

**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 системы защиты от утечки информации по различным каналам»

Выполнила:

**Шкаровская Валерия Леонидовна,
студентка группы N34511**



(подпись)

Проверил:

**Попов Илья Юрьевич,
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 Шкаровская В.Л.

(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34511

Направление (специальность) 10.03.01 Информационная безопасность

Руководитель Попов И. Ю., доцент ФБИТ

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

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование системы защиты от утечки информации по различным каналам

Задание Разработка комплекса инженерно-технической защиты информации, составляющей государственную тайну с уровнем «секретно».

Содержание пояснительной записки

Курсовая работа состоит из следующих разделов:

В первой главе произведен анализ технических каналов утечки информации. Во второй обоснована защита информации путем приведения перечня руководящих документов. В третьей главе произведен анализ защищаемых помещений. В четвертой произведен анализ технических каналов утечки информации и выбраны средства защиты. Пятая глава представляет собой анализ рынка технических средств защиты информации разных категорий. Шестая глава посвящена разработке схем расстановки выбранных технических средств в защищаемом помещении.

Руководитель

(Подпись, дата)

Студент

(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Шкаровская В.Л.

(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34511

Направление (специальность) 10.03.01 Информационная безопасность

Руководитель Попов И. Ю., доцент ФБИТ

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

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование системы защиты от утечки информации по различным каналам

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Разработка и утверждение задания и календарного плана на курсовую работу	26.09.2023	26.09.2023	
2	Создание плана курсовой работы	03.10.2023	03.10.2023	
3	Анализ теоретической составляющей	24.10.2023	26.10.2023	
4	Разработка комплекса инженерно-технической защиты информации в заданном помещении	21.11.2023	20.11.2023	
5	Представление выполненной курсовой работы	19.12.2023	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 Шкаровская В.Л.

(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34511

Направление (специальность) 10.03.01 Информационная безопасность

Руководитель Попов И. Ю., доцент ФБИТ

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

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование системы защиты от утечки информации по различным каналам

**ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА
(РАБОТЫ)**

**1. Цель и задачи
работы**

- ☒ Предложены студентом ☐ Сформулированы при участии студента
☐ Определены руководителем

Цель работы – повышение эффективности защиты информационных ресурсов организации, обнаружение и предотвращение потенциальных угроз со стороны сотрудников организации.

**2. Характер
работы**

- ☐ Расчет ☐ Конструирование
☒ Моделирование ☐ Другое


3. Содержание работы

Анализ технических каналов утечки информации. Перечень руководящих документов. Анализ защищаемых помещений. Анализ технических каналов утечки информации. Выбор средства защиты. Анализ рынка технических средств защиты информации разных категорий. Схемы расстановки выбранных технических средств в защищаемом помещении.

4. Выводы

Был проведен теоретический анализ технических каналов утечки информации. Были определены руководящие документы, а также проведен анализ защищаемых помещений, проведена оценка каналов утечки информации и выбраны меры пассивной и активной защиты информации. Был проведен анализ рынка. На схеме были расставлены все средства защиты в соответствии с нормами и правилами.

Руководитель _____
(Подпись, дата)

Студент  _____
(Подпись, дата)

«19» декабя 2023 г.

Оглавление

ВВЕДЕНИЕ	3
ПОСТАНОВКА ЗАДАЧ	4
1.1 Цель курсовой работы.....	4
1.2 Задачи, решаемые в ходе выполнения данной работы.....	4
ВЫПОЛНЕНИЕ ПОСТАВЛЕННЫХ ЗАДАЧ.....	5
2.1 Анализ технических каналов утечки информации	5
2.2 Обоснование защиты информации	7
2.3 Анализ защищаемых помещений	15
2.3.1 Организационная структура предприятия.....	15
2.3.2 Описание помещения.....	16
2.3.3 Обоснование секретности	20
2.4 Анализ технических каналов утечки информации и выбор средств защиты.....	22
2.5 Анализ рынка технических средств защиты информации.....	23
2.5.1 Средства защиты информации от утечек по (вибро-) акустическим каналам.....	24
2.5.2 Средства защиты информации от утечек по электрическим, акустоэлектрическим и электромагнитным каналам.....	25
2.5.3 Средства защиты информации от побочных электромагнитных излучений и наводок (ПЭМИН)	27
2.6 Описание расстановки технических средств защиты информации	29
ЗАКЛЮЧЕНИЕ	34
СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ	35

ВВЕДЕНИЕ

В условиях современного информационного общества, где информационные ресурсы становятся все более ценными и важными, обеспечение безопасности передачи и хранения конфиденциальной информации становится приоритетной задачей. В данной курсовой работе будет рассмотрено проектирование системы защиты от утечки информации по различным каналам. Акцент будет сделан на анализе технических каналов утечки, разработке средств защиты, и их эффективной расстановке в помещениях.

В данной работе рассмотрен процесс разработки комплекса инженерно-технической защиты информации, составляющей государственную тайну с уровнем «секретно» на объекте информатизации. Защищаемый объект состоит из 12 помещений и коридора, представляет собой административное помещение атомной электростанции «СПбАЭС» с залом для конференций, кухней, совмещенной с зоной отдыха, отделом кадров, бухгалтерией, архивом, переговорной, туалетом, кабинетом администрации, кабинетом директора, рабочим залом, отделом безопасности с кабинетом начальника.

ПОСТАНОВКА ЗАДАЧ

1.1 Цель курсовой работы

Разработка комплекса инженерно-технической защиты информации, составляющей государственную тайну с уровнем «секретно».

1.2 Задачи, решаемые в ходе выполнения данной работы

- произвести анализ технических каналов утечки информации;
- составить перечень руководящих документов;
- произвести анализ защищаемых помещений;
- произвести анализ технических каналов утечки информации, выбрать средства защиты;
- произвести анализ рынка технических средств защиты информации разных категорий;
- разработать схемы расстановки выбранных технических средств в защищаемом помещении.

ВЫПОЛНЕНИЕ ПОСТАВЛЕННЫХ ЗАДАЧ

2.1 Анализ технических каналов утечки информации

Утечка конфиденциальной информации – это бесконтрольный выход конфиденциальной информации за пределы предприятия, которому она была доверена по службе или стала известна в процессе работы.

