ВВЕДЕНИЕ

Актуальность темы исследования. Известно, что в современном мире информация имеет определенную, а часто и очень высокую ценность. Зачастую данные представлены не только на физическом или цифровом носителе, но и в устной форме, при этом большая часть конфиденциальной информации на совещании или при переговорах представлена в виде речевой информации. Защита устной информации от возможной утечки по техническим каналам является одной из наиболее приоритетных задач обеспечения информационной безопасности.

Речь представляет собой модулированные по амплитуде и частоте акустические колебания, основная энергия которых заключена в диапазоне частот 70 Гц - 7 кГц, а более 95 % смысловой информации распространяется в диапазоне 200 Гц - 5 кГц. Спокойный разговор двух людей, находящихся рядом друг с другом, происходит с уровнем звукового давления порядка 55 дБ, а выступление в конференц-зале – около 75 дБ.

Воздействуя на ограждающие конструкции помещений, акустические колебания отражаются от них. Но частичные взаимодействия звуковых волн с конструкциями вызывают колебания последних, которые в дальнейшем распространяются в виде вибраций. Из-за упругости строительных материалов, вибрации, вызванные акустическими сигналами, могут воспроизводиться на значительном расстоянии от места возникновения. Чем толще стена, тем лучше звукоизоляция. Однако высокие акустические сопротивления строительных конструкций являются причиной возникновения и распространения структурных помех (уличных шумов, ударов дверей, шагов). Речь, вызывающая акустические сигналы, представляет собой механические колебания воздушной среды, которые распространяются одинаково во все стороны от источника звука. Попадая на твердые тела, поверхности в комнате, они преобразуются в структурные (вибрационные) сигналы, которые, оставаясь по своей природе механическими распространяются по строительным конструкциям здания на значительные расстояния. Это дает возможность злоумышленнику получать информацию,

передаваемую не только акустической звуковой волной, но и структурным звуком. Структурный звук может распространяться также через стены, перегородки, оконные рамы, дверные коробки, по трубопроводам и коробам вентиляции. Поэтому помещения, в которых проводятся переговоры, как и любая другая среда передачи важной, а зачастую секретной, информации, также нуждаются в защите.

В настоящее время защита речевой информации является одной из важнейших задач в общем комплексе мероприятий по обеспечению информационной безопасности объекта или учреждения. Из этого следует, что для защиты помещения, в котором такая информация циркулирует, будут актуальны следующие вопросы.

1. Отсутствие эффективного аппарата оценки рисков, возникающих при передаче информации в защищаемом помещении.

2. Зависимость эффективности системы защиты информации от уровня квалификации эксперта.

3. Сложность обеспечения оперативного контроля над состоянием системы защиты информации.

В результате анализа данных вопросов были выявлены противоречия между:

1) ростом величины возникающих ущербов от реализации существующих угроз и недостаточной защищённостью речевой информации при проведении собраний в защищаемых помещениях;

2) потребностью в обоснованных методах риск-анализа безопасности информации в защищаемых помещениях и отсутствием актуальной модели анализа рисков;

3) выработкой рекомендаций по созданию системы защиты информации и отсутствием механизма оценки эффективности технических средств.

Объектом исследования являются защищаемые помещения, в которых циркулирует речевая информация конфиденциального характера.

Цель исследования заключается в снижении рисков безопасности конфиденциальной информации с помощью повышения эффективности защиты

защищаемых помещений, каналы утечки которых подвергаются блокированию, за счет оценки и регулирования рисков.

Для достижения цели представляется необходимым решить следующие **задачи.**

1. Анализ системы защиты информации защищаемого помещения, потенциальных угроз и каналов утечки информации. Изучение технических мер, активных и пассивных методов по защите акустической информации.
2. Формализация параметров системы защиты защищаемого помещения на основе применения методов нечетких множеств и экспертных оценок. Создание модели оценки и регулирования информационных рисков утечки конфиденциальной информации речевого характера в защищаемом помещении.
3. Создание на основе предложенной модели системы защиты информации защищаемого помещения. Оценка эффективности предложенных технических средств защиты.

Результаты, выносимые на защиту:

1. Анализ потенциальных угроз и каналов утечки информации в защищаемом помещении, активные и пассивные методы защиты.
2. Разработанная на основе нечетких множеств и экспертных методов модель оценки рисков безопасности конфиденциальной информации.
3. Разработанная на основе полученных результатов риск-анализа модель системы защиты информации защищаемого помещения.

Методы исследования. В исследовании используются методы экспертных оценок, теории множеств, а также методы теории вероятностей и системного анализа. Также применяется методы риск-анализа, методы математического моделирования.

Новизна результатов:

1. Ввиду отсутствия обязательных к исполнению требований к защите информации защищаемых помещений разработанная методика, в отличие от

ЗАКЛЮЧЕНИЕ

Защита информации при проведении совещаний имеет важное значение и основными задачами по обеспечению информационной безопасности является выявление и своевременная локализация возможных технических каналов утечки акустической информации. Таким образом, одним из этапов создания системы защиты информации защищаемого помещения является проведение первичной оценки звуко и виброизоляции ограждающих конструкций защищаемого помещения.

Важным аспектом методики анализа угроз безопасности информации является выявление каналов утечки информации, включая виды каналов утечки информации с принятием дальнейших технических мер по защите акустической информации.

Утечка информации – это ее бесконтрольный выход за пределы организации (территории, здания, помещения) или круга лиц, которым она была доверена. И естественно, что при первом же обнаружении утечки принимаются определенные меры по ее ликвидации.

Для выявления утечки информации необходим систематический контроль возможности образования каналов утечки и оценки их энергетической опасности на границах контролируемой зоны (территории, помещения). Локализация каналов утечки обеспечивается организационными, организационно-техническими и техническими мерами и средствами.

Одним из основных направлений противодействия утечке информации по техническим каналам и обеспечения безопасности информационных ресурсов является проведение специальных проверок (СП) по выявлению электронных устройств перехвата информации и специальных исследований (СИ) на подверженность акустоэлектрическим преобразованиям технических средств обработки информации, аппаратуры и оборудования, в том числе и бытовых приборов.

В данной работе были решены следующие задачи: