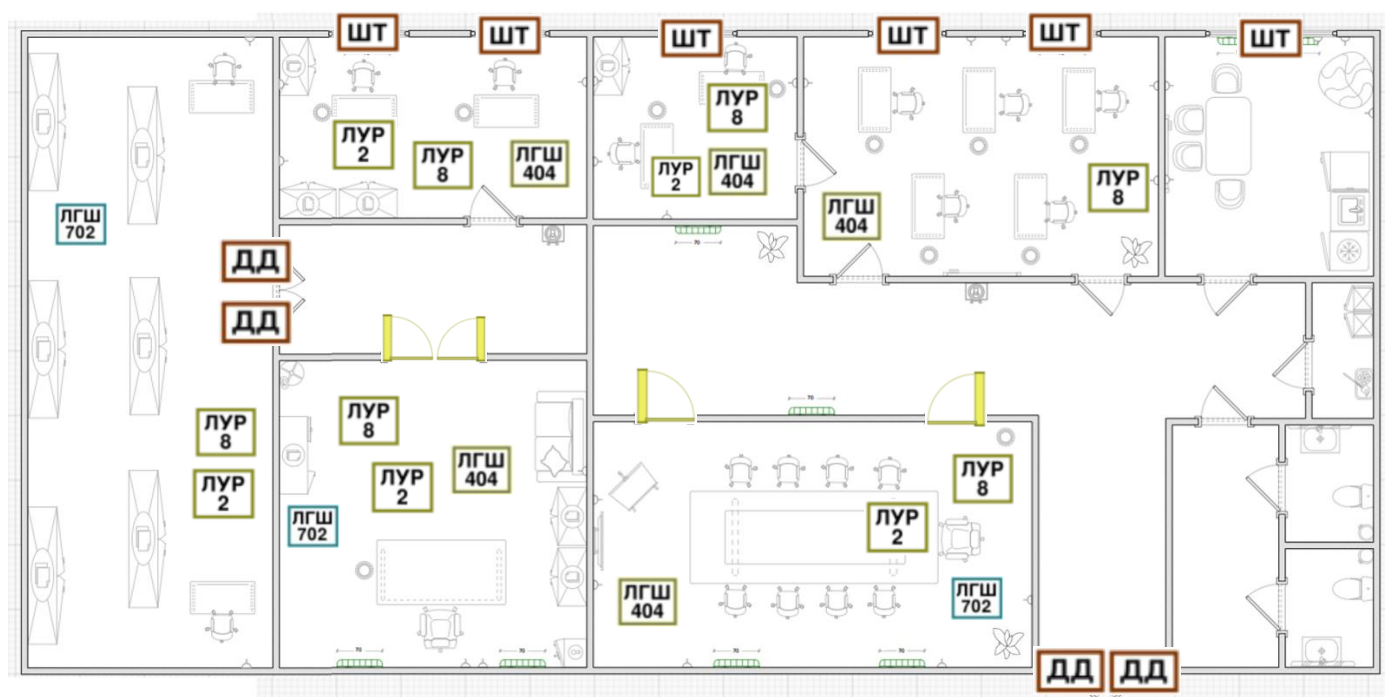
3.4.2. Подавление сигнала закладных устройств

Таблица 5 – Системы подавления сигнала закладных устройств

Характеристика	Устройство	ЛГШ 702	ЛГШ 716
Bluetooth		да	да
Wi-fi		да	да
Другие стандарты		нет	IMT-MC-450, GSM900, DSC/GSM1800, (DECT1800), IMT-2000/UMTS (3G),
Диапазон рабочих частот		не менее 2400–2483,5 МГц	не менее 2400–2483,5 МГц
Максимальная мощность		не менее 0,5 Вт	–
Питание		сетевой адаптер питания 220 В 50 Гц	не более 25 Вт
Стоимость		58 945 РУБ	85 251 РУБ

Было выбрано средство подавления сигналов “ЛГШ-702”. Устройство обладает необходимым функционалом для обеспечения защиты предприятия за меньшую стоимость.

4. РАЗМЕЩЕНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ



штора рулонная



доводчик дверной



активная защита от ПЭМИН
"Гамма ГШ-18"



средство подавления сигналов
"ЛГШ-702"



дверь звукоизолирующая



излучатель виброакустических
помех "ЛГШ-404"



размыкатель Ethernet "ЛУР-8"



размыкатель слаботочной линии
"ЛУР-2"

ЗАКЛЮЧЕНИЕ

В ходе выполнения работы был изучен план защищаемого помещения и законодательства, регулирующего требования обеспечения информационной безопасности предприятия с учетом характера защищаемых данных. Также, был составлен список потенциальных каналов утечки информации организации и необходимых технических средств защиты информации для каждого из указанных каналов.

В результате проведенной работы был составлен план размещения выбранных средств защиты информации на предприятии.

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) Указ Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера». – текст: электронный. – URL: <http://www.kremlin.ru/acts/bank/10638>

(4) Федеральный закон от 31.05.2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации». – текст: электронный. – URL: <http://www.kremlin.ru/acts/bank/18127>