

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

Факультет безопасности информационных технологий

КУРСОВАЯ РАБОТА

По дисциплине:

«Инженерно-технические средства защиты информации»

На тему:

«Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 113»

Выполнил:

Ефремов П.Ю., студент
группы N34511


(подпись)

Проверил преподаватель:

Попов И.Ю., доцент ФБИТ

(подпись)

Отметка о выполнении:

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент Ефремов П.Ю.

(Фамилия И.О.)

Факультет Безопасности информационных технологий

Группа N34511

Направление (специальность) Информационная безопасность

Руководитель Попов И.Ю., доцент ФБИТ, к.т.н

(Фамилия И.О.,

должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 113

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 работы состоит из разделов: введение, анализ предприятия и защищаемых помещений, анализ технических каналов утечки информации, требования руководящих документов, анализ рынка, размещение инженерно-технических устройств, заключение.

Рекомендуемая литература

Руководитель

(Подпись, дата)

Студент



(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Ефремов П.Ю.

(Фамилия И.О.)

Факультет Безопасности информационных технологий

Группа N34511

Направление (специальность) Информационная безопасность

Руководитель Попов И.Ю., доцент ФБИТ, к.т.н

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

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 113

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Заполнение задания на курсовую работу	21.10.2023	21.10.2023	
2	Анализ материалов	13.11.2023	13.11.2023	
3	Написание курсовой работы	26.11.2023	26.11.2023	
4	Подготовка презентации	04.12.2023	04.12.2023	
5	Защита 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 Ефремов П.Ю.

(Фамилия И.О.)

Факультет Безопасности информационных технологий

Группа N34511

Направление (специальность) Информационная безопасность

Руководитель Попов И.Ю., доцент ФБИТ, к.т.н

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

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии. Вариант 113

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

1. Цель и задачи работы

☐ Предложены студентом

☐ Сформулированы при участии студента

☒ Определены руководителем

2. Характер работы

☐ Расчет

☒ Конструирование

☐ Моделирование

☐ Другое

3. Содержание работы

Курсовая работы состоит из разделов: введение, анализ предприятия и защищаемых помещений, анализ технических каналов утечки информации, требования руководящих документов, анализ рынка, размещение инженерно-технических устройств, заключение.

4. Выводы

В результате выполнения работы был проведен анализ помещений предприятия, руководящих документов, предложен комплекс средств технической защиты и реализован план размещения устройств.

Руководитель _____

(Подпись, дата)

Студент _____



(Подпись, дата)

«21» октября 2023 г

СОДЕРЖАНИЕ

Введение.....	6
1 Анализ предприятия и защищаемых помещений	7
1.1 Анализ предприятия и обоснование защиты информации	7
1.2 Организационная структура предприятия	8
1.3 Анализ помещений предприятия.....	9
1.3.1 Схема помещения и обозначение.....	9
1.3.2 Описание критических помещений предприятия.....	12
2 Анализ технических каналов утечки информации	14
2.1 Радиоэлектронные каналы утечки информации.....	15
2.2 Акустические каналы утечки информации.....	16
2.3 Оптические каналы утечки информации	17
2.4 Материально-вещественные каналы утечки информации	18
3 Требования руководящих документов.....	19
4 Анализ рынка инженерно-технических средств защиты	21
4.1 Защита от утечек по оптическому каналу.....	21
4.2 Защита утечек по акустическому и виброакустическому каналам утечки информации	22
4.3 Средства защиты от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам.....	25
4.4 Защита от утечки информации по ПЭМИН.....	27
5 Размещение инженерно-технических средств	28
Заключение.....	31
Список использованных источников	32

ВВЕДЕНИЕ

В современной динамичной бизнес-среде, где информация является ключевым активом предприятий, обеспечение ее надежной защиты становится стратегической задачей. С развитием информационных технологий и расширением возможностей электронных коммуникаций предприятия сталкиваются с потенциальными угрозами в области информационной безопасности.

Цель данного проекта заключается в минимизации рисков, путем реализации комплекса инженерно-технических решений, направленных на обеспечение максимального уровня конфиденциальности, целостности и доступности информации на предприятии. Основное внимание уделяется выбору актуальных средств обеспечения информационной безопасности по различным каналам, анализу законодательной базы для создания комплекса решений и соблюдению требований государственной тайны, определенных соответствующей нормативно-правовой базой. В ходе проекта будет проведен анализ существующей информационной инфраструктуры предприятия, разработаны эффективные меры по защите данных, и предприняты шаги по интеграции технических средств, соответствующих стандартам безопасности.

Актуальность темы проекта обосновывается не только постоянным увеличением угроз в области информационной безопасности, но и растущими объемами обрабатываемой и хранимой информации на предприятии. В свете этих факторов даже отдельные инциденты нарушения безопасности могут повлечь серьезные последствия, включая потенциальную утечку данных с грифом «секретно», финансовые убытки и утрату доверия со стороны клиентов и партнеров, а так же риск разглашения конфиденциальной информации высокого уровня значимости.

