НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«МЭИ»
ИНЖЕНЕРНО-ЭКОНОМИЧЕСКИЙ ИНСТИТУТ
Кафедра информационной и экономической безопасности

Направление подготовки бакалавриата
10.03.01-«Информационная безопасность»

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА БАКАЛАВРА

Тема: Оценка защищённости помещения организации от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам

Студент	ИЭС-141-16			Еланёв В.К.
	группа		подпись	ФИО
Руководитель работы	доцент	к.т.н.		Рыжиков С.С.
	должность	звание	подпись	ФИО

«***Работа допущена к защите***»

Зав. кафедрой	к.т.н., доцент		Невский А.Ю.
	звание	подпись	ФИО

Дата_____

Москва 2019 г.

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «МЭИ»

Инженерно-экономический институт

Кафедра безопасности и информационных технологий

Направление подготовки бакалавриата

10.03.01– «Информационная безопасность»

ЗАДАНИЕ
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ БАКАЛАВРА

Тема: «Оценка защищенности помещения организации от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам»

Студент: ИЭс-141-16 Еланёв В.К.
группа подпись фамилия, и.,о.

Научный руководитель: доцент к.т.н. Рыжиков С.С.
должность звание подпись фамилия, и.,о.

Зав. кафедрой БИТ к.т.н, доцент Невский А.Ю.
звание подпись фамилия, и.,о.

СОДЕРЖАНИЕ РАЗДЕЛОВ ЗАДАНИЯ И ИСХОДНЫЕ ДАННЫЕ

Цель работы: провести оценку защищенности переговорной комнаты ООО «ФастПроект» от утечки конфиденциальной информации по акустическому и виброакустическому каналам и выработать рекомендации по модернизации систему защиты
Решаемые задачи: изучить теоретические аспекты темы исследования, проанализировать деятельность предприятия, выполнить анализ существующей системы информационной безопасности, описать основные аспекты модернизации механизмов защиты информации от утечки по акустическому и виброакустическому каналам в ООО «ФастПроекст» .

ГРАФИК РАБОТЫ ПО РАЗДЕЛАМ ВКР

№ п\п	Содержание разделов	Срок выполнения	Трудоемкость в %
1.	Введение и первая глава ВКР	20.03.2019	20
2.	Вторая глава ВКР	30.03.2019	40
3.	Третья глава и заключение	30.04.2019	25
4.	Разработка доклада	05.05.2019	5
5.	Разработка графической презентации к докладу	07.05.2019	5
6.	Проверка и брошюрование ВКР	10.05.2019	5

ПЕРЕЧЕНЬ ГРАФИЧЕСКОГО МАТЕРИАЛА

В каждой главе выпускной квалификационной работы должно быть не менее трех-четырех рисунков и таблиц. Для защиты подготовить презентацию с использованием MS PowerPoint с объемом до 10 слайдов. Титульный лист презентации должен иметь информацию о теме дипломной работы, фамилии, имени, отчестве дипломника. На остальных слайдах обязательно должны быть включены цели работы, основные этапы исследования, выносимые для защиты результаты.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Конституция Российской Федерации, Федеральный закон РФ от от 27.07.2006 г. N 149-ФЗ Об информации, информационных технологиях и о защите информации, ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Части 1-3, Богдановская И.Ю. Право на доступ к информации. Доступ к открытой информации М.: ЗАО Юстицинформ, 2014. С. 344. ISBN 5-02-012992-5, Васильков А.В. Безопасность и управление доступом в информационных системах. А.В. Васильков, И.А. Васильков. Учебное пособие. М.: ФОРУМ, 2015. 368 с., Вендров. А.М. Проектирование программного обеспечения экономических информационных систем: Учебник. – М.: Финансы и статистика, 2017. 352 с. ISBN: 978-5-49807-499-3, Венчковский Л.Б. Разработка сложных программных изделий. Москва: ИНФРА-М 2016г. ISBN 978-5-94374-564-8, Гвоздева В.А. Основы построения автоматизированных информационных систем: Москва: ИНФРА-М 2017г. 320 стр. ISBN: 978-5-271-42560-8, Гладких А.А. Базовые принципы информационной безопасности вычислительных сетей : учебное пособие - Ульяновск : УлГТУ, 2014.- 168 с.

СОДЕРЖАНИЕ

Введение …… 6

ГЛАВА 1. Анализ основных аспектов информационной безопасности в ООО «ФастПроект».....8

1.1 Правовые основы защиты конфиденциальной информации.....8

1.2 Анализ защищаемого помещения.....9

1.3 Анализ потенциальных угроз и каналов утечки информации.14

1.3.1. Акустический канал утечки речевой информации.....14

1.3.2. Виброакустический канал утечки речевой информации.…17

1.3.3. Оптико-электронный канал утечки речевой информации..18

1.3.4. Акустоэлектрический и электромагнитный каналы утечки речевой информации.....18

1.4 Описательная модель нарушителя.....20

Выводы по первой главе.....23

ГЛАВА 2. Оценка состояния защиты акустической информации при проведении совещаний.....25

2.1 Организационные меры при проведении совещаний.....25

2.2 Оценка защищенности защищаемого помещения от утечки речевой конфиденциальной информации.....28

2.2.1 Оценка защищенности защищаемого помещения от утечки речевой конфиденциальной информации по акустическому каналу связи 30

2.2.2 Оценка защищенности защищаемого помещения от утечки речевой конфиденциальной информации по виброакустическому каналу связи.....33

2.3 Технические меры по защите акустической информации в защищаемом помещении.....39

Выводы по второй главе.....41

ГЛАВА 3. Рекомендации по повышению уровня защищенности информации в защищаемом помещении.....42

3.1 Перечень мероприятий по совершенствованию защиты информации в защищаемом помещении.....42

3.2.1 Защита от утечки через прямой акустический канал.....44

3.2.2 Защита от утечки по виброакустическому каналу.....46

3.3 Экономическая оценка предложенной системы защиты.....49

Выводы по третьей главе.....50

Заключение.....52

Список использованных источников.....54

ВВЕДЕНИЕ

Вопросы, связанные с защитой информации существуют уже давно. Возникают ситуации, когда определенную информацию необходимо знать только определенному кругу лиц. И для обеспечения её сохранности прибегали к разнообразным способам защиты. Примерами таких способов можно назвать такие способы защиты как тайнопись или шифрование передаваемых сообщений.

Современный уровень высокой компьютеризации оказывает высокое влияние на быт и жизнедеятельность людей. Обеспечение информационной безопасности при обработке и передаче информации, а также контроль и управление различными объектами стало одной из важнейших проблем. К подобным объектам можно отнести системы связи, системы управления транспортом, и конечно системы хранения информации. Для правильного функционирования всех перечисленных систем необходимо обеспечивать безопасность и конфиденциальность хранимых в них данных.

Текущий уровень развития программного и аппаратного обеспечения персональных компьютеров сейчас находится на том уровне, когда выполнить реализацию простейшей компьютерной сети может рядовой пользователь. Но выполнить грамотный проект крупной локальной вычислительной сети может только специалист, чтобы избежать возможных проблем на этапах реализации и эксплуатации компьютерной сети.

Актуальность данной работы в том, что на текущий момент времени в любой организации обрабатывается самого различного рода, что, несомненно, приводит к необходимости обеспечения защиты данных, как при их обработке, так и при их передаче по каналам связи.

Предмет исследования – методы защиты информации. Объект исследования – реализация методов защиты информации от утечки по акустическому каналу в ООО «ФастПроект».

Цель данной работы – провести оценку защищённости переговорной комнаты ООО «ФастПроект» от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам и выработать рекомендации по модернизации системы защиты.

В ходе выполнения выпускной квалификационной работы необходимо выполнить следующие задачи:

1 Изучить теоретические аспекты темы исследования;

2 Проанализировать деятельность предприятия;

3 Выполнить анализ существующей системы информационной безопасности;

4 Описать основные аспекты модернизации механизмов защиты информации от утечки по акустическому и виброакустическому каналам в ООО «ФастПроект».

В первой главе рассмотрены правовые основы защиты конфиденциальной информации. Был проведен анализ предприятия и защищаемого помещения. Рассмотрены акустический каналы утечки речевой информации. Составлена модель нарушителя и выявлены возможные каналы утечки речевой информации.

Вторая глава посвящена проведению оценки защищенности от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам через входную дверь и систему отопления.

В третьем главе рассмотрены предложения по модернизации системы защиты информации в защищаемом помещении с помощью как активных, так и пассивных методов защиты. Были предложены меры защиты, наиболее подходящие для данной переговорной комнаты.

ГЛАВА 1. АНАЛИЗ ОСНОВНЫХ АСПЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ООО «ФАСТПРОЕКТ»

1.1 Правовые основы защиты конфиденциальной информации

Конфиденциальная информация — документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

С развитием информационного общества проблемы, связанные с защитой конфиденциальной информации, приобретают всё большее значение. В настоящее время в российском законодательстве данные вопросы полно и системно не решены. Развернутая классификация конфиденциальной информации, приводится в перечне сведений конфиденциального характера, установленном Указом Президента РФ от 6 марта 1997 г. № 188.

К сведениям конфиденциального характера согласно Указа Президента РФ от 06.03.1997 № 188 "Об утверждении Перечня сведений конфиденциального характера", отнесены:

сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях. При этом сведения, ставшие известными работнику органа записи актов гражданского состояния в связи с государственной регистрацией акта гражданского состояния, являются персональными данными;

сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20.08.2004 К" 119-ФЗ "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства" и другими нормативными правовыми актами Российской Федерации;

служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с ГК РФ и федеральными законами (служебная тайна);

сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.);

сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с ГК РФ и федеральными законами (коммерческая тайна);

о сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

На основе перечня сведений, указанных выше в ООО «ФастПроект», составляется Перечень сведений, составляющих коммерческую/служебную тайну и конфиденциальную информацию (Приложение А). Данный Перечень дает полное и всестороннее перечисление сведений, на которые распространяется режим сохранности конфиденциальной информации в ООО «ФастПроект».

1.2 Анализ защищаемого помещения

ООО «ФастПроект» занимается инженерно-техническим проектированием, а в частности разработкой проектной, конструкторской и другой технической документации, предназначенной для осуществления строительства. А именно:

- Инженерно-техническое проектирование производственных и промышленных зданий и сооружений (ЛМК)
- Инженерно-техническое проектирование бытовых и хозяйственных зданий и сооружений (ЛМК)

- Инженерно-техническое проектирование бескаркасных арочных сооружений (рулонная сталь)

- Инженерно-техническое проектирование коммерческих, общественных и административных зданий (ЛМК)

- Инженерно-техническое проектирование как в комплексе услуг «под ключ», так и отдельно по частям проекта (конструктивным, архитектурным, инженерно-технического решениям)

- Анализ и разработка (доработка) чертежей, документации и обработка инженерных решений, внесение предложений или их изменение, с целью увеличения срока эксплуатации и уменьшения стоимости инженерного проекта.

