

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

Факультет безопасности информационных технологий

КУРСОВАЯ РАБОТА

По дисциплине:

«Инженерно-технические средства защиты информации»

На тему:

«Разработка комплекса инженерно-технической защиты информации в помещении»

Выполнил:

Растворцева Е. Е., студент группы N34531



Проверил:

Попов Илья Юрьевич, доцент ФБИТ, кандидат технических наук

(отметка о выполнении)

(подпись)

Санкт-Петербург

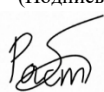
2023 г.

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

Студент	Растворцева Екатерина Евгеньевна			
	(Фамилия И.О.)			
Факультет	Безопасности Информационных Технологий			
Группа	N34531			
Направление (специальность)	11.03.03 - Технологии защиты информации			
Руководитель	Попов Илья Юрьевич, доцент ФБИТ, кандидат технических наук			
	(Фамилия И.О., должность, ученое звание, степень)			
Дисциплина	Инженерно-технические средства защиты информации			
Наименование темы	Разработка комплекса инженерно-технической защиты информации в помещении			
Задание	Разработка комплекса инженерно-технической защиты информации в помещении			

Краткие методические указания

Рекомендуемая литература

Руководитель	Попов Илья Юрьевич	(Подпись, дата)
Студент	Растворцева Екатерина Евгеньевна	 (Подпись, дата)

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»
ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

Студент Растворцева Екатерина Евгеньевна
(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34531

Направление (специальность) 11.03.03 - Технологии защиты информации

Руководитель Попов Илья Юрьевич, доцент ФБИТ, кандидат технических наук
(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Разработка комплекса инженерно-технической защиты информации в помещении

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Заполнение задания на курсовую работу	16.09.2023	16.09.2023	
2	Анализ информации	28.10.2023	28.10.2023	
3	Разработка комплекса инженерно-технической защиты информации в заданном помещении	8.12.2023	8.12.2023	
4	Представление выполненной курсовой работы	19.12.2023	19.12.2023	

Руководитель Попов Илья Юрьевич
(Подпись, дата)

Студент Растворцева Екатерина Евгеньевна
(Подпись, дата)

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

Студент	Растворцева Екатерина Евгеньевна (Фамилия И.О.)		
Факультет	Безопасности Информационных Технологий		
Группа	N34531		
Направление (специальность)	11.03.03 - Технологии защиты информации		
Руководитель	Попов Илья Юрьевич, доцент ФБИТ, кандидат технических наук (Фамилия И.О., должность, ученое звание, степень)		
Дисциплина	Инженерно-технические средства защиты информации		
Наименование темы	Разработка комплекса инженерно-технической защиты информации в помещении		

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

1. Цель и задачи работы

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

Цель данной работы – повышение защищенности рассматриваемого помещения. Задачами является анализ Защищаемого помещения, оценка каналов утечки информации и выбор мер защиты информации.

2. Характер работы

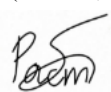
- ☐ Расчет ☒ Конструирование
☐ Моделирование ☐ Другое

3. Содержание работы

1. Введение. 5. Анализ рынка технических средств 6. Описание расстановки технических средств
2. Анализ технических каналов утечки информации. 7. Заключение
3. Руководящие документы 8. Список литературы
4. Анализ защищаемых помещений

4. Выводы

В результате работы был произведен комплексный анализ возможных технических каналов утечки информации в предложенных помещениях, предложены меры пассивной и активной защиты информации

Руководитель	Попов Илья Юрьевич (Подпись, дата)
Студент	 Растворцева Екатерина Евгеньевна (Подпись, дата)

«___» _____ 20__ г

СОДЕРЖАНИЕ

Введение	6
1 Анализ технических каналов утечки информации	7
1.1 Физические каналы утечки информации.....	8
1.2 Технические каналы утечки информации	9
1.3 Информационные каналы утечки.....	10
2 Руководящие документы	11
3 Анализ защищаемых помещений	12
3.1 Описание помещений	13
3.2 Анализ возможных ТКУИ и мер их защиты	13
4 Анализ рынка технических средств защиты информации.....	15
4.1 Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации.....	17
4.2 Защита от ПЭМИН	18
4.3 Защита от утечек по оптическому каналу	18
5 Описание расстановки технических средств.....	19
ЗАКЛЮЧЕНИЕ	4
Заключение	5
Список литературы	6

ВВЕДЕНИЕ

В условиях жесткой конкуренции большое внимание организаций-конкурентов конечно же привлекает конфиденциальная информация. Ведь, чем больше информации доступно, тем больше шансов найти уязвимости соперника. Поэтому каналы передачи и обмена конфиденциальной информации в процессе их функционирования могут быть подвергнуты атакам со стороны злоумышленников, что, в свою очередь, может привести к возникновению каналов утечки конфиденциальной информации.