Эта утечка может быть следствием:

- разглашения конфиденциальной информации;
- ухода информации по различным, главным образом техническим, каналам;
- несанкционированного доступа к конфиденциальной информации различными способами.

Далее в ходе курсовой работы будет рассматриваться только утечка информации по техническим каналам.

Технический канал утечки информации (ТКУИ) – совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Утечка (информации) по техническому каналу – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

На рисунке 1 приведена структура технического канала утечки информации.



Рисунок 1 – Структура технического канала утечки информации

На вход ТКУИ поступает информация в виде первичного сигнала, представляющего собой носитель с информацией от её источника.

Источниками сигнала могут быть:

- объект наблюдения, отражающий электромагнитные и акустические волны;
- объект наблюдения, излучающий собственные (тепловые) электромагнитные волны в оптическом и радиодиапазонах;
- передатчик функционального канала связи;
- закладное устройство;
- источник опасного сигнала;
- источник акустических волн, модулированных информацией.

Информация от источника поступает на вход канала на языке источника, поэтому полученную информацию передатчик преобразует в форму, обеспечивающую запись ее на носитель информации, соответствующий среде распространения.

Среда распространения сигнала – физическая среда, по которой информативный сигнал может распространяться и регистрироваться приемником. Она характеризуется набором физических параметров, определяющих условия перемещения сигнала. Основными параметрами, которые надо учитывать при описании среды распространения, являются:

- физические препятствия для субъектов и материальных тел;
- мера ослабления сигнала на единицу длины;
- частотная характеристика;
- вид и мощность помех для сигнала.

Приемник после этого производит следующие действия:

- выбор носителя с нужной получателю информацией;
- усиление принятого сигнала до значений, обеспечивающих съем информации;
- съем информации с носителя;

— преобразование информации в форму сигнала, доступную получателю (человеку, техническому устройству), и усиление сигналов до значений, необходимых для безошибочного их восприятия.

Классификация технических каналов утечки информации приведена на рисунке 2.



Рисунок 2 – Классификация технических каналов утечки информации

2.2 Обоснование защиты информации

Для предприятий атомной энергии, которые являются объектами критической информационной инфраструктуры, устанавливается особый режим охраны государственной тайны.

Для обоснования защиты информации мы проведём анализ существующих руководящих документов.

1. Федеральный закон № 170 от 21 ноября 1995 г. «Об использовании атомной энергии»

1. Глава V. Государственное регулирование безопасности при использовании атомной энергии

1. Статья 23. Государственное регулирование безопасности при использовании атомной энергии

2. Статья 25. Полномочия органов государственного регулирования безопасности
 3. Статья 26. Разрешения (лицензии) на право ведения работ в области использования атомной энергии
 4. Статья 27. Разрешения на право ведения работ в области использования атомной энергии, выдаваемые работникам объектов использования атомной энергии
2. Федеральный закон № 187 от 26 июля 2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации»
1. Статья 3. Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры
 2. Статья 4. Принципы обеспечения безопасности критической информационной инфраструктуры
 3. Статья 10. Система безопасности значимого объекта критической информационной инфраструктуры
 4. Статья 11. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры
 5. Статья 12. Оценка безопасности критической информационной инфраструктуры
 6. Статья 13. Государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры
3. Федеральный закон № 5485-1 от 21 июля 1993 г. «О государственной тайне»
1. Раздел VI. Защита государственной тайны
 1. Статья 21. Допуск должностных лиц и граждан к государственной тайне

2. Статья 21.1. Особый порядок допуска к государственной тайне
 3. Статья 22. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне
 4. Статья 23. Условия прекращения допуска должностного лица или гражданина к государственной тайне
 5. Статья 24. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне
 6. Статья 25. Организация доступа должностного лица или гражданина к сведениям, составляющим государственную тайну
 7. Статья 26. Ответственность за нарушение законодательства Российской Федерации о государственной тайне
 8. Статья 27. Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну
 9. Статья 28. Порядок сертификации средств защиты информации
4. Постановление Правительства РФ № 669 от 12 июля 2016 г. «Об утверждении Положения о стандартизации в отношении продукции (работ, услуг), для которой устанавливаются требования, связанные с обеспечением безопасности в области использования атомной энергии, а также процессов и иных объектов стандартизации, связанных с такой продукцией»
1. Обеспечение средствами стандартизации необходимого уровня безопасности объектов использования атомной энергии
 2. Обеспечение единой технической политики в сфере стандартизации в отношении обеспечения безопасности объектов использования атомной энергии

3. Внедрение средствами стандартизации передовых технологий в области использования атомной энергии с учетом того, что технические и организационные решения, принимаемые для обеспечения безопасности объекта использования атомной энергии, должны быть апробированы прежним опытом, испытаниями, исследованиями, опытом эксплуатации прототипов
5. Постановление Правительства РФ № 749 от 26 июня 2017 г. «Об установлении зон безопасности с особым правовым режимом объекта использования атомной энергии»
 1. Пункт 2. Ограничения на въезд и пребывание граждан на территории зоны безопасности
 2. Пункт 3. Ограничения на полеты летательных аппаратов
6. Приказ ФСТЭК № 31 от 14 марта 2014 г. «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»
 1. Пункт 2. Требования к организации защиты информации в автоматизированной системе управления
 1. Разработка системы защиты автоматизированной системы управления
 2. Внедрение системы защиты автоматизированной системы управления и ввод ее в действие
 3. Обеспечение защиты информации в ходе эксплуатации автоматизированной системы управления
 4. Обеспечение защиты информации при выводе из эксплуатации автоматизированной системы управления
 2. Пункт 3. Требования к мерам защиты информации в автоматизированной системе управления

7. Приказ ФСТЭК № 235 от 21 декабря 2017 г. «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»

1. Пункт 3. Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов критической информационной инфраструктуры
2. Пункт 4. Требования к организационно-распорядительным документам по безопасности значимых объектов
3. Пункт 5. Требования к функционированию системы безопасности в части организации работ по обеспечению безопасности значимых объектов критической информационной инфраструктуры

8. Приказ ФСТЭК № 239 от 25 декабря 2017 г. «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