1 АНАЛИЗ ПРЕДПРИЯТИЯ И ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

1.1 Анализ предприятия и обоснование защиты информации

Объектом защиты является фирма ООО “Resb”, занимающаяся разработкой структуры и написанием компьютерной программы, необходимой для создания и реализации поставленной задачи, а именно разработкой системного программного обеспечения. Основным видом деятельности организации по ОКВЭД является «62.01 Разработка компьютерного программного обеспечения».

Разработка проектов происходит в сотрудничестве с государственными компаниями. В частности, связанных со сведениями, составляющими государственную тайну. Уровень “секретно” был установлен, так как обрабатываемая информация в соответствии с Постановлением Правительства РФ от 4 сентября 1995 г. N 870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности”, включая последние изменения от 30 октября 2021 г.» и попадает под «иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесённый интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности». Как следствие, необходимо оборудовать офисное помещение инженерно-техническими средствами защиты информации определенного класса. Для определения класса рассматриваемой АС необходимо ориентироваться в соответствии с РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Группа представлена в Таблице А.1 и содержит пять классов — 1Д, 1Г, 1В, 1Б и 1А.

Таблица А.1 – Классы защищенности автоматизированных систем для первой группы

Первая группа (многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней	1А	В случае обработки секретной информации с грифом «особая важность»
---	----	--

конфиденциальности, и не все пользователи имеют право доступа ко всей информации АС)	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

На основании данной таблицы и вывода о том что данная АС является многопользовательской, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС можно обозначить класс защищенности у рассматриваемой организации - 1В.

1.2 Организационная структура предприятия

Информационные потоки, представленные на Рисунке 1, в организации представляют собой систему передачи данных и сообщений между различными элементами организационной структуры. Эти потоки играют ключевую роль в обеспечении эффективной коммуникации и взаимодействия между различными уровнями управления, подразделениями и сотрудниками организации.

К информации, передающейся по открытым потокам, относятся бухгалтерская и финансовая отчетность, налоговые сведения.

К защищаемой информации, передающейся по закрытым потокам, относятся персональные, с, коммерческая тайна и сведения о разрабатываемом технологических решений, представляющие гостайну.

Закрытые информационные потоки выделены черным цветом, открытые - красные.

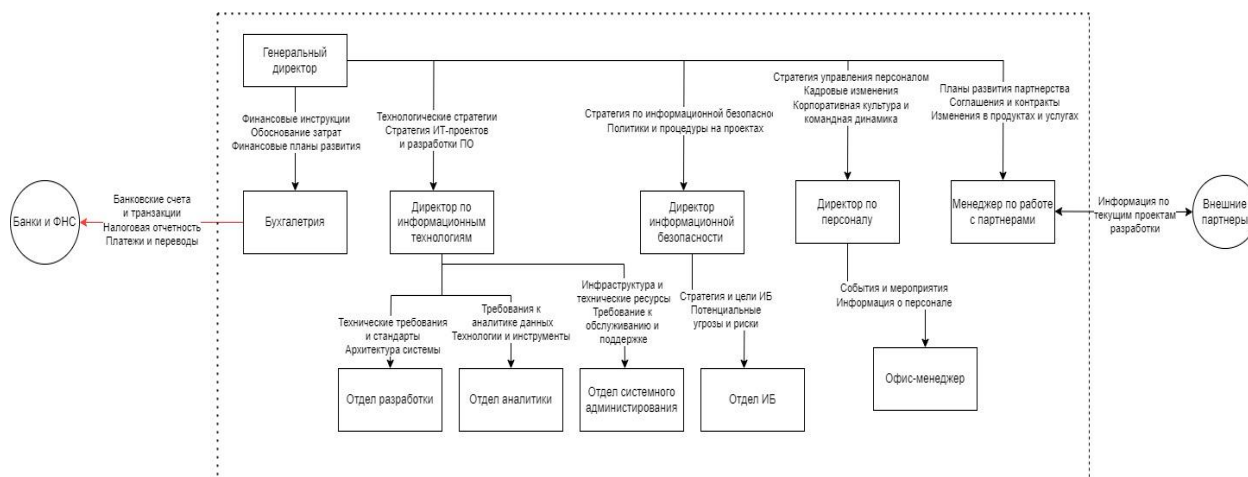


Рисунок 1 – Информационные потоки организации

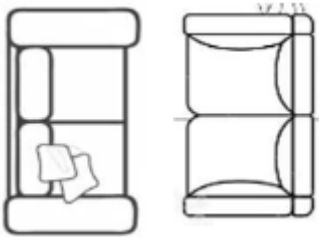


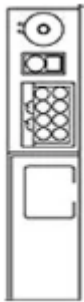
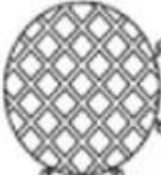
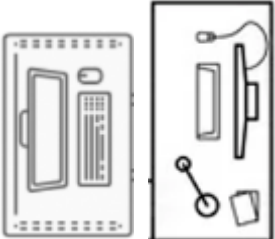

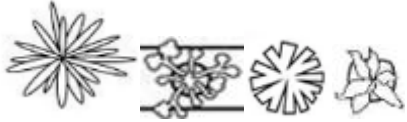
1.3 Анализ помещений предприятия

1.3.1 Схема помещения и обозначение

Анализируемое помещение представляет собой офис, состоящий из серверной, переговорной, кабинета директора, архива, выделенного помещения для системного администрирования, кабинета директора информационной безопасности, холла, состоящего из нескольких коридоров, выделенной «ореп-зоны» для отделов разработки и аналитики, выделенного помещением для отдела бухгалтерии, кабинета для директора по персоналу и менеджера по работе с партнерами, кабинета для отдела ИБ и нескольких санузлов. Описание элементов предоставлено в Таблице А.2

