**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 защиты

информации на предприятии»

**Выполнил:**

Пастухова Анастасия Александровна,

 студентка группы N34531

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

**Проверил:**

Попов Илья Юрьевич,

кандидат технических наук, 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** | Пастухова Анастасия Александровна | | | | | | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  | | (Фамилия И.О.) |
| **Факультет** |  | Факультет Безопасности Информационных Технологий | | | | | | |
| **Группа** | N34531 | | |  |  |  | |  |
| **Направление (специальность)** | | | | | | Технологии защиты информации | | |
| **Руководитель** | | Попов Илья Юрьевич, доцент ФБИТ, кандидат технических наук | | | | | | |
| (Фамилия И.О., должность, ученое звание, степень) | | | | | | | | |
| **Дисциплина** | | Инженерно-технические средства защиты информации | | | | | | |
| **Наименование темы** | | | | Проектирование инженерно-технической защиты информации на предприятии | | | | |
| **Задание** | Разработка системы инженерно-технической защиты информации на предприятии | | | | | | | |
| **Краткие методические указания:** | | | | | | | | |
| Объект исследований курсовой работы ограничивается заданным помещением. | | | | | | | | |
| **Содержание пояснительной записки** | | | | | | | **Введение:** краткое введение в курсовую работу | |
| **Организационная структура предприятия:** описание структуры предприятия | | | | | | | | |
| **Обоснование защиты информации:** описание угроз и каналов утечки информации | | | | | | | | |
| **Анализ защищаемых помещений:** анализ помещений на предмет возможных утечек | | | | | | | | |
| **Анализ рынка технических средств:** сравнительный анализ рынка ИТСЗИ | | | | | | | | |
| **Описание расстановки технических средств:** описание расстановки ИТСЗИ | | | | | | | | |
| **Заключение:** выводы к курсовой работе | | | | | | | | |
| Руководитель | |  | | | | | | |
|  |  |  |  |  |  |  | | (Подпись, дата) |
| Студент |  | | | | | | | 20.12.2023 |
|  |  |  |  |  |  |  | | (Подпись, дата) |

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

| **Студент** | Пастухова Анастасия Александровна | | | | |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | (Фамилия И.О.) |
| **Факультет** |  | Факультет Безопасности Информационных Технологий | | | |
| **Группа** | N34531 | | |  |  |
| **Направление (специальность)** | | | | | Технологии защиты информации |
| **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 | |

| **№**  **п/п** | **Наименование этапа** | **Дата завершения** | | **Оценка и подпись**  **руководителя** |
| --- | --- | --- | --- | --- |
| **Планируемая** | **Фактическая** |
| 1 | Анализ теоретической составляющей | 27.10.2023 | 27.10.2023 |  |
| 2 | Написание введения и основной части | 15.11.2023 | 15.11.2023 |  |
| 3 | Разработка комплекса инженерно-технической защиты информации в заданном помещении | 26.11.2023 | 26.11.2023 |  |
| 4 | Оформление курсовой работы | 10.11.2023 | 10.11.2023 |  |

****

| Руководитель | |  | |
| --- | --- | --- | --- |
| Студент | | 20.12.2023 | |
|  |  | (Подпись, дата) | |

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ**

| **Студент** | Пастухова Анастасия Александровна | | | | |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | (Фамилия И.О.) |
| **Факультет** |  | Факультет Безопасности Информационных Технологий | | | |
| **Группа** | N34531 | | |  |  |
| **Направление (специальность)** | | | | | Технологии защиты информации |
| **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

**Цель курсовой работы:** Повышение защищенности рассматриваемого помещения

**Задачи курсовой работы:**

* анализ защищаемого помещения;
* оценка каналов утечки информации;
* выбор мер пассивной и активной защиты информации.

\

1. **Характер работы**

Расчет

Моделирование

Конструирование Другое:

1. **Содержание работы**

Введение, Организационная структура предприятия.Обоснование защиты информации. Анализ защищаемых помещений. Анализ рынка технических средств. Описание расстановки технических средств. Заключение. Список литературы

1. **Выводы**

В результате была предложена защита от утечек информации по оптическому,акустическому, виброакустическому, электромагнитному каналам, обеспечена защита от ПЭМИН. 

Итоговая цена системы защиты информации составляет 779 800 рублей. 

| Руководитель | |  | |
| --- | --- | --- | --- |
|  |  | (Подпись, дата) | |
| Студент |  | | 20.12.2023 |
|  |  | (Подпись, дата) | |



«25» декабря 2023 г.