1. Пункт 2. Требования к обеспечению безопасности в ходе создания, эксплуатации и вывода из эксплуатации значимых объектов
 1. Установление требований к обеспечению безопасности значимого объекта
 2. Разработка организационных и технических мер по обеспечению безопасности значимого объекта
 3. Внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие
 4. Обеспечение безопасности значимого объекта в ходе его эксплуатации

5. Обеспечение безопасности значимого объекта при выводе его из эксплуатации
 2. Пункт 3. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов
 3. Пункт 4. Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов
9. Федеральные нормы и правила в области использования атомной энергии «Общие положения обеспечения безопасности атомных станций» (НП-001-15)
1. Пункт 3. Основные принципы безопасности, реализуемые в проекте атомной станции и ее систем
10. Федеральные нормы и правила в области использования атомной энергии «Правила устройства и эксплуатации локализирующих систем безопасности атомных станций» (НП-010-16)
1. Пункт 2. Общие требования к локализирующим системам безопасности атомных станций
 2. Пункт 10. Эксплуатация локализирующих систем безопасности и их элементов
- Регламенты и нормативные документы госкорпорации «Росатом» (11–13):
11. Приказ Государственной корпорации по атомной энергии «Росатом» от 30.10.2018 № 1/31-НПА «Об утверждении Административного регламента Государственной корпорации по атомной энергии «Росатом» по предоставлению государственной услуги «Аккредитация органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия продукции, для которой устанавливаются требования, связанные с обеспечением безопасности в области использования атомной энергии, обязательным требованиям»»

12. Приказ Государственной корпорации по атомной энергии «Росатом» от 03.10.2017 № 1/31-НПА «Об утверждении Требований к обозначению зоны безопасности с особым правовым режимом объекта использования атомной энергии»
13. Приказ Государственной корпорации по атомной энергии «Росатом» от 28.09.2017 № 1/29-НПА «Об утверждении порядка взаимодействия подразделений ведомственной охраны Государственной корпорации по атомной энергии "Росатом" с территориальными органами федерального органа исполнительной власти в сфере обеспечения безопасности, органами внутренних дел Российской Федерации, войсками национальной гвардии Российской Федерации»
14. ГОСТ Р МЭК 61513-2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Общие требования»
 1. 5 Общий жизненный цикл безопасности систем контроля и управления
 1. 5.2 Получение требований систем контроля и управления из проектных основ безопасности атомной станции
 2. 5.3 Выходная документация
 3. 5.4 Проектирование общей архитектуры систем контроля и управления и назначение функций систем контроля и управления
 4. 5.5 Общее планирование
 5. 5.6 Выходная документация
 2. 6 Жизненный цикл системы безопасности
 1. 6.2 Требования
 2. 6.3 Планирование системы
 3. 6.4 Выходная документация
 4. 6.5 Квалификация системы
 3. 7 Общая интеграция и ввод в эксплуатацию
 1. 7.2 Цели, которые должны быть достигнуты

2. 7.3 Выходная документация
4. 8 Общая эксплуатация и техническое обслуживание
 1. 8.2 Цели, которые должны быть достигнуты
 2. 8.3 Выходная документация
- 15.ГОСТ Р МЭК 61226-2011. «Атомные станции. Системы контроля и управления, важные для безопасности. Классификация функций контроля и управления»
 1. 6 Процедура классификации
 1. 6.2 Определение основ проекта
 2. 6.3 Идентификация и классификация функций
 2. 7 Установление технических требований по категориям
 1. 7.2 Требования, относящиеся к функциям
 2. 7.3 Требования, относящиеся к системам контроля и управления
 3. 7.4 Требования к оборудованию
 4. 7.5 Требования, связанные с аспектами качества
16. «Вопросы защиты государственной тайны» от 30.03.1994 г. №614.«Об утверждении перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г. №1203.
17. «О межведомственной комиссии по защите государственной тайны» от 8 ноября 1995 г. №1108.
18. «Вопросы Межведомственной комиссии по защите государственной тайны» от 20 января 1996 г. №71 с изменениями, внесенными Указами Президента Российской Федерации от 21 апреля 1996 г. №573, от 14 июня 1997 г. №594.
19. «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. №644.
20. Положение о государственной системе защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки

по техническим каналам Постановление Совета Министров – Правительства Российской Федерации от 15 сентября 1993 г. №921–51.

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

2.3 Анализ защищаемых помещений

2.3.1 Организационная структура предприятия

Наименование организации: “СПбАЭС”.

Область деятельности: Электроэнергетика и производство ядерной энергии.

