Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный технический университет»

В. В. АЛЕКСЕЕВ, В. А. ГРИДНЕВ, М. В. МОИСЕЕВА, А. П. РЫЖКОВ, А. В. ЯКОВЛЕВ

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИЯ И ПРИМЕНЕНИЯ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОГО КОМПЛЕКСА МОНИТОРИНГА ХАРАКТЕРИСТИК ЗАЩИЩЕННОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Рекомендовано Научно-техническим советом университета в качестве монографии

Научное издание

Тамбов
♦Издательский центр ФГБОУ ВО «ТГТУ»♦
2022

УДК 004.056
ББК 32973.261-018
Т33

Р е ц е н з е н т ы :

Кандидат технических наук, профессор,
ведущий специалист по защите информации, научный руководитель
Центрально-Черноземного регионального учебно-научного центра
по информационной безопасности
Ю. Ф. Мартемьянов

Доктор технических наук, доцент,
профессор кафедры защиты информации в системах и комплексах
вооружения ФГКВОУ ВО «Военная академия Ракетных войск
стратегического назначения имени Петра Великого»
Министерства обороны Российской Федерации
В. В. Князев

Т33 **Теоретические основы** построения и применения научно-исследовательского комплекса мониторинга характеристик защищенности конфиденциальной информации : монография / В. В. Алексеев, В. А. Гриднев, М. В. Моисеева, А. П. Рыжков, А. В. Яковлев ; под общ. ред. В. В. Алексеева. – Тамбов : Издательский центр ФГБОУ ВО «ТГТУ», 2022. – 100 с. – 400 экз.
ISBN 978-5-8265-2490-9

На основе системного подхода создана методология построения научно-исследовательского комплекса мониторинга характеристик защищенности конфиденциальной информации, обеспечившая создание ПАК «Средства защиты информации от утечки по техническим каналам». Представлено описание макета этого комплекса, специального программного обеспечения, позволяющего изучать процесс утечки информации по техническим каналам и оптимизировать характеристики системы защиты конфиденциальной информации.

Предназначена для специалистов в области защиты информации, а также студентов и слушателей курсов повышения квалификации в области информационной безопасности автоматизированных систем.

УДК 004.056
ББК 32973.261-018

ISBN 978-5-8265-2490-9

СПИСОК СОКРАЩЕНИЙ

ИБ – информационная безопасность

ИНП – измеритель напряженности поля

ЗКИ – защищенность конфиденциальной информации

КИ – конфиденциальная информация

КЗ – контролируемая зона

НИК – научно-исследовательский комплекс

ОТСС – основные технические средства и системы

ПАК – программно-аппаратный комплекс

ПО – программное обеспечение

ПЭМИН – побочные электромагнитные излучения и наводки

РПС – речеподобный сигнал

РПП – речеподобная помеха

СЗИ – средства защиты информации

СЗКИ – средства защиты конфиденциальной информации

ТЗ – техническое задание

ТСР – технические средства разведки

ВВЕДЕНИЕ

Жизнь человека становится все интенсивнее, развиваются как крупные, так и мелкие организации, в которых циркулирует конфиденциальная информация. Процесс обмена ею осуществляется, как правило, в помещениях офисного типа. В этом случае человеческая речь является источником информации, носителем которой являются электромагнитные и акустические сигналы.

Воздействие акустического сигнала на различные конструкции и инженерно-технические коммуникации приводит к возникновению в них упругих колебаний, которые могут быть зарегистрированы техническими средствами злоумышленника за границами офисного помещения. Кроме того, воздействие колебаний воздуха на тонкие отражающие поверхности помещения приводит к возникновению в них вибрации. Направляя на них лазерный луч, злоумышленник получает отраженный модулированный сигнал, демодуляция которого приводит к получению исходного речевого сигнала. Это создает предпосылки для утечки информации. Для предотвращения утечки информации из офисного помещения по акустовибрационному каналу и каналам побочных электромагнитных излучений предусмотрен ряд организационно-правовых мер, но, как показывает практика, этих мер не всегда достаточно. Поэтому помимо организационно-правовых мер, для обеспечения безопасности от утечки по акустическому и акустовибрационному каналам используются комплексы программно-аппаратных средств, реализующих активную защиту речевой информации.

Поскольку помещения офисного типа, как правило, защищены от физического проникновения и кибервоздействия, то защите от утечки информации по акустовибрационному каналу и каналам побочных электромагнитных излучений необходимо уделять больше внимания.

В этой монографии изложены теоретические основы информационной технологии защиты речевой информации от утечек, в основном по акустовибрационному каналу.

Результаты исследования, представленные в монографии, получены благодаря применению единого системного подхода к оценке защищенности информации. Это позволило не только методически правильно провести натурный эксперимент, но и на основе проведенных измерений найти эффективное управляющее воздействие на элементы системы защиты информации в помещениях офисного типа. Описана методология построения научно-исследовательского комплекса мониторинга характеристик защищенности корпоративной информации, обеспечившая создание программно-аппаратного комплек-

са (ПАК) «Средства защиты информации от утечки по техническим каналам». Представлено описание макета этого ПАК, специального программного обеспечения, позволяющего изучать процесс утечки информации по техническим каналам и оптимизировать характеристики системы защиты корпоративной информации. ПАК, кроме этого, применим в процессе подготовки специалистов по информационной безопасности (ИБ). Созданный макет ПАК предоставляет возможность изучать процесс утечки информации по техническим каналам и методы ее защиты, а также применять разнообразные модули и специальное программное обеспечение, наглядно демонстрирующие различные методы обеспечения ИБ, для их качественного и количественного сравнения. В состав данного комплекса включены испытательные стенды, моделирующие акустический, акустовибрационный, акустоэлектрический каналы и канал побочных электромагнитных излучений и наводок (ПЭМИН). На каждом из стендов размещены средства защиты информации (СЗИ), противодействующие утечке конфиденциальной информации по соответствующему техническому каналу. Разработанное для настройки СЗИ акустического и акустовибрационного каналов ПО позволяет регулировать уровень создаваемой акустической помехи для соответствия требованиям защищенности помещения и одновременно комфортного ведения разговора в данном помещении. В целях демонстрации воздействия технических СЗИ на канал ПЭМИН в ПАК войдет еще ряд модулей ПО. Разработанный ПАК целесообразно использовать не только в качестве измерительного комплекса для научно-практических целей, но и в качестве обучающего комплекса для специалистов по ИБ.

Представленные в монографии результаты исследования соответствуют направлению «Стратегии научно-технологического развития Российской Федерации», а именно: переход к передовым цифровым, интеллектуальным производственным технологиям, роботизированным системам, новым материалам и способам конструирования, создание систем обработки больших объемов данных, машинного обучения и искусственного интеллекта и составили основу материалов исследования, проводимого при финансовой поддержке РФФИ, в соответствии с грантом, договор № 20-37-90146\20.

1. МЕТОДОЛОГИЯ ПОСТРОЕНИЯ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИХ КОМПЛЕКСОВ МОНИТОРИНГА ХАРАКТЕРИСТИК ЗАЩИЩЕННОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

1.1. АНАЛИЗ ПРИНЦИПОВ И МЕТОДОВ СИСТЕМНОГО АНАЛИЗА, ПРИМЕНЯЕМЫХ ДЛЯ РАЗРАБОТКИ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИХ КОМПЛЕКСОВ

При разработке и построении научно-исследовательских комплексов (НИК) мониторинга характеристик защищенности конфиденциальной информации (ЗКИ) следует соблюдать ряд методологических принципов проектирования, производства, проведения исследований, эксплуатации и развития таких комплексов. Научно-исследовательский комплекс мониторинга характеристик защищенности конфиденциальной информации является сложной системой и для его построения могут быть использованы основные принципы разработки и построения сложных систем с учетом особенностей решаемой задачи.

Систему требований к методологии построения НИК мониторинга ЗКИ можно представить в виде совокупности двух групп [10, 11]:

1. Первая группа требований – требования общего теоретического характера. Данные требования, предъявляемые к методологии разработки и построения НИК, определяют следующие ее свойства:

– *полноты*, т.е. другими словами, достаточности для обеспечения выполнения всех задач, возлагаемых на НИК: от анализа возможных угроз информационной безопасности и до наиболее рационального распределения используемых средств защиты конфиденциальной информации;

– *непротиворечивости*, т.е. другими словами, совместимости используемых компонентов разрабатываемой методологии, обеспечивающих построение интегрированной методологической базы.

2. Вторая группа требований – требования прикладного характера. Применительно к данной группе требований создаваемая методология разработки и построения НИК должна обеспечивать:

– *унифицированность*, т.е. другими словами, решение задач разработки и построения научно-исследовательских комплексов мониторинга характеристик защищенности КИ независимо от области возможного применения таких комплексов, а также от характеристик,

применяемых при этом средств защиты и используемых технологий, обеспечивающих решение задачи защиты конфиденциальной информации;

– *реализуемость*, т.е. другими словами, возможность проведения исследований и создания НИК в реальных условиях с использованием существующей инфраструктуры систем защиты конфиденциальной информации;

– *перспективность*, т.е. другими словами, способность не только соответствовать имеющимся в настоящее время, но так же и будущим перспективным потребностям в сфере защиты конфиденциальной информации.

Кроме того, в разрабатываемой методологии построения НИК необходимо учесть, помимо основных положений, существующих в настоящее время концепций информационной безопасности, так же и возможные перспективные концепции.

Анализ предметной области показал, что методология проведения исследований проблем защищенности конфиденциальной информации усложняется тем, что на защищаемые объекты воздействует значительное и постоянно возрастающее количество угроз. Указанная особенность обуславливает потребность применения системного подхода для решения задач, связанных с проведением исследований по имеющимся проблемам мониторинга характеристик защищенности конфиденциальной информации. Применение системного подхода позволит, помимо досконального изучения процесса функционирования защищаемого объекта в условиях воздействия на него имеющихся угроз, обратить взгляды исследователей на изучение основного содержания рассматриваемых проблем, а также на разработку методов и средств наиболее рационального управления и разрешения имеющихся в настоящее время противоречий. С рассматриваемой точки зрения использование принципа системности является одним из главных как методологических, так и концептуальных принципов построения НИК мониторинга характеристик ЗКИ.

Известно, что системный подход – это учение о понятиях, методах и принципах исследования сложных систем [25, 28]. Суть используемого при разработке научно-технического комплекса системного подхода для решения рассматриваемой проблемы защиты конфиденциальной информации в отдельных помещениях сводится к изучению сущности исследуемой проблемы, а также объекта исследования в целостной совокупности. Кроме того, использование системного подхода способствует нахождению всех имеющихся факторов, отношений и связей, присутствующих в исследуемой системе и в их имеющихся взаимосвязях с окружающей средой.

С учетом сказанного системный подход применительно к формулировке теоретических основ системного анализа в процессе разработки научно-исследовательского комплекса мониторинга характеристик защищенности конфиденциальной информации предполагает на первом этапе анализ функционирования НИК как целостного объекта. Следующим этапом используемого системного подхода будет разделение исследуемого комплекса на отдельные подсистемы, нахождение и исследование связей, существующих между выделенными подсистемами, выделение из всех существующих наиболее опасных угроз, воздействующих на рассматриваемые объекты защиты, оценивание степени опасности выделенных угроз, а также возможных мер, направленных на снижение их влияния. Используемый в процессе разработки научно-исследовательского комплекса системный подход включает в себя как функциональный, так и структурный анализ. Поэтому для разработки и построения научно-исследовательских комплексов мониторинга характеристик защищенности конфиденциальной информации, с использованием системного подхода требуется решить ряд задач:

– разработка архитектуры НИК с определением всех входящих в него подсистем и взаимосвязей между ними;

– анализ разработанной архитектуры НИК для определения процессов функционирования выделенных подсистем;

– анализ возможных угроз, воздействующих на защищаемые объекты, и оценка эффективности различных средств защиты по уменьшению их влияния.

Существующие информационные технологии позволяют обеспечить большой выбор различных способов построения и реализации НИК. Выбор таких способов основан как на требованиях со стороны предполагаемых пользователей, так и на достижении требуемого результата.

Объектами проектирования НИК являются отдельные составляющие его подсистемы, выполняющие различные функции, объединение которых в единое целое позволяет решить задачи, стоящие перед научно-исследовательским комплексом.

С учетом сказанного структура методологии построения научно-исследовательских комплексов мониторинга характеристик защищенности конфиденциальной информации и используемых при этом методов для решения задач каждого из этапов представлена на рис. 1.

Анализ структуры, представленный на рис. 1, позволяет заключить, что методология построения НИК сводится к выполнению следующих этапов:

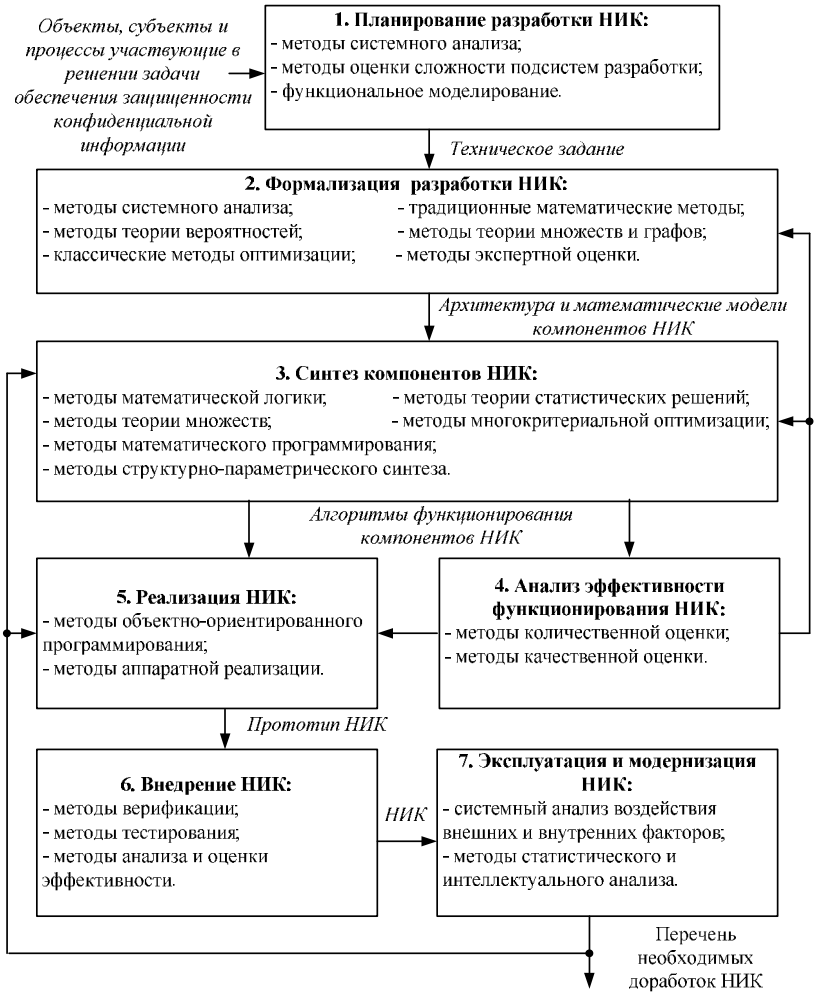


Рис. 1. Методология построения НИК

1. Этап планирования разработки НИК и анализа, предъявляемых к нему требований (предпроектная стадия) включает в себя: проведение исследований и анализ существующих научно-исследовательских комплексов мониторинга характеристик ЗКИ с обоснованием требований, предъявляемых к разрабатываемому НИК, составление технико-экономического обоснования и разработку технического задания на проектирование НИК.

