

**Министерство науки и высшего образования Российской Федерации  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет безопасности информационных технологий**

**Дисциплина:**

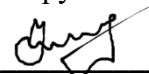
«Инженерно-технические средства защиты информации»

**ОТЧЕТ ПО КУРСОВОЙ РАБОТЕ**

«Проектирование системы защиты от утечки информации по различным каналам»

**Выполнил:**

Усольцев Артем Павлович, студент группы N34511



(подпись)

**Проверил:**

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

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023 г.

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

**ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ**

**Студент** Усольцев А.П.

(Фамилия И.О.)

**Факультет** Безопасности информационных технологий

**Группа** N34511

**Направление (специальность)** Информационная безопасность

**Руководитель** Попов И.Ю., 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. Вариант 126

**Задание** Проанализировать возможные каналы утечки информации в помещении, разработать меры пассивной и активной защиты информации, рассчитать их стоимость.

**Краткие методические указания**

**Содержание пояснительной записки**

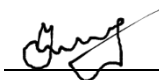
Курсовая работа содержит введение, теоретическую часть, анализ защищаемых помещений, выбор средств защиты информации, расчет стоимости мер защиты, заключение, список использованных источников.

**Рекомендуемая литература**

**Руководитель** \_\_\_\_\_

(Подпись, дата)

**Студент** \_\_\_\_\_



19.12.2023

(Подпись, дата)

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

**ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

**Студент** Усольцев А.П.

(Фамилия И.О.)

**Факультет** Безопасности информационных технологий

**Группа** N34511

**Направление (специальность)** Информационная безопасность

**Руководитель** Попов И.Ю., 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. Вариант 126

№ п/п	Наименование этапа	Дата завершения	
		Планируемая	Фактическая
1	Разработка и утверждение задания и календарного плана на курсовую работу	26.09.2023	26.09.2023
2	Создание плана курсовой работы	10.10.2023	10.10.2023
3	Анализ теоретической составляющей	17.11.2023	17.11.2023
4	Разработка комплекса инженерно-технической защиты информации в заданном помещении	01.12.2023	01.12.2023
5	Представление выполненной курсовой работы	19.12.2023	19.12.2023

**Руководитель**

(Подпись, дата)

**Студент**

19.12.2023

(Подпись, дата)

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

**АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ**

Студент Усольцев А.П.

(Фамилия И.О.)

Факультет Безопасности информационных технологий

Группа N34511

Направление (специальность) Информационная безопасность

Руководитель Попов И.Ю., 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. Вариант 126

**ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)**

**1. Цель и задачи работы**

☐ Предложены студентом

☐ Сформулированы при участии студента

☒ Определены руководителем

**2. Характер работы**

☐ Расчет

☐ Конструирование

☐ Моделирование

☒ Другое: Отчет

**3. Содержание работы**

Курсовая работа включает разделы: введение, постановка задач, технические каналы утечки информации, перечень руководящих документов, анализ защищаемых помещений, выбор средств защиты в соответствии с каналами утечки информации, заключение.

**4. Выводы**

В результате выполнения работы был проведен анализ каналов утечки информации в помещениях предприятия, разработаны меры пассивной и активной защиты информации, рассчитана стоимость предложенных мер.

Руководитель \_\_\_\_\_

(Подпись, дата)

Студент 

19.12.2023

(Подпись, дата)

«19» декабря 2023

## СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	6
ПОСТАНОВКА ЗАДАЧ .....	7
1     ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ.....	8
2     ПЕРЕЧЕНЬ РУКОВОДЯЩИХ ДОКУМЕНТОВ.....	10
3     АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ .....	21
3.1     Сведения о защищаемой организации.....	21
3.2     Описание помещения .....	22
3.3     Обоснование необходимости защиты информации.....	24
4     ВЫБОР СРЕДСТВ ЗАЩИТЫ В СООТВЕТСТВИИ С КАНАЛАМИ УТЕЧКИ ИНФОРМАЦИИ .....	25
4.1     Определение каналов утечки информации в помещениях.....	25
4.2     Анализ рынка и выбор средств защиты .....	26
4.2.1     Средства защиты информации от утечек по (вибро-)акустическому каналу .....	26
4.2.2     Средства защиты информации от утечек по электрическим, акустоэлектрическим и электромагнитным каналам .....	28
4.2.3     Средства защиты информации от побочных электромагнитных излучений и наводок.....	30
4.2.4     Средства защиты информации от утечек по оптическим каналам .....	31
5     Расстановка средств защиты.....	32
ЗАКЛЮЧЕНИЕ.....	36
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ .....	37

## **ВВЕДЕНИЕ**

Атомная энергетика остается ключевой отраслью для многих государств, обеспечивая энергетическую самодостаточность и способствуя промышленному развитию. Надежная работа атомных комплексов обеспечивает стабильные поставки электроэнергии и высокий уровень жизни населения. Следовательно, обеспечение безопасности этих объектов становится приоритетной задачей для государств.