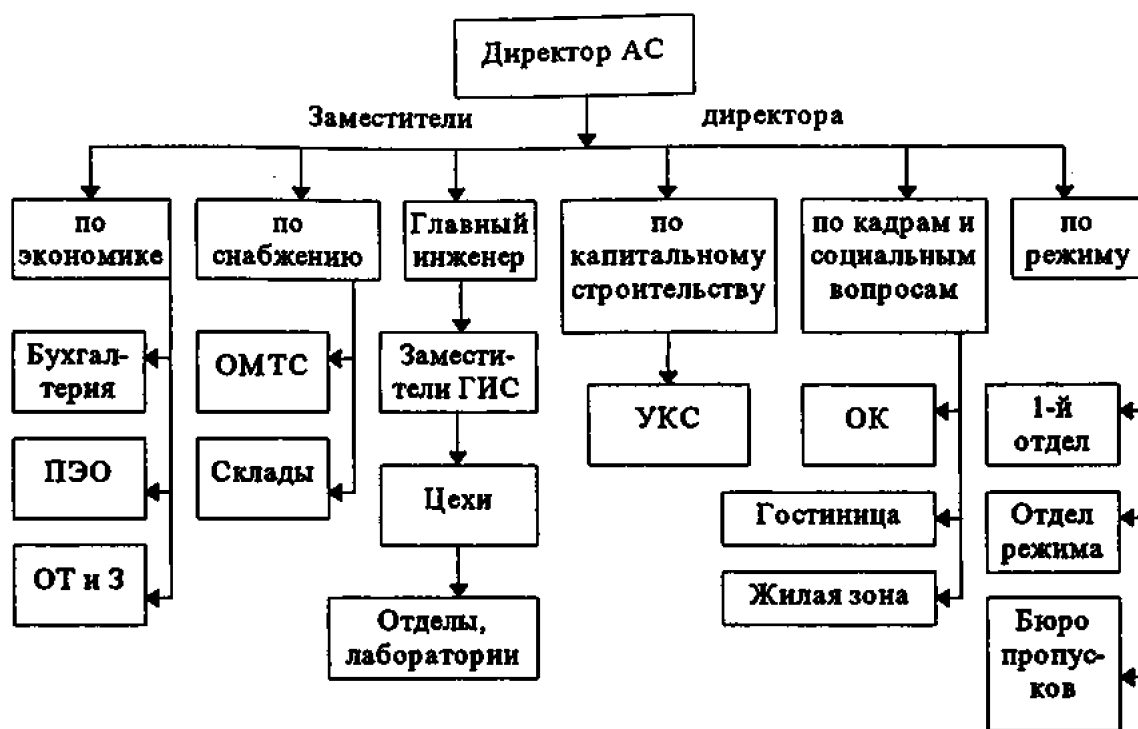


Рисунок 3 – Организационная структура предприятия

Основные информационные процессы и потоки в организации, включая описание информации ограниченного доступа представлены на рисунке 3.

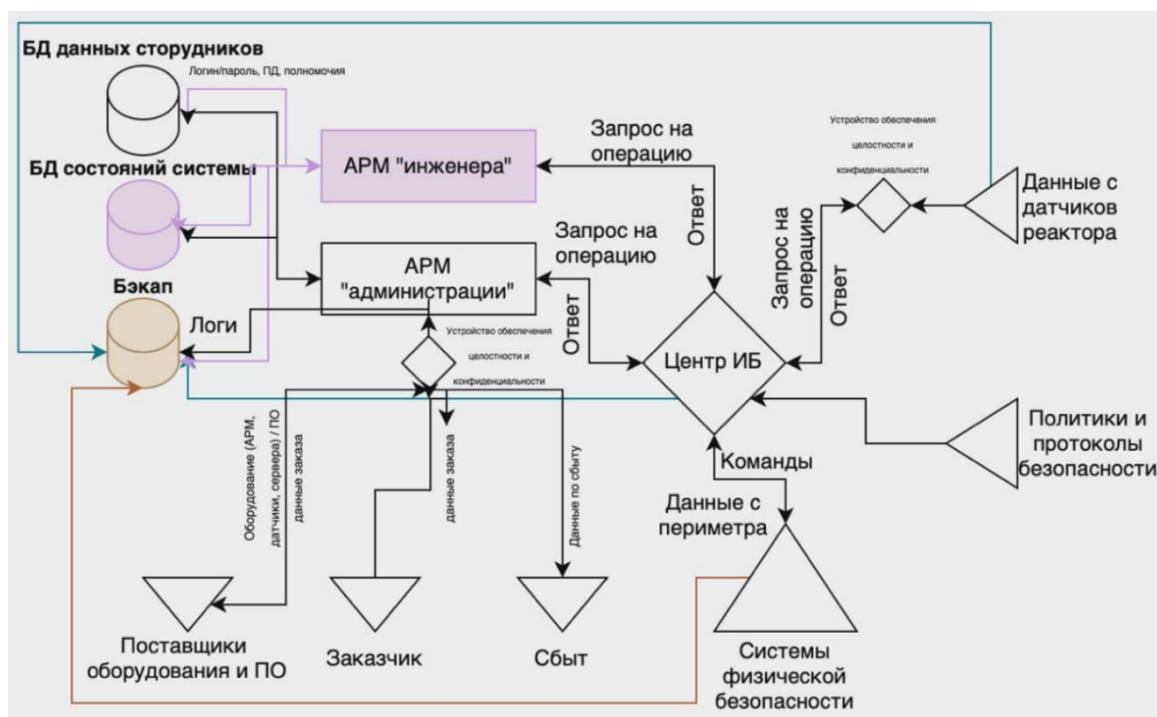


Рисунок 4 – Схема информационных потоков

2.3.2 Описание помещения

Перед тем, как перейти к разработке комплекса инженерно-технической защиты информации, необходимо описать выбранные помещения. На рисунке 4 представлен план административного помещения электростанции «СПбАЭС».

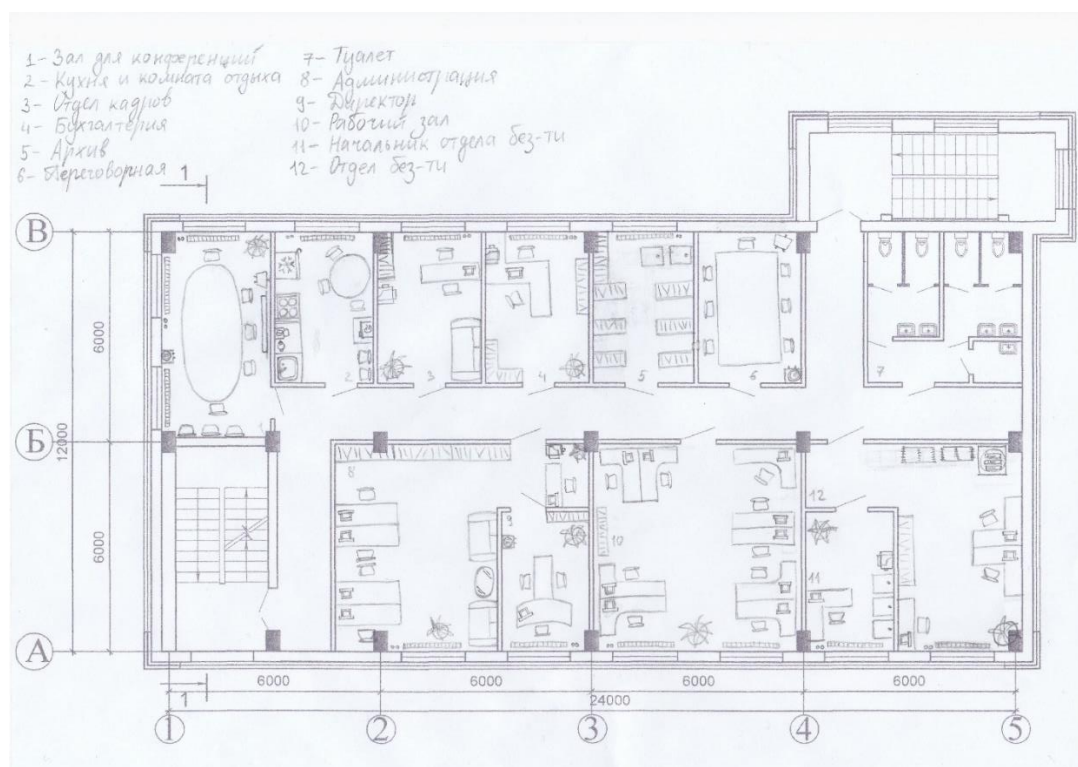



Рисунок 5 – План помещения

В таблице 2 приведено описания всех элементов, изображенных на плане помещения.