ООО «ФастПроект» является арендатором третьего этажа трехэтажного здания. На первом и втором этажах находятся помещения, принадлежащие сторонней организации. Схема контролируемой зоны ООО «ФастПроект» представлена на рисунке 1.

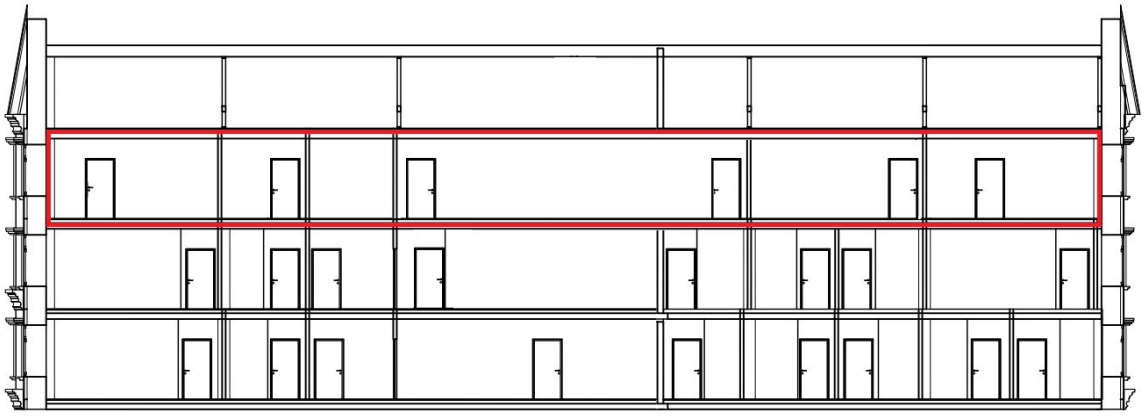

Рис.1. Контролируемая зона ООО «ФастПроект»

В настоящий момент в ООО»ФастПроект» введены следующие меры, связанные с защитой информации на предприятии:

- введен пропускной режим на этаж, принадлежащий ООО «ФастПроект»;

- разработаны правила противопожарной безопасности, внедрены системы противопожарной безопасности;
- в должностных инструкциях сотрудников перечислены пункты, связанные с неразглашением корпоративной информации и тайны;
- внедрено положение о конфиденциальном документообороте;
- на рабочих местах сотрудников установлено антивирусное программное обеспечение;
- внедрено разграничение прав доступа и парольная защита учетных записей на контроллере домена.

В переговорной комнате осуществляются встречи с заказчиками, обсуждаются вопросы относительно проектной документации, проходят внутренние совещания между руководством и начальниками подразделений организации. В обработке в переговорной комнате участвует информация следующего вида:

- Сведения, получаемые от клиентов организации в отношении реализуемых проектов;
- Сведения, предоставляемые заказчикам по реализуемым проектам;
- Информация финансового характера, относительно стоимости реализуемых проектов;
- Сведения, содержащие коммерческую тайну в отношении финансовых планов функционирования компании, маркетинговых планов работы, информации по договорам, сведения о планируемой деятельности компании.

Указанные данные, содержатся в разработанном в организации Перечне сведений, составляющих коммерческую тайну, следовательно, являются конфиденциальной информацией и подлежат защите. Так же данная информация является речевой. Из этого следует, что есть потенциальная угроза утечки конфиденциальной информации по следующим техническим канал утечки речевой информации:

- Акустический канал

- Виброакустический канал
- Оптико-электронный канал
- Акустоэлектрический канал
- Электромагнитный канал

Для анализа актуальных угроз информационной безопасности необходимо привести подробное описание объекта защиты. В данной работе речь идет о защите комнаты для переговоров. Первоначально комната была аттестована в соответствии с «Положением по аттестации объектов информатизации по требованиям безопасности информации» и «ГОСТ РО 0043-003-2012 Аттестация объектов информатизации. Общие положения»

В результате выполнения ремонтных работ были заменены: входная дверь и батарея отопления. Исходя из данного факта возникла потребность в выполнении анализа текущего уровня защиты и выработки рекомендаций в случае выявления несоответствия.

План размещения переговорной комнаты на арендуемом этаже представлен на рисунке 2. На этаже ниже, под защищаемым помещением, расположен рабочий кабинет сторонней организации. Слева от переговорной комнаты находится кабинет генерального директора организации, справа – кабинет заместителя руководителя организации.

В переговорной комнате отсутствуют основные технические средства и системы (ОТСС).

Контролируемая зона ограждена ограждающими конструкциями кабинета руководителя предприятия и кабинета заместителя руководителя предприятия. Ограждающими конструкциями помещения являются пол, потолок, стены, окно и дверь. Потолок выполнен из железобетонной плиты толщиной 160 мм.

Пол выполнен аналогично из железобетонной плиты толщиной 160 мм, поверх которой постелен линолеум толщиной 20мм. Дверь в переговорную комнату - стандартное полотно из дерево-стружечной плиты толщиной 40 мм;

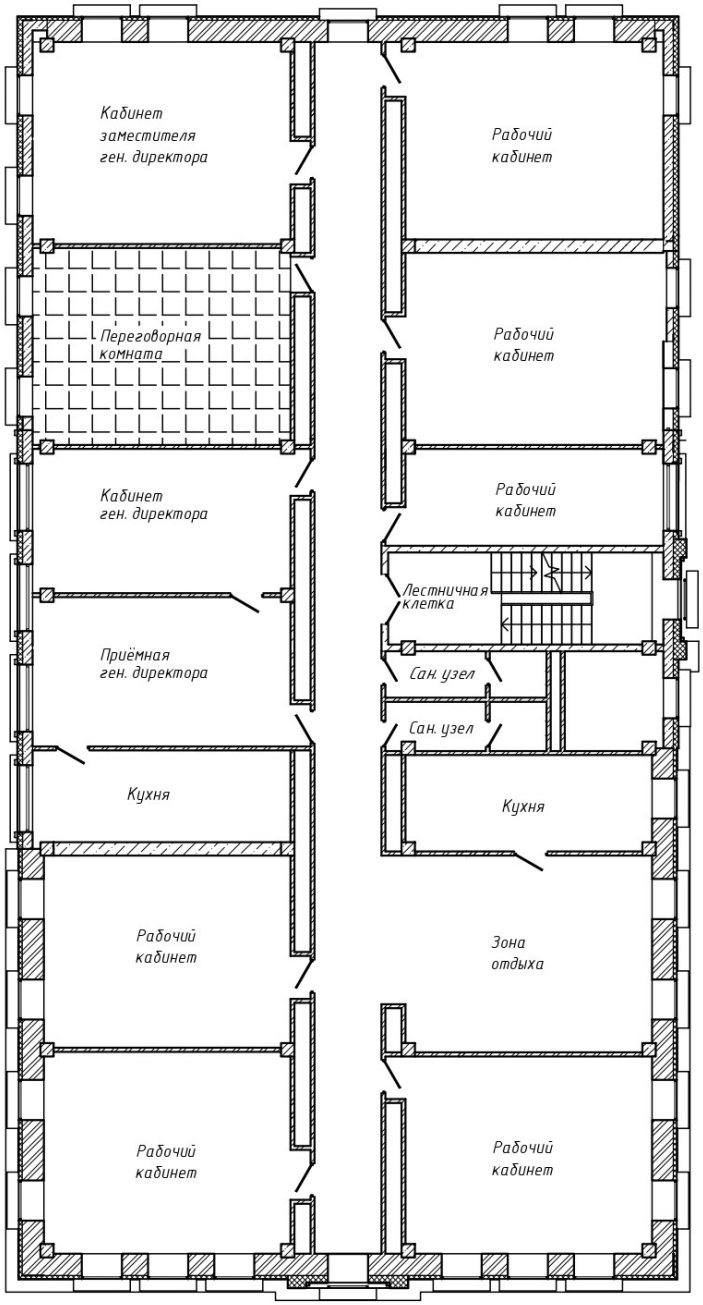

Рис.2. План размещения переговорной комнаты

Два окна в переговорной комнате расположены напротив входной двери. Окна имеют тройное остекленение. Стекла отделены от рамы резиновыми вибропоглощающими прокладками. На окнах установлены тканевые рулонные жалюзи.

Через переговорную комнату проходит система отопления, в состав которой входит два алюминиевых отопительных радиатора, а также полипропиленвоые трубы, проходящие сквозь переговорную комнату и выходящие за её пределы на первый этаж.

К вспомогательным средствам и системам относятся системы: пожарной сигнализации и оповещения о пожаре.

1.3 Анализ потенциальных угроз и каналов утечки информации

В зависимости от физической природы возникновения информационных сигналов, среды их распространения технические каналы утечки акустической (речевой) информации можно разделить на прямые акустические (воздушные), акустовибрационные (вибрационные), акустооптические (лазерные), акустоэлектрические.

1.3.1. Акустический канал утечки речевой информации

Несанкционированный доступ к конфиденциальной информации по акустическому каналу утечки может осуществляться путём:

- записи информации портативными средствами звукозаписи, скрытно установленными в защищаемом помещении;
- скрытой установки в защищаемом помещении закладных устройств с датчиками микрофонного типа, передающих информацию по радио, оптическим каналам, соединительным линиям вспомогательных средств сети электропитания напряжением 220 В, в телефонной или специально проложенным линиям;
- непреднамеренное подслушивание переговоров;
- прослушивания (записи) разговоров направленными микрофонами, установленными в ближайших строениях или транспортных средствах.

Действия со стороны злоумышленника по добыванию разведывательной информации может быть осуществлено непосредственным прослушиванием переговоров в защищаемом помещении:

- через дверь;
- через открытое окно (форточку);
- через стены, перегородки;
- через вентиляционные каналы.

Несанкционированный доступ к информации, циркулирующей в переговорной комнате во время проведения совещаний, злоумышленник может получить, используя технические средства, такие, как:

- направленные микрофоны;
- проводные микрофоны;
- радиомикрофоны;
- устройство "Электронное ухо".

Прослушивание переговоров через дверь возможно при условии, если вход в комнату для переговоров выполнен с нарушением требований по звукоизоляции. Не рекомендуется вести переговоры при открытых окнах. В таком случае непосредственный доступ к содержанию информации переговоров полностью открыт, невзирая на наличие звукоизоляции в помещении.