Таблица А.2 – Описание элементов, изображённых на плане

Обозначение	Описание
	Вентиляция
 	Компьютерные кресла
  	Кресло

Обозначение	Описание
	Диван
	Пуфик
	Журнальный стол
	Кухонный гарнитур
	Кухонный стол
	Компьютерный стол
	Телевизор
	Комнатные растения

Обозначение	Описание
	Батерея
	Принтер
	Кулер
	Мусорка
	Напольная вешалка
	Серверное оборудование
	Туалет
	Раковина
	Шкаф

Таблица А.3 – Площадь помещения

Помещение	Площадь, м ²
Серверная	6,2
Переговорная	12,2
Кабинет директора	12,5
Выделенное помещение для системных администраторов	32,5
Холл основной	33,7
Архив	3,6

Помещение директора информационной безопасности	Площадь, м ²
Выделенная «ореп-зона»	66
Выделенное помещение для отдела бухгалтерии	19,1
Кабинет для директора по персоналу и менеджера по работе с партнерами	18,8
Кабинет для отдела ИБ	17,4
Санузел №1	5
Санузел №2	3,7
Техническое помещение	2,5
Холл №2	9,8
Коридор	11,4
Коридор №2	13,8

1.3.2 Описание критических помещений предприятия

Наиболее критичными для утечки государственной тайны являются следующие помещения: серверная, переговорная комната, отдел бухгалтерии, кабинет директора с архивом, а также кабинет для директора по персоналу и менеджера по работе с партнерами. Все соответствующие помещения обозначены на плане (Рисунок 2).

Требования к режимным помещениям и их оборудованию содержатся в «Типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними», утвержденных Решением Межведомственной комиссии по защите государственной тайны от 21.01.2011 N 199. Офис располагается на 2 этаже бизнес-центра, других офисов на этаже нет. Окна офиса не соседствуют с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и прочими элементами, с которых в помещения могут проникнуть посторонние лица. Офис размещен в «непроходной» части здания, которая редко используется сотрудниками при выполнении служебных обязанностей, не связанных с доступом к государственной тайне. Бетонные стены выполнены из бетона толщиной 15 см.

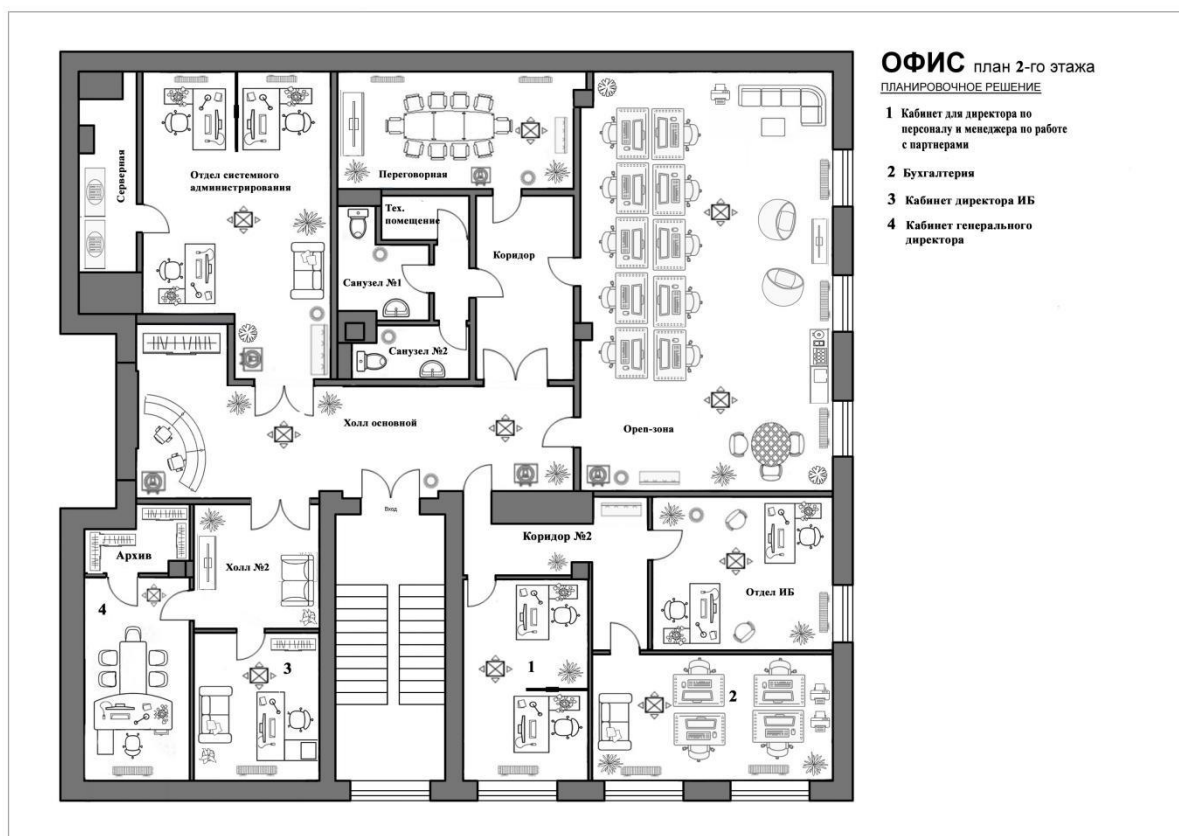


Рисунок 2 – План помещения

Рассмотрим наиболее важные факторы каждого из помещений.