Результатом первого этапа представленной методологии является разработка технического задания. Разработчик на основе имеющихся исходных данных, предоставленных заказчиком, составляет техническое задание (ТЗ). ТЗ содержит основные технические требования, предъявляемые к создаваемой системе, и в дальнейшем служит основанием для проектирования [36].

Применительно к рассматриваемой задаче разработки и построения НИК техническое задание должно включать в себя:

– назначение научно-исследовательского комплекса;

– область использования разрабатываемого научно-исследовательского комплекса;

– требования, предъявляемые к технико-экономическим показателям создаваемого научно-исследовательского комплекса. Данные требования могут быть сформулированы в том числе и в виде ограничений, налагаемых на такие используемые показатели эффективности, как комфорт ведения переговоров, размер защищаемой зоны и др.;

– условия эксплуатации научно-исследовательского комплекса, включающие, например, характеристику используемого для переговоров помещения, режим и длительность эксплуатации, а также факторы, характеризующие внешние воздействия, и т.д.;

– вероятные сроки разработки НИК;

– стоимость разработки НИК в целом, а также составляющих его элементов и подсистем;

– вероятные особые обстоятельства изготовления и эксплуатации;

– кроме того, указываются некоторые дополнительные сведения, влияющие на результаты проектирования НИК.

Собственно, разработка НИК (проектная стадия) включает в себя этапы: формализация разработки НИК, синтез компонентов НИК и анализ эффективности функционирования НИК.

2. Этап формализации разработки НИК включает в себя обоснование в соответствии со сформулированными требованиями архитектуры НИК и состава входящих в него подсистем, разработку математических моделей подсистем НИК.

В процессе разработки архитектуры (концептуальной модели) НИК определяются причинно-следственные связи как наиболее характерные для разрабатываемого комплекса, так и наиболее важные с точки зрения достижения поставленных целей проектирования.

Ключевым предназначением синтезируемой концептуальной модели является определение наиболее важных качеств структурно-функционального построения НИК, дальнейшее рассмотрение кото-

рых необходимо с точки зрения получения требуемых результатов. В разработанной концептуальной модели, как правило, в вербальном виде содержатся сведения о характере и параметрах элементарных явлений проектируемого комплекса, о виде и степени взаимодействия между ними, о месте и значении каждого элементарного явления в общем процессе функционирования НИК.

Первичной основой построения математической модели НИК служит, прежде всего, выбор определенного математического аппарата, в терминах которого будет создаваться математическая модель. Следующим этапом будет построение той самой математической модели или совокупности нескольких моделей создаваемого научно-исследовательского комплекса, отображающих возможные варианты структурно-функциональной организации НИК. В процессе создания математической модели требуется квалифицировать состав, список характеристик и данных модели в определениях выбранного математического аппарата и установить их взаимосвязь с параметрами и характеристиками создаваемого научно-исследовательского комплекса, т.е. осуществить параметризацию модели.

Ко всем создаваемым математическим моделям, применяемым в дальнейшем для проектирования систем, предъявляются, как правило, два противоречивых требования:

1) обеспечение наиболее полной адекватности модели исследуемой системе;

2) обеспечение простоты модели.

Требование простоты выбранной для исследования модели обосновано потребностью построения модели, которую можно исследовать доступными в настоящее время методами и средствами. В то же время, с другой стороны, желательно использовать модель с максимально возможной степенью детализации, отражающую все наиболее важные с точки зрения решаемой проблемы особенности структурно-функциональной организации исследуемой системы. Однако использование такой сложной модели может затруднить процесс получения конечного результата либо даже привести в ряде случаев к невозможности получения конечного результата имеющимися в распоряжении исследователя средствами в требуемые сроки и с приемлемой точностью. Кроме того, использование такой сложной модели может также привести к необходимости использования значительных материальных ресурсов в процессе проектирования и, как следствие, высокой стоимости проектирования.

Поэтому одной из сложных проблем в процессе проектирования является достижение наиболее подходящего в каждом из рассматри-

ваемых случаев компромисса, с одной стороны, между простотой модели и, с другой стороны, ее адекватностью исследуемой системе.

В этой ситуации наиболее предпочтительным является начать разработку с наиболее простых моделей. При этом становится возможным использование также наиболее простых используемых методов расчета, которые с определенной погрешностью позволят приближенно решить задачу оптимального синтеза. В дальнейшем можно оценить качество полученного таким образом решения посредством использования более адекватной имитационной модели, построенной уже с более высокой степенью детализации. Данный подход позволит значительно сократить трудоемкость поиска наилучшего (в идеальном случае – оптимального) решения задачи синтеза за счет существенного уменьшения возможных вариантов структурно-функциональной организации проектируемой системы.

Определение рационального значения детализации используемой модели – сложнейшая задача, от решения которой в относительно большой степени зависит ожидаемое качество спроектированной системы и которая требует большого опыта и высокой квалификации разработчика [12, 36].

3. Этап синтеза компонентов НИК предполагает разработку всех подсистем НИК.

Синтез наиболее эффективной системы ориентирован на создание системы, наиболее лучшим образом соответствующей своему предназначению.

Применяемые процедуры синтеза можно условно разделить на процедуры структурного и параметрического синтеза. Главной целью структурного синтеза считается выявление структуры исследуемого объекта, т.е. перечня всех типов элементов, составляющих объект, и способов связи выделенных элементов между собой в составе объекта. Главная задача параметрического синтеза заключается в нахождении числовых значений параметров выделенных элементов при заданных структуре, а также условиях работоспособности, обеспечивающих выходные параметры исследуемого объекта.

4. Этап анализа эффективности функционирования НИК предполагает оценку качества функционирования НИК, в том числе и посредством проведения моделирования, с использованием разработанных математических моделей и алгоритмов функционирования НИК. В случае когда качество функционирования НИК окажется ниже требуемого, необходимо выбрать способ улучшения структурной либо функциональной организации НИК, а также скорректировать модели, которые использовались для оптимального синтеза (повторение этапов 2 и 3).

Эффективность НИК, как и любой другой системы, оценивается определенным набором показателей эффективности. Как правило, количество таких показателей в ряде случаев может оказаться достаточно большим. Кроме того, в ряде случаев выбранные показатели эффективности могут быть противоречивыми. Это означает, что изменение структурной либо функциональной организации системы может привести к улучшению одних показателей и в то же время будет способствовать ухудшению других показателей эффективности. Отмеченное обстоятельство существенно усложняет выбор наиболее предпочтительного варианта структурно-функциональной организации проектируемого НИК. С этой точки зрения при создании научно-исследовательского комплекса желательно иметь один показатель эффективности.

Критерий эффективности является мерой эффективности НИК. Выбранный критерий эффективности позволяет обобщить свойства научно-исследовательского комплекса в одной оценке – значении критерия эффективности.

НИК, которому из всех возможных вариантов построения, удовлетворяющих заданным требованиям, соответствует максимальное (минимальное) значение критерия эффективности, называется оптимальным. В случае когда значение критерия эффективности окажется ниже (выше) требуемого, необходимо выбрать способ улучшения структурной либо функциональной организации НИК. Такое возможно как за счет изменения архитектуры и уточнения математических моделей компонентов НИК, так и за счет совершенствования алгоритмов функционирования компонентов НИК. Данные процессы определены в методологии связью четвертого этапа со вторым и третьим.

5. Этап реализации НИК включает в себя создание и отладку программ, заполнение используемой базы данных, аппаратную реализацию отдельных подсистем, а также создание рабочих инструкций для персонала.

6. Этап внедрения включает в себя комплексную отладку подсистем и комплекса в целом, обучение обслуживающего персонала, поэтапное внедрение НИК в эксплуатацию, оформление акта о приемо-сдаточных испытаниях НИК.

7. Этап эксплуатации и модернизации НИК включает в себя сбор рекламаций и статистики о функционировании НИК, исправление выявленных в процессе эксплуатации ошибок и недоработок, оформление требований к модернизации НИК и их выполнение (повторение этапов 3 и 5).

Основными этапами, обеспечивающими синтез и анализ характеристик НИК, являются второй, третий и четвертый. Рассмотрению

именно этих этапов предложенной методологии построения научно-исследовательских комплексов мониторинга характеристик защищенности конфиденциальной информации посвящен следующий ниже материал.

1.2. ОБЩЕЕ ОПИСАНИЕ АРХИТЕКТУРЫ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОГО КОМПЛЕКСА И ЕГО СОСТАВНЫХ ЭЛЕМЕНТОВ

Для определения состава НИК, осуществляющего мониторинг характеристик ЗКИ, необходимо выполнить синтез такой системы. НИК – это сложная техническая система, предназначенная для постоянного наблюдения за процессом защиты КИ посредством измерения характеристик ЗКИ и формирования управляющих воздействий на имеющиеся элементы системы защиты.

Для научно-исследовательского комплекса в целом и отдельных его подсистем являются характерными:

- используемая многоуровневая иерархическая структура;
- стохастичность потока входных событий (в том числе несанкционированного доступа к конфиденциальной информации);
- сложность информационно-логического взаимодействия имеющихся объектов защиты, существующих источников угроз, а также используемых средств защиты информации.

Решение задач анализа и синтеза НИК усложняется наличием в комплексе четырех подсистем: подсистемы средств защиты конфиденциальной информации, подсистемы измерения характеристик защищенности КИ, подсистемы оценки эффективности средств защиты и подсистемы формирования управляющих воздействий на элементы СЗКИ. Каждая из отмеченных подсистем характеризуется своими показателями качества, которые в общем случае имеют сложную, порою опосредованную взаимосвязь с результирующими показателями качества НИК. Архитектура НИК приведена на рис. 2.

Поэтому наряду с применением традиционных математических методов, теории вероятностей, а также классических методов оптимизации для решения прикладных задач анализа и синтеза НИК целесообразно использовать и методы экспертной оценки.

Схематичное изображение методики разработки НИК, соответствующей второму, третьему и четвертому этапам общей методологии построения НИК, представлено на рис. 3.

Под оптимальным НИК будем понимать такую совокупность подсистемы средств защиты конфиденциальной информации, подсистемы измерения характеристик защищенности КИ, подсистемы оценки

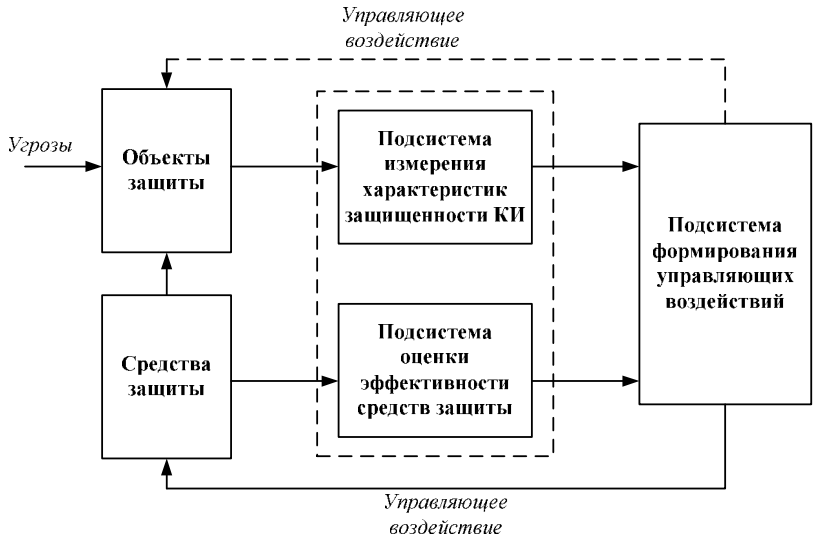


Рис. 2. Архитектура НИК

Общее описание архитектуры НИК и его составных элементов

Формализация описания подсистемы защиты конфиденциальной информации, подсистемы измерения характеристик защищенности КИ, подсистемы оценки эффективности средств защиты и подсистемы формирования управляющих воздействий

Формулирование требований, которым должен удовлетворять НИК, для качественного выполнения возложенных на него функций

Выбор частных показателей качества составных подсистем НИК и всего комплекса в целом

Синтез НИК на основе многокритериальной оптимизации

Анализ эффективности функционирования НИК

Рис. 3. Методика разработки НИК

эффективности средств защиты и подсистемы формирования управляющих воздействий на элементы СЗ, которая обеспечивает экстремальное значение обобщенного показателя, характеризующего в целом работу НИК, при возможных ограничениях на некоторые характеристики комплекса.

Поскольку разрабатываемый НИК предназначен для мониторинга характеристик защищенности КИ, то для построения такого комплекса необходимо провести анализ возможных каналов утечки информации, определить характеристики защищенности объектов, выбрать средства защиты информации от источников угроз и оценить характеристики эффективности таких средств, а также принять решение по выбору такого средства защиты, которое обеспечит требуемый уровень защищенности КИ.

Наилучшим будет решение, которое обеспечивает наиболее рациональное распределение имеющихся средств защиты, с целью получить требуемые характеристики защищенности конфиденциальной информации.

1.3. ФОРМАЛИЗАЦИЯ ОПИСАНИЯ ПОДСИСТЕМ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОГО КОМПЛЕКСА

После вербального описания НИК выполним формализацию работы научно-исследовательского комплекса. Применение формальной модели позволит оценить существующие источники угроз для защищаемого объекта, выбрать наиболее рациональное средство защиты для рассматриваемой ситуации и оценить ее эффективность, а также позволит определить базовую архитектуру комплекса и используемые технологические решения в процессе создания НИК.

Разработка математического описания научно-исследовательского комплекса базируется на основе теории статистических решений, теории множеств и математической логики. Предлагаемая структура математической модели НИК представлена на рис. 4.

Математическое представление модели содержит шесть абстрактных пространств: K – пространство источников угроз, N – пространство объектов защиты, M – пространство средств защиты, V – пространство оценок характеристик объектов, W – пространство оценок эффективности средств защиты, D – пространство принимаемых решений.

Каждый источник существующей угрозы $k \in K$, вероятность появления которого $p(k)$ может быть реализована различными способами j. Обозначим через $P(j/k)$ вероятность реализации j-го способа угрозы k. Тогда используя выражение $P(j, k) = p(k)\ P(j, k)$, можно опреде-

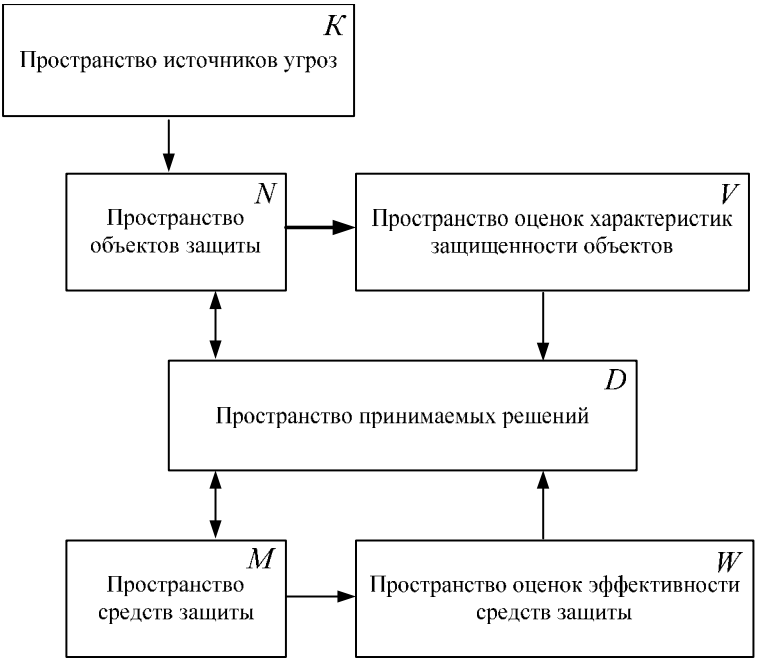


Рис. 4. Структура математической модели НИК

лить вероятность совместного распределения *k*-й угрозы и *j*-го способа ее реализации. В этом случае рассматриваемое пространство источников угроз и записанное выражение будут составлять математическую модель источников угроз.