Если ограждающие конструкции (стены, перегородки, потолок и пол) комнаты для переговоров не проверены на предмет звукоизоляции и не отвечают требованиям нормативных документов, они так же могут быть потенциальными слабыми местами для утечки информации.

Вентиляционные каналы являются одними из самых опасных с точки зрения несанкционированного доступа к информации. Они могут быть использованы для прослушки переговоров в комнате на большом расстоянии (например, через этаж здания, или через несколько кабинетов). Поэтому к защите вентиляционных каналов предъявляются особые требования.

В качестве технических средств для прослушивания переговоров в основном используются направленные микрофоны. В зависимости от вида и модели микрофона и от помехозащитной обстановки расстояния прослушивания может достигать сотни метров.

Направленные микрофоны бывают нескольких видов, а именно:

- микрофоны с параболическим отражателем;
- резонансные микрофоны;
- щелевые микрофоны;
- лазерные микрофоны.
- проводные микрофоны.

Для прослушивания злоумышленники также используют и проводные микрофоны. В основном это микрофоны со специально проложенными проводами для передачи информации или микрофоны с возможностью передачи информации по линии сети в 220 В.

Так же для передачи конфиденциальной информации используются и другие виды коммуникаций (провода сигнализации, радиотрансляция и др.) Поэтому при проведение ремонтных работ этому следуют уделять особое внимание, так как существует возможность внедрения подслушивающих устройств, в том числе и с возможностью трансляции сигнала по радио каналу.

В последнее десятилетие злоумышленники стали применять устройства с использованием телефонных линий, позволяющие прослушивать разговоры в помещениях на значительном удалении (из других районов, городов и т.д.).

Такие устройства имеют название "Электронное ухо". Они также представляют большую угрозу для безопасности переговоров.

Согласно заключению, выданному компанией, проводившей аттестацию данного помещения, ограждающие конструкции, а именно стены, потолок и пол соответствуют нормам звукоизоляции, при этом из-за замены двери, имеется возможность утечки конфиденциальной информации путем непосредственного подслушивания через дверь, т.к. она, возможно, не обладает необходимыми звукоизоляционными свойствами. Таким образом утечка конфиденциальной информации по акустическому каналу из защищаемого помещения реальна и акустический канал является актуальным.

1.3.2. Виброакустический канал утечки речевой информации.

Воздействие акустических волн на поверхность твердого тела приводит к возникновению в нем вибрационных колебаний в результате виброакустического преобразования. Эти колебания, распространяющиеся в твердой среде, могут быть перехвачены специальными средствами разведки, а речевая информация, содержащаяся в акустическом поле, при определенных условиях может быть восстановлена. С этой целью используют устройства, преобразующие вибрационные колебания в электрические сигналы, соответствующие соответствующим звуковым частотам. Такие устройства называются вибродатчиками. Сигнал, снимаемый с выхода вибродатчика, после усиления может быть прослушан, зарегистрирован на магнитном или другом носителе, а также передан в пункт приема, находящийся на удалении от места прослушивания, по проводному, радио- или иному каналу передачи информации. Обобщенная структурная схема виброакустического канала утечки информации представлена на рисунке 3.

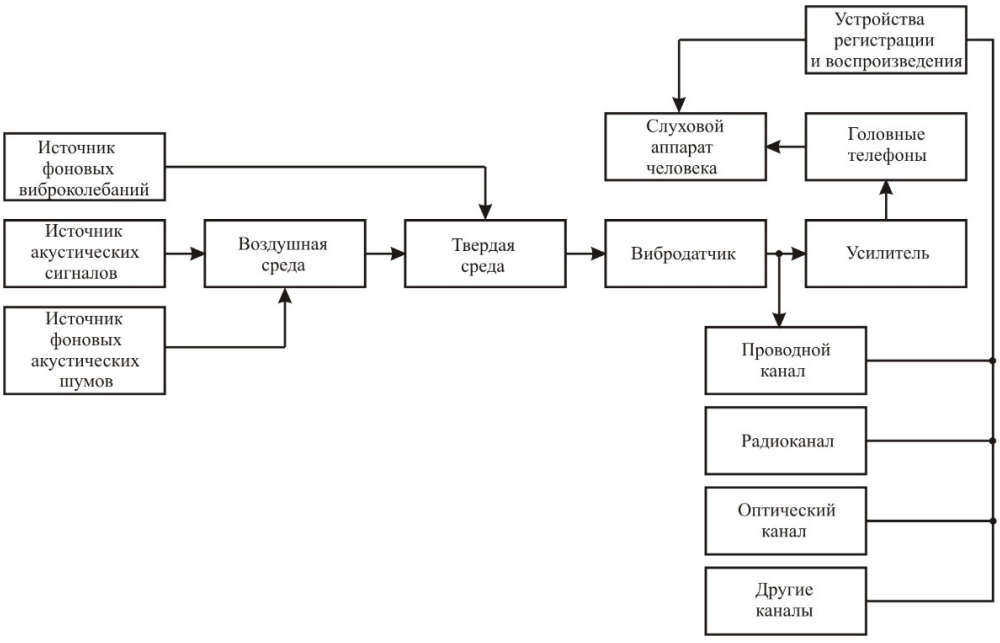

Рис. 3. Обобщенная структурная схема виброакустического канала утечки информации

Несанкционированный доступ к информации, циркулирующей в комнате совещаний, используя виброакустический канал, может быть осуществлен при помощи стетоскопов.

Стетоскопы позволяют провести прослушивание через стены толщиной до 1 м 20 см.

В зависимости от вида канала передачи информации от самого вибродатчика стетоскопы подразделяются на:

- проводные (проводной канал передачи);
- радио (канал передачи по радио);
- инфракрасные (инфракрасный канал передачи).

Согласно заключению, выданному компанией, проводившей аттестацию данного помещения, окна и ограждающие конструкции, а именно стены, потолок и пол обладают достаточной защищенностью от утечки по виброакустическому каналу. Система отопления, в связи с заменой, является потенциальным каналом утечки конфиденциальной информации. Следовательно, виброакустический канал является актуальным.

1.3.3. Оптико-электронный канал утечки речевой информации.

В случае, если переговоры ведутся в комнате, окна которой не оборудованы шторами или жалюзи, у злоумышленника есть возможность посредством облучения оконных стекол защищаемого помещения лазерными акустическими системами, установленными в ближайших строениях или транспортных средствах, зарегистрировать и распознать конфиденциальную информацию.

В соответствии с требованиями внутренних инструкций по ведению конфиденциальных переговоров, во время мероприятия окна должны быть закрыты шторами. Оптико-электронный канал является неактуальным.

1.3.4. Акустоэлектрический и электромагнитный каналы утечки речевой информации

Утечка конфиденциальной информации при ведении переговоров возможна из-за воздействия звуковых колебаний на элементы электрической схемы некоторых технических средств обработки информации.

К вспомогательным техническим средствам и системам относятся те, которые непосредственного участия в обработке конфиденциальной информации не принимают, но находятся в защищаемом помещении и могут быть причиной ее утечки. Примерами таких средств и систем могут быть системы оповещения о пожаре, некоторые типы датчиков охранно-пожарной сигнализации и др. Доступ к содержанию переговоров может быть осуществлен на значительном удалении от помещения, составляющем в некоторых случаях сотни метров.

Что касается телевизоров, то утечка конфиденциальной информации происходит здесь за счет имеющихся в них гетеродинов (генераторов частоты).

Причина утечки - модуляция звуковым колебанием при ведении разговора несущей частоты гетеродина, просачивание ее в систему с последующим излучением в виде электромагнитного поля.

В переговорной комнате присутствуют средства и системы охранно-пожарной сигнализации и оповещения о пожаре, которые относятся к вспомогательным. Однако, согласно отчету компании, которая проводила аттестацию помещения, данные вспомогательные средства отвечают нормам защищенности информации и не являются угрозой утечки акустической информации по акустоэлектрическому каналу.

Таблица 2

Оценка возможности утечки речевой конфиденциальной информации из переговорной комнаты

Наименование ТКУИ	Потенциальные угрозы	Возможность реализации угрозы
Акустический канал	Непосредственное преднамеренное или непреднамеренное подслушивание	Реализуем, так как дверь не отвечает требованиям по звукоизоляции

Продолжение таблицы 2

Виброакустический канал	Съем речевой информации с инженерных коммуникаций	Реализуем. Система отопления была заменена и возможно не отвечает требованиям по защите информации от утечки по данному каналу
Оптико-электронный канал	Съем информации посредством облучения оконных стекол защищаемого помещения лазерными акустическими системами	Не реализуем. Окна с тройным остеклением. Стекла отделены от рамы вибропоглощающими прокладками
Акустоэлектрический канал	Воздействие звуковых колебаний на элементы электрической схемы некоторых технических средств	Не реализуем. Имеющиеся вспомогательные средства соответствуют требованиям по защите акустической информации и имеют сертификаты соответствия
Электромагнитный канал	Съем информации за счет электромагнитных излучений технических средств обработки информации	Не реализуем, так как в помещении нет средств обработки информации

1.4 Описательная модель нарушителя

Под моделью нарушителя понимается совокупность количественных и качественных характеристик нарушителя, с учетом которых определяются требования к комплексу инженерно-технических средств охраны и/или его составным частям.

Составляющие модели нарушителя:

– категории нарушителя и его возможные тактические методы (внешние, внутренние, внешние в сговоре с внутренними);

– возможные действия нарушителя (применение силы, хищение, дезинформация и т.д.);

– причины и мотивы действий нарушителя (корысть, принуждение и т.д);

– возможности нарушителя (навык, опыт, количество, оснащенность-техника, оружие, транспорт).

«Внешний нарушитель» - нарушитель из числа лиц, не имеющих права доступа в охраняемые зоны;

«Внутренний нарушитель» - нарушитель из числа лиц, имеющих право доступа без сопровождения в охраняемые зоны;

«Внешняя угроза» - угроза, исходящая от внешнего нарушителя;

«Внутренняя угроза» - угроза, исходящая от внутреннего нарушителя.

Для описания моделей нарушителей в качестве критериев классификации рассматриваются:

1. Цели и задачи вероятного нарушителя:
   - проникновение на охраняемый объект без причинения объекту видимого ущерба;
   - причинение ущерба объекту;
   - преднамеренное проникновение при отсутствии враждебных намерений;
   - случайное проникновение.