Серверная граничит с отделом системного администрирования, имеет толстые стены из бетона толщиной 15 см, не имеет окон, вентиляции, батарей и доступа из коридора.

Переговорная комната граничит с несколькими помещениями, имеет достаточно тонкие стены, в комнате расположены 2 батареи, телевизор и вентиляция. Отдел бухгалтерии расположен в угловой части здания имеет 2 окна, 2 батареи, вентиляцию, 4 АРМа, 2 принтера. Кабинет директора расположен в угловой части, граничит с холлом тонкими стенками, в кабинете, одна батарея, 1АРМ и доступ к архиву, содержит 1 батарею и вентиляцию. Архив представляет собой закрытое помещение, разделение с холлом представляет собой тонкие стенки, не содержит вентиляции, окон. Кабинет для директора по персоналу и менеджера по работе с партнерами содержит окно, одну батарею, вентиляцию, 2 выделенных АРМа.

Рассмотрим технические каналы утечки и требования законодательных актов по защите информации, на основании выявленной информации составим выборку технических решений, представляющие комплекс по защите.

2 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Канал утечки данных, которыми владеет компания, может быть физическим, техническим или информационным. В рамках курсовой работы рассматривается только технический канал.

Техническим называют канал, в котором источниками информации служат шумовые сигналы, излучения и вибрации, исходящие от интересующих объектов. Распространение сигналов происходит через определенную физическую среду (волновую или электрическую).

Технический канал утечки информации (ТКУИ) представляет собой комплексный набор элементов, включая объект технической разведки, физическую среду, через которую распространяется информативный сигнал, а также средства, используемые для добывания защищаемой информации. Утечка информации через технический канал представляет собой неконтролируемый процесс распространения информации от источника защищаемой информации через физическую среду до технического устройства, осуществляющего перехват этой информации. Структура технического канала утечки информации представляет из себя два основных компонента - источник и злоумышленник. Между ними расположен канал утечки информации, состоящий из источника сигнала, среды по которой передается сигнал и приемника.

Информация, поступающая от источника, начинает свой путь через канал, используя язык источника. Для того чтобы записать эту информацию на носитель, соответствующий среде распространения, передатчик осуществляет ее преобразование в форму, соответствующую условиям данной среды.

Среда распространения сигнала представляет собой физическую среду, в которой информативный сигнал может распространяться и быть зарегистрированным приемником. Эта среда описывается набором физических параметров, определяющих условия перемещения сигнала. Основными параметрами, которые требуется учесть при характеристике среды распространения, включают:

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

Классификация технических каналов представлена на Рисунке 3.



Рисунок 3 – Классификация каналов утечки информации

В рамках выполнения работы и выбора устройств для защиты информации основной акцент нужно сделать на левую часть дерева и подробнее рассмотреть каждый из физических каналов.

2.1 Радиоэлектронные каналы утечки информации

В канале утечки информации в области радиоэлектроники в качестве сред передачи используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток, распространяющийся по металлическим проводам.

Электрические каналы утечки информации включают передачу данных через электрические сигналы, идущие по проводам. Например, изменения в электрических полях, создаваемых работой электронных устройств, могут быть несанкционированно перехвачены, предоставляя доступ к конфиденциальной информации, передаваемой по проводам связи или электропитанию.

Магнитные каналы утечки информации используют магнитные поля для передачи данных. Например, электронные устройства генерируют магнитные поля при работе, и перехват этих полей может привести к раскрытию передаваемой информации.

Электромагнитные каналы утечки информации объединяют электрические и магнитные аспекты. Радиоволны в радиодиапазоне, например, представляют собой электромагнитные волны, используемые для беспроводной передачи данных. Несанкционированное перехватывание этих волн может привести к утечке конфиденциальной информации, передаваемой по воздуху\

Известны следующие электромагнитные каналы утечки информации:

- микрофонный эффект элементов электронных схем;
- электромагнитное излучение низкой и высокой частоты;
- возникновение паразитной генерации усилителей различного назначения;
- цепи питания и цепи заземления электронных схем;
- взаимное влияние проводов и линий связи;
- высокочастотное навязывание;
- волоконно-оптические системы.

2.2 Акустические каналы утечки информации

Акустические технические каналы утечки информации делятся на акустоэлектрическом, виброакустическом и акустические.

Акустоэлектрический канал основан на воздействии звуковых волн на электрические устройства. Например, звуковые колебания, создаваемые при разговоре, могут воздействовать на электронику, и такие изменения могут быть перехвачены для извлечения информации.

Виброакустический канал использует вибрации, созданные на поверхности объекта, для передачи информации. Например, вибрации стекла окна, вызванные разговором, могут быть обнаружены и интерпретированы для утечки информации.