В условиях конкуренции, организации обращают особое внимание на защиту конфиденциальной информации, так как доступ к большому количеству информации увеличивает возможности найти слабое место у конкурента. В связи с этим, каналы передачи и обмена конфиденциальной информации могут стать целью атак со стороны злоумышленников, что в результате может привести к утечке конфиденциальных данных.

Целью данной работы является разработка процесса управления инцидентами информационной безопасности.

Рассмотрим процесс разработки комплекса инженерно-технической защиты информации, которая является государственной тайной с уровнем «секретно», на объекте информатизации. Также обсудим угрозы информационной безопасности, связанные с утечкой конфиденциальной информации.

1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Утечка информации — это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена. Утечка информации может осуществляться по различным каналам. Каналом утечки информации называют канал коммуникации, позволяющий процессу передавать информацию путем, нарушающим безопасность системы.

Каналом утечки информации называют канал коммуникации, позволяющий процессу передавать информацию путем, нарушающим безопасность системы.

- Возможны три формы утечки информации:
- разглашение информации,
- техническая утечка
- несанкционированный доступ к информации.

Все каналы проникновения и утечки информации могут быть прямыми или косвенными. Косвенные каналы подразумевают использование каналов, которые не требуют физического проникновения в помещения, где находятся компоненты системы (потеря информационных носителей, удаленное прослушивание, перехват радиоэлектромагнитных излучений).

Для использования прямых каналов требуется физическое вторжение (например, действия внутренних сотрудников, несанкционированное копирование и т. д.).

Условия возникновения утечки информации:

- Недостатки в системе безопасности: слабости и уязвимости в сетях, программном обеспечении или физической инфраструктуре могут способствовать несанкционированному доступу к информации.
- Несоблюдение политики безопасности: если сотрудники не соблюдают правила и руководства по безопасности, возникает риск утечки информации.
- Безответственное поведение сотрудников: неправильное использование технических средств, небрежное обращение с информацией или недостаточное обучение сотрудников могут стать причиной утечки информации.
- Социальная инженерия: атакующие могут использовать манипуляцию и обман, чтобы получить доступ к информации через людей, например, путем обмана сотрудника или получения его доверия.
- Внешние угрозы: хакеры, киберпреступники и другие злоумышленники могут использовать различные методы для получения доступа к информации, такие как взлом сети, фишинг-атаки или использование вредоносного ПО.

- Физические факторы: кража или утрата устройств хранения информации, неправильное уничтожение документов или физический взлом помещений могут привести к утечке информации.

1.1 Физические каналы утечки информации

Согласно статистике, главным источником утечки информации является человек. Злоумышленники используют различные методы для получения информации:

- Сотрудники осуществляют сознательные действия, включающие продажу информации за взятку, угрозы шантажа, мести или переход на другую фирму на более выгодных условиях (так называемая "кража мозгов").
- Злоумышленники могут использовать обман, создавая ложные фирмы и приглашая специалистов на собеседование, на котором выуживают информацию и затем отказывают в приеме.
- Особенности характера сотрудника, такие как болтливость и желание показаться более компетентным, могут также привести к утечке информации.
- Недостаточное знание и несоблюдение требований по защите информации также способствует возможной утечке.

Кроме того, документы и публикации являются важными каналами для утечки информации. Документ проходит через несколько этапов жизни, включая составление, оформление, размножение, пересылку, использование, хранение и уничтожение, на каждом из которых возможна утечка информации.