Пространство *N* представляет собой множество объектов защиты. В частном случае при решении задачи синтеза НИК рассматриваем один объект защиты. Реализация возможных конкретных способов влияния источников угроз на объекты защиты описывается стохастическими законами. Полагаем, что $P(K)$ – это вероятность воздействия всех существующих *K* угроз на один объект защиты, а $P(k)$ – вероятность воздействия какой-либо *k*-й угрозы всеми способами на объект защиты.

Пространство оценок характеристик защищенности объектов $V = \{v_{ijk}\}$ включает в себя множество конкретных показателей, характеризующих защищенность конфиденциальной информации при воздействии определенной угрозы, где v_{ijk} – *i*-й показатель защищенности конфиденциальной информации от *j*-го способа реализации *k*-й угрозы объекту защиты.

Постоянно проводимый контроль характеристик защищенности объектов выполняется в целях своевременного выявления, а также предотвращения утечки информации по техническим каналам за счет несанкционированного доступа к ней. Кроме того, такой контроль позволит также предупредить какие-либо возможные специальные воздействия, направленные как на уничтожение самой информации, так и на разрушение средств информатизации.

Используемое пространство средств защиты $M = \{m_{ijk}\}$ включает в себя множество конкретных средств защиты информации, где m_{ijk} – i-е используемое средство защиты от k-й угрозы, реализованной j-м способом.

Пространство оценок эффективности используемых средств защиты $W = \{w_{ijk}\}$ представляет собой множество значений параметров w_{ijk}, характеризующих удельную эффективность применяемых средств защиты m_{ijk}.

В рассматриваемом случае под эффективностью будем понимать качество функционирования используемого средства защиты, обеспечивающее реализацию возложенных на него функций по противодействию внешним угрозам. При этом использование как аналитических, так и экспертных оценок позволит осуществить отображение всех элементов множества W на элементы множества M.

Использование как аппаратных, так и программных средств позволит выполнить оценку эффективности используемых в научно-исследовательском комплексе мер защиты информации на предмет соответствия установленным требованиям.

Решение задачи обеспечения требуемого уровня защищенности конфиденциальной информации можно разделить на три частные задачи: оценивание защищенности объектов, оценивание эффективности имеющихся средств защиты и принятие управленческих решений об изменении характеристик средств защиты НИК в целях формирования заданного уровня защищенности конфиденциальной информации.

Пространство принимаемых управленческих решений $D = \{d\}$ включает в себя множество элементов d. Каждый такой элемент представляет собой конкретное принятое решение в сложившейся ситуации, а именно в условиях использования наиболее эффективных мер защиты при воздействии определенных угроз на объект защиты. В этом случае решающая функция вида $F(d/k, v, m, w)$ будет определять собой алгоритм принятия решения. Данная функция определена на всех рассматриваемых пространствах K, V, M, W. Другими словами, с помощью рассматриваемой решающей функции, по существу, происходит отображение точек из пространств источников угроз K, оце-

нок характеристик защищенности объектов V, средств защиты M и соответствующих этим средствам их оценок эффективности W в пространство принимаемых решений D. Рассматриваемое отображение также носит статистический характер.

Таким образом, введенная решающая функция $F(d/k, v, m, w)$ совместно с введенными пространствами K, V, M, W образуют общую математическую модель процесса мониторинга характеристик защищенности конфиденциальной информации. Синтез процессов реализуемых в ходе мониторинга характеристик защищенности конфиденциальной информации сводится к нахождению алгоритма отображения решающей функции $F(d/k, v, m, w)$ наилучшего в смысле принятого показателя качества.

Предлагаемый алгоритм работы решающей функции можно представить в следующем виде. При воздействии определенного вида угроз определяются характеристики защищенности объектов. Посредством сравнения оценок эффективности имеющихся средств защиты и характеристик защищенности объектов выбирается наилучшее средство в целях предотвращения либо нейтрализации воздействия источников угроз.

Требования можно предъявлять в виде условия, что используемый показатель качества должен быть не меньше (не больше) допустимого при определенных ограничениях. В качестве ограничений выступают обычно защищенность, стоимость, реализуемость, потребное количество памяти и вычислительного ресурса.

2. АНАЛИЗ ИСТОЧНИКОВ УТЕЧКИ АКУСТИЧЕСКОЙ ИНФОРМАЦИИ И ИНФОРМАЦИИ ПО КАНАЛУ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ

2.1. ОБЩИЕ СВЕДЕНИЯ О ТЕХНИЧЕСКИХ КАНАЛАХ УТЕЧКИ ИНФОРМАЦИИ

Системы связи, управления и информатизации, ведение конфиденциальных совещаний порождают электромагнитные, акустические поля и электрические сигналы, распространяющиеся в различных средах. Распространение происходит в воздухе, архитектурных конструкциях, линиях связи. Необходимым условием образования таких каналов является наличие опасного сигнала. Возможность приема и анализа этих сигналов позволяет вести разведку за акустическими каналами утечки информации. Для получения несанкционированного доступа к засекреченным сведениям достаточно обнаружить, произвести прием и исследовать носители опасного сигнала техническими средствами разведки.

Совокупность, состоящая из источника конфиденциальной информации, физической среды и технических средств разведки (ТСР), которыми добываются разведывательные данные, представляет собой технический канал утечки информации [5, 35]. Данные каналы возникают в результате образования физических полей, химических, биологических и других сред при работе объекта или формирования злоумышленником технических средств разведки [24, 35]:

– обсуждение, передача, обработка информации и создание информации связаны с возникновением соответствующих физических полей (акустическим, гидроакустическим, электромагнитным и т.п.) и сред, являющихся источниками каналов утечки информации, в том числе конфиденциальной;

– доступ к конфиденциальной информации объекта может быть осуществлен за счет съема этой информации в отраженном сигнале;

– технический канал утечки информации может быть сформирован злоумышленником за счет использования технических устройств, позволяющих преобразовать конфиденциальную акустическую информацию к условиям оптимальной ее передачи с объекта (рис. 5);

– информация об объекте может быть получена как за счет излучения объекта, так и анализа информации о воздействии объекта на окружающие физические поля и среды.

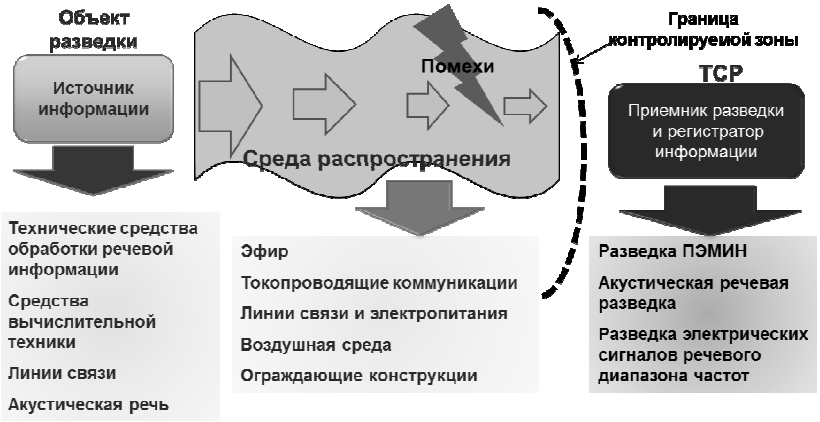


Рис. 5. Технические каналы утечки информации

Для реализации технического канала утечки информации необходимыми являются энергетические и временные соотношения – величина отношения $P_{ис}/P_{ш}$ и $T_{инф}$.

Отношение мощности информативного сигнала на входе технического средства приема конфиденциальной информации к мощности шумов ($P_{ис}/P_{ш}$) в месте расположения ТСР должно обеспечивать прием (перехват) конфиденциальной информации ТСР с чувствительностью $(P_{с}/P_{ш})_{пред}$.

Интервал работы устройств перехвата информации ($t_{пер}$) должен соответствовать времени существования конфиденциальной информации – $T_{инф}$:

$$P_{ис}/P_{ш} > (P_{с}/P_{ш})_{пред} \quad \text{и} \quad t_{пер} = T_{инф}.$$

При выполнении мероприятий по защите информации от утечки необходимо добиться выполнения условий, при которых с помощью ТСР с максимально возможными характеристиками было бы невозможно осуществить перехват конфиденциальной информации [24, 35]:

$$P_{ис}/P_{ш} < (P_{с}/P_{ш})_{пред} \quad \text{и} \quad t_{пер} \neq T_{инф}.$$

Данные выражения определяют возможные способы защиты – организационно-технические и технические.

При технических способах защиты возможно использование [5]:

– уменьшения величины $P_{ис}$ в точке расположения ТСР за счет пассивных способов защиты;

– увеличения величины $P_{ш}$ в месте расположения ТСР активными способами защиты;

– комбинированное использование активных и пассивных способов.

В связи с многообразием технических каналов утечки информации следует реализовать оптимальную систему защиты информации для каждого из защищаемых помещений с учетом особенностей расположения объектов защиты, ценности защищаемой информации, технического оснащения объектов защиты, использования прогрессивных способов и методов защиты информации. В данной работе будет детально рассмотрен акустический канал утечки информации.

2.2. АКУСТИЧЕСКИЙ КАНАЛ УТЕЧКИ ИНФОРМАЦИИ

Рассмотрим основные физические характеристики акустических волн и восприятие их человеком.

Сигнал. Если источником сигнала является голосовой аппарат человека, информация называется речевой. Сигнал возникает посредством работы голосового тракта, создающего акустические колебания, которые представляют собой возмущение воздушной среды в виде продольных волн. Под влиянием акустических колебаний в ограждающих строительных конструкциях и инженерных коммуникациях помещения возникают упругие колебания. Так, в своем исходном состоянии речевой сигнал присутствует в контролируемом помещении в виде акустических колебаний и вибраций поверхностей [36].

Звуки составляют основу речи, которая служит главным средством общения между людьми. Звук – это распространяющиеся в упругих средах (газах, жидкостях и твердых телах) механические колебания, воспринимаемые органами слуха и техническими средствами приема акустических сигналов [5, 24, 35].

Звуковыми называют колебания частотой от 16…20 до 16…20 кГц. Звук с частотой ниже 16 Гц не воспринимается человеком и называется инфразвуком; выше 20 кГц – в пределах $1{,}5\times10^4\ldots10^9$ Гц – ультразвуком; в пределах $10^9\ldots10^{13}$ Гц – гиперзвуком.

Звуковое давление является одной из характеристик произвольной точки звукового поля, определяемой вариативной составляющей звуковой волны.

Звуковое давление – это переменная часть давления, возникающего при прохождении звуковой волны в среде распространения. Звуковое давление в воздухе изменяется от 10^{-5} Па вблизи порога слышимости до ~10^3 Па – болевой порог при самых громких звуках. При средней громкости разговора переменная составляющая звукового давления порядка 0,1 Па [5, 35].

Известно, что акустические волны являются демаскирующим признаком защищаемых объектов в акустических каналах утечки информации. С помощью данных каналов утечки информации возможен перехват речевой информации в местах взаимодействия людей, а также вполне вероятно получить дополнительную информацию об акустических «портретах» различных технических устройств.

Средами распространения для каналов утечки речевой информации являются воздушная и твердая среды.

Слуховой аппарат человека является основным средством получения акустической информации, характеристики которого возможно усовершенствовать путем использования различных технических методов и средств.

Датчики регистрации механических колебаний в соответствующих средах выступают в качестве средств речевой разведки различного типа, интегрированные с различными видами регистраторов речи или приемниками электрических сигналов и электромагнитных полей (в процессе преобразования в эти поля акустических сигналов).

Существуют следующие возможные типы каналов утечки конфиденциальной акустической информации [5, 22, 24]:

– канал утечки акустической информации воздушной волной (акустический);

– канал утечки акустической информации структурной волной (акустовибрационный);

– канал утечки акустической информации с использованием облучающих сигналов (оптико-электронный);

– канал утечки акустической информации за счет акустоэлектрических преобразователей (акустоэлектрический);

– канал утечки акустической информации с закладными устройствами.

Утечка информации по акустическому каналу может осуществляться за счет воздушной акустической волны: воздух или воздух–твердое тело–воздух. В качестве средств перехвата могут служить органы слуха, направленный микрофон.

К технике, используемой в акустической разведке, предъявляют очень высокие требования. Точность полученного электрического сигнала напрямую зависит от качества микрофона. Преобразование звука должно осуществляться с высокой информационной точностью. Важно обеспечить высокую разборчивость и узнаваемость речевого сигнала, избегая появления различных искажений и шумов в пределах динамического диапазона в заданной полосе частот. Помимо этого, микрофоны должны обладать направленными свойствами, высокой чувст-

вительностью и приемлемыми массогабаритными характеристиками [4, 16, 23].

Если появляется необходимость передать перехваченный речевой сигнал за пределы контролируемой зоны, то используют проводные, радио и другие каналы, по которым сообщение передается на пункт прослушивания. В таких случаях используемые устройства называются закладными устройствами для перехвата акустической информации, иначе – радиозакладками. В состав радиозакладки может быть также включено запоминающее устройство, в которое будет записана перехваченная речевая информация. Ее передача в пункт прослушивания в таком случае осуществляется с определенной временной задержкой, что повышает скрытность радиозакладных устройств, повышая сложность их обнаружения [35].

Перехват информации, преобразованной из воздушной в вибрационные колебания, может быть осуществлен непосредственно с конструкций помещений: стены, трубы, окна и т.д. В этом случае средствами перехвата могут быть контактный вибродатчик, стетоскоп, акселерометр.

Воздействие звуковой волны на разные конструкции позволяет злоумышленнику «подсветить» тонкую перегородку (окно, лампочку и т.п.) сигналом лазера или высокочастотного генератора. Отраженный сигнал в данном случае будет промодулирован механическими колебаниями тонкой перегородки, полностью воспроизводящими акустический информационный сигнал.

Описывая акустический канал утечки информации нельзя не рассмотреть основные характеристики речевой информации. Главное назначение речи – передача информации между людьми как при непосредственном общении, так и с помощью средств связи. Речь – это последовательность звуков, произносимых, как правило, слитно, с паузами только после отдельных слов или групп звуков. Слитность произношения звуков речи вследствие непрерывности движения артикуляционных органов речи вызывает взаимное влияние смежных звуков друг на друга. Артикуляционные органы имеют разные размеры у людей, поэтому звуки речи каждого человека индивидуальны [5].

Речь характеризуется тремя группами характеристик [22, 24, 35]:

– семантическая или смысловая сторона речи – характеризует смысл тех понятий, которые передаются с ее помощью;

– фонетическая характеристика речи – данные, характеризующие речь с точки зрения ее звукового состава, а именно частотой встречаемости в речи различных звуков и их сочетаний;

– физическая характеристика – величины и зависимости, характеризующие речь как звуковое явление.