Таблица 2 – Описание элементов, изображенных на плане помещения

Обозначение	Название
	Стулья
	Журнальный столик
	Растение
	Серверная стойка
	Полки
Обозначение	Название
	Стеллажи
	МФУ
	Питьевой кулер
	Электрочайник
	Кофемашина
	Электроплита
	Холодильник

Обозначение	Название
	Микроволновая печь
	Раковины
	Санузел
	Батареи центрального отопления
	Отопительные стояки
	Персональные компьютеры (ПК)
	Сейфы
	Стол
	Диваны
	Флипчарты
	Экран проектора потолочный

Рассматриваемые помещения имеют следующую площадь:

- зал для конференций: 17,99 м²;
- кухня и комната отдыха: 11,92 м²;
- отдел кадров: 12,58 м²;
- бухгалтерия: 12,65 м²;
- архив: 12,05 м²;
- переговорная: 12,65 м²;
- туалет: 17,27 м²;

- администрация: 23,98 м²;
- кабинет директора: 9,91 м²;
- рабочий зал: 34,69 м²;
- отдел безопасности: 25,31 м²;
- кабинет начальника ОБ: 9,91 м².

Зал для конференций (17,99 м²) предназначен для проведения конференций и совещаний. В зале есть конференц-стол, стулья, флипчарт и экран проектора, растение и кулер. Кухня и комната отдыха (11,92 м²) оборудована бытовой техникой (электрочайник, кофемашина, электроплита, холодильник, микроволновая печь), столом и стульями. Отдел кадров (12,58 м²) включает рабочее место (стол, ПК, МФУ, стулья), стеллаж, диван для ожидания. Бухгалтерия (12,65 м²) оборудована рабочим местом (стол, ПК, МФУ, стулья), стеллажами, растением. Архив (12,05 м²) предназначен для хранения документов с использованием стеллажей и сейфов для особо важных документов. Переговорная (12,65 м²) оборудована конференц-столом, стульями, флипчартом и кулером.

Туалет (17,27 м²) разделен на мужской и женский, совмещенный с инвалидным, и оснащен унитазами, раковинами и необходимыми аксессуарами.

Администрация (23,98 м²) включает в себя рабочие места (столы, ПК, МФУ и стулья), стеллажи, два дивана с туалетным столиком между ними, растения. Кабинет директора (9,91 м²) представляет собой индивидуальное пространство входом через администрацию с рабочим местом (стол для переговоров, ПК, стулья), стеллажом, растением и кулером. Рабочий зал (34,69 м²) предназначен для коллективной работы сотрудников и содержит рабочие места (столы, ПК и стулья), стеллажом и растением.

Отдел безопасности (25,31 м²) включает рабочие места (столы, ПК и стулья) стеллаж, полки и растение. Кабинет начальника ОБ (9,91 м²) содержит рабочее место (стол, ПК, МФУ и стул), сейфы для хранения важных

документов и растение.

Каждое помещение, помимо переговорной, оборудовано батареей центрального отопления, отопительными стояками и розетками.

Административное здание АЭС расположено на втором этаже малоэтажного здания с окнами, выходящими в закрытый контролируемый двор. Окна этажа не примыкают к пожарным и эвакуационным лестницам, крышам пристроек, выступам на стенах, балконам и другим элементам, исключая возможность несанкционированного проникновения в помещения. Стены здания и внутренние перегородки выполнены из железобетона с толщиной не менее 10 см.

Часть внутренних перегородок изготовлена из железобетона с толщиной не менее 5 см, обеспечивая надежную конструкцию. Другая часть перегородок выполнена из звукоизоляционного гипсокартона, способствуя созданию комфортных рабочих условий. Общая архитектурная конфигурация здания минимизирует риски безопасности, и окна не предоставляют прямого доступа с улицы, обеспечивая надежную защиту от посторонних лиц.

2.3.3 Обоснование секретности

Согласно Руководящему документу Государственной технической комиссии при Президенте РФ «Классификация автоматизированных систем и требований по защите информации» от 30 марта 1992 г.: «При разработке АС, предназначенной для обработки или хранения информации, являющейся собственностью государства и отнесенной к категории секретной, необходимо ориентироваться в соответствии с РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации на классы защищенности АС не ниже (по группам) 3А, 2А, 1А, 1Б, 1В».

Таблица 1 – Классы защищенности автоматизированных систем

<p>Первая группа (многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, и не все пользователи имеют право доступа ко всей информации АС)</p>	1А	В случае обработки секретной информации с грифом «особая важность»
	1Б	В случае обработки секретной информации с грифом не выше «совершенно секретно»
	1В	В случае обработки секретной информации с грифом не выше «секретно»
	1Г	АС, в которых циркулирует служебная информация
	1Д	АС, в которых циркулируют персональные данные
<p>Вторая группа (АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности)</p>	2А	Информация, составляющая государственную тайну
	2Б	Служебная тайна или персональные данные
<p>Третья группа (АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности)</p>	3А	Информация, составляющая государственную тайну
	3Б	Служебная тайна или персональные данные

По постановлению Правительства РФ от 4 сентября 1995 г. N 870 "Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности" к секретным сведениям следует относить все сведения, отличные от сведений:

1. особой важности: сведений в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации.

2. совершенно секретных : сведений в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб интересам государственного органа или отрасли экономики Российской Федерации в одной или нескольких из указанных областей.

Соответственно класс защищенности у рассматриваемой организации 1В, так как в ней обрабатывается секретная информация и предприятие является многопользовательской АС, где не все пользователи имеют права доступа ко всей информации.