Для снижения возможности утечки информации руководство организации предпринимает следующие меры:

- Разрабатывает перечень документов, которые относятся к коммерческой тайне (информации, позволяющей предприятию получить большую прибыль по сравнению с конкурентами).
- Уточняет список лиц, которым разрешено работать с документами.
- Организует учет входящих и исходящих документов, а также устанавливает правила работы с ними.
- Определяет правила хранения документов, включая инвентаризацию, номенклатуру дел и наличие сейфов.
- Устанавливает правила уничтожения документов.

1.2 Технические каналы утечки информации

Искусственный канал утечки создается путем внедрения в линии связи закладных устройств, установки в рабочих помещениях малогабаритных приборов перехвата.

ТКУИ подразделяют на:

- Акустические;

В акустических каналах основной средой передачи речи и звуков является воздух. Для перехвата этой информации используются высокочувствительные микрофоны и специальные направленные микрофоны. Эти микрофоны обычно соединяются с портативными звукозаписывающими устройствами или специальными миниатюрными передатчиками.

Звуковые волны используются для передачи конфиденциальной информации без разрешения или авторизации. Примеры таких каналов могут включать запись и передачу конфиденциальных разговоров, использование скрытых микрофонов или устройств для записи и передачи аудио-сигналов из помещения.

- Электромагнитные;

Электромагнитные каналы утечки информации используют электромагнитные волны, чтобы передать конфиденциальные данные без разрешения. Примеры включают использование радиоустройств или устройств, способных перехватывать электромагнитные волны, излучаемые компьютерами, смартфонами и другими электронными устройствами.

- Оптические;

Оптические каналы утечки информации основаны на использовании световых волн для передачи конфиденциальных данных. Средой распространения здесь может служить или свободное пространство, или же оптоволоконные линии. Примеры включают использование скрытых видеокамер или устройств, способных перехватывать световые волны, излучаемые экранами компьютеров или устройств чтения информации с мониторов.

- Радиоэлектронные;

Носителями выступают магнитные, электрические, электромагнитные поля диапазона, и электрическая энергия, которую распространяют металлические провода. Этот канал обычно используют, чтобы передавать информацию, которую улавливает микрофон специальному приемнику.

Примеры включают использование несанкционированных радиопередатчиков или приемников для перехвата радиосигналов, передаваемых между электронными устройствами.

- Материально-вещественные.

Примеры включают использование незащищенных физических документов или устройств, содержащих конфиденциальную информацию, и использование

несанкционированного доступа к таким материалам для выявления и передачи информации без разрешения.

1.3 Информационные каналы утечки

К категории информационных каналов утечки относят каналы:

- Линий связи.
- Рабочих станций и периферийных устройств.
- Локальной сети и интернета.
- Машинных носителей информации.

2 РУКОВОДЯЩИЕ ДОКУМЕНТЫ

Основными документами в области защиты информации являются:

- Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера»;
- Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
- Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»;
- Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне»;
- Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) «О сертификации средств защиты информации»;
- Федеральный закон от 27 июля 2006 г. No 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 1 ноября 2012 г. No 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Закон РФ «О государственной тайне» от 21.07.1993 N 5485-1.
- СТР Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам
- Положение о Межведомственной комиссии по защите государственной тайны (с изменениями на 3 августа 2018 года)

3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

Перед проектированием технических средств защиты на объекте проведем анализ защищаемых помещений. Уровень секретности – 3.