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 7](#_heading=h.1fob9te)

[1. ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ 8](#_heading=h.3znysh7)

[1.1 Общие сведения о защищаемой организации 8](#_heading=h.2et92p0)

[1.2 Информационные потоки 9](#_heading=h.tyjcwt)

[2. ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ 11](#_heading=h.3dy6vkm)

[3. АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ 12](#_heading=h.1t3h5sf)

[3.1 Схема помещения 12](#_heading=h.4d34og8)

[3.2 Описание помещений 13](#_heading=h.2s8eyo1)

[3.3 Анализ возможных каналов утечки информации 14](#_heading=h.17dp8vu)

[3.3.1 Оптический канал 14](#_heading=h.3rdcrjn)

[3.3.2 Акустический, виброакустический каналы 14](#_heading=h.26in1rg)

[3.3.3 Электромагнитный канал 14](#_heading=h.lnxbz9)

[3.3.4 Закладные устройства 14](#_heading=h.35nkun2)

[3.3.5 Материально-вещественный канал 15](#_heading=h.1ksv4uv)

[4. АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ 16](#_heading=h.44sinio)

[4.1 Оптический канал 16](#_heading=h.2jxsxqh)

[4.2 Акустический, виброакустический канал 16](#_heading=h.z337ya)

[4.3 Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам 18](#_heading=h.3j2qqm3)

[4.4 Защита от ПЭМИН 19](#_heading=h.1y810tw)

[4.5 Защита от утечки информации через закладные устройства. 20](#_heading=h.4i7ojhp)

[4.6 Защита от утечки информации по материально-вещественному каналу 21](#_heading=h.2xcytpi)

[5. ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ 22](#_heading=h.1ci93xb)

[ВЫВОД 25](#_heading=h.3whwml4)

[СПИСОК ИСТОЧНИКОВ 26](#_heading=h.2bn6wsx)

**ВВЕДЕНИЕ**

**Цель курсовой работы:**

Повышение защищенности рассматриваемого помещения.

**Задачи курсовой работы:**

* анализ защищаемого помещения;
* оценка каналов утечки информации;
* выбор мер пассивной и активной защиты информации.

В современном информационном обществе вопросы обеспечения безопасности и защиты конфиденциальной информации становятся все более актуальными и приобретают важное значение для предприятий любого масштаба. В условиях активного цифрового развития и расширения использования информационных технологий возникает необходимость эффективной защиты конфиденциальных данных от внешних угроз, кибератак, а также внутренних утечек информации.

Основное внимание уделяется разработке комплекса мероприятий, направленных на минимизацию уязвимостей информационных систем и созданию эффективной системы защиты данных.

В работе будут рассмотрены основные аспекты проектирования системы защиты информации на предприятии, включая анализ угроз информационной безопасности, выбор и реализацию соответствующих технических средств защиты, разработку политики безопасности, обучение персонала и многое другое.

Исследование планируется провести на основе анализа существующих методов защиты информации, нормативно-правовой базы в области информационной безопасности, а также на основе изучения передовых практик в данной области. Результаты и рекомендации, представленные в данной работе, будут иметь практическую значимость для предприятий, стремящихся обеспечить надежную защиту своей конфиденциальной информации.

1. **ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ**

## **1.1 Общие сведения о защищаемой организации**

**Наименование организации**: ООО “SpaceY”.

**Область деятельности**: Организация частных суборбитальных полетов.

**Цели для защиты**: Основные информационные процессы и потоки в организации, включая договора, контракты с компаниями-партнерами и поставщиками, внутренние приказы и нормативные акты, а также различные делопроизводственные документы.

Защите также подлежат особые виды информации:

* персональные данные клиентов и работников;
* коммерческая тайна;
* профессиональная тайна (для инженеров, обслуживающих ракету);
* государственная тайна (о месте запуска ракеты носителя и составе ракетного топлива).

Прибыль (месячная/годовая), расходы, стоимость информационных активов:

1. Прибыль:

месячная: 25 млн.р;

годовая: 300 млн.р;

*Из расчета, что выручка компании составит 135 млн.р. в месяц и 1.62 млрд.р. в год, благодаря тому, что будет совершаться хотя бы 1 полет в 2 месяца, на корабле подобном SpaceShipTwo с 6 местами для пассажиров по 45 млн.р.*

1. Расходы (в месяц):

выплата заработной платы всем сотрудникам: 54 млн. рублей;

аренда ангара, офиса, коммунальные платежи: 15 млн. рублей;

усредненная себестоимость полета: 35 млн. рублей;

логистические расходы: 6 млн. рублей.

3. Персонал организации 158 человек:

1. 100 инженеров ракетостроения (разной специализации) и пилоты,
2. 10 руководителей различных внутренних подразделений и секретарь,
3. 5 охранников
4. 3 бухгалтеров,
5. 3 работника пресс-службы,
6. 5 работников пиар-службы,
7. 5 маркетологов и бизнес-аналитиков,
8. 5 работников СИБ,
9. 2 системных администратора,
10. 10 программистов (фронтенд/бекенд разработчики, инженеры высоконагруженных систем, тестировщики, координатор).