Одной из ключевых угроз, с которыми сталкиваются объекты атомной энергетики, является утечка информации – как непреднамеренная, так и преднамеренная. Предотвращение таких утечек требует обеспечения надежной защиты всех каналов передачи информации. Для обеспечения безопасности используются различные технические решения, направленные на предотвращение несанкционированного распространения информации и перекрытие возможных каналов утечки.

Данная работа направлена на разработку комплекса инженерно-технических решений для защиты информации в административных помещениях атомной электростанции. В состав данного офисного пространства входят рабочие кабинеты, переговорные, архивное хранилище, общие помещения и другие зоны. Учитывая статус данных помещений как административного центра атомной электростанции, особое внимание уделяется защите информации, отнесенной к категории государственной тайны уровня "секретно".

## ПОСТАНОВКА ЗАДАЧ

Целью данной курсовой работы является разработка комплекса инженерно-технической защиты информации, составляющей государственную тайну с уровнем секретности «секретно».

Для достижения цели работы необходимо выполнить следующие задачи:

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

## **1 ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ**

Утечка информации - бесконтрольный выход информации за пределы организации или предприятия, которым она была доверена по службе или стала известна в процессе работы.

Утечка информации может быть следствием добровольного или принудительного разглашения информации, ухода информации по различным каналам или же несанкционированного доступа к информации.

Согласно теме курсовой работы, рассматриваться будет именно утечка информации по техническим каналам.

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

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

На вход ТКУИ поступает информация в виде первичного сигнала. Источниками сигнала могут являться:

- отраженные электромагнитные и акустические волны;
- собственные 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, проходит через среду распространения и записывается на носитель информации после преобразования передатчиком. Средой распространения сигнала в данном будет являться физическая среда, внутри которой сигнал может распространяться и регистрироваться.

Основными параметрами среды являются:

- наличие физических препятствий;
- мера ослабления сигнала на единицу длины;
- частотная характеристика;
- вид и мощность помех для сигнала.



Общая классификация технических каналов утечки информации представлена на рисунке 1.



Рисунок 1 – Общая классификация технических каналов утечки информации

## **2 ПЕРЕЧЕНЬ РУКОВОДЯЩИХ ДОКУМЕНТОВ**

В данном списке находятся основные документы, регулирующие деятельность в области предотвращения утечки информации по техническим каналам:

- «Вопросы Государственной технической комиссии при Президенте Российской Федерации» от 19 февраля 1999 г. No212.
- «Вопросы защиты государственной тайны» от 30.03.1994 г. No614.
- «Об утверждении перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г. No1203.
- «О межведомственной комиссии по защите государственной тайны» от 8 ноября 1995 г. No1108.
- «Вопросы Межведомственной комиссии по защите государственной тайны» от 20 января 1996 г. No71 с изменениями, внесенными Указами Президента Российской Федерации от 21 апреля 1996 г. No573, от 14 июня 1997 г. No594.
- «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. No644.
- «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. No188.
- Инструкция No0126–87.
- 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. No921– 51.
- «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» от 3 ноября 1994 г. No1233.
- «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 15 апреля 1995 г. No333.
- «О внесении дополнения в Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств

защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 30 апреля 1997 г. №513.

- «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 4 сентября 1995 г. №870.

- «Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам» от 2 августа 1997 г. №973.

- «О сертификации средств защиты информации» от 26 июня 1995 г. №608.

Ниже представлены законы Российской Федерации, которые необходимо учитывать в работе:

- «О государственной тайне» от 21 июля 1993 г. №5151–1.

- «Об информации, информатизации и защите информации» от 20 февраля 1995 г. №24-ФЗ.

- «О безопасности» от 5 марта 1992 г. №2446–1.

- «О федеральных органах правительственной связи и информации» от 19 февраля 1993 г. №4524–1.

- «О связи» от 16 февраля 1995 г. №15-ФЗ.

- «Об участии в международном информационном обмене» от 4 июля 1996 г. №85-ФЗ.

Ниже представлен перечень распорядительных документов ФСТЭК:

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

- СТР-К. Специальные требования и рекомендации по технической защите конфиденциальной информации.

- Методика сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров.

- Временные методики сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров по требованиям безопасности информации.

- Временный порядок аттестации объектов информатизации по требованиям безопасности информации.

- Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения.

- Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.

– Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.

– Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники.

– Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации.

– Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования.

– Руководящий документ Гостехкомиссии России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей.

– Руководящий документ. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам.