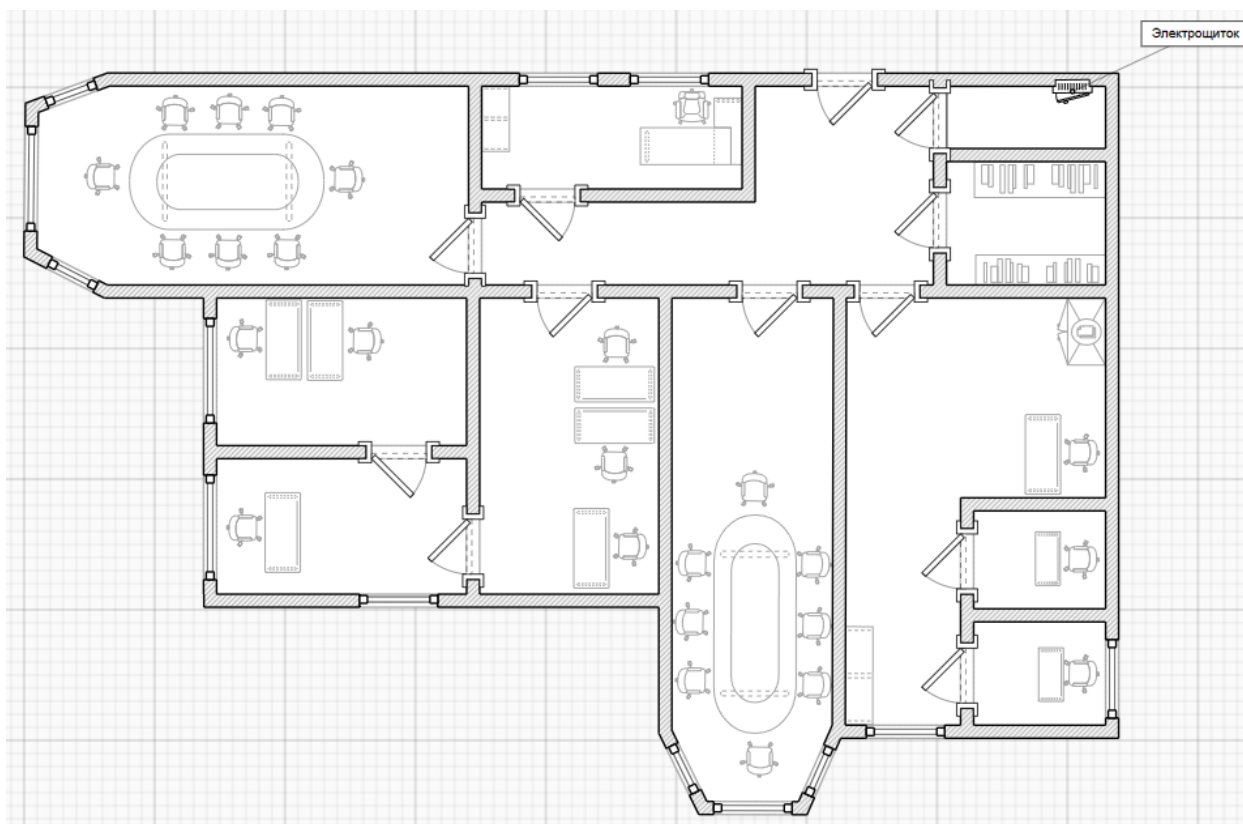
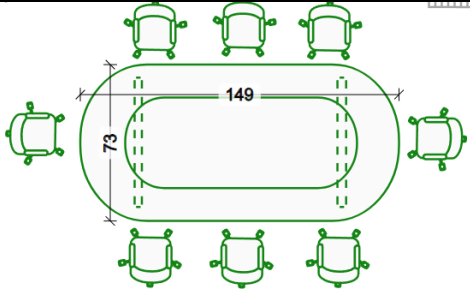
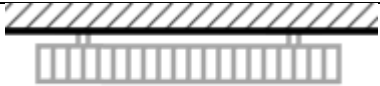
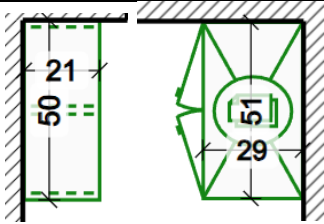


Рисунок 1 – План защищаемого помещения

Таблица 1 – Обозначение объектов на плане здания

Обозначение	Описание
	Рабочее место
	Рабочее место руководителя

	Стулья и стол в переговорной
	Радиатор
	Шкафы

3.1 Описание помещений

Защите подлежат помещения в одноэтажном здании. Параметры помещений:

- Кабинет директора 30.29 кв.м.
- Холл 39.3 кв.м.
- Склад 6.8 кв.м.
- Переговорная 1 50 кв.м.
- Переговорная 2 44 кв.м.
- Электрощитовая 4 кв. м.
- Кабинет с коридором 40 кв.м.
- Кабинет сотрудника (2) 8 кв.м.
- Кабинет сотрудника (3) 24 кв.м.