Понятность является основной характеристикой, определяющей пригодность канала как для передачи, так и для перехвата сообщений. Фактическое определение данной характеристики осуществляется статистическим методом с привлечением диктора и определенного количества слушателей. Разработан также косвенный метод количественного определения понятности через ее разборчивость [35].

Разборчивость – это отношение числа правильно принятых элементов речи (слогов, слов, фраз) к общему числу переданных по каналу элементов [34].

Для оценки и контроля защищенности речевой информации в соответствии с методикой расчета словесной разборчивости речи, рекомендованной Гостехкомиссией, использован инструментально-расчетный метод, основанный на экспериментальных исследованиях, проведенных Н. Б. Покровским [26].

Современный российский метод предложен Я. И. Железняком, Ю. К. Макаровым и А. А. Хоревым. Фактически он повторяет метод Н. Б. Покровского, с тем лишь отличием, что анализ сигнала производится в пяти октавных полосах частот.

Числовое значение словесной разборчивости рассчитывается на основе измерения отношения уровней речевого сигнала и шума в местах возможного расположения злоумышленником технических средств акустической разведки. Показателями защищенности являются [5, 35]: словесная разборчивость речи и распределение отношений сигнал/шум в октавных полосах. Измерения проводятся в контрольных точках для нормированного энергетического спектра речевого сигнала.

2.3. ЭЛЕКТРОМАГНИТНЫЙ КАНАЛ УТЕЧКИ ИНФОРМАЦИИ

Как известно, современное офисное помещение содержит большое количество различных радио- и электроустройств (приемники, чайники и кофеварки, вентиляторы и т.п.), а также проводников, выходящих за пределы контролируемой зоны. Побочные электромагнитные излучения и наводки (ПЭМИН) на соседние проводники (различные кабели, цепи заземления и питания, металлические трубы коммунальных систем и т.п.) за счет явления электромагнитной индукции неизбежно сопровождают работу любых радиоэлектронных средств, в том числе и ЭВМ. Перехват ПЭМИН с помощью специальных технических средств образует электромагнитный канал утечки информации.

Одним из первых исследований ПЭМИН еще в начале XX века начал молодой и очень талантливый американский ученый Герберт

О. Ярдли, который в возрасте 26 лет возглавил криптографическую службу США. Он пытался найти способы выявления и перехвата скрытых радиопередач в интересах армии США и при проведении своих исследований обнаружил наличие побочных излучений. Ярдли предположил, что эти излучения также могут нести полезную информацию.

Все, что было связано с понятием «ПЭМИН» (во многих странах это называется TEMPEST – Transient ElectroMagnetic Pulse Emanation STandard), в течение долгого времени относилось к государственной тайне. Первой открытой публикацией по этой теме можно считать статью голландского инженера Вима ван Эка «Электромагнитное излучение видеодисплейных модулей: Риск перехвата?», опубликованная в 1985 году. В этой работе автор описал возможные методы перехвата сигнала видеомонитора компьютера. В марте того же года на выставке Securecom-85 в Каннах Вим ван Эк наглядно продемонстрировал перехват композитного, т.е. состоящего из широкополосного и узкополосного излучения, сигнала монитора. Этот эксперимент показал, что перехват побочных излучений видеомонитора ЭВМ возможен, и для этого требуется всего лишь немного доработанный обычный телевизионный приемник. После этого завеса тайны исследований ПЭМИН была прорвана и открытые публикации по данной тематике приобрели массовый характер.

Но лишь в конце 80-х – начале 90-х годов XX века технологии TEMPEST стали развиваться наиболее интенсивно. Причиной этому послужило стремительное развитие цифровой криптографии. Применение для обеспечения конфиденциальности информации, передаваемой по каналам связи, стойких алгоритмов шифрования не оставляло шансов противнику получить сколь-нибудь существенную информацию о содержании перехваченных сообщений. Для получения хотя бы части передаваемой информации до того, как она будет зашифрована либо после расшифрования принятого сообщения, у злоумышленников осталась одна возможность – перехват ПЭМИН.

Наглядно электромагнитный канал утечки информации в самом общем виде можно пояснить с помощью рис. 6.

Данная модель позволяет также рассматривать процессы внутри ОТСС объекта информатизации, где источниками и получателями сообщений будут платы и различные узлы, а линиями связи – соединяющие их проводники. В этом случае электромагнитный канал утечки образуется при передаче информации из одного узла в другой.

Развитие информационно-телекоммуникационных систем происходило одновременно с совершенствованием технических средств и

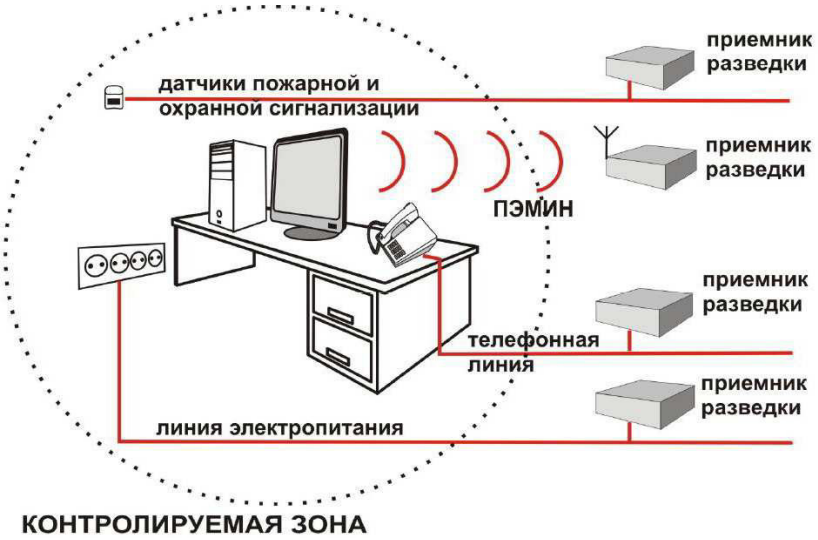


Рис. 6. Модель электромагнитного канала утечки информации

методов промышленного шпионажа и военной разведки, направленных на получение конфиденциальной информации из информационных систем различного назначения. Техническая разведка в настоящее время перестала быть исключительной прерогативой государственных спецслужб. Теперь технической разведкой занимаются и коммерческие организации против конкурирующих фирм. Это в свою очередь послужило причиной все более интенсивного развития методов и средств противодействия технической разведке.

Быстрый прогресс методов и средств перехвата информации по каналу ПЭМИН в значительной степени обусловлен также и тем, что проникновение в локальную сеть какой-либо организации (физическое или логическое) возможно только при наличии уязвимостей в ее защите. При правильной настройке элементов сети администратором, правильном применении программно-аппаратных средств защиты информации, точном соблюдении всех необходимых организационных мер потенциальным злоумышленникам придется искать альтернативные способы незаконного получения информации, которые не требовали бы несанкционированного доступа в локальную сеть.

К настоящему времени методология защиты отдельных ЭВМ от утечки информации по электромагнитному каналу разработана достаточно полно. Более того, она отражена в государственных нормативных документах [11]. А вот защита информации в локальной сети ор-

ганизации оказалась задачей более сложной, чем защита отдельной ЭВМ. Современные локальные сетевые информационно-коммуникационные системы различных организаций взаимодействуют с другими локальными сетями и связаны с глобальной сетью Интернет. Наличие у организаций *web*-сайтов, использование сотрудниками личной и корпоративной электронной почты, доступ сотрудников к информационным ресурсам Интернета – все это существенно затрудняет защиту информации.

В сетевых информационных системах субъектов хозяйственной деятельности, кредитно-финансовых организаций, органов государственной власти и местного самоуправления хранится, обрабатывается и передается информация, в получении которой заинтересованы иностранные разведки и конкуренты. Даже если эта информация и не имеет грифа секретности, то в совокупности она может привести к утечке довольно важных сведений.

Кроме того, с развитием электронного документооборота широкое распространение получает технология электронной подписи и другие методы криптографической защиты данных. Это требует обеспечения защиты не только самих конфиденциальных электронных данных, но и криптографических ключей, которые также хранятся и обрабатываются с помощью ЭВМ.

Все это обусловливает актуальность исследования электромагнитных каналов утечки информации и разработку методов защиты данных от утечки по этим каналам.

Введем математическую модель технического канала утечки информации, представленную на рис. 7. Данная математическая модель соответствует практически любому техническому каналу утечки информации, независимо от физической природы его образования, в том числе и электромагнитному каналу, представленному на рис. 6.

Для формального описания представленной математической модели применительно к электромагнитному каналу будем полагать, что с выхода источника поступают блоки последовательностей дискрет-

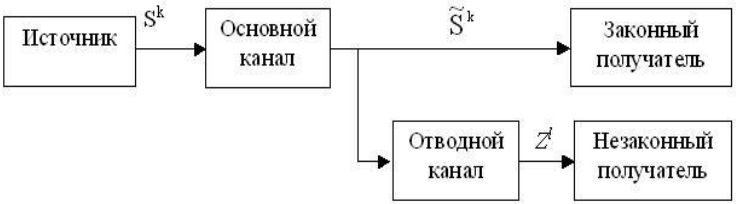


Рис. 7. Математическая модель канала утечки

ных символов фиксированной длины k из алфавита мощностью S: $s_1, s_2, \ldots, s_{k-1}, s_k$.

Для упрощения представим основной канал в виде дискретного канала без памяти

$$\left\{S,\ p\left(\tilde{s}\middle|s\right),\ \tilde{S}\right\},$$

где S – входной алфавит; $\tilde{S}$ – выходной алфавит; $\left\|p\left(\tilde{s}\middle|s\right)\right\|$ – матрица переходных вероятностей.

Отводной канал формализуем аналогично основному

$$\left\{\tilde{S},\ p\left(z\middle|\tilde{s}\right),\ Z\right\}.$$

Достоверность информации в отводном канале всегда будет ниже, чем в основном, так как злоумышленник всегда лишен некоторых возможностей, присущих законному пользователю, а значит $\tilde{S} \neq Z$.

Средняя взаимная информация между k-последовательностями источника и l-последовательностями на выходе отводного канала будет определяться разностью энтропии источника $H(S^k)$ и условной энтропии источника при известных l-последовательностях на выходе отводного канала $H(S^k/Z^l)$

$$I(S^k,\ Z^l) = H(S^k) - H(S^k/Z^l).$$

При $H(S^k \mid Z^l) = H(S^k)$ средняя взаимная информация $I(S^k,\ Z^l) = 0$, т.е. информация в отводном канале отсутствует. Если же $H(S^k \mid Z^l) = 0$, то $I(S^k, Z^l) = H(S^k)$, т.е. вся информация об источнике передается по отводному каналу. Эти два случая можно считать граничными. В промежуточных же случаях количество информации, передаваемой по отводному каналу, будет не нулевым, но и не будет полным.

Если известны количественные показатели защищенности информации от утечки по каналу ПЭМИН, то критерием защищенности информации может служить сравнение их значений с допустимыми. Введем такие показатели на основе формальной модели, представленной на рис. 7.

Количественным показателем защищенности информации может служить энтропия на выходе канала утечки. Для упрощения задачи определения значения этого показателя будем считать источник стационарным, т.е. таким, у которого статистические характеристики выходных последовательностей, определяемые в различные моменты времени, идентичны:

$$P(s_{t1}, s_{t2}, \ldots, s_{tk}) = p(s_{t1+c}, s_{t2+c}, \ldots, s_{tk+c}),$$

где c – вещественное число.

Из теории случайных процессов известно, что стационарные случайные последовательности обладают также свойством эргодичности, т.е. статистические параметры каждой из реализаций, определенные на достаточно длинном временном интервале, и усредненные параметры их реализаций равны.

Строго говоря, дискретные последовательности, соответствующие реальным сообщениям, ни стационарными, ни эргодичными не являются. Но сделанное нами допущение можно считать корректным, если временные интервалы являются ограниченными, при этом достаточно большими, чтобы можно было измерять статистические параметры исследуемых последовательностей.

Энтропия источника может рассматривать как предел

$$H_s = \lim_{k\to\infty} H(S^k),$$

где $H(S^k) = \frac{1}{k} H(s_1, s_2, \ldots, s_k) = \frac{1}{k} M\left(\log 1 / p(\bar{s})\right)$; $M(x)$ – математическое ожидание случайной величины x; $p(\bar{s})$ – распределение вероятностей на S^k.

Приведенное выше определение энтропии аналогично другому ее определению

$$H_s = \lim_{k\to\infty} H(S_k \mid s_1, s_2, \ldots, s_{k-1}),$$

где $H(S_k \mid s_1, s_2, \ldots, s_{k-1})$ – условная энтропия k-го элемента последовательности при известных предыдущих $k - 1$ элементах.

Для источника без памяти

$$p(\bar{s}) = \prod_{i=1}^{k} p(s_i) \quad \text{и} \quad H_s = H(S),$$

где $H(S) = M\left(\log(1/p(s))\right)$ – энтропия последовательностей сообщений.

Так как для псевдослучайных последовательностей, соответствующих реальным сообщениям, зависимость сохраняется только между несколькими смежными элементами, то можно с достаточной точностью статистически описать источник, если известны его одномерные $p(s_i)$, двумерные $p(s_{i-1}, s_i)$ и трехмерные $p(s_{i-2}, s_{i-1}, s_i)$ распределе-

ния вероятностей и соответствующие им значения неопределенностей $H(s_i)$, $H(S_i \mid s_{i-1})$, $H(S_i \mid s_{i-1}, s_{i-2})$. Для многих типовых источников требуемые статистические характеристики представлены в научных справочниках [12]. В остальных случаях их можно получить экспериментально.

При определении количественных показателей защищенности информации для источников данных, имеющих различные избыточности, удобнее пользоваться такой характеристикой, как нормированная величина неопределенности

$$\Delta = \frac{H(S^k \mid Z^l)}{H(S^k)}.$$

При применении данного показателя на практике может возникнуть проблема нахождения значения неопределенности, при которой информацию можно считать достаточно защищенной. Но введенный показатель может быть полезен при теоретических исследованиях информационной безопасности.

Поскольку электромагнитный канал утечки информации можно рассматривать как обычный канал передачи, то его важной характеристикой является нормированная пропускная способность, которая определяется как

$$C = \frac{1}{k} \max_{P(S^k)} I(S^k; Z^l).$$

В этом случае критерием защищенности информации будет выполнение условия $H_s > C$, что следует из теоремы К. Шеннона. Из этой же теоремы совершенно очевидно следует, что если длина кодовой комбинации стремится к бесконечности, то вероятность ошибки декодирования стремится к единице.

Введенные показатели защищенности C и Δ взаимосвязаны. При условии, что распределение $p(\bar{s})$ обеспечивает максимум пропускной способности, получим

$$C = \frac{1}{k} \max(H(S^k) - H(S^k \mid Z^l)) = \frac{H(S^k)}{k} - \Delta.$$

В случае безызбыточного источника взаимосвязь показателей защищенности информации будет еще проще $C = 1 - \Delta$, но, к сожалению, для оценки защищенности безызбыточных источников и источников детерминированных сообщений данные показатели вообще не

применимы. Это обусловлено тем, что невозможность правильного декодирования всего сообщения не исключает возможность правильного декодирования его отдельных блоков или же отдельных символов, а для указанных источников эти данные сами по себе могут содержать важные сведения и представлять интерес для разведки.