Акустический канал основан на передаче звуковых волн для утечки информации. Например, запись звука среды может содержать разговоры или другую конфиденциальную информацию.

Организационно-технические меры подразделяются на активные(звукоизоляция, звукопоглощение) и пассивные(звукоподавление, защищенные акустические системы)

Защита от утечки по акустическим каналам реализуется:

- применением звукопоглощающих облицовок, специальных дополнительных тамбуров дверных проемов, двойных оконных переплетов;
- использованием средств акустического зашумления объемов и поверхностей;
- закрытием вентиляционных каналов, систем ввода в помещения отопления, электропитания, телефонных и радиосвязей;
- использованием специальных аттестованных помещений, исключающих появление каналов утечки информации.

2.3 Оптические каналы утечки информации

Оптические каналы утечки информации основаны на использовании световых сигналов для передачи данных. Существуют три основных вида: инфракрасный, видимый и ультрафиолетовый каналы. Инфракрасный канал использует инфракрасные световые волны для передачи данных. Например, инфракрасные сигналы, передаваемые между устройствами, могут быть перехвачены для получения конфиденциальной информации.

Видимый канал использует световые волны видимого спектра для передачи данных. Например, световые мигания на экране могут быть использованы для передачи информации, которая может быть зафиксирована визуально или с помощью оптических устройств.

Ультрафиолетовый канал использует ультрафиолетовые световые волны для передачи данных. Например, ультрафиолетовые метки на документе могут быть использованы для скрытой передачи информации, которую можно раскрыть с помощью специальных оптических устройств.

С целью защиты информации от утечки по оптическому каналу рекомендуется:

- располагать объекты защиты так, чтобы исключить отражение света в стороны возможного расположения злоумышленника (пространственные ограждения);
- уменьшить отражательные свойства объекта защиты;
- уменьшить освещенность объекта защиты (энергетические ограничения);
- использовать средства преграждения или значительного ослабления отраженного света: ширмы, экраны, шторы, ставни, темные стекла и другие преграждающие среды, преграды;
- применять средства маскирования, имитации и другие с целью защиты и введения в заблуждение злоумышленника;
- использовать средства пассивной и активной защиты источника от неконтролируемого распространения отражательного или излученного света и других излучений;
- осуществлять маскировку объектов защиты, варьируя отражательными свойствами и контрастом фона;
- применять маскирующие средства сокрытия объектов можно в виде аэрозольных завес и маскирующих сеток, красок, укрытий.

2.4 Материально-вещественные каналы утечки информации

В материально-вещественном канале утечки информации, нарушение конфиденциальности данных происходит путем неправомерного распространения информации за пределы контролируемой зоны вещественных носителей. В данном контексте вещественными носителями являются часто используемые материалы, такие как черновики документов и использованная копировальная бумага, а также портативные устройства хранения данных, такие как жесткие диски (HDD), твердотельные накопители (SSD), и карточки памяти.

В рамках курсовой работы не рассматривается данный канал, так как кражей или копированием информации, зафиксированной на материальных носителях борются в первую очередь организационными мерами, вводя строгий порядок учета и работы с данными видами носителей.

3 ТРЕБОВАНИЯ РУКОВОДЯЩИХ ДОКУМЕНТОВ

Постановлениями Правительства Российской Федерации в области предотвращения утечки информации по техническим каналам являются:

- Постановление №333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 15 апреля 1995 г. в котором описаны процесс предотвращения утечек и перечень действий для защиты информации;

- Постановление №870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 4 сентября 1995 г. в котором описаны виды гостайны и обозначена классификация информации по типам секретности;

- Постановление №608 «О сертификации средств защиты информации» от 26 июня 1995 г. в котором описан процесс сертификации различных устройств

Основные законы и указы, которые нужно использовать:

- Закон “О государственной тайне”;
- Федеральный Закон №149 - “Об информации, информационных технологиях и защите информации”;

- Указ Президента РФ от 30.11.1995 №1203 "Об утверждении Перечня сведений, отнесенных к государственной тайне".;

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

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

Также на сайте ФСТЭК существует отдельный раздел, содержащий специальные нормативно-технические документы ФСТЭК России – нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации:

- 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. 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 Гостехкомиссии России. Защита от несанкционированного доступа к информации;
- программное обеспечение средств защиты информации;
- Руководящий документ. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам.

4 АНАЛИЗ РЫНКА ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ

4.1 Защита от утечек по оптическому каналу

Для обеспечения безопасности оптического канала утечки информации можно применить следующие пассивные меры, описанные в Таблице А.4:

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

Шторы — часто распространенные средства для предотвращения скрытного наблюдения через окна кабинета, однако падает уровень освещенности кабинета.

Тонированные пленки на стеклах не рассматриваются из-за того, что легко выявить окна помещений с повышенными требованиями к безопасности информации, что из-за соображений скрытности защиты делать не следует. Для обеспечения скрытности защиты применять пленку надо на всех окнах, по крайней мере, этажа, а лучше здания, что в общем здании не является самым оптимальным решением

Жалюзи на окнах - исключают возможность наблюдения через окно, так же крайне эффективны при защите от солнечных лучей.