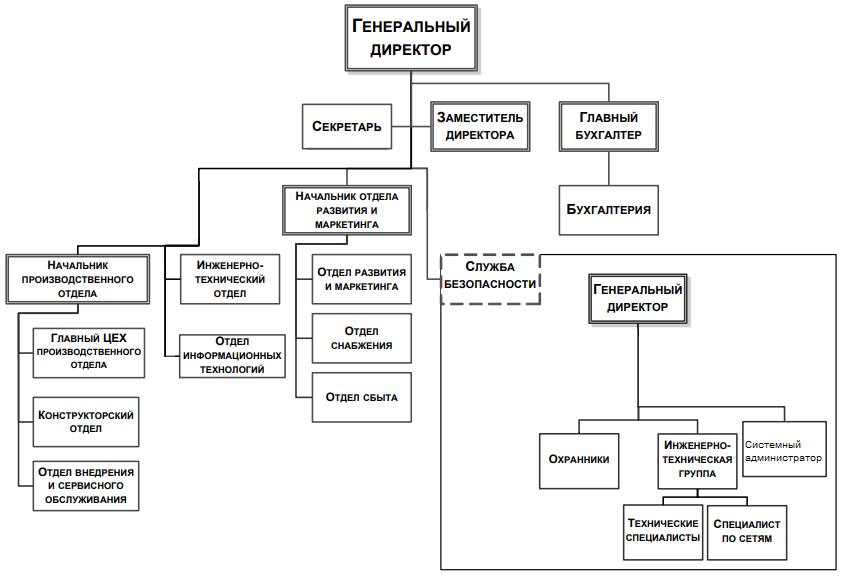
****

Рисунок 1 - Организационная структура предприятия

* 1. **Информационные потоки**

Информационные потоки представляют собой жизненно важный элемент для эффективной работы любой организации. Они являются основным каналом передачи данных, знаний и коммуникации между подразделениями, сотрудниками и внешними стейкхолдерами. Рассмотрение информационных потоков в контексте организации позволяет увидеть важность эффективного управления информацией для достижения целей и обеспечения конкурентоспособности.

Типы информационных потоков в организациях:

* Внутренние информационные потоки - это информация, передаваемая внутри организации между различными отделами, сотрудниками и уровнями управления. Внутренние потоки могут быть формальными (например, отчеты, инструкции, приказы) и неформальными (устные обсуждения, электронные сообщения).
* Внешние информационные потоки - представляют собой обмен информацией между организацией и внешней средой, такой как клиенты, поставщики, партнеры, регуляторы. Эти потоки включают в себя заказы, отчетность, рекламные материалы и другую коммуникацию с внешними организациями и физ. лицами.

На рисунке 2 представлены информационные потоки организации «SpaceY», которые передаются по открытым и закрытым каналам в зависимости от степени значимости информации, а также некоторые из этих каналов являются односторонними от подчиненных субъектов в вышестоящим.

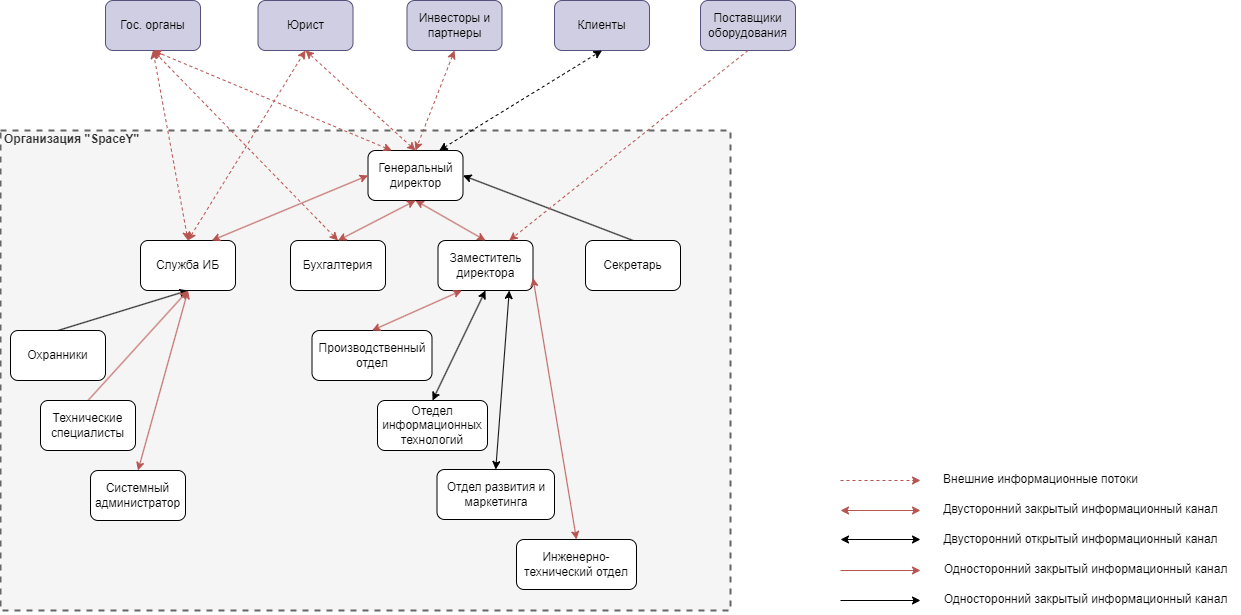


Рисунок 2 – схема информационных потоков организации

1. **ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ**

**2.1 Информация предприятия, составляющая государственную тайну**

Согласно Закону РФ "О государственной тайне" статье 5 «Перечень сведений, составляющих государственную тайну»:

* Раздел I (сведения в военной области): Сведения, раскрывающие свойства, рецептуру или технологию производства ракетных топлив, а также баллиститных порохов, взрывчатых веществ или средств взрывания военного назначения, а также новых сплавов, спецжидкостей, новых топлив для вооружения и военной техники.
* Раздел II (сведения в области экономики, науки и техники): Сведения о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства.