Если злоумышленнику известен оптимальный алгоритм декодирования, то средняя вероятность правильного приема всего блока данных на выходе отводного канала будет определяться так же, как и для основного канала:

$$P_{\text{ПД}} = \sum_{\bar{s}} p(\bar{s} = \bar{s}')\, p(\bar{s}),$$

где $\bar{s}$ – блок данных на выходе источника; $\bar{s}'$ – блок данных на выходе декодера канала при оптимальном алгоритме декодирования.

Отсутствие точной информации о структуре подблоков и об их числе M_k существенно затрудняет расчет вероятности правильного декодирования. В этом случае можно определить верхнюю и/или нижнюю границы вероятностей правильного декодирования, которые называются соответственно граница Галлагера и граница Аримото. Эти показатели также связаны с информационным показателем защищенности – пропускной способностью канала утечки C. Граница Галлагера [37] для $R_{\text{И}} < C$ определяется выражением

$$\underline{P}_{\text{ПД}} \geq \exp\left[-K(\max E(\rho, Q) - \rho R_{\text{И}})\right], \quad 0 \leq \rho \leq 1.$$

Граница Аримото [37] определяется выражением

$$\overline{P}_{\text{ПД}} \leq \exp\left[-K\left(\rho R_{\text{И}} + \min E(\rho, Q)\right)\right], \quad -1 \leq \rho \leq 0,$$

где $E(\rho, Q) = -\ln \sum_{\bar{z}} \left[\sum_{\bar{s}} Q(\bar{s}) P(\bar{z} \mid \bar{s})^{\frac{1}{1+\rho}} \right]^{1+\rho}$ – функция Галлагера; $P(\bar{z} \mid \bar{s})$ – усредненные переходные вероятности в канале утечки; $Q(\bar{s})$ – усредненное распределение вероятностей входных блоков; $R_{\text{И}} = \dfrac{\ln M_K}{K}$ – скорость источника; ρ – произвольное число, выбираемое из условия максимума или минимума функции Галлагера.

Расчет верхней и нижней границ вероятностей правильного декодирования и определение матрицы переходных вероятностей при неизвестном количестве блоков M_k также могут быть сопряжены с определенными трудностями. Но в случае, когда блоки данных представ-

ляют собой типичные последовательности достаточно большой длины, эти задачи упрощаются.

В некоторых случаях к утечке данных может привести даже ситуация, при которой весь блок данных декодируется с ошибкой, но некоторые информационные символы из этого блока декодером отводного канала определены правильно. В этом случае показателями защищенности информации от утечки по каналу ПЭМИН могут быть вероятность правильного декодирования отдельного *i*-го символа блока $P_{\text{ПДС}}(i)$ и/или средняя вероятность правильного декодирования символа декодером отводного канала $\tilde{P}_{\text{ПДС}}$:

$$P_{\text{ПДС}}(i) = \frac{1}{2^k}\sum_{j=1}^{2^k} P\left(\hat{s}_i = s_i^{(j)} \mid \bar{s}^{(j)}\right);$$

$$\tilde{P}_{\text{ПДС}} = \frac{1}{k2^k}\sum_{i=1}^{k}\sum_{j=1}^{2^k} P\left(\hat{s}_i = s_i^{(j)} \mid \bar{s}^{(j)}\right),$$

где $\bar{s}^{(j)}$ – символ, который был передан.

Подводя итоги вышеизложенному, можно дать некоторые рекомендации по практическому применению рассмотренных показателей защищенности информации от утечки по каналам ПЭМИН.

При анализе защищенности источника, обладающего избыточностью, целесообразен такой показатель, как пропускная способность канала утечки *C*. В этом случае, если источник имеет энтропию H_S, критерием защищенности будет выполнение условия $H_s > C$ (согласно теореме Шеннона–Вольфовица).

При анализе защищенности источника, обладающего избыточностью, и источника с фиксированным набором комбинаций целесообразно использовать показатель вероятности правильного приема блока или же верхние и нижние границы этой вероятности (границы Галлагера и Аримото).

Для оценки защищенности безызбыточных источников или источников типичных сообщений целесообразно использовать такой показатель, как вероятность правильного декодирования отдельного символа или среднюю вероятность правильного декодирования символов на выходе канала утечки.

Из теории цифровой связи [15] известно, что вероятность ошибки декодирования бита (*BER* – Bit Error Rate) напрямую связана с соотношением сигнал/шум (*S*/*N* – Signal to Noise, или *SNR* – Signal Noise

Ratio) в точке приема. Поэтому совершенно очевидно, что для нахождения числовых значений введенных показателей защищенности информации от утечки по каналам ПЭМИН необходима методика, основанная на определении соотношения *S*/*N* на границе контролируемой зоны (КЗ) или в другой точке, где возможно размещение технических средств разведки. Под контролируемой зоной понимается территория, или помещение, в пределах которых исключено бесконтрольное пребывание посторонних лиц и/или объектов.

В настоящее время в методиках Федеральной службы по техническому и экспортному контролю (ФСТЭК) отказались от неточного трехзонного описания ПЭМИ и используют так называемую беззонную формулу, которая позволяет найти более точное оценочное значение уровней напряженности электрического и магнитного полей, возникающих при работе технических средств (ТС), без необходимости выявления зоны, в которую попадает точка наблюдения.

Данная методика предназначена для решения следующих практических задач:

– установления требуемого радиуса контролируемой зоны (КЗ) R_2 путем определения возможных расстояний распространения информативных сигналов от ТС и проведения оценки защищенности технических средств и систем обработки, передачи и хранения конфиденциальной информации;

– проведения контроля защищенности технических средств, удовлетворяющих требованиям стандартов по электромагнитной совместимости (ГОСТ 29216, ГОСТ 22505, ГОСТ Р 50628);

– выбора в пределах КЗ (при необходимости) оптимального места размещения технических средств, удовлетворяющих требованиям стандартов по электромагнитной совместимости;

– ежегодного контроля защищенности конфиденциальной информации на объекте информатизации.

В основу методики положен инструментально-расчетный метод, основанный на предварительном измерении уровней напряженности электрического и магнитного полей в непосредственной близости от исследуемого ТС и последующем пересчете полученных результатов измерений в точке, расположенной на границе контролируемой зоны.

Частотный спектр ПЭМИ исследуемого ТС определяют инструментальным путем по идентификационным признакам заданного (тестового) режима его работы. Для определения полного набора информативных спектральных составляющих сигналов ПЭМИ антенны измерителя напряженности поля устанавливают на минимальном расстоянии от исследуемого ТС (несколько десятков сантиметров). Ана-

лиз спектра проводят в диапазоне частот от 9 кГц до 1000 МГц. По результатам анализа определяют набор значений $f_1, f_2, ..., f_i, ..., f_M$.

Направление максимального излучения для каждой из гармоник спектра информативного сигнала определяют путем вращения ОТСС на 360° вокруг своей оси в горизонтальной плоскости. Для этого ОТСС устанавливают на специальный поворотный стол, не имеющий в своей конструкции металлических деталей (рис. 8). При этом расстояние R_0 от исследуемого ОТСС до антенны ИНП должно составлять 1 м.

Направлением максимального излучения считают направление, при котором отсчетное устройство ИНП регистрирует максимальное значение измеряемой величины.

Исходя из требований минимального влияния суммарной погрешности (ошибки в выборе расстояния) на результат измерений, значение расстояния R_0 от исследуемого ТС (источника ПЭМИ) до места установки антенны ИНП должно составлять 1 м. При этом отсчет рекомендуемого расстояния R_0 должен проводиться с использованием измерительной рулетки.

В соответствии с инструкцией по эксплуатации применяемого ИНП на частотах $f_1, f_2, ..., f_i, ..., f_M$ измеряют (в дБ) ряды значений напряженности поля $pH_1, pH_2, ..., pH_N$ в диапазоне частот от 9 кГц до 30 МГц и $E_1, E_2, ..., E_K$ в диапазоне частот от 9 кГц до 1000 МГц, создаваемые информативным сигналом.

Расчетная часть метода заключается в:

– расчете возможных расстояний R распространения информативного сигнала от ОТСС для его каждой спектральной составляющей;

– установлении требуемого радиуса контролируемой зоны R_2 для ОТСС в целом.

В существующих документах ФСТЭК заданы требования к ослаблению информативного сигнала, вызванного ПЭМИ ТС, обрабатывающих информацию, на границе КЗ. Для прогнозирования уровней напряженности электрического и магнитного полей, вызванных ПЭМИ

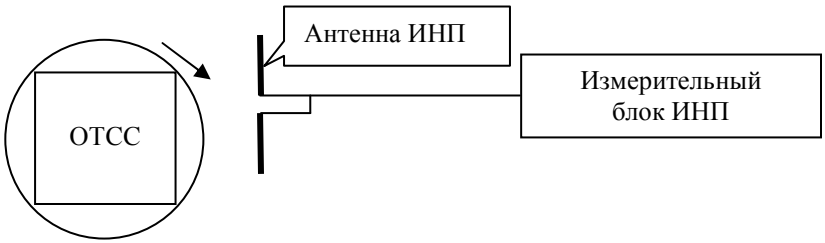


Рис. 8. Схема измерений параметров ПЭМИ

ТС, также используется инструментально-расчетная методика, включающая измерение уровней напряженности электрического и магнитного полей в некоторой контрольной точке, которая, как правило, расположена на удалении 1 м от ТС, и последующий пересчет полученных результатов измерений в точку на границе КЗ. При этом расчет ослабления уровней как электрического, так и магнитного полей проводится по одной и той же формуле.

Однако такой подход приводит к значительной неточности в оценке уровней напряженности электрического и магнитного полей, обусловленной ПЭМИ ТС, на границе КЗ. Эта неточность в общем случае может привести к недооценке величины затухания информативного сигнала на границе КЗ, что в свою очередь ведет к возможной утечке информации по электромагнитному каналу. В [2, 4, 16] убедительно показано, что затухания уровней напряженности электрического и магнитного полей существенно различаются из-за характерных различий в условиях их распространения. На частотах менее 30 МГц это может привести к занижению требуемого радиуса КЗ до 30 раз. Таким образом, для расчета затуханий уровней напряженности электрического и магнитного полей при их распространении от ТС до границы КЗ требуется использовать две различные формулы – отдельно для электрического и для магнитного полей.

2.4. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

В процессе проведения исследований была уточнена классификация методов и средств защиты конфиденциальной информации по акустическому и акустовибрационному каналам.

Для защиты речевой информации от утечки по акустическому и акустовибрационному каналам используются пассивные и активные методы и средства защиты.

Пассивные методы защиты направлены на решение ряда задач [22, 35]:

– ослабление акустических сигналов на границе контролируемой зоны до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;

– обнаружение излучений акустических закладок и побочных электромагнитных излучений диктофонов в режиме записи.

Одним из активных способов защиты речевой информации является создание маскирующих акустических и вибрационных помех в целях уменьшения отношения сигнал/шум на границе контролируемой

зоны до величин, обеспечивающих невозможность выделения информационного акустического сигнала средством разведки [35].

Безопасность информации будет достигнута при выполнении обязательного условия – уровень отношения сигнал/шум не должен превышать установленного значения. Специально вычисляемое значение этого отношения гарантирует, что на фоне шумовых помех информационный сигнал будет невозможно восстановить до уровня, обеспечивающего распознавание [13].

Рассмотрим более подробно пассивные методы защиты, в частности звукоизоляцию помещений.

Звукоизоляция помещений направлена на локализацию источников акустических сигналов внутри них и проводится в целях исключения перехвата акустической информации по прямому акустическому (через щели, окна, двери, технологические проемы, вентиляционные каналы и т.д.) и вибрационному (через ограждающие конструкции, трубы водоснабжения, теплоснабжения и газоснабжения, канализации) каналам (рис. 9).

Основное требование к звукоизоляции помещений заключается в том, чтобы за его пределами отношение акустический сигнал/шум отвечало допустимому значению, исключающему выделение речевого сигнала на фоне естественных шумов средством разведки [36].

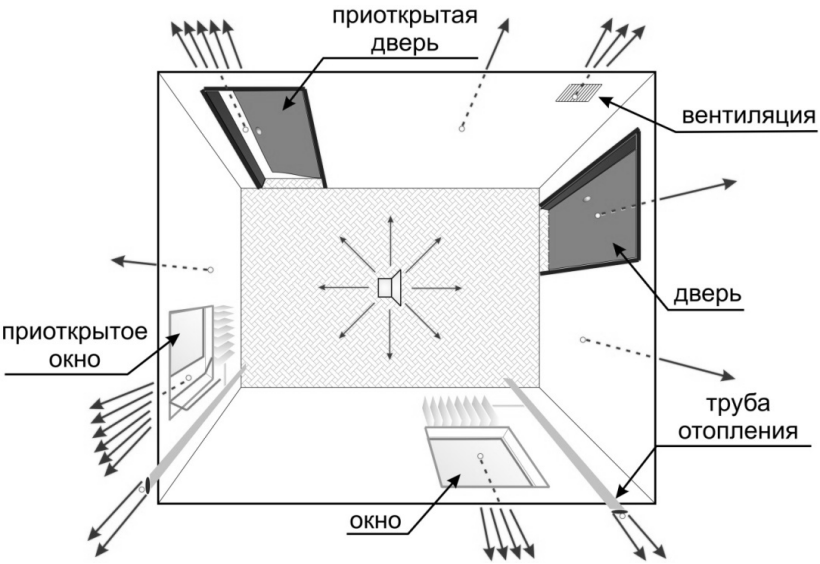


Рис. 9. Утечка речевой информации из помещения

Звукоизоляция помещений обеспечивается специальными архитектурными и инженерными средствами и решениями, а также применением звукопоглощающих строительных и отделочных материалов.

Акустическая волна, попадая на границу поверхностей с разными плотностями, отражается. Меньшая часть волны проникает в материал звукоизолирующей конструкции и распространяется в нем, теряя свою энергию в зависимости от его акустических свойств. Под действием акустической волны звукоизолирующая поверхность совершает сложные колебания, также поглощающие энергию падающей волны.

Эффективными средствами звукоизоляции выделенных помещений являются акустические экраны, устанавливаемые на наиболее опасных направлениях распространения звука.

Различные материалы обеспечивают разные уровни звукопоглощения. Этот показатель зависит от пористости материала – чем больше размер и количество открытых пор, тем более высоким уровнем звукопоглощения владеет материал, а значит, тем более высокий уровень защиты обеспечивает. Поэтому в основном в качестве шумопоглотителей используются мягкие и волокнистые материалы, например рулонная каменная вата или стекловата.

Слабой стороной в обеспечении шумоизоляции выделенного помещения являются окна и двери. В отличие от стен, двери наделены большими зазорами, которые достаточно трудно удалить. Помимо этого, двери выполнены из материала, уступающего по плотности материалу стен. Стандартные двери не способны обеспечить необходимый уровень защиты информации, поэтому необходимо приложить силы для увеличения их звукоизолирующей способности. Это достигается за счет использования двери большей толщины, можно повысить коэффициент звукоизолированности.

Еще одним местом, требующим внимания, являются окна помещения. Окна имеют определенные лимиты поглощения звука, которые предусмотрены их производителем, качеством материалов и другими пунктами. Однако заводских норм часто бывает недостаточно для того, чтобы обеспечить безопасность переговоров.