В кабинете руководителя и переговорных стоит по одному ПК и столу, проектору. В переговорных также находятся телевизоры. Стены здания кирпичные. В наличии 12 окон. В помещениях присутствуют батареи, которые могут служить каналом утечки информации. В кабинете находится один стационарный телефон.

3.2 Анализ возможных ТКУИ и мер их защиты

После изучения руководящих документов была создана таблица 2, отражающая результаты анализа всех потенциальных каналов утечки информации. Также была составлена

таблица устройств, необходимых для обеспечения комплексной безопасности. Данные результаты представлены в таблице 2.

Таблица 2 – Активная и пассивная защита информации

Канал утечки	Источник	Пассивная защита	Активная защита
Акустический, акустоэлектрический	Окна, двери, электрические сети, проводка	Звукоизоляция переговорной, фильтры для сетей электропитания	Устройства акустического зашумления
Вибрационный, виброакустический	Все твердые поверхности помещения, батареи	Изолирующие звук и вибрацию обшивки стен, дополнительное помещение перед переговорной,	Устройства вибрационного зашумления
Оптический	Окна, двери	Жалюзи на окнах, доводчики на дверях	Бликующие устройства
Электромагнитный, электрический	Розетки, АРМ, бытовая техника	Фильтры для сетей электропитания	Устройства электромагнитного зашумления

4 АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Устройства для перекрытия акустического и виброакустического Пассивная защита представляет собой:

- усиленные двери,
- тамбурное помещение перед переговорной,
- дополнительная отделка переговорной звукоизолирующими материалами.

Виброакустическая активная защита — это система, предназначенная для зашумления помещений. Для обеспечения безопасности помещений, где осуществляется работа с государственной информацией уровня "секретно", рассматриваются технические средства активной защиты информации для объектов информатизации категории не ниже 1В. Следует провести сравнительный анализ подходящих средств активной защиты помещений через виброакустический канал (см. Таблица 3).

Таблица 3 – Сравнительный анализ средств активной защиты от утечки информации по виброакустическому каналу

Модель	Цена, руб.	Характеристики	Состав
Соната АВ-4Б	44 200	Диапазон воспроизводимого шумового сигнала 175 - 11200 Гц	Блоки электропитания и управления - Соната-ИП4.1, Соната-ИП4.2, Соната-ИП4.3; Генераторы акустоизлучатели – СА-4Б, СА-4Б1; Генератор-вибровозбудитель – СВ-4Б; Размыкатель телефонной линии – Соната-ВК4.1; Размыкатель слаботочной линии – Соната-ВК4.2; Размыкатель линии Ethernet – Соната-ВК4.3; Пульт управления – Соната ДУ4.3; Блоки сопряжения с внешними устройствами – Соната-СК4.1, Соната-СК4.2; Техническое средство защиты речевой информации от утечки по опτικο- электронному (лазерному) каналу - "Соната-АВ4Л": Генераторный блок "АВ-4Л" + вибровозбудитель "СП4Л"; Аксессуары – труба, фиксатор стены, кабель.
ЛГШ-404	35 100	Диапазон рабочих частот 175 - 11200 Гц	Изделие «ЛГШ-404» – генератор шума; Вибровозбудитель «ЛВП-10» – для установки на стены, трубы и окна; Акустический излучатель «ЛВП-2а» - для возбуждения маскирующих акустических помех; Виброэкран «ЛИСТ-1» – для защиты от наблюдения и акустических микрофонов; Размыкатель «ЛУР» – для размыкания слаботочных линий.
Шорох-5Л	15 300	Диапазон частот 80 - 11300	Блок питания и управления «БПУ-1» с активными вибровозбудителями «ПЭД-8А» и активными акустическими излучателями «АИ-8А/Н» и «АИ-8А/Мини»
SEL SP-157 «Шагренъ»	31 200	Диапазон частот 90 - 11200 Гц	Центральный генераторный блок помех SEL SP-157G, вибрационный преобразователь SEL SP-157VP, акустический излучатель SEL SP- 157AS, вибрационный преобразователь повышенной мощности SEL SP-157VPS, акустический излучатель повышенной мощности SEL SP-157ASP.