2.4 Анализ технических каналов утечки информации и выбор средств защиты

В помещениях присутствуют декоративные элементы, где можно спрятать закладное устройство. В каждом помещении, помимо переговорной, имеются розетки, а значит, актуальны электрический и электромагнитный каналы утечки информации. Также есть угроза снятия информации по вибрационному, оптическому, акустическому, виброакустическому, акустоэлектрическому каналам.

Материально-вещественный канал утечки информации регулируется строгой политикой компании в отношении физических носителей информации, и в рамках курсовой работы не рассматривается.

Для обеспечения комплексной безопасности государственной тайны типа «секретно» требуется оснастить помещение средствами защиты, приведенными в таблице 3.

Таблица 3 – Активная и пассивная защита информации

Каналы	Источники	Пассивная защита	Активная защита
акустический / акустоэлектрический	окна, двери, проводка	звукоизоляция переговорной, фильтры для сетей электропитания	устройства акустического зашумления
вибрационный / виброакустический	все твердые поверхности помещения, батареи	изолирующие звук и вибрацию обшивки стен	устройства вибрационного зашумления
Каналы	Источники	Пассивная защита	Активная защита
электромагнитный / электрический	розетки, АРМы, бытовая техника	фильтры для сетей электропитания	устройства электромагнитного зашумления
оптический	окна, двери	жалюзи / шторы на окнах, тонирующие пленки на окна, доводчики на дверях	бликующие устройства

2.5 Анализ рынка технических средств защиты информации

Проведем анализ рынка решений по инженерно-технической защите информации. Выберем решения, подходящие для защиты государственной тайны уровня «секретно».

Все приспособления защиты информации можно разделить на два

класса – пассивные и активные. Пассивные – измеряют, определяют, локализуют каналы утечки, ничего не внося при этом во внешнюю среду. Активные – «зашумляют», «выжигают», «раскачивают» и уничтожают всевозможные спецсредства негласного получения информации.

2.5.1 Средства защиты информации от утечек по (вибро-) акустическим каналам

Пассивная защита (вибро-)акустического каналов утечки информации представляет собой:

- усиленные двери;
- дополнительная отделка переговорной звукоизолирующими материалами.

Активная защита представляет собой систему (вибро-)акустического зашумления. В таблице 4 приведен сравнительный анализ подходящих средства активной защиты помещений по (вибро-)акустическим каналам.

Таблица 4 – Сравнительный анализ средств активной защиты от утечек по (вибро-)акустическим каналам

Устройство	Цена, руб.	Диапазон частот, Гц	Состав
Шорох 5Л	21 500	80-11 300	Устройство оснащено световым и звуковым индикаторами работы. Возможность управления устройством с помощью пульта ДУ. Максимальное количество излучателей – 40. Количество октавных полос для регулировки уровня мощности шума – 7.
ЛГШ-404	35 100	175–11 200	Вариативность количества подключаемых к генераторному блоку преобразователей. К двухканальному виброакустическому генератору шума ЛГШ-404 можно одновременно подключить до 20 ЛВП-10 и до 20 ЛВП-2А. Счетчик времени наработки и световая индикация режима работы.

Устройство	Цена, руб.	Диапазон частот, Гц	Состав
Соната-АВ-4Б	44 000	175– 11 200	Блок электропитания и управления, генератор-акустоизлучатель, генератор-вибровозбудитель, размыкатель телефонной линии, размыкатель слаботочной линии, размыкатель линии Ethernet, пульт управления, блок сопряжения с внешними устройствами, техническое средство защиты речевой информации от утечки по оптоэлектронному (лазерному) каналу
Гамма СВА301	28 600	90– 11 200	Имеет четыре канала формирования помех, к каждому из которых могут подключаться вибропреобразователи пьезоэлектрического или электромагнитного типа, а также акустические системы, обеспечивающие преобразование электрического сигнала, формируемого прибором, в механические колебания в ограждающих конструкциях защищаемого помещения, а также в акустические колебания воздуха

По результатам анализа была выбрана система Соната-АВ-4Б, так как:

- есть возможность подключения к одному питающему шлейфу, что облегчает процесс проектирования и монтажа;
- есть индивидуальная регулировка интегрального уровня и корректировка спектра каждого генератора, что улучшает действие системы;
- имеет среднюю цену из представленных средств активной защиты;
- позволяет уменьшить затраты благодаря использованию единой линии связи и электропитания.

2.5.2 Средства защиты информации от утечек по электрическим, акустоэлектрическим и электромагнитным каналам

Пассивная защита основывается на установке фильтров для сетей электропитания во всех помещениях.

Активная защита основывается на создании в сети белого шума, который скрывает колебания, порождаемые воздействием звуковой волны или работающей электрической техникой. В таблице 5 приведен сравнительный анализ подходящих средства активной защиты помещений по электрическим каналам.

Таблица 5 – Сравнительный анализ средств активной защиты от утечек по электрическим каналам

Устройство	Цена, руб.	Состав
Соната- PC1	16 520	Диапазон частот до 1 ГГц, регулировка уровня шума в 1 частотной полосе. Возможность локального проводного управления в случае использования в составе комплекса ТСЗИ (встроенный модуль Rebus)
Соната-PC3	32 400	Диапазон частот до 2 ГГц, диапазон регулировки. Возможность регулирования уровня излучаемых электромагнитных шумов; возможность блокировки прибора от несанкционированного доступа; световой и звуковой индикаторы работы и контроля уровня излучения; совместимость с проводными пультами ДУ линейки СОНАТА
Сетевой Генератор шума «ЛГШ-221»	36 400	Диапазон частот 10 кГц – 400 МГц, диапазон регулировки уровня шума не менее 20 ДБ. Световой индикатор работы в стандартном режиме; световая и звуковая сигнализация в случае отказа и перехода в аварийный режим работы; счетчик отработанных часов; возможность интеграции в программно-аппаратный комплекс ДУ и контроля «Паутина»

Устройство	Цена, руб.	Состав
Двухканальный генератор зашумления SEL SP-44	24 000	Диапазон частот 10 кГц – 400 МГц, диапазон регулировки уровня шума не менее 20 ДБ. Генератор регулируемого шума. Индикация нормального / аварийного режима работы. Электропитание от сети переменного тока 220В 50 Гц. Устройство имеет высший класс устойчивости к импульсным помехам и допускает длительную работу в условиях эквивалентного короткого замыкания.