2. Степень принадлежности вероятного нарушителя к объекту:
   - вероятный нарушитель - сотрудник охраны;
   - вероятный нарушитель - сотрудник учреждения;
   - вероятный нарушитель - посетитель;
   - вероятный нарушитель - постороннее лицо.

3. Степень осведомленности вероятного нарушителя об объекте:
   - детальное знание объекта;
   - осведомленность о назначении объекта, его внешних признаках и чертах;

- неосведомленный вероятный нарушитель.

4. Степень осведомленности нарушителя о системе охраны объекта:

- полная информация о системе охраны объекта;
- информация о системе охраны вообще и о системе охраны конкретного объекта охраны;
- информация о системе охраны вообще, но не о системе охраны конкретного объекта;
- неосведомленный вероятный нарушитель.

5. Степень профессиональной подготовленности вероятного нарушителя:

- специальная подготовка по преодолению систем охраны;
- вероятный нарушитель не имеет специальной подготовки по преодолению систем охраны.

6. Степень физической подготовленности вероятного нарушителя:

- специальная физическая подготовка;
- низкая физическая подготовка.

7. Владение вероятным нарушителем способами маскировки.

8. Степень технической оснащенности вероятного нарушителя.

9. Способ проникновения вероятного нарушителя на объект.

На основе изложенных критериев выделяют четыре категории нарушителя:

1) нарушитель первой категории - специально подготовленный по широкой программе, имеющий достаточный опыт нарушитель-профессионал с враждебными намерениями, обладающий специальными знаниями и средствами для преодоления различных систем защиты объектов;

2) нарушитель второй категории - непрофессиональный нарушитель с враждебными намерениями, действующий под руководством другого субъекта, имеющий определенную подготовку для проникновения на конкретный объект;

3) нарушитель третьей категории - нарушитель без враждебных намерений, совершающий нарушение безопасности объекта из любопытства или из каких-то иных личных намерений;

4) нарушитель четвертой категории - нарушитель без враждебных намерений, случайно нарушающий безопасность объекта.

Предполагаемый злоумышленник (нарушитель первой категории) – это человек подготовленный, знающий все каналы утечки информации в комнатах для ведения переговоров, профессионально владеющий способами и средствами добывания сведений, содержащих конфиденциальную информацию. В качестве данного нарушителя может выступать сотрудник сторонней организации.

Модель нарушителя и угроз позволяет сделать вывод о том, что акустический и виброакустический каналы являются наиболее опасными для утечки конфиденциальной информации, циркулирующей в переговорной комнате при проведении совещаний. Следовательно, в основу развития данной выпускной квалификационной работы войдёт анализ данных каналов утечки речевой конфиденциальной информации, а также методы и средства по уменьшению рисков, которые могут возникнуть вследствие утечки информации.

Выводы по первой главе

ООО «ФастПроект» занимается инженерно-техническим проектированием, а в частности разработкой проектной, конструкторской и другой технической документации, предназначенной для осуществления строительства. Соответственно, вся обрабатываемая информация для данной организации является ценной. Исходя из данного факта, в организации реализована система защиты информации, а помещения, в которых осуществляется обмен информацией конфиденциального характера, проходили специализированную аттестацию по отсутствию каналов утечки информации. В результате выполнения ремонтных работ в переговорной комнате была заменена дверь, а также проведена замена системы отопления. Данные факты изменили

существующую ранее общую структуру переговорной комнаты, что могло повлиять на возникновение возможных каналов утечки информации по акустическому и виброакустическому каналу. На основании данного факта было принято решение о проведении подробного анализа защиты помещения, и выработке рекомендаций по её модернизации.

ГЛАВА 2. ОЦЕНКА СОСТОЯНИЯ ЗАЩИТЫ АКУСТИЧЕСКОЙ ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ СОВЕЩАНИЙ

Проанализировав основные и вспомогательные технические средства, и системы, находящиеся в защищаемом помещении, а также его конструктивные и архитектурные особенности, приступим к оценке защищённости ЗП от утечки по акустическому и виброакустическому каналам связи.

2.1 Организационные меры при проведении совещаний

Основные положения организационно-режимных мероприятий обеспечения конфиденциальности информации, циркулирующей в защищаемом помещении:

- совещание с участием представителей сторонних организаций должно проводиться с разрешения директора ООО «ФастПроект», который, в свою очередь, назначает ответственного за проведение совещания;
- ответственное лицо, совместно с представителями службы безопасности и соответствующими техническими специалистами проводит необходимые организационные и технические мероприятия, направленные на обеспечение сохранения конфиденциальности обсуждаемых вопросов;
- очерёдность рассмотрения вопросов, вынесенных на совещание, должна исключать участие лиц, не имеющих отношение к рассматриваемым вопросам (ответственное лицо должно составить проект программы совещания и список участников, в котором указывается фамилия, имя отчество, место работы, должность и вопросы, в обсуждении которых он может принимать участие);
- участники пропускаются на совещание по спискам при предъявлении документов, удостоверяющих личность;
- меры при защите информации при проведении совещаний с участием представителей сторонних организаций направлены на подготовку

соответствующего помещения и предотвращение утечки информации из него, с учётом особенностей проводимого совещания.

Целесообразно и обоснованно применение следующих организационных мер:

- перед проведением совещания необходимо проводить визуальный осмотр помещения на предмет выявления закладных устройств. Осмотр должен проводиться систематизировано и тщательно, обращая внимание на любую мелочь, на первый взгляд незначительную: наличие посторонних предметов, бытовой аппаратуры или предметов интерьера. Осмотр по возможности, должен проводиться сотрудником службы безопасности и человеком, хорошо знакомым с обычной обстановкой помещения, например, сотрудником безопасности и режима;
- непосредственно перед проведением совещания, сотрудник безопасности и режима должен осматривать прилегающие к защищаемому помещению прилегающие помещения на предмет удаления из них сотрудников или посторонних лиц, которые могут вести подслушивание непосредственно через систему вентиляционных коммуникаций или через стену при помощи специальной аппаратуры; закрывать эти помещения на время проведения совещания и вести контроль за доступом в них;
- количество лиц, участвующих в конфиденциальных переговорах должно быть ограничено до минимума;
- вход посторонних лиц во время проведения совещания должен быть запрещён;
- должна быть чётко разработана охрана выделенного помещения во время совещания, а также наблюдение за обстановкой на этаже. Во время проведения закрытого совещания необходимо не допускать близко к дверям комнаты никого из посторонних лиц или сотрудников организации. Стоя под дверью, или поблизости от неё, злоумышленник может подслушать то, о чем говориться в комнате. Особенно это вероятно в те моменты, когда кто-то входит

или выходит из зала, так как на то время, пока дверь остаётся открытой, разборчивость речи резко повышается. Помимо этого, выходя или входя, человек может не совсем плотно закрыть за собой дверь, что также повысит разборчивость речи. Для реализации этой меры необходимо, чтобы в течение всего времени, которое длится совещание, у двери комнаты дежурил охранник, осуществляющий контроль за дверью и коридором около входа в комнату, а также следить за тем, чтобы никто из посторонних не проник внутрь;

- Для большей надежности, у дверей зала должен дежурить охранник из постоянного штата организации, так как подобное дежурство создает возможность подслушивания непосредственно охранником;
- по возможности проведение совещаний переносить на нерабочее время;
- любые работы в комнате, проводимые вне времени проведения конфиденциальных совещаний, например, уборка, ремонт бытовой техники, мелкий косметический ремонт, должен проводиться в обязательном присутствии сотрудника службы безопасности. Наличие этих сотрудников поможет обезопасить помещение от установки подслушивающих устройств сотрудниками организации или же посторонними лицами (электромонтёр, рабочие, уборщица и так далее);
- после проведения совещания комната должна тщательно осматриваться, закрываться и опечатываться;
- между совещаниями комната должна быть закрыта и опечатана ответственным лицом. Ключи от комнаты должны быть переданы дежурной смене охраны под расписку и храниться в комнате охраны, доступ к ним должен быть регламентирован руководством.

Перечисленные меры организационной защиты информации в защищаемом помещении считаются весьма действенными и не несут серьезных материальных затрат или проблем с персоналом и могут применяться как

отдельно, так и совместно, что позволит значительно повысить степень защиты информации рассматриваемого помещения.

2.2 Оценка защищенности защищаемого помещения от утечки речевой конфиденциальной информации

Оценка защищенности помещения состоит из четырёх этапов, приведенных ниже.

На первом этапе проводится осмотр защищаемого помещения на предмет наличия в ограждающих конструкциях и инженерно-технических сооружениях люков вентиляционных шахт, трубопроводов, акустических отверстий и т.п. Помимо осмотра защищаемого помещения необходимо произвести анализ прилегающих помещений. Результаты по данному этапу приведены в первой главе.

На втором этапе осуществляется выбор контрольных точек для размещения контрольно-измерительных приборов.

На третьем этапе проводится установка и коммутация комплекса контрольно-измерительных приборов и аппаратуры для проведения анализа тестового сигнала. Измерительная аппаратура собирается по блок-схеме, приведенной на рисунке 4.

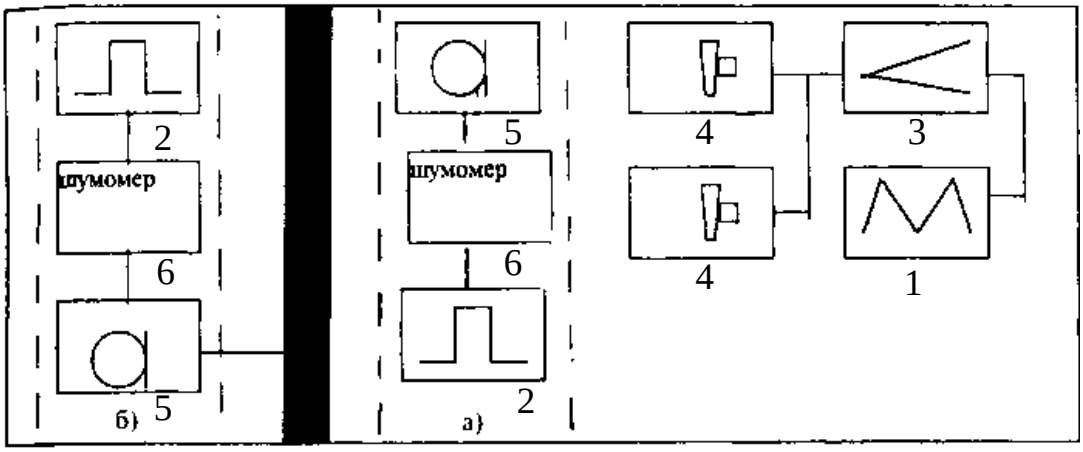

Рис. 4. Блок-схема измерений: а) в помещении; б) вне помещения.