Для предотвращения наблюдения через приоткрытую дверь или создания ситуации с незакрытой дверью по ошибке или умыслу персонала применяют доводчик двери, который плавно закрывает дверь после ее открытия, тем самым перекрывает путь доступа.

Таблица А.4 – Пассивные меры по защите оптического канала

Наименование	Плюсы	Минусы	Стоимость, руб
Жалюзи обычные	Легко регулировать уровень света, создавая комфортное освещение в помещении	Требуется дополнительная уборка	987
Шторы “Blackout”	Могут обеспечивать дополнительную изоляцию света	Падает уровень освещения	1850

Тонированные пленки 50х300см 50%	Обеспечивают полную изоляцию помещения от света в зависимости от процента поглощения	Привлекают внимание	487
--	---	------------------------	-----

Для обеспечения защиты оптического канала были выбраны шторы в количестве 7 шт и доводчик дверной “Булат Ultimate” (ДД-100 А-S, -42°С + 50°С °С, морозостойкий, 120 кг, серебро) по цене 2409 рублей за 1 штуку на каждую дверь офиса в количестве 23 шт.

Дополнительной мерой является установка «Дверь звукоизоляционная усиленная ДВ скрытые RW 47 db RAL с скрытым коробом» в кабинеты генерального директора, директора ИБ, отдел бухгалтерии, кабинета менеджера по работе с партнерами и переговорную комнату, то есть в количестве 5 штук по цене 122 141 рублей за штуку.

4.2 Защита утечек по акустическому и виброакустическому каналам утечки информации

Пассивная защита акустического и виброакустического каналов утечки информации представляет собой:

- усиленные двери;
- тамбурное помещение перед переговорной(обеспечено планировкой помещения);
- дополнительная отделка переговорной звукоизолирующими материалами.

Из-за ценовой политики отделки помещения, которая составляет примерно от 3700 до 4500 рублей за квадратный метр помещения, выбор был сделан в пользу активной защиты по данному каналу. В свою очередь защита представляет собой систему виброакустического зашумления. Для защиты помещения для работы с государственной тайной уровня «секретно» рассматриваются технические средства активной защиты информации, представленные в Таблице А.5.

Таблица А.5 – Устройства для активной защиты по акустическому и виброакустическому каналам

Устройство	Цена, руб	Диапазон частот, Гц	Комплектация и особенности устройства
БУРАН(полная комплектация)	81000	100 –11 200	<p>Число помеховых каналов – три (виброакустических – 2, акустических – 1). Возможность подключения большого числа преобразователей - до 50 шт. (виброакустических – до 40 шт., акустических – до 10 шт.).</p> <p>Оптимальное использование мощности каналов за счет мониторинга уровня их нагрузки. Возможность дистанционного включения системы по проводному каналу. Соответствует требованиям ФСТЭК России к средствам защиты акустической речевой информации по 2 классу защиты и может устанавливаться в выделенных помещениях.</p>
Барон	62500	150 -15000	<p>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</p>

			акустические колебания воздуха. Для защиты объектов информатизации 1 категории и противодействия техническим средствам перехвата речевой информации
СОНАТА АВ-4Б	44200	90-11200	Есть возможность подключения к одному питающему шлейфу. Это делает легче процесс проектирования и монтажа Индивидуальная регулировка интегрального уровня и корректировка спектра каждого генератора улучшает действие системы

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

- есть возможность подключения к одному питающему шлейфу. Это делает легче процесс проектирования и монтажа;
- индивидуальная регулировка интегрального уровня и корректировка спектра каждого генератора улучшает действие системы;
- в сравнении с другими устройства полностью подходит под 3-ю категорию защиты и дешево.

Категория выделенных помещений, согласно СТР-97, устанавливается в зависимости от степени секретности обсуждаемых вопросов и условий эксплуатации (расположения) этих помещений.

К помещениям 1 категории относятся помещения, специально предназначенные для проведения совещаний по вопросам особой важности, а также отдельные служебные кабинеты руководства учреждения (предприятия), в которых могут вестись обсуждения и переговоры по вопросам особой важности.

К помещениям 2 категории относятся помещения, специально предназначенные для проведения совещаний по совершенно секретным вопросам, а также служебные кабинеты руководящего состава учреждения (предприятия) и основных его подразделений, в которых могут вестись обсуждения и переговоры по совершенно секретным вопросам.

К помещениям 3 категории относятся служебные кабинеты и рабочие комнаты подразделений учреждения (предприятия), в которых проводятся обсуждения и переговоры по вопросам со степенью секретности не выше секретно, а также актовые и конференц-залы, предназначенные для массовых открытых мероприятий, но эпизодически используемые для проведения закрытых мероприятий.

Таким образом, было выбрано средство комплекс виброакустической защиты помещения «Соната АВ-4Б», дополнительная информация по включению генератора-акустоизлучателя СОНАТА СА-4Б для по цене 7440 рублей за штуку для вентиляции, Соната СВ-4Б по цене 7440 рублей для стен, потолков, окон, дверей, потолков, трубопроводов.

Руководствуясь следующими стандартами по эксплуатации:

- 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 м² перекрытия;
- окна – один на окно (при установке на оконный переплет);
- двери – 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;
- один на каждый вентиляционный канал или дверной тамбур;
- один на каждые 8...12 м³ надпотолочного пространства или других пустот.