Так как наша организация имеет доступ к местоположению космодромов, составу ракетного топлива, технологии производства ракетных комплексов и прочей информации, касающейся ракетно-космической промышленности, то большинству сотрудников придется работать с государственной тайной и сведениями, относящимися к категории “*секретно*”.

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 этаже, 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 проверке желательно проводить периодически, чтобы исключить возможность утечки.

**2.2 Руководящие документы в области защиты информации,**

**составляющей государственную тайну**

Основными документами в области защиты информации, составляющей

государственную тайну, являются:

− Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне»;

− Закон РФ «О государственной тайне» от 21.07.1993 N 5485–1;

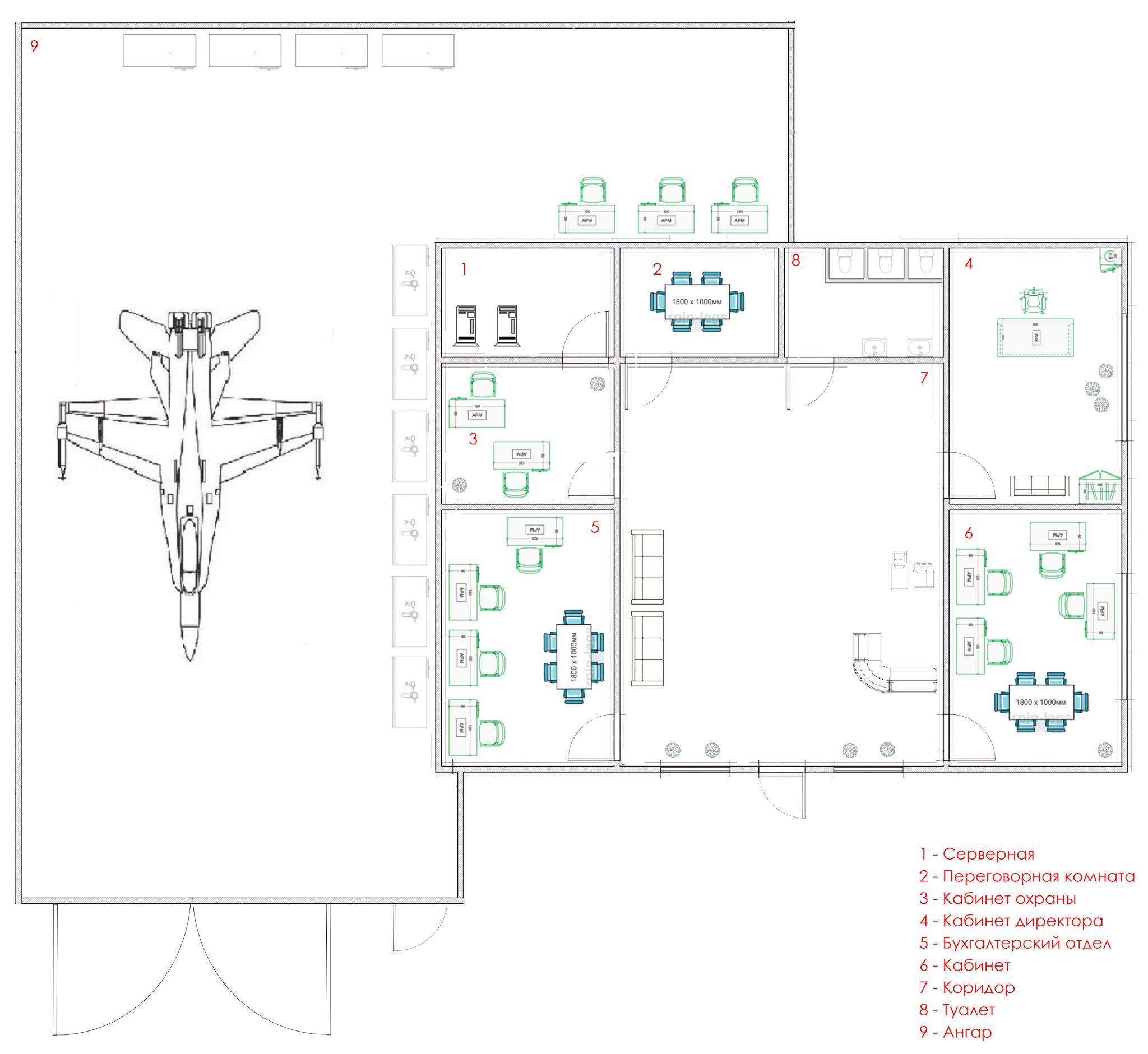
− Межведомственная комиссия по защите государственной тайны решение № 199 от 21.01.2011г. "О Типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними";

– Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам.