Акустическое экранирование целесообразно использовать и при временном использовании помещения для защиты акустической информации. Часто применяются складные акустические экраны, используемые для дополнительной звукоизоляции дверей, окон, технологических проемов, систем кондиционирования, проточной вентиляции и других элементов ограждающих конструкций, имеющих звукоизоляцию, не удовлетворяющую действующим нормам [35].

Что касается активных способов защиты информации от утечки по акустическим каналам, то их необходимо использовать как для воздушной, структурной волны, так и для преобразованного в электромагнитные колебания информативного сигнала.

Для предотвращения съема информативного сигнала и корректного воссоздания сообщений возможно использование помехи на основе акустических и электрических колебаний различного генезиса [12].

В результате образующиеся помехи воздействуют на приемную часть технических средств разведки, искажая сигналы, прослушиваемые злоумышленниками, затрудняя или делая невозможным получение полезной информации и сокращая дальность действия оборудования.

Помехи по происхождению бывают естественными и искусственными.

Естественные – это помехи природного происхождения – атмосферные, образуемые электрическими процессами в атмосфере (грозовые разряды), космические (электромагнитные излучения Солнца, звезд и Галактики), акустические шумы океанов, морей, дождя и т.п.

Искусственные помехи создаются устройствами, излучающими энергию электромагнитных или акустических колебаний. В зависимости от причин возникновения эти помехи могут быть:

– непреднамеренными, вызываемыми источниками искусственного происхождения (шум транспорта, разговоры в помещении и т.п.);

– преднамеренными, создаваемыми специально для исключения возможного перехвата информации и нарушения функционирования акустических ТСР.

Непреднамеренные помехи формируются источниками как естественного, так и искусственного происхождения и не предназначены для нарушения функционирования акустических ТСР. Вместе с тем при организации и проведении комплекса защитных мероприятий их необходимо учитывать в суммарной помехе.

Преднамеренные искусственные акустические помехи, генерируемые специальными средствами, делятся в зависимости от характера их воздействия на ТСР на маскирующие и имитирующие помехи.

Маскирующие помехи увеличивают количество принятых сигналов, снижающих информативность сообщения, создающих фон, на котором затрудняется или полностью исключается обнаружение, распознавание, выделение информативных сигналов.

Имитирующие (дезинформирующие) помехи – сигналы, создаваемые техническим средством помех для внесения ложной информации в акустические ТСР. По структуре они близки к защищаемым,

поэтому создают в оконечном устройстве ТСР сигналы, подобные реальным (информативным), снижают пропускную способность системы, вводят в заблуждение операторов, перехватывающих акустическую информацию, приводят к потере части информативных сигналов [36].

По принципу взаимодействия с защищаемым информативным сигналом различают аддитивные и мультипликативные помехи.

Аддитивная помеха – помеха, представляемая не зависящим от сигнала случайным слагаемым, которое складывается с сигналом.

Мультипликативная помеха – помеха, представляемая не зависящим от сигнала случайным множителем, влияющим на уровень сигнала и его спектральную структуру.

Следовательно, аддитивные помехи суммируются с информативным сигналом, а мультипликативные помехи перемножаются с сигналом. Типичным примером аддитивной помехи служит флуктуационный шум, а мультипликативной – замирание информативных сигналов.

В последнее время в системах акустической и виброакустической маскировки используются шумовые, речеподобные и комбинированные помехи.

Наиболее широко используются [13, 35, 36]:

– «белый» шум – шум с постоянной спектральной плотностью в речевом диапазоне частот;

– «розовый» шум – шум со спадом спектральной плотности на 3 дБ на октаву в сторону высоких частот;

– «коричневый» шум со спадом 6 дБ спектральной плотности на октаву в сторону высоких частот;

– шумовая речеподобная помеха – шум с огибающей амплитудного спектра, подобной речевому сигналу.

Речеподобные помехи формируются из наложения определенного количества речевых сигналов [4, 38].

Характерным представителем помех, формируемых из речевых фрагментов, некоррелированных со скрываемым сигналом, является помеха – «речевой хор». Она формируется путем смешения фрагментов речи нескольких человек.

При этом в качестве подобного сигнала возможно использовать сам скрываемый сигнал с помощью синтезатора речеподобных помех – фонемного клонера. Формирование помеховых сигналов проходит в два этапа [5, 35]:

1) с помощью компьютера и специального программного обеспечения из записи голоса одного или нескольких человек путем кло-

нирования основных фонемных составляющих их речи синтезируется «псевдоречь», представляющая некоторую последовательность сигналов;

2) синтезатор помехи, в памяти которого содержится «псевдоречь», по случайному закону берет из этой последовательности сигналов случайные куски, которые и поступают на вход тракта помехового канала.

Помехи, формируемые из скрываемого сигнала, бывают двух типов [32, 34]: речеподобная реверберационная и речеподобная инверсионная.

Речеподобная реверберационная помеха формируется из фрагментов скрываемого речевого сигнала путем многократного их наложения с различными уровнями.

Речеподобная инверсионная помеха формируется из скрываемого речевого сигнала путем сложной инверсии его спектра. На рисунке 10 представлена иллюстрация формирования речеподобной инверсионной помехи.

Комбинированные помехи формируются путем смешения различного вида помех, например помех типа «речевой хор» и «белый» шум, речеподобных реверберационной и инверсионной помех.

Методом математического моделирования получены зависимости словесной разборчивости W от интегрального отношения сигнал/шум q в полосе частот 180…5600 Гц для различных видов помеховых сигналов. Результаты проведенных расчетов представлены на рис. 11.

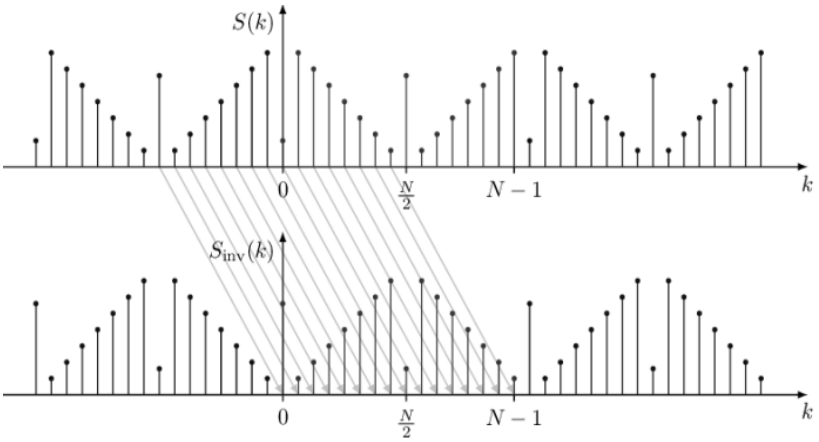


Рис. 10. Спектр речеподобной инверсионной помехи

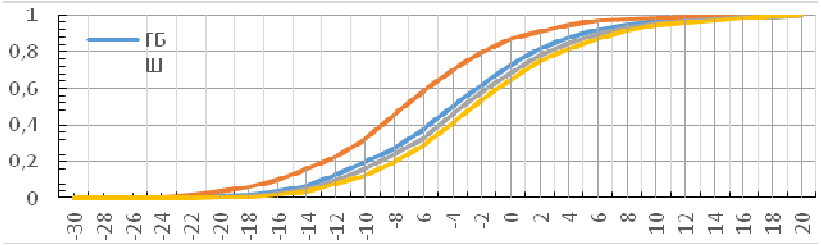


Рис. 11. График зависимости словесной разборчивости от интегрального отношения сигнал/шум в полосе частот 180…5600 Гц:
РПШ – речеподобный шум; РШ – розовый шум;
ГБШ – гауссовский белый шум; КШ – коричневый шум

Анализ полученных результатов показал, что наиболее эффективными являются помехи типа «розовый» шум и шумовая речеподобная помеха. При использовании для скрытия смыслового содержания ведущегося разговора (W = 0,4) помех этих типов необходимо обеспечить превышение уровня помех над уровнем скрываемого сигнала в точке возможного размещения датчика средства акустической разведки на 4,9…5,0 дБ, а для скрытия тематики разговора (W = 0,2) – на 8,8…9,0 дБ.

Помеха типа «белого» шума по сравнению с помехами типа «розовый» шум и шумовая речеподобная обладает худшими маскирующими свойствами, проигрывая по энергетике 0,8…1,2 дБ.

Значительно более низкими маскирующими свойствами обладает «коричневый» шум – шумовая помеха со спадом спектральной плотности 6 дБ на октаву в сторону высоких частот. По сравнению с помехами типа «розовый» шум и шумовая речеподобная она проигрывает по энергетике 4,1…4,2 дБ, а при равной мощности приводит к повышению разборчивости более чем в полтора раза (табл. 1).

В системах акустической и виброакустической маскировки используются помехи как «белого» и «розового» шумов, так и речеподобные помехи [12, 13]. В комплексах защиты применяют для маскировки речи помехи, похожие по своей структуре на маскируемую речь. Это могут быть помехи от внешнего источника или помехи, создаваемые синтезатором речеподобных помех фонемным клонером. Помехи, создаваемые подобным синтезатором, являются не просто речеподобными, фонемный клонер обеспечивает формирование таких помех, которые в максимальной степени соответствуют звукам речи конкретного лица или группы лиц, чьи переговоры защищаются от подслушивания.

Технические характеристики современных систем акустической защиты представлены в табл. 2.

1. Значения отношений сигнал/шум, при которых обеспечивается требуемая эффективность защиты акустической (речевой) информации

Вид помехи	Словесная разборчивость W, %	Отношение сигнал/шум q_i в октавных полосах					Отношение сигнал/шум в полосе частот 180…5600 Гц
		250	500	1000	2000	4000	
«Белый» шум	20	+0,8	–2,2	–10,7	–18,2	–24,7	–10,0
	30	+3,1	+0,1	–8,4	–15,9	–22,4	–7,7
	40	+5,1	+2,1	–6,4	–13,9	–20,4	–5,7
«Розовый» шум (шум со спадом спектральной плотности 3 дБ на октаву)	20	–5,9	–5,9	–11,4	–15,9	–19,4	–8,8
	30	–3,7	–3,7	–9,2	–13,7	–17,2	–6,7
	40	–1,9	–1,9	–7,4	–11,9	–15,4	–4,9
«Коричневый» шум (шум со спадом спектральной плотности 6 дБ на октаву)	20	–14,1	–11,1	–3,6	–15,1	–15,6	–13,0
	30	–12,0	–9,0	–11,5	–13,0	–13,5	–10,8
	40	–10,0	–7,2	–9,7	–11,2	–11,7	–9,0
Шумовая речеподобная помеха	20	–3,9	–7,9	–12,9	–15,9	–16,9	–9,0
	30	–1,7	–5,7	–10,7	–13,7	–14,7	–6,8
	40	+0,1	–3,9	–8,9	–11,9	–12,9	–5,0

2. Технические характеристики современных систем акустической защиты

Наименование	Диапазон рабочих частот, Гц	Вид маскирующих сигналов	Число каналов	Тип преобразователей	Производитель
«Прибой»	100… 8000	«Белый» шум	4	АПВ, АПС, АПК, АПО	Беларусь
«Прибой-Р»		«Белый» шум + речеподобные сигналы	4		
ANG-2000	250… 5000	«Белый» шум	1	*OMS*-2000 *TRN*-2000	США
WNG-023	100… 12 000		1	Встроенный	Россия
«Шорох-2М»			1	КВП-2, КВП-6, КВП-7	
«Порог-2М»	250… 5000		1	Нет данных	
VNG-006/ *VNG*-012*GL*	400… 5000		5	Электро-магнитные и пьезо-электрические	
«Барон»	90… 11 200	«Белый» шум + речеподобные сигналы	4		
СТБ 231 «Бирюза»	90… 11 200	«Белый» шум	3	Нет данных	
СТБ 232			1		
ЛГШ-402	Нет данных		2	ЛВП-2с, ЛВП-2о, ЛВП-2т	
ЛГШ-404	90… 11 200	«Белый» шум и цифровые последовательности	2		

Наличие различных видов шумовых помех дает возможность защищающему акустику помещения нейтрализовать такой, достаточно широко используемый злоумышленником, способ снятия информации сразу с нескольких разнесенных в пространстве датчиков с последующим вычитанием полученных сигналов для компенсации помеховой составляющей. Поэтому в современных комплексах акустической защиты используют несколько видов помех и независимых каналов помех.

Например, в комплексе «Барон-2» использованы помехи типов:

- «белый» шум;
- речеподобная помеха фонемного клонера;
- смесь сигналов трех радиовещательных станций;
- помеха от внешнего источника;
- смесь шумовой помехи, сигналов радиовещательных станций и помехи от внешнего источника.

В системе постановки акустических помех «Шорох-1» используются три независимых канала генерации шумов.

Речеподобная комбинированная (реверборационная и инверсионная) помеха используется в системе акустической маскировки «Эхо». Помеха формируется путем многократного наложения смещенных на различное время задержек разноуровневых сигналов, получаемых путем умножения и деления частотных составляющих скрываемого речевого сигнала [4].

2.5. ОЦЕНИВАНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО КАНАЛУ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ И НАВОДОК

Проведем специальные исследования в целях определения оценок защищенности конфиденциальной информации от утечки по каналу побочных электромагнитных излучений и наводок для двух ПЭВМ.

Сначала проведем необходимые измерения и расчеты для канала побочных электромагнитных излучений. При выполнении измерений напряженности электромагнитного поля выполним следующие операции:

1) по идентификационным признакам определим частотный спектр ПЭМИ исследуемого ОТСС, состоящий из набора спектральных составляющих $f_1, f_2, \ldots, f_i, \ldots, f_k$;

2) определим направление максимального ПЭМИ по каждой спектральной составляющей f_i;

3) в направлении максимального излучения измерим напряженность электромагнитного поля по магнитной pH_i (в диапазоне частот

от 9 кГц до 30 МГц) и электрической E_i (в диапазоне частот от 9 кГц до 1000 МГц) составляющим, создаваемым информативным сигналом;

4) выключив ОТСС, измерим уровни помех на выявленных частотах;

5) результаты измерений и расчетов заносятся в соответствующие протоколы. Для расчетов воспользуемся разработанным программным обеспечением, реализующим модель, представленную на рис. 4. Скриншот окна интерфейса разработанного ПО представлен на рис. 12.

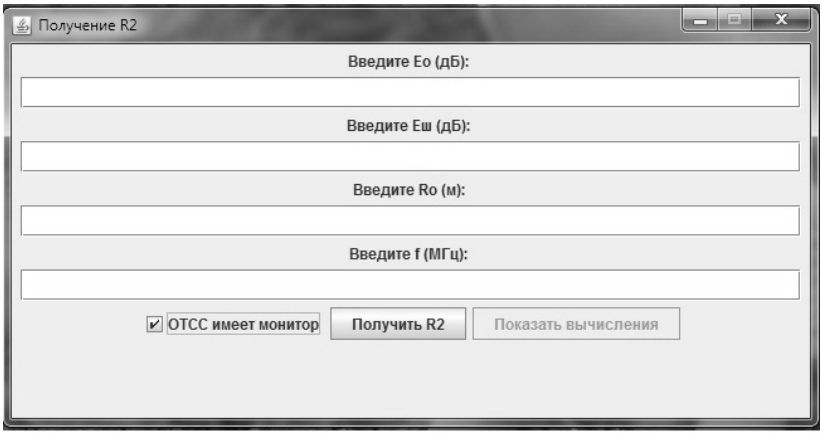


Рис. 12. Окно интерфейса разработанного ПО

ПРОТОКОЛ № 1
измерения побочных электромагнитных излучений
от ПЭВМ, заводской номер 8619700300446

1. Измерению уровней побочных электромагнитных излучений подвергалось ОТСС ПЭВМ, заводской номер 8619700300446, в комплектации, приведенной в табл. 1.