Так же стоит добавить блок электропитания и управления «Соната-ИП 4.3» стоимостью 21600 рублей, пульт управления «Соната-ДУ 4.3» стоимостью 7680 рублей для автоматизированного управления.

4.3 Средства защиты от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам

Активная защита основывается на создании в сети белого шума, который скрывает колебания порождаемые воздействием звуковой волны или работающей электрической техникой. Ниже, в Таблице А.6 приведен сравнительный анализ подходящих средства активной защиты помещений по данному каналу.

Таблица А.6 – Сравнительная характеристика средств ЗИ по электромагнитному каналу

Устройство	Цена, руб	Диапазон частот, Гц	Комплектация и особенности устройства
Генератор шума ЛГШ-221	36400 руб	10 кГц - 400 МГц	Световой индикатор работы в стандартном режиме. Световая и звуковая сигнализация в случае отказа и перехода в аварийный режим работы. Счетчик отработанных часов. .
Двухканальный генератор зашумления SEL SP-44	26000 руб	10 кГц – 400 МГц	Генератор регулируемого шума. Индикация нормального / аварийного режима работы. Электропитание от сети переменного тока 220В Устройство имеет высший класс устойчивости к импульсным помехам и допускает длительную работу в условиях эквивалентного короткого замыкания.
Соната-РС3	32 400 руб	до 2 ГГц	Возможно дистанционное управление посредством проводного пульта. 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.

После проведенного анализа был выбран генератор шума Соната-РС3. Особенности конструкции этого устройства позволяют находить эффективные и экономичные решения при оснащении объекта вычислительной техники, где присутствует значительное

количество вычислительных средств. Данная модель занимает лидирующее положение среди популярных устройств, предназначенных для защиты электрических каналов. Кроме того, она совместима с системой Соната «АВ», в частности, с моделью 4Б, которая была выбрана в качестве средства защиты виброакустического канала.

4.4 Защита от утечки информации по ПЭМИН

ПЭМИН, или побочные электромагнитные излучения и наводки, представляют потенциальную угрозу для конфиденциальности компьютерной информации. Возможным методом защиты от нежелательного раскрытия данных является использование техники зашумления, известной также как радиомаскировка.

Метод зашумления предполагает применение генераторов шума в помещении, где размещены вычислительные устройства, обрабатывающие конфиденциальную информацию. Эти генераторы шума спроектированы для создания дополнительного фонового шума, который может перекрыть или затруднить перехват побочных электромагнитных излучений.

В данном разделе при комплексном выборе средств логичным подходом является выбор в пользу устройства того же производства, а именно, Соната-РЗ, стоимостью 97200 рублей. 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 индуцирования в них маскирующих шумовых напряжений. Диапазон частот соответствует требованиям документа "Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок" (ФСТЭК России, 2014) - по 2 классу защиты, что является оптимальным решением.

5 РАЗМЕЩЕНИЕ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ

В рамках анализа рынка инженерно-технических средств были рассмотрены различные устройства и выбран оптимальный комплекс для защиты помещений. Итоговая смета представлена в Таблице А.7.

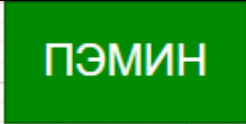

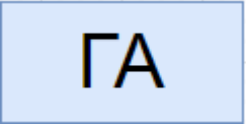
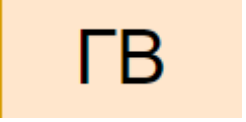
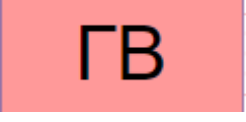
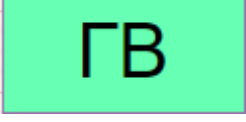

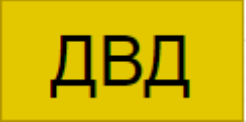


Таблица А.7 – Итоговая смета

Устройство	Стоимость, руб	Количество	Общая стоимость
Соната-РЗ от ПЭМИН	97200	1	97200
Соната-РСЗ	32400	5	162000
Блок электропитания и управления «Соната-ИП 4.3»	21600	1	21600
Генератор-акустоизлучатель «Соната СА-4Б»	7440	10	74400
Генератор-вибровозбудитель «Соната СВ-4Б»	7440	85	632400
Пульт управления «Соната-ДУ 4.3»	7680	1	7680
Шторы “Blackout”	1850	7	12950
Доводчик дверной “Булат Ultimate”	2409	23	55407
Дверь звукоизоляционная усиленная	122 141	5	610705
Размыкатель линии Ethernet «Соната ВК4.3»	6000	4	24000
Размыкатель слаботочной линии «Соната-ВК4.2»	6000	4	24000

Размещение инженерно-технических средств защиты информации производилось в соответствии с руководством по эксплуатации «Система виброакустической и акустической защиты "Соната-АВ"». Жалюзи были установлены на каждом окне, доводчик на каждой двери. Усиленные двери, как представлено на рисунке, установлены в 5 ключевых местах.

Соната-РСЗ» подключена к системе электроснабжения согласно рекомендациям производителя, на схеме отдельно не обозначена. Обозначение устройств, отмеченных на схеме отражено в Таблице А.8.