В результате анализа был выбран генератор шума Соната-РС3. Особенности конструкции устройства позволяют получать эффективные и недорогие решения при оборудовании объекта вычислительной техники с большим количеством средств вычислительной техники. Данная модель является одним из наиболее популярных устройств по защите электрических каналов и имеет совместимость с системой Соната «АВ» модель 4Б, которая была выбрана в качестве устройства для защиты виброакустического канала.

2.5.3 Средства защиты информации от побочных электромагнитных излучений и наводок (ПЭМИН)

ПЭМИН предполагает использование генераторов шума в помещении, где установлены средства обработки конфиденциальной информации. Зашумление обеспечивается генераторами. Типы генераторов представлены в таблице 6.

Таблица 6 – Сравнительный анализ средств активной защиты от ПЭМИН

Устройство	Цена, руб.	Состав
СКИТ-МШ	16 800	Широкополосный генератор электромагнитных помех
Генератор шума Пульсар	24 525	Имеет защиту регулятора уровня выходного шумового сигнала от несанкционированного доступа, сигнализирует о таковом. Имеет индикаторы нормального режима работы (диод) и аварийного режима (свет и звук).
СОНАТА-РЗ	97 200	Изделие обеспечивает защиту от утечки за счет побочных электромагнитных излучений и наводок путем излучения в окружающее пространство электромагнитного поля шума, а также наводок на линии сети электропитания и заземления путем индицирования в них маскирующих шумовых напряжении
Генератор шума SEL SP-21B2 "Спектр"	112 000	Генератор шума переносной портативный, диапазон частот 0,1–1000 МГц

Выберем СОНАТА-РЗ. Он совместим с выбранными ранее средствами активной защиты по виброакустическому и электрическому каналам. Также у СОНАТА-РЗ есть сертификат ФСТЭК.

2.5.4 Средства защиты информации от утечек по оптическим каналам

Для прекращения функционирования оптического канала утечки информации через окно можно применить следующие меры:

- шторы на окнах;
- жалюзи;
- тонированные пленки на стеклах.

Шторы – традиционные средства для предотвращения скрытного наблюдения через окна кабинета, но они существенно ухудшают естественную освещенность кабинета и накапливают пыль.

Тонированные пленки на стеклах исключают возможность наблюдения за объектами защиты в кабинете, незначительно уменьшают освещенность кабинета, но позволяют легко выявить окна помещений с повышенными требованиями к безопасности информации.

Наиболее приемлемый вариант защиты – жалюзи на окнах. Они не только исключают возможность наблюдения через окно, но и эффективны по основному назначению – защите от солнечных лучей.

Для прекращения функционирования оптического канала утечки информации через приоткрытую дверь можно применить доводчик двери, который плавно и до конца закрывает дверь.

2.6 Описание расстановки технических средств защиты информации

Согласно информации, приведённой в предыдущих пунктах, выбранные средства защиты информации включают в себя:

- усиленные двери (4 мм+), обшитые металлом (2 мм+) со звукоизолирующей прокладкой на металлическом каркасе;
- система Соната-АВ-4Б;
- устройство Соната-РС3;
- устройство Соната-Р3;
- жалюзи на окна;
- доводчики на двери.

Перейдём к оценке количества компонентов и расстановке выбранных технических средств. Согласно руководству по эксплуатации «Система

вибраакустической и акустической защиты "Соната-АВ". Руководство по эксплуатации» для предварительной оценки необходимого количества излучателей необходимо исходить из следующих норм:

- один на каждые 3...5 метров периметра для капитальной стены при условии установки излучателей на уровне половины высоты помещения;
- один на каждые 15...25 м² перекрытия потолка/пола;
- один на каждое окно (при установке на оконный переплет);
- один на каждую дверь (при установке на верхнюю перекладину дверной коробки);
- один на каждую трубу системы (водо-/тепло-/газо-)снабжения.

Ориентировочное количество пьезоизлучателей может быть определено из расчета: один ПИ-45 на каждое стекло.

Необходимое количество аудиоизлучателей можно оценить из следующих норм:

- один на каждый вентиляционный канал или дверной тамбур;
- один на каждые 8...12 м³ надпотолочного пространства или других пустот.

Основным правилом, которым следует руководствоваться при выборе мест установки излучателей в каждом конкретном помещении, является обеспечение максимального уровня вибрационного и акустического шума в предполагаемом канале утечки информации при обеспечении приемлемого уровня мешающего акустического шума в защищаемом помещении.

В таблице 7 приведена смета затрат на выбранные средства защиты информации.

Таблица 7 – Смета на выбранные средства защиты информации

Средство защиты	Цена, руб.	Количество, шт.	Стоимость, руб.
Усиленная звукоизолирующая дверь Ultimatum Next ПВХ	91 681	2	183 362

Средство защиты	Цена, руб.	Количество, шт.	Стоимость, руб.
Система Соната-АВ-4Б	44 200	1	44 200
Устройство Соната-РС3	32 400	1	32 400
Устройство Соната-РЗ	97 200	1	97 200
Блок электропитания и управления Соната-ИП4.3	21 600	1	21 600
Генератор акустоизлучатель Соната- СВ-4Б1	3 540	32	113 280
Генератор вибровозбудитель Соната- СВ-4Б	7 440	40+42+26+9	870 480
Размыкатель телефонной линии Соната ВК4.1	6 000	4	24 000
Размыкатель слаботочной линии Соната ВК4.2	6 000	1	6 000
Размыкатель линии «Ethernet» Соната ВК4.1	6 000	2	12 000
Пульт управления Соната-ДУ 4.3	7 680	1	7 680
Горизонтальные жалюзи Унистайл	1 990	13	25 870
Дверной доводчик Geze TS 4000/2000	1 118	14	15 652
Итого:			1 453 724

Усиленная звукоизолирующая дверь стоит в архиве и переговорной. Жалюзи установлены на каждом окне, а доводчики на каждой двери, кроме внутренних дверей в туалете. Элементы комплексной системы Соната-АВ-4Б расположены в соответствии с рисунком 5. Соната-РС3 подключена к системе электроснабжения согласно рекомендациям производителя. Соната-РЗ подключена напрямую к Соната-ИП4.3.