На основе проведенного анализа было выбрано применение системы СОНАТА АВ-4Б. Усовершенствованные настройки аппаратуры модели 4Б позволяют объединять источники электропитания для обмена информацией, что обеспечивает возможность создания энергоэффективной системы автоматического контроля всех компонентов, изменения настроек генераторов и установки гибкой системы виброакустической защиты. Кроме того, данная система обладает защитой от использования оптико-электронных устройств.

4.1 Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации

Пассивная защита Пассивная защита включает в себя установку фильтров для сетей электропитания в каждом помещении.

Активная защита состоит в создании в сети белого шума, который прикрывает колебания, вызванные звуковыми волнами или работой электрического оборудования.

Таблица 4 – Сравнительный анализ средств активной защиты от утечки информации по электрическим каналам

Модель	Цена, руб.	Характеристики	Примечания
ЛГШ-513	39 000	Присутствует регулировка уровня шума; Диапазон частот 0,01 – 1800 МГц	Генератор шума по цепям электропитания, заземления и ПЭМИН
СОНАТА-РЗ.1	33 120	Присутствует регулировка уровня шума; Диапазон частот до 2 ГГц	Предназначено для защиты информации от утечки информации за счет побочных электромагнитных излучений и наводок на линии электропитания и заземления, линии проводной связи и токоведущие инженерные коммуникации
ГАММА ГШ-18	29 400	Присутствует регулировка уровня шума; Диапазон частот 0,01 – 1800 МГц	Генератор шума ПЭМИН. Есть регулировка уровня шума, управление осуществляется аттенюаром, есть возможность увеличить уровень шума за счет подключения внешней антенны
ГНОМ- 3М	57 200	Отсутствует регулировка уровня шума; Диапазон частот 0,15 – 1800 МГц	Генератор шум по цепям электропитания, заземления и ПЭМИН. Дистанционное управление отсутствует. Есть возможность подключать внешние антенны.

В результате анализа было решено использовать "Соната-РЗ.1" в качестве средства защиты от утечки по электрическим каналам. Это устройство имеет сертификат ФСТЭК. ПЭМИН "Соната-РЗ.1" обеспечивает защиту информации от утечки, создавая побочные

электромагнитные излучения и наводки путем излучения электромагнитного поля шума в окружающее пространство, а также создавая маскирующие шумовые напряжения для нейтрализации наводок на линии сети электропитания и заземления.

4.2 Защита от ПЭМИН

Для активной защиты от ПЭМИН было выбрано устройство "Соната-РЗ.1". Этот выбор обусловлен совместимостью устройства с уже ранее выбранным средством защиты "Соната АВ-4Б". Кроме того, устройство имеет приемлемую цену, возможность регулировать уровень шума, управлять им с помощью пульта и удобную индикацию исправности.

4.3 Защита от утечек по оптическому каналу

Для защиты от утечек по оптическому каналу необходимо установить шторы, жалюзи или другие средства, которые закроют вид извне. Были выбраны жалюзи как наиболее удобное и экономичное решение.

5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

По информации из 4 главы, выбранные средства защиты информации включают в себя:

- Усиленные двери (толщина не менее 4 см), обшитые металлом (толщина не менее 2 мм) со звукоизолирующей прокладкой на металлическом каркасе – 4 шт.;
- «Соната АВ-4Б»;
- «Соната-РЗ.1»;
- Жалюзи на 12 окон.

Перейдём к оценке количества компонентов и расстановке выбранных технических средств. «Соната АВ-4Б» содержит генераторы-акустоизлучатели «СА-4Б1» и генераторы-вибровозбудители «СВ-4Б1».

Согласно официальному сайту НПО, «Анна», необходимое количество генераторов-вибровозбудителей «СВ-4Б1» можно предварительно оценить 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 м² перекрытия;
- один на окно (при установке на оконный переплет);
- один на дверь (при установке на верхнюю перекладину дверной коробки);
- трубы систем водо-, тепло- и газоснабжения - один на каждую вертикаль (отдельную трубу) вида коммуникаций.

Необходимое количество генераторов-акустоизлучателей «СВ-4Б1» можно предварительно оценить из следующих норм:

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

Составим смету по результатам выбора средств защиты информации от утечки.