1. **АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ**

**3.1 Схема помещения**

Необходимо провести анализ защищаемого помещения, чтобы разместить технические средства защиты на объекте. План помещения рабочего предприятия и основного офиса для сотрудников ИС представлен на рисунке 3, а описание обозначений - на рисунке 4.

****Рисунок 3 – план защищаемого помещения

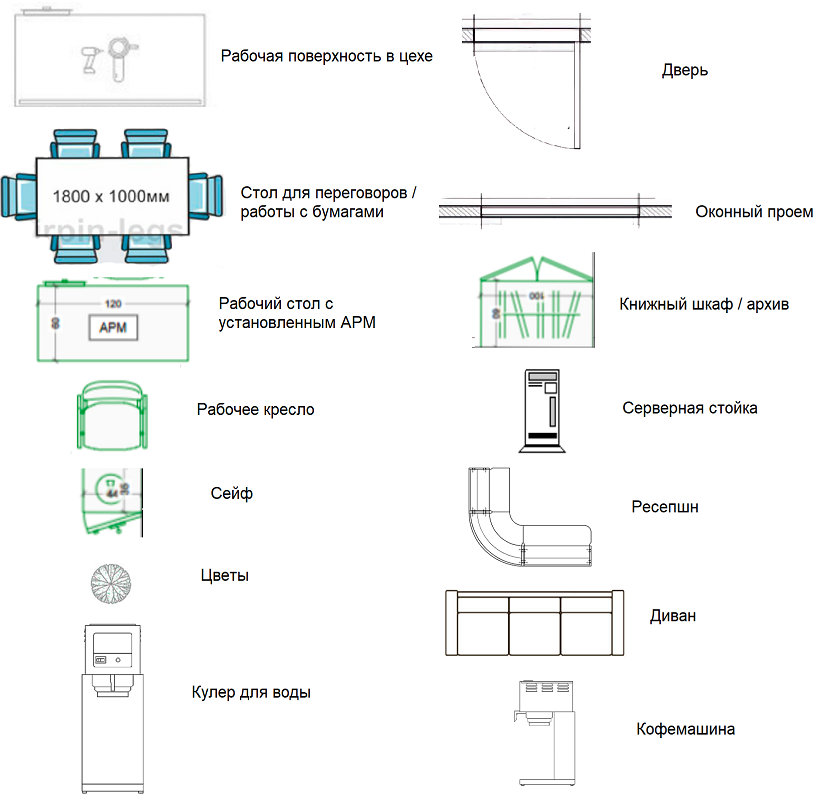
****

Рисунок 4 – условные обозначения на плане помещения

**3.2 Описание помещений**

Помещения включают в себя следующие объекты (таблица 3.2).

Таблица 3.2 - Предназначение и наполнение комнат

| Помещение | Предназначение | Объекты |
| --- | --- | --- |
| Серверная | Место с серверами | Серверная стойка |
| Переговорная | Проведение закрытых переговоров | Мебель |
| Охрана | Сбор данных со всех источников слежения | АРМ, мебель |
| Кабинет директора | Рабочее место директора | АРМ, сейф, мебель |
| Бухгалтерия | Место работы бухгалтеров | АРМ, мебель |
| Кабинет для сотрудников | Место работы сотрудников | Офисная мебель, АРМ |
| Коридор/приемная | Переход в другие помещения, место ожидания | Ресепшн, АРМ, диваны, кулер для воды, кофемашина |
| Санузел | Место для санитарных и гигиенических процедур | Раковины, унитазы |
| Ангар | Цех со средствами подготовки самолета к полету | Оборудование для подготовки самолета |

Офис организации, в котором планируется вести работу с государственной тайной, расположен в одноэтажном здании. Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см.

На южной стене расположены окна, выходящие на улицу, и главные ворота в ангар. Напротив, площадка для маневров самолета и никаких построек в радиусе 1 км.

Доступы к помещениям здания ограничен системой контроля и управления доступом, куда имеют пропуск только сотрудники организации-арендатора. Клиенты получают временный одноразовый пропуск, чтобы попасть внутрь офиса или переговорную комнату.

Особое внимание следует уделить следующим помещениям:

− Кабинет директора: директор работает с информацией, составляющей

государственную и коммерческую тайну;

− Переговорная: в помещении могут вестись обсуждения информации,

содержащей государственную и коммерческую тайну;

– Серверная: хранение самой важной информации организации и архивных документов;

− Кабинет бухгалтера: обрабатывается информация, составляющая коммерческую тайну;

− Кабинет сотрудников: сотрудники могут работать с информацией,

составляющей государственную и коммерческую тайну.