Требования по защите информации на объектах типа АЭС сформулированы на основе следующих документов:

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

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

- i. Статья 23. Государственное регулирование безопасности при использовании атомной энергии
- ii. Статья 25. Полномочия органов государственного регулирования безопасности
- iii. Статья 26. Разрешения (лицензии) на право ведения работ в области использования атомной энергии
- iv. 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»
  - a. Статья 3. Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры
  - b. Статья 4. Принципы обеспечения безопасности критической информационной инфраструктуры
  - c. Статья 10. Система безопасности значимого объекта критической информационной инфраструктуры
  - d. Статья 11. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры
  - e. Статья 12. Оценка безопасности критической информационной инфраструктуры
  - f. 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»
  - a. Раздел VI. Защита государственной тайны
    - i. Статья 21. Допуск должностных лиц и граждан к государственной тайне
    - ii. Статья 21.1. Особый порядок допуска к государственной тайне
    - iii. Статья 22. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне
    - iv. Статья 23. Условия прекращения допуска должностного лица или гражданина к государственной тайне
    - v. Статья 24. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне
    - vi. Статья 25. Организация доступа должностного лица или гражданина к сведениям, составляющим государственную тайну
    - vii. Статья 26. Ответственность за нарушение законодательства Российской Федерации о государственной тайне

- viii. Статья 27. Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну
      - ix. 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»
  - a. Обеспечение средствами стандартизации необходимого уровня безопасности объектов использования атомной энергии
  - b. Обеспечение единой технической политики в сфере стандартизации в отношении обеспечения безопасности объектов использования атомной энергии
  - c. 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»
  - a. Пункт 2. Ограничения на въезд и пребывание граждан на территории зоны безопасности
  - b. 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»
  - a. Пункт 2. Требования к организации защиты информации в автоматизированной системе управления

- i. Разработка системы защиты автоматизированной системы управления
    - ii. Внедрение системы защиты автоматизированной системы управления и ввод ее в действие
    - iii. Обеспечение защиты информации в ходе эксплуатации автоматизированной системы управления
    - iv. Обеспечение защиты информации при выводе из эксплуатации автоматизированной системы управления
  - b. 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»
- a. Пункт 3. Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов критической информационной инфраструктуры
  - b. Пункт 4. Требования к организационно-распорядительным документам по безопасности значимых объектов
  - c. 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»
- a. Пункт 2. Требования к обеспечению безопасности в ходе создания, эксплуатации и вывода из эксплуатации значимых объектов
    - i. Установление требований к обеспечению безопасности значимого объекта
    - ii. Разработка организационных и технических мер по обеспечению безопасности значимого объекта
    - iii. Внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие

- iv. Обеспечение безопасности значимого объекта в ходе его эксплуатации
- v. Обеспечение безопасности значимого объекта при выводе его из эксплуатации
- b. Пункт 3. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов
- c. 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)
  - a. 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)
  - a. Пункт 2. Общие требования к локализирующим системам безопасности атомных станций
  - b. 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. ИСО 50001-2023 «Системы энергетического менеджмента. Требования и руководство по применению»
  - a. 9.1 Требование бизнеса по управлению доступом
  - b. 9.2 Процесс управления доступом пользователей



- с. 9.3 Ответственность пользователей
  - d. 9.4 Управление доступом к системам и приложениям
  - e. 10.1 Средства криптографической защиты информации
  - f. 13.1 Менеджмент информационной безопасности сетей
  - g. 13.2 Передача информации
13. ГОСТ Р ИСО/МЭК 13335-1-2006. «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 1.
14. 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»
15. 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»
16. ГОСТ Р МЭК 61513-2011 Атомные станции. Системы контроля и управления, важные для безопасности. Общие требования.
- a. 5 Общий жизненный цикл безопасности систем контроля и управления
    - i. 5.2 Получение требований систем контроля и управления из проектных основ безопасности атомной станции
    - ii. 5.3 Выходная документация
    - iii. 5.4 Проектирование общей архитектуры систем контроля и управления и назначение функций систем контроля и управления
    - iv. 5.5 Общее планирование
    - v. 5.6 Выходная документация
  - b. 6 Жизненный цикл системы безопасности
    - i. 6.2 Требования
    - ii. 6.3 Планирование системы
    - iii. 6.4 Выходная документация

- iv. 6.5 Квалификация системы
  - c. 7 Общая интеграция и ввод в эксплуатацию
    - i. 7.2 Цели, которые должны быть достигнуты
    - ii. 7.3 Выходная документация
  - d. 8 Общая эксплуатация и техническое обслуживание
    - i. 8.2 Цели, которые должны быть достигнуты
    - ii. 8.3 Выходная документация
17. МЭК ТО 63415-2023 «Атомные станции. Системы контроля и управления. Применение формальных моделей киберзащищенности для проектирования и оценки архитектуры киберзащищенности контроля и управления»
- И другие стандарты международной электротехнической комиссии (МЭК/IEC) – IEC 60880:2006, IEC 62645:2014, IEC 62859:2016, проект IEC 63096
18. Документы международного агентства по атомной энергии – NSS 17, NST036, NST037, NST038, NST045, NST047
19. ГОСТ Р МЭК 61226-2011. «Атомные станции. Системы контроля и управления, важные для безопасности. Классификация функций контроля и управления»
- a. 6 Процедура классификации
    - i. 6.2 Определение основ проекта
    - ii. 6.3 Идентификация и классификация функций
  - b. 7 Установление технических требований по категориям
    - i. 7.2 Требования, относящиеся к функциям
    - ii. 7.3 Требования, относящиеся к системам контроля и управления
    - iii. 7.4 Требования к оборудованию
    - iv. 7.5 Требования, связанные с аспектами качества
20. ГОСТ Р ИСО/МЭК 27001-2021 «Системы менеджмента информационной безопасности. Требования»
- a. 5 Руководство
    - i. 5.2 Политика
    - ii. 5.3 Роли, обязанности и полномочия в организации
  - b. 6 Планирование
    - i. 6.1 Действия по рассмотрению рисков и возможностей

- ii. 6.2 Цели информационной безопасности и планы по их достижению
    - c. 7 Обеспечение и поддержка
      - i. 7.1 Ресурсы
      - ii. 7.2 Квалификация
      - iii. 7.3 Осведомленность
      - iv. 7.4 Взаимодействие
      - v. 7.5 Документированная информация
    - d. 8 Функционирование
      - i. 8.1 Оперативное планирование и контроль
      - ii. 8.2 Оценка рисков информационной безопасности
      - iii. 8.3 Обработка рисков информационной безопасности
    - e. 9 Оценивание исполнения
      - i. 9.1 Мониторинг, оценка защищенности, анализ и оценивание
      - ii. 9.2 Внутренний аудит
      - iii. 9.3 Проверка со стороны руководства
21. ГОСТ Р ИСО/МЭК 27002-2021 «Свод норм и правил применения мер обеспечения информационной безопасности»
- a. 5 Политики информационной безопасности
    - i. 5.1 Руководящие указания в части информационной безопасности
  - b. 6 Организация деятельности по информационной безопасности
    - i. 6.1 Внутренняя организация деятельности по обеспечению информационной безопасности
  - c. 8 Менеджмент активов
    - i. 8.1 Ответственность за активы
    - ii. 8.2 Категорирование информации
    - iii. 8.3 Обращение с носителями информации
  - d. 9 Управление доступом
22. ГОСТ Р ИСО/МЭК 13335-1-2006 Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»
- a. 3 Концепции безопасности и взаимосвязи
    - i. 3.2 Активы
    - ii. 3.3 Угрозы

- iii. 3.4 Уязвимости
- iv. 3.5 Воздействие
- v. 3.6 Риск
- vi. 3.7 Защитные меры
- vii. 3.8 Ограничения
- viii. 3.9 Взаимосвязь компонентов безопасности

23. ГОСТ Р 56205-2014 ИЕС/TS 62443-1-1:2009. «Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели»

- a. 5 Базовые концепции
  - i. 5.6 Оценка угроз и рисков
  - ii. 5.7 Степень завершенности программ безопасности
  - iii. 5.8 Политики безопасности

### **3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ**

#### **3.1 Сведения о защищаемой организации**

Наименование организации: «СПбАЭС».

Область деятельности: Электроэнергетика и производство ядерной энергии.

Прибыль (месячная/годовая): 0.5 млрд руб/мес, 6 млрд руб/год.

Расходы:

- Топливо - 5 млрд руб/год;
- Утилизация отходов - 1 млрд руб/год;
- Обслуживание и ремонт - 5 млрд руб/год;
- Безопасность - 0.5 млрд руб/год;
- Вывод из эксплуатации - до 100 млрд руб;
- Оплата труда - 0.5 млрд руб/год;
- Страхование, лицензирование - 50 млн руб/год;
- Прочие административные расходы - 10 млн руб/год;

Стоимость информационных активов:

- Информационные системы - 80 млн руб;
- ПО - 90 млн руб;
- Базы данных - 300 млн руб;
- Коммуникационные системы - 50 млн руб;
- Информационная безопасность - 80 млн руб.

Персонал организации:

- административно-управленческий и общецеховой персонал (начальник цеха или отдела, его заместители, экономист, кладовщик, технологи);
- оперативный персонал (имеется в составе подразделений, непосредственно связанных с реализацией и обеспечением непрерывного круглосуточного технологического процесса на АЭС);
- ремонтный персонал;
- службы, производственные участки и бригады;
- лаборатории, состоящие иногда из нескольких групп.

Установленная мощность СПбАЭС - 4000 МВт. Численность персонала - 5000 человек.

На рисунке 2 представлена схема информационных потоков предприятия.

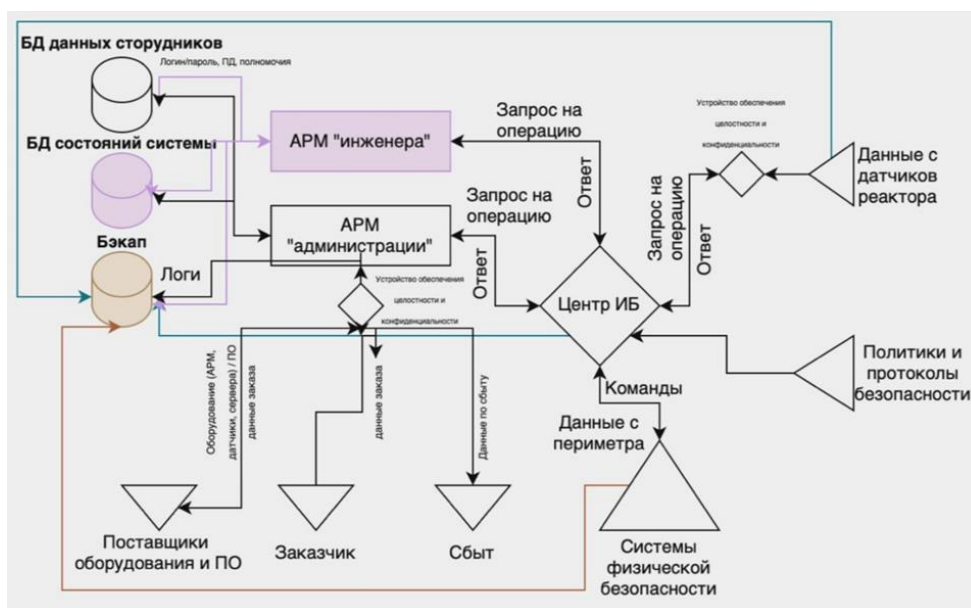


Рисунок 2 – Схема информационных потоков

На рисунке 3 представлена организационная структура предприятия.



Рисунок 3 – Организационная структура предприятия

### 3.2 Описание помещения

Перед тем, как перейти к разработке комплекса инженерно-технической защиты информации, необходимо описать выбранные помещения. На рисунке 4 представлен план объекта (административный офис «СПБАЭС»).



Рисунок 4 – План административного офиса

Рассматриваемые помещения имеют следующую площадь:

- кабинет директора: 17.02 м<sup>2</sup>;
- рабочая зона: 42.93 м<sup>2</sup>;
- архив: 24.58 м<sup>2</sup>;
- переговорная: 19.69 м<sup>2</sup>;
- санузел: 10.77 м<sup>2</sup>;
- свободная зона: 46.77 м<sup>2</sup>.

Кабинет директора оборудован креслом, двумя столами, автоматизированным рабочим местом (АРМ), двумя тумбами и вешалкой-стойкой.

Рабочая зона предназначена для коллективной работы сотрудников и содержит 12 столов, кресел и АРМ'ов. Также в ней установлено 6 тумб, 4 стеллажа, кулер для воды и 2 вешалки-стойки.

В архиве находятся 6 стеллажей, 2 тумбы, стол, кресло и АРМ.

Переговорная оборудована 1 большим столом, 6 стульями, тумбой, магнитно-маркерной доской и 2 вешалками.

Санузел представлен в виде одного помещения с 6 унитазами и 2 раковинами.

Свободная зона предназначена для перемещения по этажу, в ней находится 1 столик и диван.

В каждом помещении, кроме свободной зоны и санузла, установлены радиаторы (кабинет директора – 1 радиатор, остальные помещения – 2 радиатора), также каждое помещение, за исключением свободной зоны, оборудовано вентиляцией.

Помещение расположено на втором этаже малоэтажного здания, окна выходят в закрытый контролируемый двор. Окна не соседствуют с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и прочими элементами, с которых в помещения могут проникнуть посторонние лица. Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см. Часть внутренних перегородок железобетонные, толщиной не менее 5 см, другая часть сделана из звукоизоляционного гипсокартона.

### **3.3 Обоснование необходимости защиты информации**

Объектом защиты в рамках данной работы является офис управления на ядерной электростанции. В соответствии с Практическим руководством по обеспечению безопасности ядерной информации, разработанным Международным агентством по атомной энергии (МАГАТЭ), самым высоким уровнем конфиденциальности для предприятий данного типа является уровень "секретно".

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».

В класс 1В включены многопользовательские автоматизированные системы, где информация различных уровней конфиденциальности обрабатывается и хранится одновременно, и не все пользователи имеют доступ ко всей информации системы. Кроме того, в таких системах обрабатывается информация не выше уровня "секретно".

В нашем случае в автоматизированной системе присутствуют как административные руководители, так и подчиненные, работники архива, экономического и научного отделов, которые не должны иметь доступа к информации из других отделов и к личным данным других сотрудников. Следовательно, определим уровень защищенности автоматизированной системы как 1В.



## **4 ВЫБОР СРЕДСТВ ЗАЩИТЫ В СООТВЕТСТВИИ С КАНАЛАМИ УТЕЧКИ ИНФОРМАЦИИ**

### **4.1 Определение каналов утечки информации в помещениях**

В большинстве помещений расположены стеллажи, шкафы и тумбы, которые могут использоваться для скрытия устройств для слежки.

Также, в большей части помещений находятся средства вычислительной техники (АРМ'ы), что создает потенциальные каналы утечки информации через электрический и электромагнитный каналы.

Помещения расположены на втором этаже, из-за чего существует угроза потенциального сбора информации через оптические и акустические каналы.

Во всех помещениях находятся радиаторы или вентиляции, с которых возможен съем информации в виде вибраций. Соответственно, имеет место быть вибрационный канал утечки.

Материально-вещественный канал утечки информации в данном случае исключается ввиду строгой политики компании, касающейся учета физических носителей информации.

Перечень средств защиты информации, необходимых для обеспечения комплексной безопасности в соответствии с определенным уровнем конфиденциальности информации - государственной тайны уровня "секретно", - представлен в таблице 1.

Таблица 1 – Активная и пассивная защита информации.

<b>Каналы утечки информации</b>	<b>Источники</b>	<b>Возможная пассивная защита</b>	<b>Возможная активная защита</b>
Вибрационный / виброакустический	Твердые поверхности: вентиляционные шахты, радиаторы	Изолирующие звук и вибрацию обшивки стен	Устройства вибрационного зашумления
Акустический / акустоэлектрический	Окна, двери, проводка	Звукоизоляция переговорной комнаты, фильтры для сетей электропитания	Устройства акустического зашумления

<b>Каналы утечки информации</b>	<b>Источники</b>	<b>Пассивная защита</b>	<b>Активная защита</b>
Оптический	Окна и двери	Жалюзи или шторы, тонирующие пленки, доводчики на дверях	Бликующие устройства
Электромагнитный / электрический	АРМы, электросети	Фильтры для сетей электропитания	Устройства электромагнитного зашумления

К пассивным техническим средствам защиты относятся экранирующие устройства и сооружения, маски различного назначения, разделительные устройства в сетях электроснабжения, защитные фильтры. Цель пассивного способа защиты – максимально ослабить сигнал от источника информативного сигнала, например, за счет отделки стен звукопоглощающими материалами или экранирования технических средств.

Активными же техническими средствами защиты являются устройства, обеспечивающие создание маскирующих активных помех (или имитирующих их) для средств технической разведки или нарушающие нормальное функционирование средств негласного съема информации. Активные способы предупреждения утечки информации можно подразделить на обнаружение и нейтрализацию этих устройств.

## **4.2 Анализ рынка и выбор средств защиты**

Рассмотрим различные средства защиты информации от утечек по определенным ранее каналам.

### **4.2.1 Средства защиты информации от утечек по (вибро-)акустическому каналу**

В качестве средств пассивной защиты (вибро-)акустического канала утечки информации будем использовать усиленные двери, а также дополнительную отделку переговорной звукоизолирующими материалами.

Активная защита представляет собой систему виброакустического зашумления.

Проведем сравнительный анализ подходящих средств активной защиты помещений от утечек информации по виброакустическому каналу (таблица 2).

Таблица 2 – Сравнение средств активной защиты от утечек по (вибро-)акустическим каналам

Устройство	Стоимость, руб	Частотный диапазон:, Гц	Состав системы
Соната «АВ» 4Б	44 200	175-11200	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 оптикоэлектронному (лазерному) каналу.
Буран	63 300	100-11200	Виброакустический генератор, вибропреобразователь для стен, вибропреобразователь для коммуникаций, вибропреобразователь для рам, вибропреобразователь для окон, преобразователь акустический, модуль дистанционного управления по проводному каналу, размыкатель аналоговых телефонных линий, размыкатель линий оповещения и сигнализации, размыкатель компьютерных сетей

Устройство	Стоимость, руб	Частотный диапазон, Гц	Состав системы
ЛГШ-404	51 900	175-11200	Генераторный блок, вибровозбудитель, акустический излучатель, виброекран, размыкатель слаботочных линий, размыкатель телефонных линий, размыкатель для Ethernet

По результатам анализа была выбрана система Соната «АВ» модели 4Б, так как:

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

#### **4.2.2 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.

Проведем сравнительный анализ подходящих средств активной защиты помещений от утечек информации по электрическим каналам (таблица 3).

Таблица 3 – Сравнение средств активной защиты от утечек по электрическим каналам

Устройство	Стоимость, руб.	Особенности
Соната-РС2	23 600	Частотный диапазон: до 2 ГГц. Регулировка уровня шума в 3 частотных полосах. Светодиодная и звуковая индикация системы контроля интегрального уровня шумового напряжения. Возможно дистанционное включение прибора с пульта управления
Соната-РС3	32400	Частотный диапазон до 2 ГГц. 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 СОНАТА.
Сетевой генератор шума ЛГШ-221	36400	Частотный диапазон: 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».
Двухканальный генератор зашумления SEL SP-44	24000	Частотный диапазон: 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 доступных устройств был выбран генератор шума Соната-РС3. Этот конкретный тип совместим с ранее выбранной системой Соната «АВ» модели 4Б, что упрощает процесс установки всей системы без необходимости дополнительной настройки

или адаптации. Превосходит свою прошлую версию «Соната-РС2» функционалом. Помимо этого, данное устройство отличается высокой эффективностью и при этом имеет относительно низкую стоимость, что делает его привлекательным выбором для обеспечения необходимой защиты системы.

#### **4.2.3 Средства защиты информации от побочных электромагнитных излучений и наводок**

Защита от ПЭМИН предполагает использование генераторов шума в помещении, где установлены средства обработки конфиденциальной информации.

Проведем сравнительный анализ подходящих генераторов (таблица 4).

Таблица 4 – Сравнение средств активной защиты от ПЭМИН

<b>Устройство</b>	<b>Стоимость, руб.</b>	<b>Особенности</b>
Генератор шума «Пульсар»	24 525	Диапазон регулировки уровня выходного шумового сигнала не менее 20 дБ. Количество переключаемых уровней выходного шумового сигнала – 5. Вид индикации: светодиодная + звуковая
Соната-РЗ	97 200	Возможность дополнительного повышения уровня излучаемого электромагнитного поля шума в диапазоне частот 0,01...200 МГц за счет применения опционально поставляемой дополнительной антенны ВЕЕР. Вид индикации: светодиодная + звуковая.
Генератор шума ЛГШ-504	156 000	Низкочастотный/высокочастотный сигнал. Частотный диапазон: 0,009-1000 МГц. Управление: ПАК Паутина по Ethernet. Предусмотрена регулировка уровня шума.

Поскольку существенных преимуществ той или иной модели выявлено не было, выберем устройство Соната-РЗ, учитывая среднюю цену и совместимость с другими устройствами линейки СОНАТА.

#### **4.2.4 Средства защиты информации от утечек по оптическим каналам**

Для защиты информации от утечки по оптическому каналу можно применить следующие средства пассивной защиты: шторы, тонированные пленки на стеклах, жалюзи. Поскольку первые два средства имеют недостаток в виде существенного ухудшения освещенности помещения, в качестве средства пассивной защиты будем использовать жалюзи.

Для защиты информации от утечки по оптическому каналу утечки информации через приоткрытую дверь можно применить доводчик двери, который будет способствовать закрытию дверей и блокировать возможность наблюдения за выбранным помещением из соседних.

## 5 РАССТАНОВКА СРЕДСТВ ЗАЩИТЫ

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;
- жалюзи на окна;
- доводчики на двери;
- система Соната «АВ» модели 4Б;
- генератор шума Соната-РСЗ;
- генератор шума Соната-РЗ.

Согласно руководству по эксплуатации системы "Соната-АВ", для предварительной оценки необходимого количества излучателей необходимо исходить из следующих норм:

- стены - один на каждые 3...5 метров периметра для капитальной стены при условии установки излучателей на уровне половины высоты помещения;
- потолок, пол - один на каждые 15...25 м<sup>2</sup> перекрытия;
- один на окно (при установке на оконный переплет);
- один на дверь (при установке на верхнюю перекладину дверной коробки);
- трубы систем водо- (тепло- и газо-) снабжения - один на каждую вертикаль (отдельную трубу) вида коммуникаций.

Пьезоизлучатели ставятся по одному на стекло.

Необходимое количество аудиоизлучателей можно предварительно оценить из следующих норм:

- один на каждый вентиляционный канал или дверной тамбур;
- один на каждые 8...12 м<sup>3</sup> надпотолочного пространства или др. пустот.

С учетом данных норм расположим элементы комплексной системы Соната-АВ-4Б на плане. Результат представлен на рисунке 5.