Таблица 5 – Расчет стоимости мер защиты

Мера защиты	Цена, руб.	Количество, шт.	Стоимость, руб.
Блок электропитания и управления «Соната-ИП4.3»	21 600	1	21 600
Генератор- акустоизлучатель «СА-4Б1»	6 400	18	115 200
Генератор-вибровозбудитель «СВ-4Б1»	6 400	29	185 600
Пульт управления «Соната-ДУ4.3»	7 700	1	7 700
Генераторный блок «АВ-4Л»	10 320	1	10 320
Размыкатель телефонной линии «Соната-ВК4.1»	6 000	1	6 000
Размыкатель линии Ethernet «Соната- ВК4.3»	6 000	1	6 000
Размыкатель слаботочной линии «Соната-ВК4.2»	6 000	1	6 000
Средство активной защиты информации от утечки за счет ПЭМИН «Соната- РЗ.1»	32 100	1	32 100
Усиленные звукоизолирующие двери UltimatumNext	75 283	4	301 132
Жалюзи «Эскар»	2 632	5	13 160
Итого:			704 812

Жалюзи установлены на каждом окне. Средством защиты от ПЭМИН является устройство «Соната-РЗ». «Соната-РС2» подключена к системе электроснабжения согласно рекомендациям производителя, на схеме отдельно не обозначена.