**3.3 Анализ возможных каналов утечки информации**

**3.3.1 Оптический канал**

Возможен частичный просмотр некоторых помещений офиса со стороны улицы через окна или дверные проемы, например при фотографировании или ином визуальном наблюдении.

**3.3.2 Акустический, виброакустический каналы**

Помещение расположено на первом этаже, а окна выходят на улицу. Несмотря на то, что вблизи нет других зданий, возможно прослушивание с улицы или рабочего цеха с использованием направленных микрофонов. Возможен съем речевой информации с оконных стекол с помощью лазера.

Во всех помещениях офиса имеется вентиляция, а значит есть вероятность прослушивания с использованием стетоскопов, спускаемых микрофонов.

В комнате, где ведутся закрытые разработки и обсуждения сведений, составляющих государственную или коммерческую тайну, имеются батареи отопления, что допускает вероятность прослушивания через систему отопления с использованием стетоскопов.

**3.3.3 Электромагнитный канал**

Возможен съем информации через систему электропитания, так как по всему офису находятся розетки и электропровода.

Из проводных каналов связи за пределы помещения выходит только ethernet кабель общего шлюза. Возможны съем и навязывание информации на этом канале связи.

Так как работа с секретными сведениями ведется с использованием компьютеров, возможно прослушивание паразитных электромагнитных полей, восстановление из них информации.

**3.3.4 Закладные устройства**

В помещении имеется множество мест, где можно спрятать закладное устройство: цветочные горшки, шкафы и полки с оборудованием, мусорные корзины. Кроме того, возможно размещение закладных устройств в стенах, либо их маскировка под розетки, светильники, выключатели.

**3.3.5 Материально-вещественный канал**

Материально-вещественный канал утечки информации присутствует. И угроза утечки по этому каналу нивелируется использованием СКУДа.

1. **АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ**

**4.1 Оптический канал**

В качестве средства защиты информации от утечек по оптическому каналу через окна необходимо использовать смарт пленку для переговорного помещения и одностороннюю зеркальную плёнку на все окна.

Таблица 1 – ИТСЗИ на оптический канал

| Наименование средства | Достоинства | Стоимость ₽ |
| --- | --- | --- |
| Односторонняя зеркальная пленка, 61 м2 | Закрывает обзор извне, ухудшает возможность прослушки направленным микрофоном | 47 444 |
| Смарт-плёнка, 5 м2 | Закрывает обзор извне, ухудшает возможность прослушки направленным микрофоном | 50 179 |

**4.2 Акустический, виброакустический канал**

Для пассивной звукоизоляции мы воспользуемся услугами сторонних компаний, которые предоставляют услуги по звукоизоляции помещений. А конкретнее, необходимо провести пассивную звукоизоляцию переговорного помещения (общая площадь 5.2 кв.м.), расчёты стоимости которой можно увидеть в таблице 2.

Таблица 2 – ИТСЗИ для пассивной звукоизоляции

| Наименование средства | Достоинства | Стоимость ₽ |
| --- | --- | --- |
| Звукоизоляция пола, 5,2 м2 | Соответствует всем требованиями организации. Низкая стоимость | 22 520 |
| Звукоизоляция потолка, 5,2м2 | 19 660 |
| Звукоизоляция стен, 10,4 м2 | 25 200 |
| Звукоизолирующие двери | 32 000 |

В таблице 3 приведён анализ рынка излучателей виброакустических помех распространяемых в данное время.

Таблица 3 – Сравнение излучателей виброакустических помех

| Наименование средства | Достоинства | Стоимость ₽ |
| --- | --- | --- |
| Соната АВ-4Б | Комплект состоит из блоков электропитания и управления, генераторов-акусто излучателей, генераторов-вибровозбудителей, размыкателя телефонной линии, размыкателя слаботочной линии, размыкателя линии Ethernet, пульта управления, блоков сопряжения из внешних  устройств. | 44 200 |
| Шорох 5Л | Устройство оснащено световым и звуковым индикаторами работы. Возможность управления устройством с помощью пульта ДУ. | 21 500 |
| SEL SP-157 Шагрень | Защита паролем настроек системы. Отсчёт времени наработки генерации шума по каждому каналу с выводом на экран. Непрерывный контроль состояния системы и каждого отдельного излучателя. | 47 400 |

В соответствии с таблицей 3 было принято решение о выборе системы «СОНАТА АВ-4Б». В сравнении с ценовым аналогом предоставляет возможность единой системы и единого управления для всех устройств ИТСЗИ «Соната».

**4.3 Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам**

Активная защита заключается в использовании системы белого шума в сети, которая создает фоновый шум, маскирующий колебания, вызванные звуковыми волнами или работой электронных устройств. Модели устройств, относительно которых будет идти дальнейший анализ, и их характеристики представлены в таблице 4.