1 - генератор шума; 2 - октавные фильтры; 3 - усилитель мощности;

4 - акустические системы; 5 - измерительный микрофон; 6 - шумомер

На четвертом этапе выполняются измерение тестового сигнала и анализ (расчет) проведённых измерений.

В состав измерителя акустического и виброакустического сигнала необходима следующая аппаратура:

Для измерителя акустического сигнала:

- измерительный микрофон;
- микрофонный усилитель;
- измеритель шумов и вибраций.

Для измерителя виброакустического сигнала:

- измерительный вибродатчик с предусилителем;
- измеритель шумов и вибраций.

При измерениях в качестве тестового сигнала используют гармонические сигналы с частотами соответствующими среднегеометрическим частотам октавных полос: 250; 500; 1000; 2000; 4000 Гц и уровнями звукового давления, не менее типовых уровней (L) речевого сигнала в октавных полосах частотного диапазона речи, которые приведены в таблице 3.

Таблица 3

Типовые уровни речевого сигнала в октавных полосах частотного диапазона речи

Октавные полосы	250 Гц	500 Гц	1000 Гц	2000 Гц	4000 Гц
L (dB) для речи средней громкости (интегральный уровень 70 (dB)	66	66	61	56	53

Для уменьшения погрешностей измерения, вызываемых дифракционными волновыми акустическими процессами, дополнительно проводятся по три измерения на каждой из приведенных выше частот. Результирующее значение вычисляется как среднее арифметическое трех измерений.

Размещение измерительной аппаратуры зависит от характера ограждающей конструкции.

Размещение акустического излучателя:

- для ограждающей конструкции типа - стена, дверь, окно и т.п. акустический излучатель размещается на высоте 1-1,5м от пола и на расстоянии 1,5м от ограждающей конструкции. Ось апертуры акустического излучателя направляется в сторону ограждающей конструкции по нормали к ее поверхности;

Измерительный микрофон при измерении:

- уровня излучаемого тестового сигнала в защищаемом помещении размещается на осевой линии апертуры акустического излучателя на расстоянии 1 м от плоскости апертуры и на расстоянии 0,5м от поверхности ограждающей конструкции или элемента инженерно-технической системы;
- уровня акустического сигнала и акустического шума в контрольной точке размещается в выбранной точке контроля на расстоянии 0,5м от поверхности ограждающей конструкции,

Измерительный вибродатчик размещается в выбранной контрольной точке непосредственно на поверхности ограждающей конструкции или на контролируемом элементе инженерно-технической системы.

2.2.1 Оценка защищенности защищаемого помещения от утечки речевой конфиденциальной информации по акустическому каналу

При расчетах проводится сравнительный анализ полученных октавных коэффициентов звукоизоляции с их нормативными значениями и делается вывод о защищенности помещения от утечки речевой конфиденциальной информации по акустическому каналу. Результаты оформляются документально. Рекомендуемая форма протокола приведена в приложении1.

Проведение оценки защищенности ЗП от утечки по акустическому каналу предполагает изначально проверку соответствия установленным требованиям разности величин измеренного параметра акустической защищенности

помещения и требуемого ($Q_{изм}$ - $Q_{норм.}$ (dB). Сущность проводимых расчетов заключается в уточнении значений акустического давления измеренного звукового сигнала в соответствии с приведенными ниже математическими выражениями.

Среднее значение величины акустического давления для контрольной точки на октавных полосах:

$$L_{2ср} = \sum F_i / n, \text{ при } i = \{1..n\} \quad (1)$$

Уточнение значения акустического давления производится из условий следующей системы:

$$\begin{cases} L_{2сигн.} = L_{сигн.+шум}, \text{ если } L_{2сигн.+шум} - L_{шум} \geq 10\text{дБ} \\ L_{2сигн.} = L_{сигн.+шум} - \Delta, \text{ если } L_{2сигн.+шум} - L_{шум} < 10\text{дБ} \end{cases}, \quad (2)$$

где величина Δ определяется из таблицы 4;

$L_{шум}$ = 30 дБ.

Таблица 4

Таблица значений Δ

$(L_{2сигн.+шум})$-$(L_{шум})$	≥ 10	6 ÷10	÷ 6	3	2	1	0,5
Δ	0	1	2	3	4	7	0

Параметр акустической защищенности в точках контролируемой зоны для каждой октавной полосы (250, 500, 1000, 2000, 4000Гц) вычисляется по формуле:

$$Q_{изм.i} = L_{1сигн.i} - L_{2сигн.i}, \quad (3)$$

где: $L_{1сигн.i}$ –акустическое давление внутри помещения;

$L_{2сигн.i}$ - акустическое давление вне помещения в контрольной точке.

Выберем $Q_{нормі}$ из таблицы 5 для условий, соответствующих реальным в данной работе (защищаемое помещение не оборудовано системами звукоусиления).

Таблица 5

Требования нормативных значений

Место возможного перехвата речевой конфиденциальной информации		Нормативное значение параметра акустической защищенности помещения, дБ	
		Помещения, не оборудованные системами звукоусиления	Помещения, оборудованные системами звукоусиления
Смежные помещения		46 $Q_{норм.}$ (dB)	60
Уличное пространство	Улица без транспорта	36	50
	Улица с транспортом	26	40

$Q_{нормі}$= 46 дБ.

Соответствие параметра акустической защищенности помещения установленным требованиям определяется по следующей системе:

$$\begin{cases} \text{соответствует, если } Q_{расчі} - Q_{нормі} \geq 0 \\ \text{не соответствует, если } Q_{расчі} - Q_{нормі} < 0 \end{cases} ; \quad (4)$$

В качестве контрольной точки выбирается внешняя сторона входной двери в соответствии с определенным ранее размещением измерительной аппаратуры. Результаты расчёта приведены в таблице 6.

Таблица 6

Параметры для контрольной точки

Параметры	250 Гц	500 Гц	1000 Гц	2000 Гц	4000 Гц

1	2	3	4	5	6
L1 (dB)	80	80	75	70	67

Продолжение таблицы 6

1	2	3	4	5	6
$L2_{сигн + шум}$(dB)*	55,9	57,2	58,1	54,7	51,4
$L2_{сигн}$(dB)*	55,9	57,2	58,1	54,7	51,4
$Q_{изм.}$ (dB)*	24,1	22,8	16,9	15,3	15,6
$Q_{норм.}$ (dB)	46	46	46	46	46
$Q_{изм} - Q_{норм.}$ (dB)	-21,9	-23,2	-29,1	-30,7	-30,4
Соответствие	–	–	–	–	–

Исходя из результатов таблицы 6, можно сделать вывод, что параметры не соответствуют установленным требованиям, значит, требуется предпринять меры по улучшению акустической защищенности элементов помещения и контролируемой зоны.

2.2.2 Оценка защищенности защищаемого помещения от утечки речевой конфиденциальной информации по виброакустическому каналу

Измерению была подвергнута отопительная труба.

Произведем расчет величины вибрационного сигнала - V_{c2i}, при помощи таблицы 7 и формул приведенных ниже:

$$V_{c2i} = \begin{cases} V_{(с+ш)i} & V_{(с+ш)i} - V_{шi} \geq 10 \\ V_{(с+ш)i} - \Delta \quad \text{при} & V_{(с+ш)i} - V_{шi} < 10 \end{cases}, \qquad (5)$$

Таблица 7

Частотный диапазон речи

Номер полосы	Частотные границы полосы $f_н$…..$f_в$ Гц	Среднегеометрическая частота полосы f_i Гц	Весовой коэффициент полосы, k_i
1	90…175	125	0,01
2	175…355	250	0.03
3	355…710	500	0.12
4	710…1400	1000	0.20
5	1400…2800	2000	0.30
6	2800…5600	4000	0.26
7	5600…11200	8000	0.07

Коэффициент затухания вибрационного сигнала в тракте «источник речи – контрольная точка» вычисляется по формуле приведенной ниже:

$$ZV_i = L_{c1i} - V_{c2i} \quad (6)$$

Расчёт уровня скрываемого вибрационного сигнала V_{ci} для каждой октавной полосы (в соответствии с типовым значением (для данного ЗП) интегральным уровнем речи L_s (очень громкая речь) (таблица 8)) производится по формуле:

$$V_{ci} = L_{si} - ZV_i \quad (7)$$

Расчет отношения сигнал/шум q_i для каждой октавной полосы производится по формуле:

$$q_i = V_{ci} - V_{ши} \quad (8)$$

Относительный уровень интенсивности формант Q_i для каждой октавной полосы рассчитывается формуле:

$$Q_i = q_i - \Delta A_i, \quad (9)$$

где ΔA_i - разность между спектральными уровнями речи и формант. Ее значение выбирается для каждой полосы из таблицы 9.

Таблица 8

Ориентировочные значения уровня громкости некоторых звуков и типовой интегральный уровень очень громкой речи

Звук	Уровень громкости, дБ	Среднегеометрическая частота полосы, Гц	Типовой интегральный уровень очень громкой речи Ls, дБ
Тиканье часов	20	250	72
Шепот на расстоянии 1м	30	500	72
Тихий разговор	40	1000	67
Речь средней громкости	60	2000	62
Громкая речь	70	4000	59
Очень громкая речь	76		
Крик	80		
Шум самолетного мотора:			
- на расстоянии 5м	120		
- на расстоянии 3м	130		

Таблица 9

Числовое значение ΔA

Среднегеометрические частоты октавных полос f_{cpi}, Гц	50	500	1000	2000	4000
Числовое значение ΔA (формантного параметра спектра речевого сигнала в	18	14	9	6	5

октавной полосе), дБ					

По графику, приведенного на рисунке 4, определим коэффициент восприятия формант для каждой *i*-ой октавной полосы P_i

На рисунке 4 показана зависимость коэффициента восприятия формант *P* от относительного уровня интенсивности формант *Q*.