2. При измерениях руководствовались следующими нормативно-методическими документами: «Временная методика оценки защищенности ОТСС, предназначенных для обработки, хранения и(или) передачи по линиям связи конфиденциальной информации».

3. Измерения проводились по электрической и магнитной составляющим электромагнитного поля с применением средств измерений, приведенных в табл. 2.

Таблица 1 – Комплектация ОТСС

Наименование составной части	*Тип (модель)*	*Заводской (серийный) номер*
Системный блок		*8619700300446*
Монитор	*LG FLATRON W2243S*	*908XYG5H306*
Клавиатура	*Logitech 600*	*820-000039*
Графический манипулятор	*Genius GM 350008M*	*147326108017*

Таблица 2 – Применяемые средства измерений

Вид оборудования	*Наименование, заводской номер*	*Основные технические характеристики*	*Сведения о поверке, сертификате и знаке соответствия*
Измерительный приемник – анализатор спектра	*IFR 2399C, № I10112161*	*Диапазон частот 0,009… 3000 МГц*	*Свидетельство о поверке № 051114-02, действительно до 21.07.2015*
Комплект измерительных антенн	*АИР3-2, № 03709; АИР5-0, № 1573*	*Диапазон частот: 0,009… 30 МГц; 0,009… 2000 МГц*	*Свидетельство о поверке № 051114-02, действительно до 21.07.2015*
Токосъемник индукционный	*ТИ2-3, № 0191*	*Диапазон частот 0,009… 300 МГц*	*Свидетельство о поверке № 051114-04, действительно до 22.07.2015*
Генератор	*Г4-116, № 11911; Г4-79, № 30353*	*Диапазон частот 0,009… 2500 МГц*	*Не требуются*

Продолжение табл. 2

Вид оборудования	*Наименование, заводской номер*	*Основные технические характеристики*	*Сведения о поверке, сертификате и знаке соответствия*
Цифровой осциллограф	*С1-75, № 371882*	*Полоса пропускания амплитудно-частотной характеристики от 0 до 250 МГц*	*Не требуются*

В качестве тест-сигнала использовался сигнал, создаваемый специализированной тестирующей программой. Для определения значений зоны R_2 использовался метод, изложенный в «Методике ... ».

4. Результаты измерений и расчета приведены в табл. 3.

Таблица 3 – Результаты измерений и расчета

f, *МГц*	$E_о$, *дБ*	$H_о$, *дБ*	$E_ш$, *дБ*	$H_ш$, *дБ*	$E_с$, *дБ*	$H_с$, *дБ*	R_i, *м*
30	*40,5*	*23,5*	*8*	*6,5*	*40*	*20*	*9,1*

Обозначения: $E_о$ ($H_о$), $E_ш$ ($H_ш$), дБ, – измеренные уровни напряженности электромагнитного поля по электрической (магнитной) составляющей при работе ОТСС в тестируемом режиме и при выключенном ОТСС соответственно; $E_с$ ($H_с$), дБ, – рассчитанные уровни напряженности электромагнитного поля по электрической (магнитной) составляющей, создаваемые информативным сигналом.

Величины $E_о$, $E_ш$ и $E_с$, дБ, связаны между собой соотношением

$$E_с = 20\lg\sqrt{10^{E_о/10} - 10^{E_ш/10}}\,.$$

Измерения по электрической и магнитной составляющим электромагнитного поля проводились относительно 1 мкВ/м и 1 мкА/м соответственно, в полосе частот 0,2 кГц – для диапазона 9…150 кГц, 9 кГц – для диапазона 0,15…30 МГц и 120 кГц – для диапазона свыше 30 МГц.

Вывод: радиус требуемой контролируемой зоны без принятия дополнительных мер спецзащиты должен составлять для ПЭВМ, заводской номер 8619700300446, 9,1 метров при ее работе с конфиденциальной информацией.

Доцент кафедры ИСиЗИ
ФГБОУ ВО «ТГТУ» _____ *В. А. Гриднев*

Дата проведения измерений: 10 мая 2020 г.

ПРОТОКОЛ № 2
измерения побочных электромагнитных излучений
от ПЭВМ, заводской номер 6672700300183

1. Измерению уровней побочных электромагнитных излучений подвергалось ОТСС ПЭВМ, заводской номер 6672700300183, в комплектации, приведенной в табл. 1.

Таблица 1 – Комплектация ОТСС

Наименование составной части	*Тип (модель)*	*Заводской (серийный) номер*
Системный блок		*6672700300183*
Монитор	*LG FLATRON W2243S*	*332XVG4H912*
Клавиатура	*Logitech 600*	*870-001044*
Графический манипулятор	*Genius GM 350008M*	*023159800136*

2. При измерениях руководствовались следующими нормативно-методическими документами: «Временная методика оценки защищенности ОТСС, предназначенных для обработки, хранения и(или) передачи по линиям связи конфиденциальной информации».

3. Измерения проводились по электрической и магнитной составляющим электромагнитного поля с применением средств измерений, приведенных в табл. 2.

В качестве тест-сигнала использовался сигнал, создаваемый специализированной тестирующей программой. Для определения значений зоны R_2 использовался метод, изложенный в «Методике ... ».

4. Результаты измерений и расчета приведены в табл. 3.

Таблица 2 – Применяемые средства измерений

Вид оборудования	*Наименование, заводской номер*	*Основные технические характеристики*	*Сведения о поверке, сертификате и знаке соответствия*
Измерительный приемник – анализатор спектра	*IFR 2399C, № I10112161*	*Диапазон частот 0,009… 3000 МГц*	*Свидетельство о поверке № 051114-02, действительно до 21.07.2015*
Комплект измерительных антенн	*АИР3-2, № 03709; АИР5-0, № 1573*	*Диапазон частот: 0,009…30 МГц; 0,009… 2000 МГц*	*Свидетельство о поверке № 051114-02, действительно до 21.07.2015*
Токосъемник индукционный	*ТИ2-3, № 0191*	*Диапазон частот 0,009… 300 МГц*	*Свидетельство о поверке № 051114-04, действительно до 22.07.2015*
Генератор	*Г4-116, № 11911; Г4-79, № 30353*	*Диапазон частот 0,009… 2500 МГц*	*Не требуются*
Цифровой осциллограф	*С1-75, № 371882*	*Полоса пропускания амплитудно-частотной характеристики от 0 до 250 МГц*	*Не требуются*

Таблица 3 – Результаты измерений и расчета

f, *МГц*	$E_о$, *дБ*	$H_о$, *дБ*	$E_ш$, *дБ*	$H_ш$, *дБ*	$E_с$, *дБ*	$H_с$, *дБ*	R_i, *м*
33	*40*	*20*	*8*	*6*	*40*	*20*	*9,0*

Обозначения: $E_о$ ($H_о$), $E_ш$ ($H_ш$), дБ, – измеренные уровни напряженности электромагнитного поля по электрической (магнитной) составляющей при работе ОТСС в тестируемом режиме и при выключенном ОТСС соответственно; $E_с$ ($H_с$), дБ, – рассчитанные уровни напряженности электромагнитного поля по электрической (магнитной) составляющей, создаваемые информативным сигналом. Величины $E_о$, $E_ш$ и $E_с$, дБ, связаны между собой соотношением

$$E_с = 20\lg\sqrt{10^{E_о/10} - 10^{E_ш/10}}.$$

Измерения по электрической и магнитной составляющим электромагнитного поля проводились относительно 1 мкВ/м и 1 мкА/м соответственно, в полосе частот 0,2 кГц – для диапазона 9…150 кГц, 9 кГц – для диапазона 0,15…30 МГц и 120 кГц – для диапазона свыше 30 МГц.

Вывод: радиус требуемой контролируемой зоны без принятия дополнительных мер спецзащиты должен составлять для ПЭВМ, заводской номер 6672700300183 (рабочая станция отдела кадров), МКУ «ГЕО» 9,0 метров при ее работе с конфиденциальной информацией.

Доцент кафедры ИСиЗИ
ФГБОУ ВО «ТГТУ» _____ *В. А. Гриднев*

Дата проведения измерений: 10 мая 2020 г.

Анализ представленных расчетов показал, что за пределы контролируемой зоны (выделенных помещений) выходят следующие токопроводящие коммуникации:

– цепь электропитания;
– цепь заземления;
– линейная цепь сети;
– телефонная линия;
– трубы системы отопления.

Расположение данных токопроводящих коммуникаций позволяет подключить к ним измерительный прибор в непосредственной близости от границы контролируемой зоны. Это позволяет прибегнуть к упрощенным исследованиям защищенности информации от утечки за счет наводок на токопроводящие цепи, выходящие за пределы контролируемой зоны.

При выполнении измерений наводок информативного сигнала на токопроводящие цепи, выходящие за пределы контролируемой зоны, выполним следующие операции (упрощенная методика):

1) для определения частотного спектра ПЭМИ исследуемого ОТСС воспользуемся частотами f_1, f_2, ..., f_i, выявленными при инструментальном контроле ПЭМИ данного ОТСС;

2) подключим с помощью индукционного токосъемника ТИ2-3 измерительный приемник-анализатор спектра *IFR 2399C* к линиям на границе КЗ (в непосредственной близости) и при обнаружении информативного сигнала делается вывод о неэффективности принятых мер защиты.

Результаты проведенных исследований отразим в протоколах контроля защищенности информации.

ПРОТОКОЛ № 1
контроля защищенности информации, обрабатываемой ПЭВМ, заводской номер 8619700300446, от ее утечки за счет наводок информативного сигнала на цепи электропитания, заземления, линейную цепь сети, трубы системы отопления и телефонную линию

1. Измерениям подвергался информативный сигнал, наведенный от ОТСС ПЭВМ, заводской номер 8619700300446, на цепи электропитания, заземления, линейную цепь сети, трубы системы отопления и телефонную линию, расположенные совместно с ОТСС в аудитории б/С и имеющие выход за пределы контролируемой зоны (аудитории). Комплектация ОТСС указана в табл. 1.

Таблица 1 – Комплектация ОТСС

Наименование составной части	*Тип (модель)*	*Заводской (серийный) номер*
Системный блок		*8619700300446*
Монитор	*LG FLATRON W2243S*	*332XVG4H912*
Клавиатура	*Logitech 600*	*870-001044*
Графический манипулятор	*Genius GM 350008M*	*023159800136*

Минимальная протяженность коммуникации до границы КЗ – 2,2 м.

2. При проведении измерений руководствовались следующими нормативными документами: «Временная методика оценки защищенности конфиденциальной информации, обрабатываемой ОТСС, от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации».

3. Измерения проводились с применением средств измерений, указанных в табл. 2.

Таблица 2 – Применяемые средства измерений

Вид оборудования	*Наименование, заводской номер*	*Основные технические характеристики*	*Сведения о поверке, сертификате и знаке соответствия*
Измерительный приемник – анализатор спектра	*IFR 2399C, № I10112161*	*Диапазон частот 0,009… 3000 МГц*	*Свидетельство о поверке № 051114-02, действительно до 21.07.2015*
Токосъемник индукционный	*ТИ2-3, № 0191*	*Диапазон частот 0,009… 300 МГц*	*Свидетельство о поверке № 051114-04, действительно до 22.07.2015*

В качестве тест-сигнала использовался сигнал, создаваемый специализированной тестирующей программой.

4. Информативный сигнал измерялся на частотах обнаруженных информативных ПЭМИ в диапазоне 0,1…250 МГц путем подключения к коммуникации индукционного токосъемника ТИ2-3, соединенного с входом измерительного приемника – анализатора спектра IFR 2399C, в непосредственной близости от границы контролируемой зоны.

Результаты измерений наведенного в токопроводящих коммуникациях информативного сигнала на границе КЗ представлены в табл. 3.

Таблица 3 – Результаты измерений

F, *МГц*	$U_{с+ш}$, *дБ*	$U_{ш}$, *дБ*	$U_{с}$, *дБ*	*Вывод*
Цепь электропитания				
30	*8,5*	*8,5*	*0*	*Защищенность обеспечивается*
Цепь заземления				
30	*6,5*	*6,5*	*0*	*Защищенность обеспечивается*
Телефонная линия				
30	*5*	*5*	*0*	*Защищенность обеспечивается*
Трубы системы отопления				
30	*4*	*4*	*0*	*Защищенность обеспечивается*
Линейная цепь сети				
30	*9*	*8*	*2*	*Защищенность не обеспечивается*

Обозначения: $U_{с+ш}$ – измеренное значение напряжения смеси сигнала и помехи (коммуникации) при работе ОТСС в тестирующем режиме; $U_{ш}$ – измеренное среднеквадратическое значение напряжения помех (коммуникации); $U_{с}$ – значение напряжения информативной составляющей сигнала, рассчитываемой по формуле

$$U_{с} = 20\lg\sqrt{10^{U_{с+ш}/10} - 10^{U_{ш}/10}}\text{, дБ.}$$

Измерения проводились в полосе частот 9 кГц – для диапазона до 30 МГц и 120 кГц – для диапазона свыше 30 МГц.

Вывод: защищенность информации, обрабатываемой ПЭВМ, заводской номер 8619700300446, от ее утечки за счет наводок информативного сигнала на цепи электропитания, заземления, трубы системы отопления и телефонную линию обеспечивается и дополнительные меры защиты не требуются, а за счет наводок информативного сигнала на линейную цепь сети защищенность информации не обеспечивается и требуются дополнительные меры защиты.

Доцент кафедры ИСиЗИ
ФГБОУ ВО «ТГТУ» _____ *В. А. Гриднев*

Дата проведения измерений: 10 мая 2020 г.

ПРОТОКОЛ № 2
контроля защищенности информации, обрабатываемой ПЭВМ, заводской номер 6672700300183, от ее утечки за счет наводок информативного сигнала на цепи электропитания, заземления, линейную цепь сети, трубы системы отопления и телефонную линию

1. Измерениям подвергался информативный сигнал, наведенный от ОТСС ПЭВМ, заводской номер 6672700300183, на цепи электропитания, заземления, линейную цепь сети, трубы системы отопления и телефонную линию, расположенные совместно с ОТСС в аудитории 4/С и имеющие выход за пределы контролируемой зоны (выделенного помещения). Комплектация ОТСС указана в табл. 1.

Таблица 1 – Комплектация ОТСС

Наименование составной части	*Тип (модель)*	*Заводской (серийный) номер*
Системный блок		*6672700300183*
Монитор	*LG FLATRON W2243S*	*332XVG4H912*
Клавиатура	*Logitech 600*	*870-001044*
Графический манипулятор	*Genius GM 350008M*	*023159800136*

Минимальная протяженность коммуникации до границы КЗ – 1,8 м.

2. При проведении измерений руководствовались следующими нормативными документами: «Временная методика оценки защищенности конфиденциальной информации, обрабатываемой ОТСС, от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации».

3. Измерения проводились с применением средств измерений, указанных в табл. 2.

Таблица 2 – Применяемые средства измерений

Вид оборудования	*Наименование, заводской номер*	*Основные технические характеристики*	*Сведения о поверке, сертификате и знаке соответствия*
Измерительный приемник – анализатор спектра	*IFR 2399C, № I10112161*	*Диапазон частот 0,009… 3000 МГц*	*Свидетельство о поверке № 051114-02, действительно до 21.07.2015*
Токосъемник индукционный	*ТИ2-3, № 0191*	*Диапазон частот 0,009…300 МГц*	*Свидетельство о поверке № 051114-04, действительно до 22.07.2015*

В качестве тест-сигнала использовался сигнал, создаваемый специализированной тестирующей программой.