Таблица А.8 – Обозначение устройств на схеме.

Устройство	Обозначение на схеме
Соната-РЗ от ПЭМИН	
Блок электропитания и управления «Соната-ИП 4.3»	
Генератор-акустоизлучатель «Соната СА-4Б»	
Генератор-вибровозбудитель «Соната СВ-4Б» (стены)	
Генератор-вибровозбудитель «Соната СВ-4Б» (потолок, пол)	
Генератор-вибровозбудитель «Соната СВ-4Б» (батарея, окно, дверь)	
Шторы “Blackout”	
Доводчик дверной “Булат Ultimate”	
Дверь звукоизоляционная усиленная	Обозначены красным
Размыкатель линии «Ethernet» «Соната-ВК4.3»	
Размыкатель слаботочной линии «Соната-ВК4.2»	

План расположения представлен на рисунке 4.

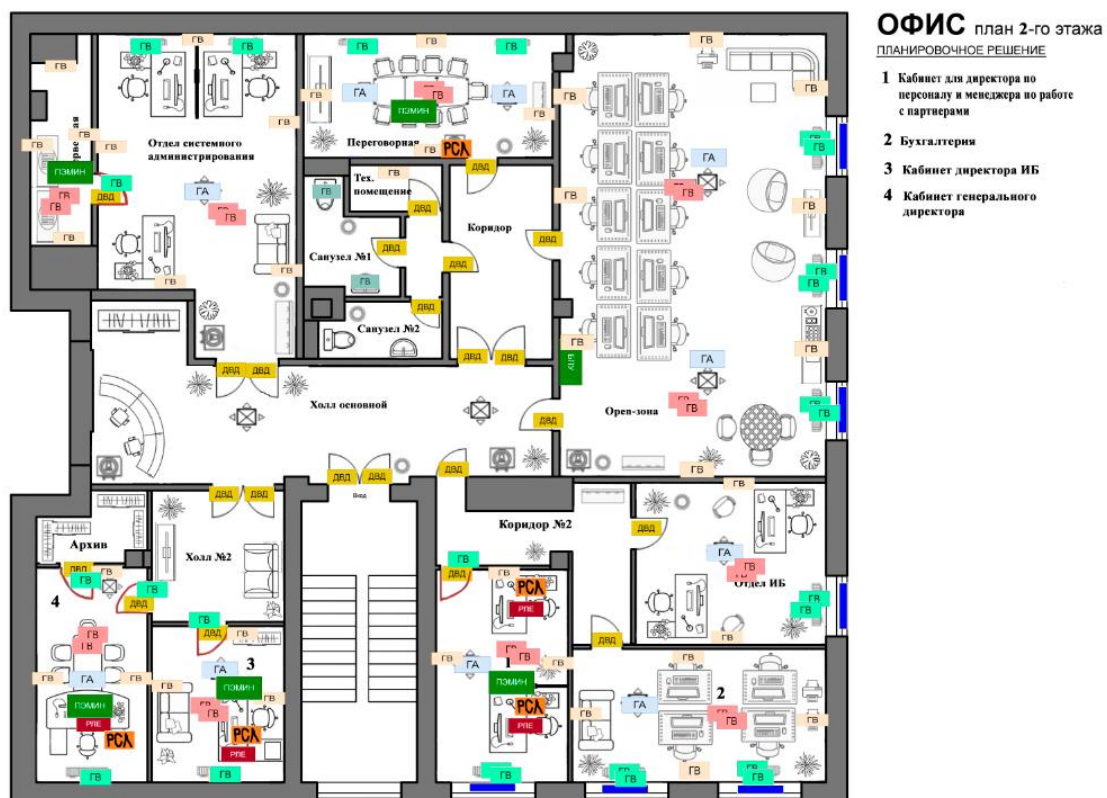


Рисунок 4 – План расположения устройств

ЗАКЛЮЧЕНИЕ

В результате выполнения данной работы был проведен теоретический анализ технических каналов утечки информации. Также были определен перечень руководящих документов, 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 1698342 рублей. Дополнительно была предложена схема расстановки устройств.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. М. Е. Бурлаков, М. Н. Осипов Акустические и виброакустические каналы утечки информации. Теоретические основы и базовый практикум [Текст] / М. Е. Бурлаков, М. Н. Осипов — 1-е изд.. — Самара: Издательство Самарского университета, 2021 — 94 с.
2. Рагозин, Ю. Н. Инженерно-техническая защита информации : учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург : Интермедия, 2018. — 168 с.— ISBN 978-5-4383-0161-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/103203>.
3. ЦЛС Прогресс. Требования к режимным помещениям и их оборудованию: официальный сайт. – Москва. – URL: <https://licenziya-fsb.com/trebovaniya-k-rezhimnym-pomeshheniyam>. – Текст: электронный.
4. ГОСТ Р 50.1.056–2005 «Техническая защита информации. Основные термины и определения».
5. Руководящий документ Государственной технической комиссии при Президенте РФ «Классификация автоматизированных систем и требований по защите информации» от 30 марта 1992 г.
6. «Система виброакустической и акустической защиты "Соната-АВ". Руководство по эксплуатации» - Москва.