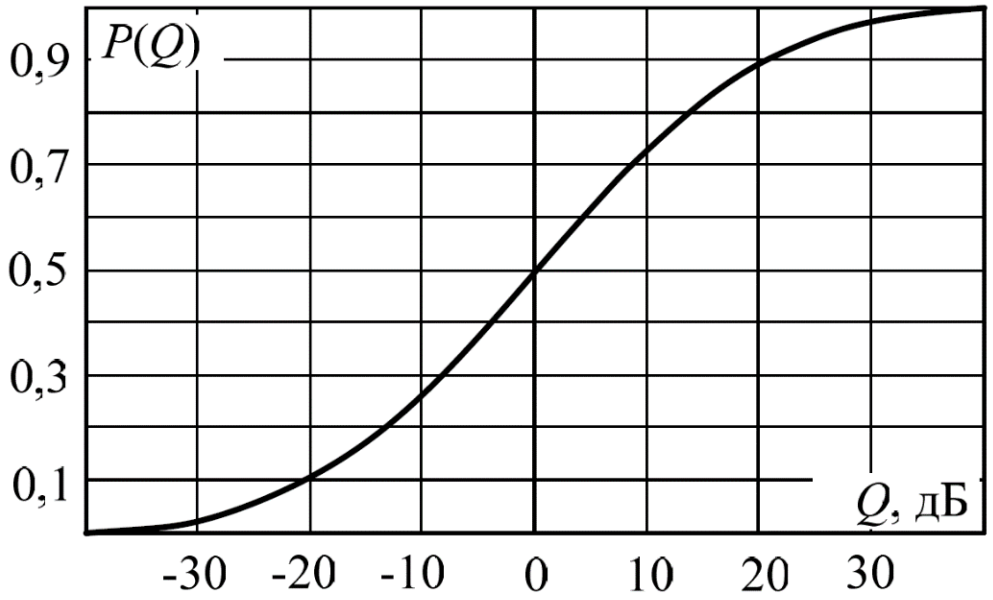

Рис. 4. Зависимость коэффициента восприятия формат от относительного уровня интенсивности формат

Интегральный индекс артикуляции речи (формантная разборчивость) рассчитывается по формуле:

$$R_i = k_i * P_i, \quad (10)$$

где k_i - весовой коэффициент *i*-й октавной полосы (таблица 5)

Общий индекс артикуляции речи R:

$$R = \sum_{i}^{n} R_i \quad (11)$$

По графикам, изображенным на рисунках 5 и 6, определим числовые значения слоговой *S*, а затем и словесной W разборчивости.

Результаты всех расчётов запишем в таблицу 12

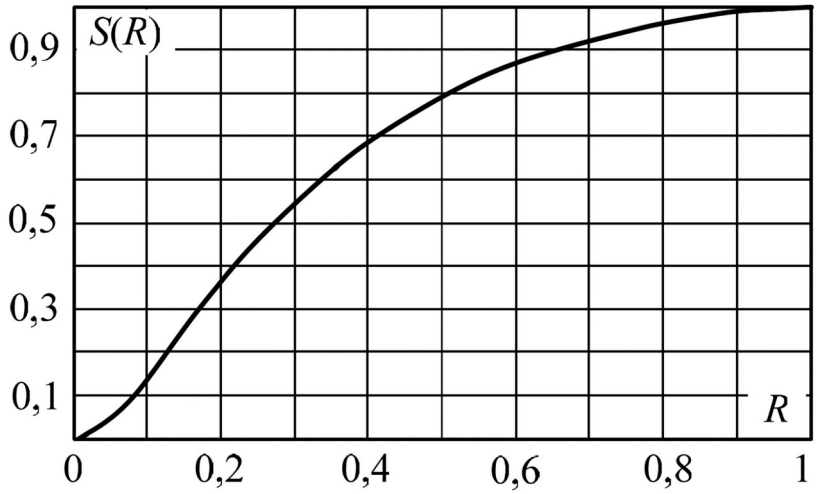

Рис.5. Зависимость слоговой разборчивости от индекса артикуляции речи

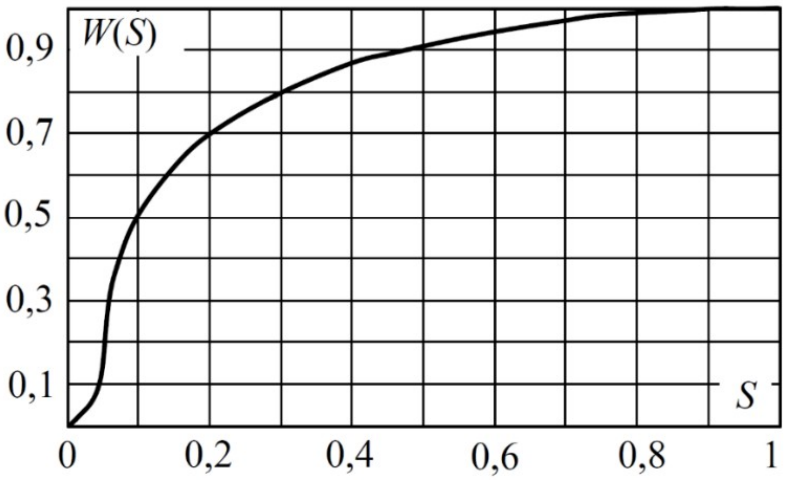

Рис.6. Зависимость словесной разборчивости от слоговой разборчивости речи

Определим характеристику качества понятности речи относительно полученного значения словесной разборчивости по таблице 10.

Таблица 10

Слоговая и словесная разборчивость

Разборчивость		
	Слоговая S	Словесная W
Предельно допустимая	25-40	75-87
Удовлетворительная	40-50	87-93
Хорошая	50-80	93-98

Отличная	80 и выше	98 и выше

Результаты измерений и расчетов по приведенным выше формулам приведены в таблице 11 и 12 соответственно.

Таблица 11

Таблица измерений

Измеряемые показатели (дБ)		Номер октавной полосы (средняя геометрическая частота)				
		1 (250 Гц)	2 (500 Гц)	3 (1000 Гц)	4 (2000 Гц)	5 (4000 Гц)
$V_{ші}$	1	-15	-30	-15	-30	-30
1	L_{c1i}	72.1	72.2	67	62.1	59.3
	$V_{(с+ш)i}$	45	12.5	32	27	11
Сред.	L_{c1i}	72.1	72.2	67	62.1	59.3
	$V_{(с+ш)i}$	45	12.5	32	27	11

Таблица 12

Таблица расчетов

Номер октавной полосы	1	2	3	4	5
V_{c2i}	45	12,5	32	27	11
ZV_i	27,1	59,7	35	35,1	48,3
L_{si}	72	72	67	62	59
V_{ci}	44,9	12,3	32	26,9	10,7
q_i	59,9	42,3	47	56,9	40,7
Q_i	41,9	28,3	38	50,9	35,7
P_i	1	0,95	1	1	1
R_i	0,03	0,114	0,2	0,3	0,26
R	0,90				
S	0,99				
W	~1				

Полученное итоговое значение словесной разборчивости и сравнение с табличными данными позволяет сделать вывод о том, что в нашем случае величина разборчивости находится на отметке «отличная» (W>0,98), следовательно, возможность несанкционированного получения конфиденциальной информации через виброакустических канал утечки по трубам отопления реален.

2.3 Технические меры по защите акустической информации в защищаемом помещении.

Методы и средства защиты речевой информации от утечки по акустическому и виброакустическому каналам основаны на уменьшении отношения «сигнал/шум». При этом различают пассивные и активные методы[6].

Пассивные методы направлены на уменьшение уровня информативного сигнала за счет улучшения звуко- и виброизоляции инженерных конструкций и установки фильтрующих устройств в проводных коммуникациях.

Активные методы основаны на увеличении уровня шума по отношению к естественному (фоновому) и реализуются с помощью технических средств, основу которых составляют различные генераторы шума.

На практике чаще всего используют так называемые «белый», «розовый» и речеподобный шумы (рисунок 7), (графики 1, 2, 3 соответственно), различающиеся формой огибающей спектра.

Целесообразность использования того или иного вида помех определяется многими факторами (в частности преследуемыми целями: маскирование, имитация, обеспечение максимальной комфортности переговоров и т.п.). С точки зрения обеспечения минимума интегрального уровня помех, наиболее эффективной является речеподобная помеха. С точки зрения защиты речевой информации при проведении конфиденциальных переговоров технические

средства защиты можно подразделить на две группы: средства защиты помещений и средства защиты собственно речевой информации.

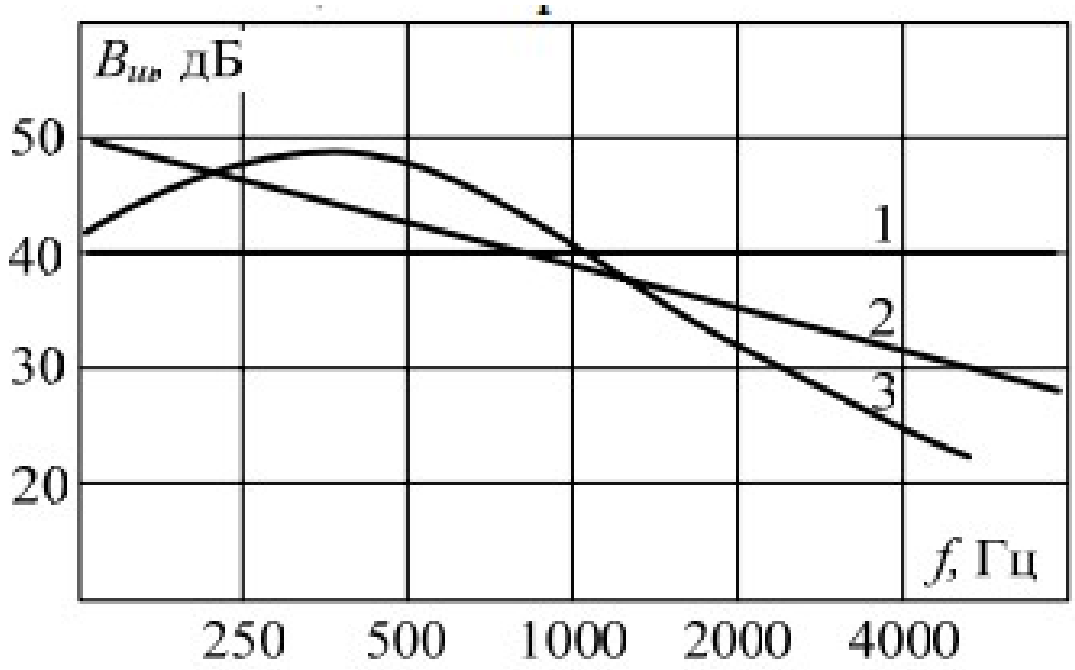

Рис.7. Виды шумов

К первой группе относится аппаратура постановки помехи на границе защищаемого помещения («вдоль» ограждающих конструкций) – это генераторы акустического и виброакустического шума. Ко второй группе – аппаратура акустического зашумления, располагающаяся в непосредственной близости от места нахождения участников переговоров.