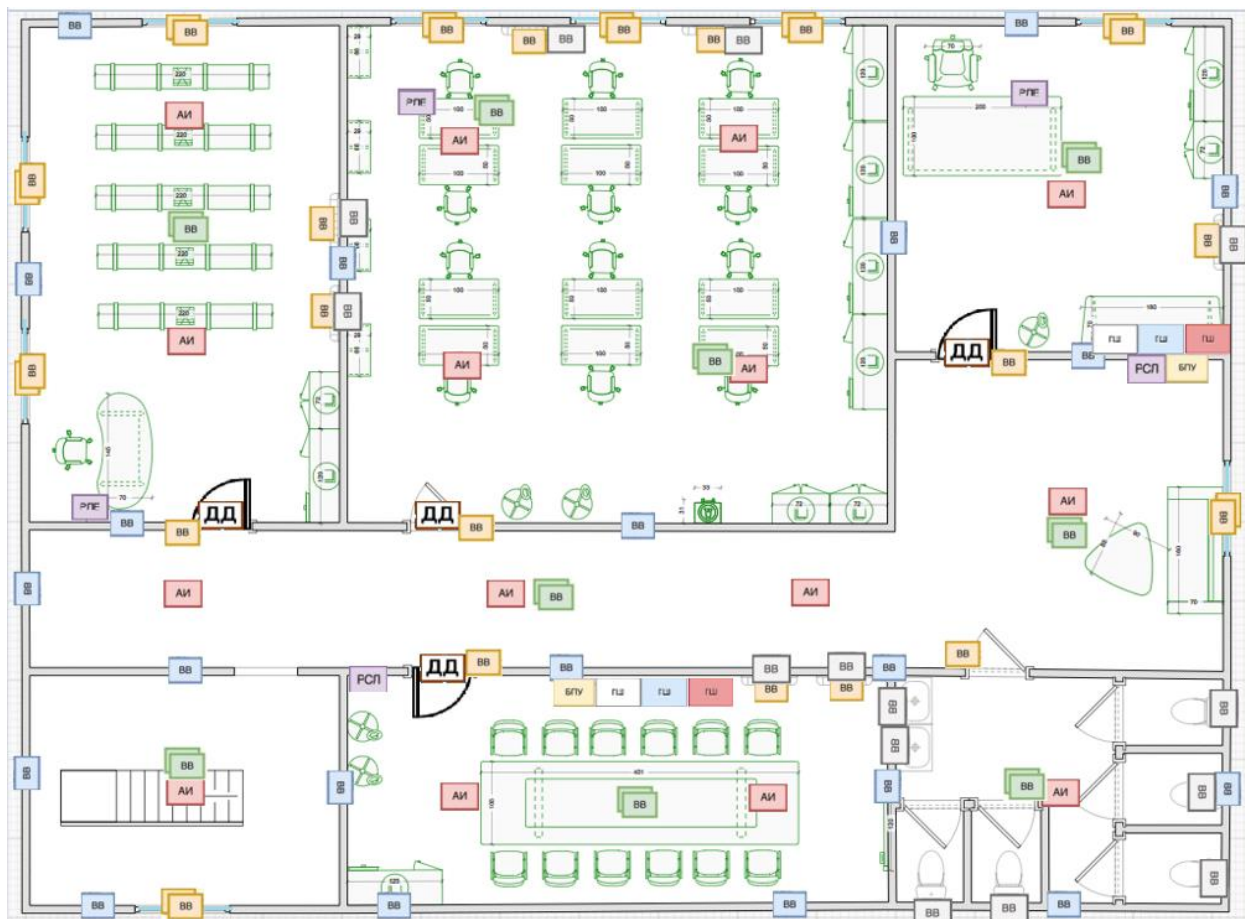



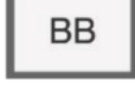
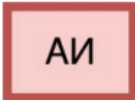
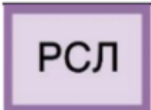
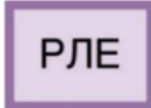





Рисунок 5 – Схема расстановки устройств

В таблице 5 приводится расшифровка условных обозначений схемы расстановки устройств.

Таблица 5 – Условные обозначения

Средство защиты	Обозначение
Блок электропитания и управления Соната-ИП4.3	БПУ
Система Соната-АВ-4Б	ГШ
Устройство Соната-РС3	ГШ
Устройство Соната-Р3	ГШ

Средство защиты	Обозначение
Генератор вибровозбудитель Соната-СВ-4Б (двери/окна/батареи, стены, пол/потолок, трубы)	   
Генератор акустоизлучатель Соната-СВ-4Б1	
Размыкатель слаботочной линии Соната ВК4.2	
Размыкатель линии «Ethernet» Соната ВК4.1	
Усиленная звукоизолирующая дверь Ultimatum Next ПВХ	
Дверной доводчик Geze TS  4000/2000	
Жалюзи Verend	

В таблице 6 представлены расходы на данные средства защиты.

Таблица 6 – Расходы на средства защиты

Устройство	Цена, руб.	Количество, шт.	Стоимость, руб
Блок электропитания и управления Соната-ИП4.3	21 600	2	43 200
Система Соната-АВ-4Б	44 200	2	88 400
Устройство Соната-РС3	32 400	2	64 800
Устройство Соната-РЗ	97 200	2	194 400
Генератор акустоизлучатель Соната-СВ-4Б1	3 540	15	53 100
Генератор вибровозбудитель Соната-СВ-4Б	7 440	85	632 400
Размыкатель слаботочной линии Соната ВК4.2	6 000	2	12 000
Размыкатель линии «Ethernet» Соната ВК4.1	6 000	2	12 000
Пульт управления Соната-ДУ 4.3	7680	1	7680
Усиленная звукоизолирующая дверь Ultimatum Next ПВХ	91 681	3	275 043
Жалюзи Verend	1 430	9	12 870
Дверной доводчик Geze TS 4000/2000	1 118	4	4 472
			1 400 365

Итого: 1 400 365 рублей.

## **ЗАКЛЮЧЕНИЕ**

В ходе данной работы был проведен анализ технических каналов утечки информации, составлен перечень руководящих документов, определяющих нормы и стандарты в области защиты информации, был проведен анализ защищаемых помещений для выбранной организации. Далее были выбраны средства защиты в соответствии с определенными техническими каналами утечки информации, проведен анализ рынка технических средств защиты информации разных категорий и выбраны наиболее подходящие для защищаемого помещения средства защиты. Данные средства были отмечены на схеме помещения. По итогам работы была составлена смета на основе действующих цен на выбранные технические средства защиты информации. Необходимые расходы составили 1 400 365 рублей.

Таким образом, все поставленные задачи были выполнены, цель достигнута

## **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

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".