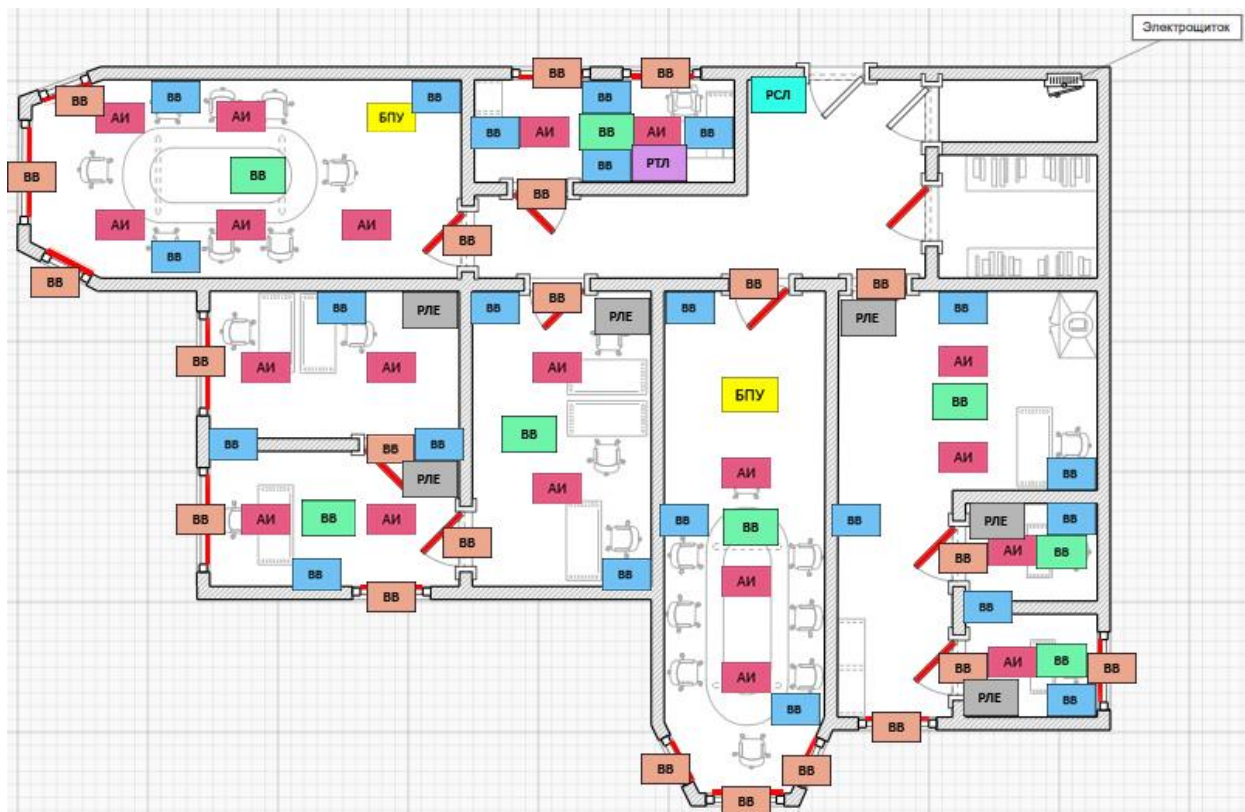


Рисунок 2 – Информационные потоки организации

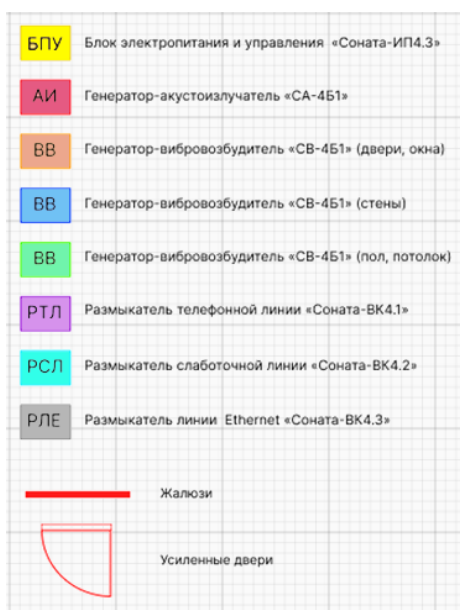


Рисунок 3 – Обозначения. Информационные потоки организации

ЗАКЛЮЧЕНИЕ

В результате проведенного анализа потенциальных каналов утечки информации в защищаемом помещении были выявлены несколько основных уязвимых точек, через которые может осуществляться несанкционированное раскрытие информации. Эти каналы включают акустические, виброакустические, оптические, акустоэлектрические, электрические, электромагнитные и оптико-электронные технические каналы, а также каналы, связанные с ПЭМИН.

Для защиты от этих потенциальных утечек были рассмотрены доступные на рынке технические средства противодействия. Были проведены исследования по эффективности каждого из них и выбраны подходящие для защищаемого объекта, разработан план установки выбранных средств защиты. В нем было определено местоположение и конкретные действия по установке каждого из средств.

В результате была предложена система защиты от утечек информации через различные технические каналы. Предложенные средства защиты охватывают акустические, виброакустические, оптические, акустоэлектрические, электрические, электромагнитные и оптико-электронные каналы, а также защищают от ПЭМИН.

ЗАКЛЮЧЕНИЕ

В результате проведенного анализа потенциальных каналов утечки информации в защищаемом помещении были выявлены несколько основных уязвимых точек, через которые может осуществляться несанкционированное раскрытие информации. Эти каналы включают акустические, виброакустические, оптические, акустоэлектрические, электрические, электромагнитные и оптико-электронные технические каналы, а также каналы, связанные с ПЭМИН.

Для защиты от этих потенциальных утечек были рассмотрены доступные на рынке технические средства противодействия. Были проведены исследования по эффективности каждого из них и выбраны подходящие для защищаемого объекта, разработан план установки выбранных средств защиты. В нем было определено местоположение и конкретные действия по установке каждого из средств.

В результате была предложена система защиты от утечек информации через различные технические каналы. Предложенные средства защиты охватывают акустические, виброакустические, оптические, акустоэлектрические, электрические, электромагнитные и оптико-электронные каналы, а также защищают от ПЭМИН.

СПИСОК ЛИТЕРАТУРЫ

1. Трунова, А. А. Анализ каналов утечки конфиденциальной информации в информационных системах предприятий / А. А. Трунова. — Текст: непосредственный // Молодой ученый. — 2016. — № 3 (107). — С. 69-72. — URL: <https://moluch.ru/archive/107/25842/> (дата обращения: 09.12.2023).
2. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010.- 436 с.
3. Ларионцева Е. А. Основные виды каналов утечки информации // CyberLeninka. – 2011
4. Кармановский, Н. С. Организационно-правовое и методическое обеспечение информационной безопасности : учебное пособие / Н. С. Кармановский, О. В. Михайличенко, С. В. Савков. — Санкт-Петербург: НИУ ИТМО, 2013. — 148 с. —Текст: электронный // Лань: электроннобиблиотечная система. — URL: <https://e.lanbook.com/book/43579> (дата обращения: 18.12.2023).