Очевидно, что в первом случае при достаточно комфортных условиях для находящихся в помещении людей не гарантируется защита речевой информации по всему объему помещения (например, от утечки за счет скрытно установленных внутри помещения специальные технические средства (СТС) типа радиомикрофонов, диктофонов и т.п.). Следовательно, требуются дополнительные организационно-технические меры по выявлению и/или блокированию таких СТС.

Во втором случае вероятность утечки речевой информации за счет любых СТС, содержащих микрофоны, близка к нулю, но возникает проблема

обеспечения комфортности переговоров, поскольку участники находятся под непосредственным воздействием акустического шума.

Выводы по второй главе

Оценка защищенности была проведена в соответствии с методикой оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам. В результате измерений и расчетов было выявлено, что входная дверь и система отопления не соответствуют нормам показателей защищенности от утечки по акустическому и виброакустическому каналам.

Исходя из данного факта необходимо предусмотреть меры, как активные, так и пассивные, направленные на улучшение защищенности помещения от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам.

ГЛАВА 3. РЕКОМЕНДАЦИИ ПО ПОВЫШЕНИЮ УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В ЗАЩИЩАЕМОМ ПОМЕЩЕНИИ

3.1 Перечень мероприятий по совершенствованию защиты информации в защищаемом помещении

Для осуществления полной защищенности акустической (речевой) информации при проведении совещания в рассматриваемой организации, необходимо применение в комплексе последующих предложенных рекомендаций.

Для защиты акустической (речевой) информации используются активные и пассивные методы и средства:

1. Энергетическое скрытие путем:

- звукоизоляции акустического сигнала;
- звукопоглощения акустической волны;
- зашумления помещения или твердой среды распространения другими широкополосными звуками, которые обеспечивают маскировку акустических сигналов.

2. Обнаружение, локализация и изъятие закладных устройств.

К пассивным методам относится звукоизоляция и экранирование.

В условиях совещания неуместно уменьшение громкости речи, поэтому для защиты такой информации следует применять звукоизоляцию, звукопоглощение и глушение звука.

Звукоизоляция локализует источники акустических сигналов в замкнутом пространстве, в данном случае в комнате для переговоров. Основное требование к звукоизоляции: за пределами комнаты соотношение сигналов/помеха не должно превышать максимально допустимые значения, исключающие добывание информации злоумышленниками [12].

Применительно к рассматриваемому объекту, необходима звукоизоляция отопительной системы, а также использование звукоизолирующих покрытий для двери.

Для предотвращения утечки информации по отопительным системам необходимо использование экранирования батарей. Экраны изготовляются в основном из алюминия и покрываются сверху слоем пенопласта или какого-либо другого изолирующего материала.

Звукоизоляцию в помещении можно повысить, применив звукопоглощающие материалы.

Так как для достижения наибольшей эффективности снижения уровня опасного сигнала площадь акустической отделки помещений должна составлять не менее 60%, то для защиты помещения лучше всего применить для отделки стен и потолка панели из пенопласта (с зазором 3 мм).

Кроме пассивных методов, рассмотренных выше, целесообразно применение и активных методов, например, генераторы шума.

Одним из распространенных генератором шума является устройство DNG-2300, предназначенный для защиты помещений от подслушивания при помощи радиотехнических, лазерных, акустических и других средств. Позволяет защищать от утечки информации через стены, окна, трубы отопления и водоснабжения, вентиляционные колодцы и т. п.[13]

Устройство работает в режиме «дежурного приема», то есть включается только в случае, если в защищенном помещении начинается разговор.

Другим, аналогичным по назначению устройством, является изделие «Кабинет» СНПО «Элерон», предназначенное для предотвращения прослушивания речевой информации за пределами защищаемого помещения. Принцип действия основан на создании маскирующего вибрационного шума в ограждающих конструкциях и акустического шума в объеме помещения и вне его.

В целом, как показывает практика, применение описанных генераторов шума не нарушает комфортности при работе в защищенном с их помощью помещении. Однако, с точки зрения полной комфортности работы человека в помещении, по мнению специалистов, является комплекс виброакустической защиты «Стена-105», в котором реализованы возможности по оптимальной настройке помехового сигнала. Имеющаяся в комплексе система настройки спектра помехи (эквалайзер) позволяет обеспечить необходимое превышение уровня помехи над уровнем речевого сигнала при минимальном воздействии на людей, то есть создать оптимальную помеху. Использование именно этого генератора рекомендуется для рассматриваемой комнаты для совещаний.

3.2 Повышение защищенности информации в защищаемом помещении

3.2.1 Защита от утечки через прямой акустический канал

Защита от утечки через прямой акустический канал является весьма сложной задачей, так как генераторы шума для данного канала работают в том же диапазоне частот, что и человеческая речь. Это существенно мешает нормальной работе людей в помещении, где установлен такой генератор, поэтому для защиты данного помещения будет использована одинарная звукоизолирующая тяжелая дверь с прокладками из пористой резины.

На данный момент установлено стандартное полотно из дерево-стружечной плиты толщиной 40 мм, без уплотнительных прокладок.

Для обеспечения требуемого значения параметра акустической защищенности выбираем другую конструкцию двери, с условием, что $Q_{fi} > Q_{нормi}$ ($Q_{fi} = Q_{нормi}$). Для защиты помещения будет использована одинарная звукоизолирующая тяжелая дверь с прокладками из пористой резины. Показатели звукоизоляции данной двери отражены в таблице 13. Данные будем заносить в таблицу 14.

Таблица 13

Звукоизоляция тяжелой двери с прокладками из пористой резины

Конструкция	**Примечание**	**Значение Q_{fi} (дБ) для частоты f (Гц)**				
		250	**500**	**1000**	**2000**	**4000**
Дверь звукоизолирующая тяжелая. Прокладки из пористой резины	Одинарная	36	45	51	50	49

В строке $Q_{изм.}+Q_{fi}$ таблицы 13, прибавим значения Q_{fi} (дБ) для частоты f (Гц) к предыдущему параметру акустической защищенности $Q_{изм}$ в точках контролируемой зоны для каждой октавной полосы (250, 500, 1000, 2000, 4000Гц)

Таблица 14

Пересчет параметров для КТ. Монтаж звукоизолирующей двери

Параметры	**250 Гц**	**500 Гц**	**1000 Гц**	**2000 Гц**	**4000 Гц**
L1 (dB)	66	66	61	56	53
$L2_{сигн+шум}$(dB)*	49,2	50,5	52,1	46,8	39,6
$L2_{сигн}$(dB)*	49,2	50,5	52,1	46,8	39,6
$Q_{изм.}+Q_{fi}$ (dB)*	16,8+36 =52,8	15,5+45=60,5	8,9+51=59,9	9,2+50=59,2	13,4+49=62,4
$Q_{норм.}$ (dB)	36	36	36	36	36
$Q_{изм}+Q_{fi}$ - $Q_{норм.}$ (dB)	16,8+36 - 36=16,8	15,5+45- 36=24,5	8,9+51- 36=23,9	9,2+50- 36=23,2	13,4+49- 36=26,4
Соответствие	+	+	+	+	+

Нормативный параметр акустической защищённости $Q_{норм.}$ (dB) оставляем прежний. Делаем пересчет $Q_{изм}+Q_{fi}$ - $Q_{норм.}$ (dB) и заносим данные в таблицу 14.

Используя выражение 4, по величине параметра акустической защищенности помещения сделаем выводы о степени его соответствия установленным требованиям и занесем данные в таблицу 14.

В данном случае можно сделать вывод, что параметры соответствуют установленным требованиям, но изначально защищенное помещение уже оборудовано стандартным полотном из дерево-стружечной плиты толщиной 40

мм без уплотняющих прокладок, таблица 15 показывает параметры для контрольных точек после демонтажа данной двери.

Таблица 15

Пересчет параметров для контрольных точек. Демонтаж обыкновенной двери

Параметры	**250 Гц**	**500 Гц**	**1000 Гц**	**2000 Гц**	**4000 Гц**
L1 (dB)	66	66	61	56	53
$L2_{сигн+шум}$(dB)*	49,2	50,5	52,1	46,8	39,6
$L2_{сигн}$(dB)*	49,2	50,5	52,1	46,8	39,6
$Q_{изм.}+Q_{fi}$ (dB)*	52,8	60,5	59,9	59,2	62,4
$Q_{норм.}$ (dB)	36	36	36	36	36
$Q_{изм}+Q_{fi}-Q_{норм.}$ (dB)	16,8	24,5	23,9	23,2	26,4
$Q_{изм}+Q_{fi}-Q_{норм.}-Q_{fi}$ (dB)	16,8-14=2,8	24,5-16=8,5	23,9-22=1,9	23,2-22=1,2	26,4-20=6,4
Соответствие	+	+	+	+	+

Тем самым установив одинарную тяжелую звукоизолирующую дверь с прокладками из пористой резины и демонтировав стандартное полотно из дерево-стружечной плиты толщиной 40 мм без уплотняющих прокладок, исходя из таблицы 15 можно сделать вывод, что все параметры соответствуют установленным требованиям.

3.2.2 Защита от утечки по виброакустическому каналу

В качестве средства защиты будет выбран виброакустический генератор шума «Стена-105», изображенный на рисунке 9.

Характеристики:

- Диапазон рабочих частот (Dfраб), Гц 100….8000
- Число независиморегулируемых виброканалов 2
- Число аудиоканалов 1
- Выходное напряжение (Uвых), В:
  - Виброканал 1 80
  - Виброканал 2 80

- Выходная мощность аудиоканала (Рвых при Rнагр=4Ом), Вт: 10
- Количество излучателей на канал, шт. 20
- Напряжение питания (Uпит), В: 220
- Габаритные размеры, мм: 200х225х55
- Цена: 16 000 рублей.



Рис. 9. Виброакустический генератор шума «Стена-105»

Прибор «Стена-105» предназначен для защиты помещений от утечки речевой информации по естественным и искусственно созданным каналам через элементы строительных конструкций здания (плиты перекрытия, стены, перегородки), системы отопления, окна, двери.

Принцип работы устройства основан на генерации шумовой помехи тонального диапазона частот со сложным алгоритмом ее постановки и суммарной мощностью сигнала 10 Вт, в то время как мощность речи человека на совещании составляет 10–40 мкВт. Это делает невозможным работу контактных средств съема информации, а также применение средств шумоочистки речи для последующего выделения смыслового содержания проводимых в помещении разговоров.

Прибор имеет два независимо регулируемых вибро- и один аудиоканал, что позволяет сформировать наиболее оптимальную систему виброакустической защиты помещения с учетом его особенностей (типов перекрытий, стен, перегородок, количества и типа окон, дверей, конструкции системы отопления).