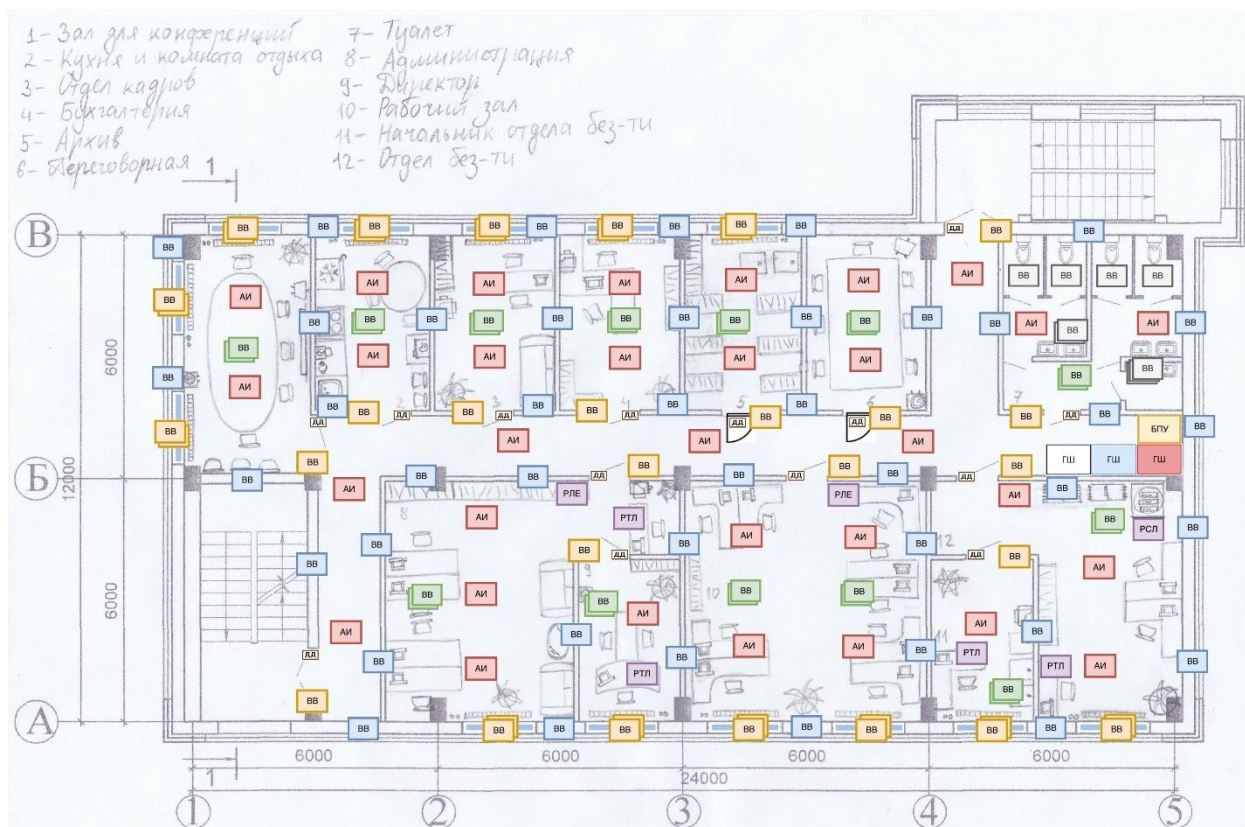
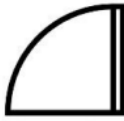

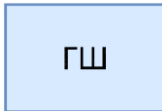

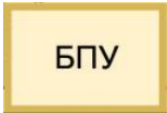
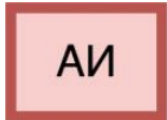


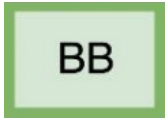

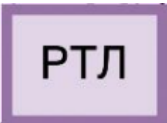
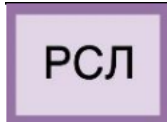
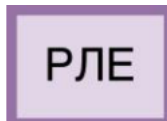
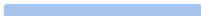



Рисунок 5 – Схема расстановки устройств

В таблице 8 приводится расшифровка условных обозначений схемы расстановки устройств.

Таблица 8 – Условные обозначения схемы расстановки устройств

Средство защиты	Условное обозначение
Усиленная звукоизолирующая дверь Ultimatum Next PBX	
Система Соната-АВ-4Б	
Устройство Соната-РС3	
Устройство Соната-Р3	

Средство защиты	Условное обозначение
Блок электропитания и управления Соната-ИП4.3	
Генератор акустоизлучатель Соната- СВ-4Б1	
Генератор вибровозбудитель Соната-СВ-4Б (двери/окна/батареи, стены, пол/потолок, трубы)	   
Размыкатель телефонной линии Соната ВК4.1	
Размыкатель слаботочной линии Соната ВК4.2	
Размыкатель линии «Ethernet» Соната ВК4.1	
Горизонтальные жалюзи Унистайл	
Дверной доводчик Geze TS 4000/2000	

ЗАКЛЮЧЕНИЕ

В результате выполнения данной работы был проведен теоретический анализ технических каналов утечки информации. Далее были определены руководящие документы, а также проведен анализ защищаемых помещений, проведена оценка каналов утечки информации и выбраны меры пассивной и активной защиты информации.

По итогам работы была составлена смета на основе действующих цен на технические средства защиты информации, итоговое значение суммы затрат составило 1 453 724 рублей.

В заключении, на схеме были расставлены все средства защиты в соответствии с нормами и правилами.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждено 30.08.2002 приказом Председателя Гостехкомиссии России No 282.
2. ГОСТ Р 50.1.056–2005 «Техническая защита информации. Основные термины и определения».
3. Руководящий документ Государственной технической комиссии при Президенте РФ «Классификация автоматизированных систем и требований по защите информации» от 30 марта 1992 г.
4. «Система виброакустической и акустической защиты "Соната-АВ". Руководство по эксплуатации» - Москва.
5. Решение Межведомственной комиссии по защите государственной тайны от 21 января 2011 г. N 199 "О Типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними".
6. Detector System. Средства защиты переговоров [HTML] (https://detsys.ru/catalog/sredstva_zashchity_peregovorov/) (Дата обращения: 18.12.2022).