Таблица 4 – активная защита от утечек информации по электрическим каналам.

| Наименование средства | Достоинства | Стоимость ₽ |
| --- | --- | --- |
| Соната-РС3 | Звуковая и световая индикация работы. Возможно дистанционное управление посредством проводного пульта. | 32 400 |
| ЛГШ-221 | Сетевой генератор шума. Устройство оснащено световым и звуковым индикаторами работы. Возможность управления устройством с помощью пульта ДУ. | 36 400 |
| Генератор шума Покров | Централизованное управление и контроль по Ethernet (для исполнения 2), для применения в системах пространственного зашумления. Независимая регулировка уровней электромагнитного поля шумового сигнала и шумового сигнала в линии электропитания  и заземления. | 32 800 |

На основании анализа, проведенного в таблице 4, был выбран генератор шума «Соната-РС3». Оптимальный вариант по соотношению цена и качество позволяют установить достаточное количество подобных устройств в помещениях. Кроме того, он легко интегрируется в экосистему устройств «Соната».

**4.4 Защита от ПЭМИН**

Таблица 5 – активная защита от ПЭМИН

| Наименование средства | Достоинства | Стоимость ₽ |
| --- | --- | --- |
| Соната-Р3.1 | Просто интегрируется в экосистему «Соната». Долгое время на рынке | 39 000 |
| ЛГШ-513 | Изделие «ЛГШ-513» оснащено визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа). | 33 120 |
| Генератор шума Пульсар | Имеет защиту регулятора уровня выходного шумового сигнала от нелегального доступа (и сигнализирует об этом). Индикаторы нормального режима работы (диод) и аварийного режима (свет и звук). | 24 525 |

В качестве средства активной защиты от побочных электромагнитных излучений и наводок был выбран генератор шума «Соната-Р3.1». Одним из главных аргументов для выбора была лёгкая и удобная интеграция с нашим предыдущим выбором.

**4.5 Защита от утечки информации через закладные устройства.**

Таблица 6 – сравнение средств для поиска закладных устройств

| Наименование средства | Достоинства | Стоимость ₽ |
| --- | --- | --- |
| SPYDER | Позволяет осуществлять поиск устройств, передающих информацию по радиоканалу, инфракрасному каналу, различным проводным линиям под напряжением до 400В, а также позволяет оценить вероятность утечки информации по виброакустическому и акустическому каналам. | 140 000 |
| ST 600 ПИРАНЬЯ | Широкая комплектация, долгое время на рынке, множество отзывов, совместим с другими устройствами компании-производителя. | 195 000 |
| ST 500 ПИРАНЬЯ | Широкая комплектация, долгое время на рынке, множество отзывов, совместим с другими устройствами компании-производителя. Множество режимов под любой режим работы закладного устройства | 429 000 |

Таким образом, было принято решение о выборе устройства «Spyder» из-за его цены и его возможностей справляться с возможностями, которые на него возложены.

**4.6 Защита от утечки информации по материально-вещественному каналу**

Для обеспечения безопасности материально-вещественного канала утечки информации нужно организовать СКУД и поставить охранника, который должен осуществлять досмотр на входе в помещение.

1. **ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ**

На рисунке 5 представлена схема расположения инженерно-технических средств защиты информации, описание которых можно найти в таблице 7.

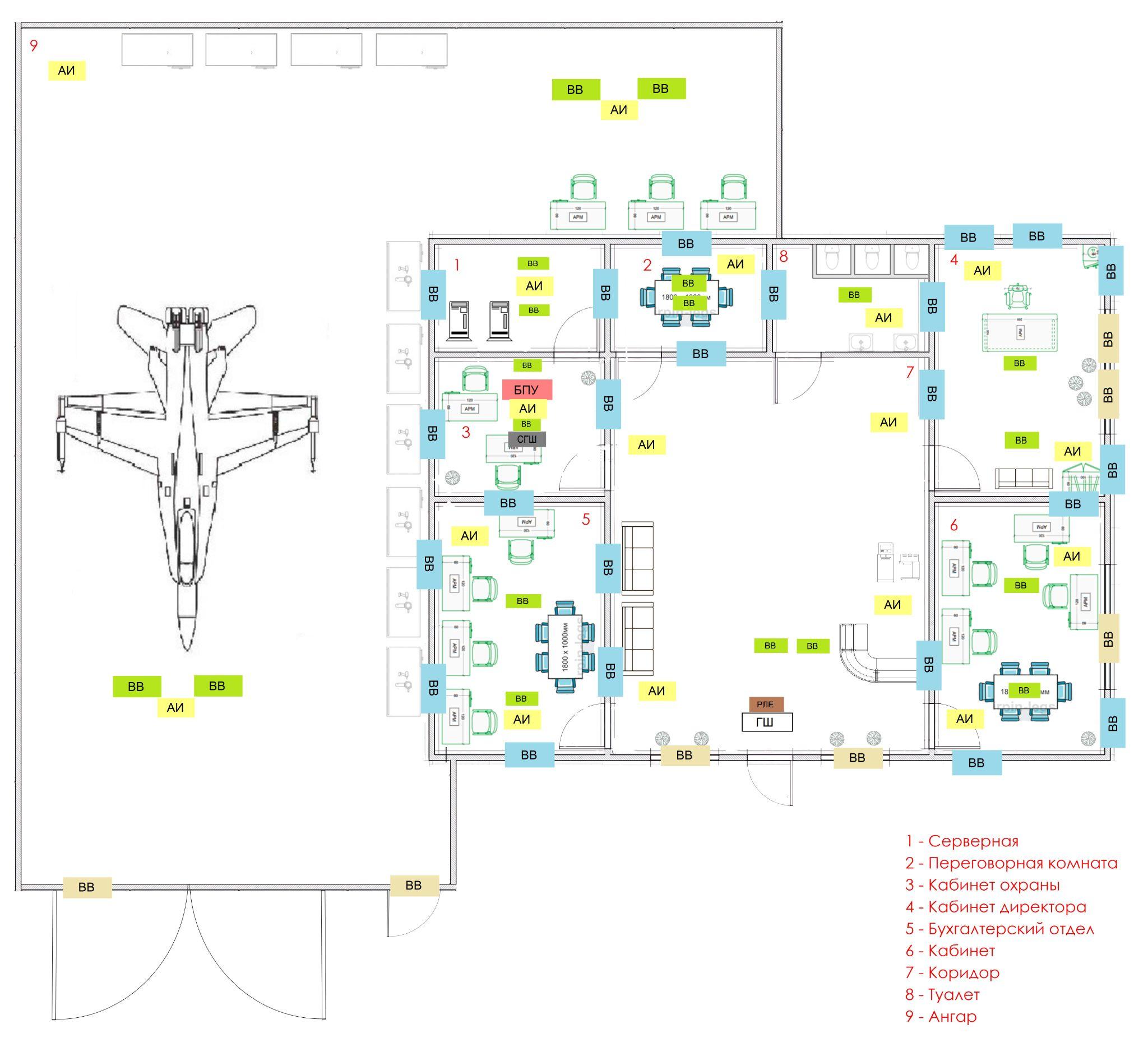


Рисунок 5 – схема расположения ИТСЗИ в офисе

Таблица 7 – количество и обозначение элементов схемы

| Обозначение | Описание | Количество |
| --- | --- | --- |
|  | Генератор-вибровозбудитель «Соната СА-4Б1» (потолок, пол) | 19 |
|  | Генератор-вибровозбудитель «Соната СВ-4Б» (окна) | 7 |
|  | Генератор-вибровозбудитель «Соната СВ-4Б» (стены) | 25 |
|  | Размыкатель линии «Ethernet» «Соната-ВК4.3» | 1 |
|  | Генератор-акустоизлучатель «Соната СА-4Б1» (вентиляция) | 17 |
|  | Блок электропитания и управления «Соната-ИП4.3» | 1 |
|  | Генератор Шума Соната-РС3 | 1 |
|  | Сетевой генератор шума Соната-Р3.1 | 1 |

Таблица 8 – итоговая стоимость всех устройств

| Меры защиты | Цена, руб | Кол-во | Итого |
| --- | --- | --- | --- |
| Блок электропитания и управления «Соната-ИП4.3» | 21600 | 1 | 21 600 |
| Генератор-акустоизлучатель «Соната СА-4Б1» | 3540 | 17 | 60 180 |
| Генератор-вибровозбудитель «Соната СB&-4Б» | 7440 | 51 | 379 440 |
| Рызмыкатель линии «Ethernet» «Соната ВК4.1» | 6000 | 1 | 6 000 |
| Пульт управления «Соната-ДУ 4.3» | 7680 | 1 | 7 680 |
| SPYDER | 140000 | 1 | 140 000 |
| Звукоизолирующая дверь | 32000 | 1 | 32 000 |
| Звукоизоляция переговорного помещения | 67 380 | 1 | 67 380 |
| Генератор Шума Соната-РС3 | 32400 | 1 | 32400 |
| Сетевой генератор шума Соната-Р3.1 | 33 120 | 1 | 33 120 |
| **Итого** | | | **779 800** |

# ВЫВОД

В ходе данной работы был произведен теоретический обзор существующих каналов утечки информации, анализ потенциальных каналов утечки информации в защищаемом помещении и описаны необходимые меры их защиты. Был проанализирован рынок существующих технических средств для противодействия рассматриваемым каналам утечки информации и выбраны подходящие для нашего объекта. Был разработан план установки и произведен расчет стоимости предложенных активных и пассивных средств защиты информации.

В результате была предложена защита от утечек информации по оптическому, акустическому, виброакустическому, электромагнитному каналам, обеспечена защита от ПЭМИН.

Итоговая цена системы защиты информации составляет 779 800 рублей.

**СПИСОК 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. Титов А. А. Инженерно-техническая защита информации: учебное пособие. Томск: ТУСУР, 2010. — 195 с