Возможность подключения к устройству излучателей любых типов (электромагнитных, пьезоэлектрических, акустических) делает возможным построение системы виброакустической защиты в помещениях с ранее установленными датчиками.

При использовании «Стены-105» с виброизлучателями «СТД-Б», который представлен на рисунке 10, гарантируется обеспечение уровня помехи в соответствии с требованиями нормативной документации при выполнении условий. Данный выброизлучатель устанавливается по одному на трубу прямой и обратной подачи воды системы отопления. Схема размещения виброизлучателя представлена на рисунке 11.



Рис.10. Виброизлучатель «СТД-Б»

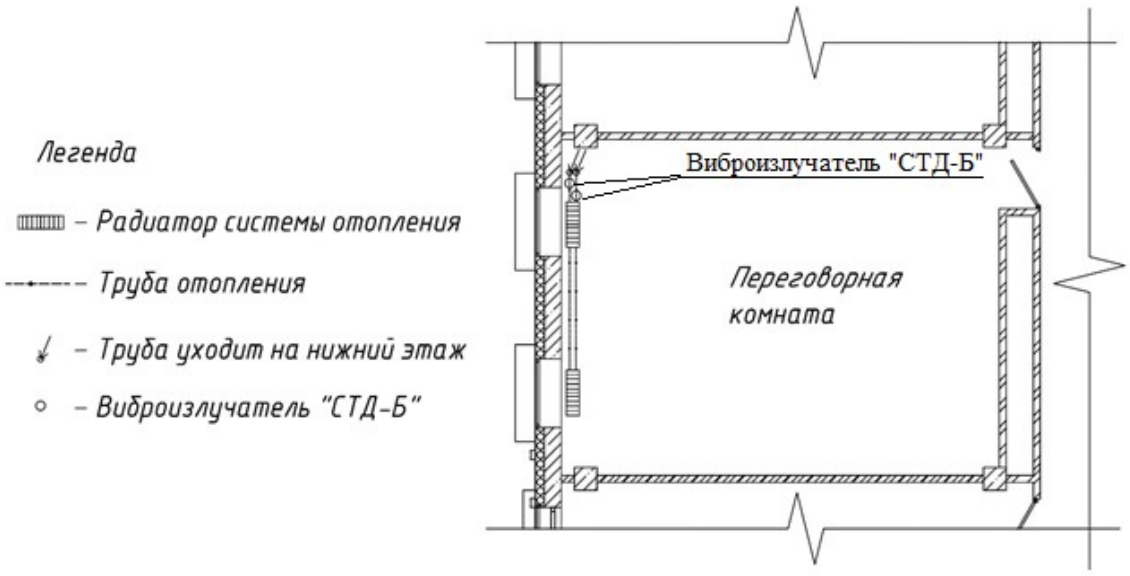

Рис.11. Схема размещения виброизлучателей «СТД-Б»

3.3 Экономическая оценка предложенной системы защиты

С учетом рисков, представленных в первой главе составлена таблица годового ущерба от утечки конфиденциальной информации по акустическому и виброакустическому каналам связи (таблица 16).

Таблица 16

Утечка речевой конфиденциальной информации

Способы нарушения информационной безопасности	Разовый ущерб	Частота возникновения (число в год)	Годовой ущерб
Утечка через прямой акустический канал	10 000	10	100 000
Утечка через виброакустический канал	10 000	4	40 000

Как видно из таблицы 16, за счёт использования мер по перекрытию технических каналов утечки информации, снижение ожидаемых годовых потерь снизится на 70 000 рублей (стоимость аппаратуры с учетом установки 20 000 рублей, стоимость двери с учетом проведения установки и регламентных работ 50 000 рублей).

Из формулы 12 можно рассчитать эффективность предпринятых мероприятий:

Эффективность=(∑затрат)/ΔПотерь*100% (12)

Эффективность=70 000/ 140000*100% (13)

Эффективность=50% (14)

Как видно из уравнения 14 сумма затраченных средств составляет 50% от разницы между первоначально ожидаемыми потерями и потерями, ожидаемыми после внедрения средств по обеспечению информационной безопасности.

Выводы по третьей главе

Защищаемое помещение является местом проведения конфиденциальных переговоров организации, где обсуждаются различные вопросы деятельности данного заведения, вопросы финансирования, которые не должны быть известны третьим лицам.

Для защиты по акустическому каналу был рассмотрен генератор шума DNG-2300. Однако, в целях улучшения комфортности проведения совещаний, было предложено заменить существующую дверь из дерево-стружечной плиты толщиной 40 мм без уплотнительных прокладок на одинарную тяжелую звукоизолирующую дверь с прокладками из пористой резины, что позволит уменьшить риск утечки речевой конфиденциальной информации по акустическому каналу при сохранении комфорта при проведении совещаний.

Для защиты по виброакустическому каналу были рассмотрены: устройство «Кабинет» СНПО «Элерон» и комплекс виброакустической защиты «Стена-105». В результате анализа данного оборудования, был выбран комплекс виброакустической защиты «Стена-105» с виброизлучателями «СТД-Б». В целом, как показывает практика, применение описанных генераторов шума не нарушает комфортности при работе в защищенном с их помощью помещении. Однако, с точки зрения полной комфортности работы человека в помещении

является комплекс виброакустической защиты «Стена-105», в котором реализованы возможности по оптимальной настройке помехового сигнала.

Предложенная система защиты информации является актуальной, поскольку затраты на ее установку явно ниже стоимости циркулируемой в помещении информации.

Вывод об эффективности установленной системы защиты можно сделать на основе расчета коэффициентов звукоизоляции и виброизоляции, которые выше нормативных значений, указанных в сборнике временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам.

ЗАКЛЮЧЕНИЕ

Цель данной работы - провести оценку защищённости переговорной комнаты ООО «ФастПроект» от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам и выработать рекомендации по модернизации системы защиты.

ООО «ФастПроект» занимается инженерно-техническим проектированием, а в частности разработкой проектной, конструкторской и другой технической документации, предназначенной для осуществления строительства. Соответственно, вся обрабатываемая информация для данной организации является ценной. Исходя из данного факта, в организации реализована система защиты информации, а помещения, в которых осуществляется обмен информацией конфиденциального характера, проходили специализированную аттестацию по отсутствию каналов утечки информации. В результате выполнения ремонтных работ в переговорной комнате была заменена дверь, а также проведена замена системы отопления. Данные факты изменили существующую ранее общую структуру переговорной комнаты, что могло повлиять на возникновение возможных каналов утечки информации. На основании данного факта было принято решение о проведении подробного анализа защиты помещения, и выработке рекомендаций по её модернизации.

Оценка защищенности была проведена в соответствии с методикой оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам. В результате измерений и расчетов было выявлено, что входная дверь и система отопления не соответствуют нормам показателей защищенности от утечки по акустическому и виброакустическому каналам.

Исходя из данного факта необходимо предусмотреть меры, как активные, так и пассивные, направленные на улучшение защищенности помещения от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам.

Для защиты по акустическому каналу был рассмотрен генератор шума DNG-2300. Однако, в целях улучшения комфортности проведения совещаний, было предложено заменить существующую дверь из дерево-стружечной плиты толщиной 40 мм без уплотнительных прокладок на одинарную тяжелую звукоизолирующую дверь с прокладками из пористой резины, что позволит уменьшить риск утечки речевой конфиденциальной информации по акустическому каналу при сохранении комфорта при проведении совещаний.

Для защиты по виброакустическому каналу были рассмотрены: устройство «Кабинет» СНПО «Элерон» и комплекс виброакустической защиты «Стена-105». В результате анализа данного оборудования, был выбран комплекс виброакустической защиты «Стена-105» с виброизлучателями «СТД-Б». В целом, как показывает практика, применение описанных генераторов шума не нарушает комфортности при работе в защищенном с их помощью помещении. Однако, с точки зрения полной комфортности работы человека в помещении является комплекс виброакустической защиты «Стена-105», в котором реализованы возможности по оптимальной настройке помехового сигнала.

-

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Конституция Российской Федерации
2. Федеральный закон РФ от от 27.07.2006 г. N 149-ФЗ Об информации, информационных технологиях и о защите информации
3. ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Части 1-3
4. Богдановская И.Ю. Право на доступ к информации. Доступ к открытой информации М.: ЗАО Юстицинформ, 2014. С. 344. ISBN 5-02-012992-5
5. Васильков А.В. Безопасность и управление доступом в информационных системах. А.В. Васильков, И.А. Васильков. Учебное пособие. М.: ФОРУМ, 2015. 368 с.
6. Вендров. А.М. Проектирование программного обеспечения экономических информационных систем: Учебник. – М.: Финансы и статистика, 2017. 352 с. ISBN: 978-5-49807-499-3
7. Венчковский Л.Б. Разработка сложных программных изделий. Москва: ИНФРА-М 2016г. ISBN 978-5-94374-564-8
8. Гвоздева В.А. Основы построения автоматизированных информационных систем: Москва: ИНФРА-М 2017г. 320 стр. ISBN: 978-5-271-42560-8
9. Гладких А.А. Базовые принципы информационной безопасности вычислительных сетей : учебное пособие - Ульяновск : УлГТУ, 2014.- 168 с.
10. Гребенюк Е. И. , Гребенюк Н. А. Технические средства информатизации: Екатеринбург: ИД «Академия» 2018 г. 272 стр. ISBN: 978-5-9775-0874-2
11. Гришина Н. В. Организация комплексной системы защиты информации. — М.: Гелиос АРВ, 2017. — 256 с, ил. ISBN 978-5-85438-171-0
12. Гришина Н.В. Комплексная система защиты информации на предприятии, Н.В. Гришина. Учебное пособие. М. : ФОРУМ, 2014. - 240 с.
13. Ищейнов В.Я, Защита конфиденциальной информации. В.Я. Ищейнов, М.В. Мецатунян. Учебное пособие. М. : ФОРУМ, 2015. 256 с.

Приложение А

к Соглашению от «__» _____20__г.

Перечень
сведений, составляющих коммерческую/служебную тайну
и конфиденциальную информацию

Настоящий Перечень дает полное и всестороннее перечисление сведений, на которые распространяется режим сохранности конфиденциальной информации в ООО «ФастПроект».

- Сведения, предоставляемые заказчикам по реализуемым проектам;
- Информация финансового характера, касаемо стоимости реализуемых проектов;
- Сведения, содержащие коммерческую тайну в отношении финансовых планов функционирования компании, маркетинговых планов работы, информации по договорам, сведения о планируемой деятельности компании.

__/Ф.И.О. руководителя/___ ___/подпись/__

м.п.