4. Информативный сигнал измерялся на частотах обнаруженных информативных ПЭМИ в диапазоне 0,1…250 МГц путем подключения к коммуникации индукционного токосъемника ТИ2-3, соединенного с входом измерительного приемника – анализатора спектра IFR 2399C, в непосредственной близости от границы контролируемой зоны.

Результаты измерений наведенного в токопроводящих коммуникациях информативного сигнала на границе КЗ представлены в табл. 3.

Таблица 3 – Результаты измерений

F, МГц	$U_{с+ш}$, *дБ*	$U_{ш}$, *дБ*	$U_{с}$, *дБ*	*Вывод*
Цепь электропитания				
33	*9*	*9*	*0*	*Защищенность обеспечивается*
Цепь заземления				
33	*8,5*	*8,5*	*0*	*Защищенность обеспечивается*

Продолжение табл. 3

F, *МГц*	$U_{с+ш}$, *дБ*	$U_{ш}$, *дБ*	$U_{с}$, *дБ*	*Вывод*
Телефонная линия				
33	*7*	*7*	*0*	*Защищенность обеспечивается*
Трубы системы отопления				
33	*5*	*5*	*0*	*Защищенность обеспечивается*
Линейная цепь сети				
33	*9*	*8*	*2*	*Защищенность не обеспечивается*

Обозначения: $U_{с+ш}$ – измеренное значение напряжения смеси сигнала и помехи (коммуникации) при работе ОТСС в тестирующем режиме; $U_{ш}$ – измеренное среднеквадратическое значение напряжения помех (коммуникации); $U_{с}$ – значение напряжения информативной составляющей сигнала, рассчитываемой по формуле

$$U_{с} = 20\lg\sqrt{10^{U_{с+ш}/10} - 10^{U_{ш}/10}}\text{, дБ.}$$

Измерения проводились в полосе частот 9 кГц – для диапазона до 30 МГц и 120 кГц – для диапазона свыше 30 МГц.

Вывод: защищенность информации, обрабатываемой ПЭВМ, заводской номер 6672700300183, от ее утечки за счет наводок информативного сигнала на цепи электропитания, заземления, трубы системы отопления и телефонную линию обеспечивается и дополнительные меры защиты не требуются, а за счет наводок информативного сигнала на линейную цепь сети защищенность информации не обеспечивается и требуются дополнительные меры защиты.

Доцент кафедры
ИСиЗИ ФГБОУ ВО «ТГТУ» _____ *В. А. Гриднев*

Дата проведения измерений: 10 мая 2020 г.

В результате проведены специальные исследования двух образцов ОТСС, обрабатывающих информацию конфиденциального характера: ПЭВМ, выделенная для работы с программным средством криптографической защиты «КриптоПРО *CSP*», и ПЭВМ, выделенная для

обработки и хранения персональных данных сотрудников. Целью исследований являлась оценка защищенности конфиденциальной информации от утечки по каналам ПЭМИН в соответствии с временными методиками Гостехкомиссии при правительстве РФ от 2002 года.

По результатам специальных исследований установлено:

– радиус требуемой контролируемой зоны без принятия дополнительных мер специальной защиты должен составлять для ПЭВМ, заводской номер 8619700300446, 9,1 метра при ее работе с конфиденциальной информацией;

– радиус требуемой контролируемой зоны без принятия дополнительных мер специальной защиты должен составлять для ПЭВМ, заводской номер 6672700300183, 9 метров при ее работе с конфиденциальной информацией;

– защищенность информации, обрабатываемой ПЭВМ, заводской номер 8619700300446, от ее утечки за счет наводок информативного сигнала на цепи электропитания, заземления, трубы системы отопления и телефонную линию обеспечивается и дополнительные меры защиты не требуются, а за счет наводок информативного сигнала на линейную цепь сети защищенность информации не обеспечивается, и требуются дополнительные меры защиты;

– защищенность информации, обрабатываемой ПЭВМ, заводской номер 6672700300183, от ее утечки за счет наводок информативного сигнала на цепи электропитания, заземления, трубы системы отопления и телефонную линию обеспечивается и дополнительные меры защиты не требуются, а за счет наводок информативного сигнала на линейную цепь сети защищенность информации не обеспечивается, и требуются дополнительные меры защиты.

В качестве дополнительных мер защиты конфиденциальной информации от утечки по каналу электромагнитных наводок [17] на линейные цепи локальной сети можно было бы рекомендовать установку фильтра нижних частот с частотой среза 30 МГЦ, подавляющего наводки на линейную цепь локальной сети для ПЭВМ аудитории 6/С и частотой среза 33 МГЦ, подавляющего наводки на линейную цепь локальной сети для ПЭВМ преподавательской 4/С. Но в этом случае сохраняется опасность утечки конфиденциальной информации по каналу побочных электромагнитных излучений, так как обеспечить контролируемую зону радиусом 9,1 метра для ПЭВМ аудитории 6/С и 9 метров – для ПЭВМ преподавательской 4/С невозможно. Можно установить системные блоки ПЭВМ в экраны [18] и повторно провести специсследования ПЭМИ. Если опасность утечки конфиденциальной информации сохранится, то придется применять средства активной защиты, например генератор шума «Соната» [19].

3. ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ДЛЯ ИССЛЕДОВАНИЯ И НЕЙТРАЛИЗАЦИИ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

3.1. ПОДСИСТЕМА ЗАЩИТЫ ОТ УТЕЧКИ ПО АКУСТИЧЕСКОМУ КАНАЛУ

Защищенность помещения от утечки информации по акустическим техническим каналам может быть определена уровнем разборчивости речи за его пределами. Под разборчивостью понимают некоторую интегральную оценку речевого сигнала и определяют как степень, с которой речь может быть понята слушателям.

Разборчивость речи – относительное количество правильно принятых элементов (слогов, слов, фраз) артикуляционных таблиц. Элементы речи составляют слоги, звуки, слова, фразы и цифры. Соответственно можно выделить слоговую, звуковую, словесную, смысловую и цифровую разборчивость. Между ними существует статистическая взаимосвязь [23].

Для оценки разборчивости речи применяются субъективные и объективные методы. Субъективные методы заключаются в измерении разборчивости речи артикуляционными бригадами. Для субъективных методов характерно то, что речевой или слуховой аппарат человека являются составной частью измерительной системы. Наиболее удобным и достоверным субъективным методом считается метод артикуляции. На практике его использование для оценки эффективности защиты речевой информации неприемлемо по ряду причин:

– к артикуляционной бригаде предъявляются достаточно высокие требования: речь дикторов не должна иметь селективных признаков, у аудиторов должны отсутствовать дефекты слуха, участникам должно быть не менее 18 и не более 35 лет, в составе бригады должно быть не менее трех дикторов (двух мужчин и одной женщины) и трех аудиторов;

– результаты метода существенно зависят от степени тренированности дикторов;

– продолжительность артикуляционных измерений может составлять несколько недель при работе бригады не более 4 ч в сутки;

– процедура анализа протоколов очень громоздка;

– проблемой является создание специальных артикуляционных таблиц, тип которых в значительной степени влияет на результаты измерений.

Главными достоинствами субъективных методов являются универсальность (возможность применения для оценки качества любого канала передачи речевых сигналов) и простота (участие аудиторов с относительно низким уровнем технической квалификации).

Расчет разборчивости речи можно проводить с помощью объективных методов без проведения артикуляционных измерений. Существующие объективные методы определения разборчивости речи можно подразделить на группы: формантные, теоретико-информационные, модуляционные и эмпирические (рис. 13).

Значительное количество известных объективных методов приводит к неоднозначности результатов оценки разборчивости речи. Каждый метод обладает своими достоинствами и недостатками. Достоинствами формантных методов являются использование вероятности в качестве меры разборчивости и свойство аддитивности восприятия формант человеком. Модуляционные методы с единых позиций учитывают влияние как шумовой, так и реверберационной помех на разборчивость речи. Теоретико-информационный метод применяется при

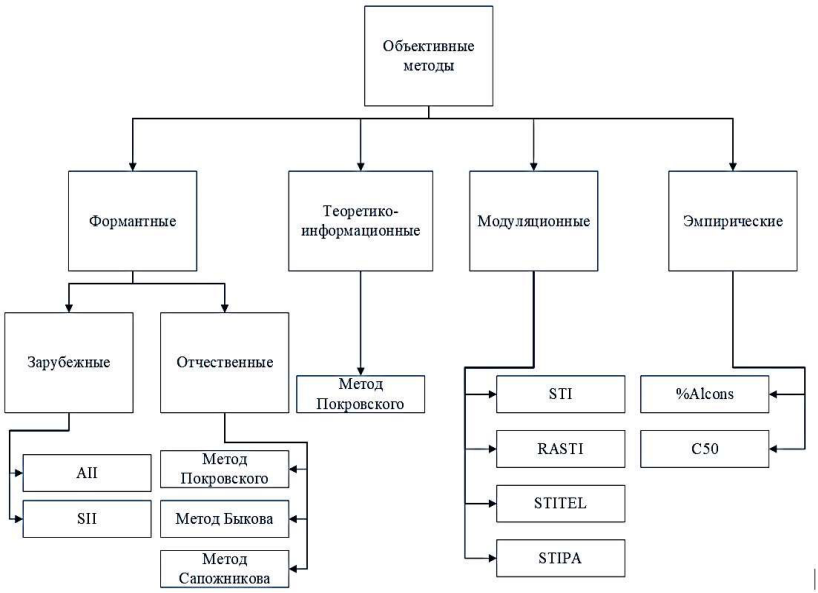


Рис. 13. Объективные методы расчета разборчивости речи

экспертизе цифровых линий связи, где неэффективны модуляционные и формантные методы. Эмпирические методы полезны в условиях, когда влиянием шумовой помехи можно практически пренебречь. Считается, что наибольшей точностью оценок обладают методы, основанные на формантной теории речи, наименьшей – эмпирические [17, 26].

Инструментально-расчетный метод, применяемый в настоящее время для оценки и контроля защищенности речевой информации, основан на версии формантного метода Н. Б. Покровского [26]. Помимо версии Покровского существуют и другие версии формантного метода (версии Ю. С. Быкова и М. А. Сапожкова), однако версия Н. Б. Покровского более популярна, так как в ней рассматривается полоса частот 100…10 000 Гц, что позволяет осуществлять акустическую экспертизу не только линии связи, но и помещений.

Существует современный российский метод, предложенный в 2000 году Я. И. Железняком, Ю. К. Макаровым и А. А. Хоревым, фактически повторяет метод Н. Б. Покровского, с тем лишь отличием, что анализ сигнала проводится в пяти октавных полосах частот. Так же предполагается автоматизация вычислений, что в свою очередь обуславливает необходимость аппроксимации измеряемых величин аналитическими соотношениями.

В качестве показателя эффективности защиты акустической информации [26, 32 – 34] достаточно часто используют словесную разборчивость *W*.

Для оценки разборчивости речи используют инструментально-расчетный метод, при котором числовое значение словесной разборчивости рассчитывается на основе измерения отношения уровней речевого сигнала и шума в местах предполагаемой утечки речевой информации.

Показатель словесной разборчивости речи *W*, диапазон значений которого варьируется от 0 до 1, вычисляется по формуле

$$W = \begin{cases} 1{,}54R^{0{,}25}\left[1-\exp\left(-11R\right)\right], & \text{если } R < 0{,}15; \\ 1-\exp\left(-\dfrac{11R}{1+0{,}7R}\right), & \text{если } R \geq 0{,}15, \end{cases}$$

где *R* – интегральный индекс артикуляции речи.

Индекс *R* вычисляется по формуле

$$R = \sum_{i=1}^{N} (p_i k_i),$$

где i – номер октавной полосы; N – количество октавных полос, в которых проводится измерение; p_i – коэффициент восприятия формант слуховым аппаратом человека; k_i – весовой коэффициент.

Коэффициент p_i вычисляется по формуле

$$p_i = \begin{cases} \dfrac{0{,}78 + 5{,}46\exp\left[-4{,}3\cdot 10^{-3}\left(27{,}3 - |Q_i|\right)^2\right]}{1 + 10^{0{,}1|Q_i|}}, & \text{если } Q_i \le 0; \\ 1 - \dfrac{0{,}78 + 5{,}46\exp\left[-4{,}3\cdot 10^{-3}\left(27{,}3 - |Q_i|\right)^2\right]}{1 + 10^{0{,}1|Q_i|}}, & \text{если } Q_i > 0, \end{cases}$$

где Q_i – уровень шума, дБ.

Уровень шума Q_i вычисляется по формуле

$$Q_i = q_i - \Delta A_i,$$

где q_i – отношение «уровень речевого сигнала/уровень шума», дБ; ΔA_i – значение формантного параметра спектра речевого сигнала, дБ.

Отношение уровней речевого сигнала и шума q_i вычисляется по формуле

$$q_i = L_{\text{с}i} - L_{\text{ш}i} - \Delta L_t,$$

где $L_{\text{с}i}$ – средний спектральный уровень речевого сигнала, дБ; $L_{\text{ш}i}$ – уровень шума в месте измерения в i-й октавной полосе, дБ; ΔL_t – поправка (20…40 дБ), позволяющая получить превышение сигнала над шумом в контрольной точке и повышение достоверности и точности измерений.

Числовые значения формантного параметра спектра речевого сигнала ΔA_i и весового коэффициента k_i в октавных полосах приведены в табл. 3 [17, 26].

Процесс восприятия речи в шуме сопровождается потерями составных элементов речевого сообщения. Понятность речевого сообщения характеризуется количеством правильно принятых слов, отражающих семантическую понятность, выраженную в категориях подробности справки о перехваченном разговоре, составляемой злоумышленником.

Исследования показали возможность ранжирования понятности перехваченного речевого сообщения и принятие некоторой шкалы оценок качества перехваченного речевого сообщения [5]:

– сообщение содержит количество правильно понятых слов, достаточное для составления подробной справки о содержании перехваченного разговора;

3. Числовые значения ΔA_i и k_i в октавных полосах

Наименование параметров	Среднегеометрические частоты октавных полос $f_{ср\,i}$, Гц						
	125	250	500	1000	2000	4000	8000
Значение формантного параметра спектра речевого сигнала в октавной полосе ΔA_i, дБ	25	18	14	9	6	5	4
Значение весового коэффициента в октавной полосе k_i	0,01	0,03	0,12	0,20	0,30	0,26	0,07

– сообщение содержит количество правильно понятых слов, достаточное только для составления краткой справки-аннотации, отражающей предмет, проблему, цель и общий смысл разговора;

– сообщение содержит отдельные правильно понятые слова, позволяющие установить предмет разговора;

– возможно установить факт наличия речи, но нельзя установить предмет разговора.

В соответствии с ГОСТ Р 50840–95 понимание передаваемой речи с большим напряжением внимания, переспросами и повторениями наблюдается при слоговой разборчивости 25…40%, а при слоговой разборчивости менее 25% имеет место неразборчивость связного текста на протяжении длительных интервалов времени. При словесной разборчивости срыв связи будет составлять менее 71%.

Составление подробной справки о содержании перехваченного разговора невозможно при словесной разборчивости менее 60…70%, а краткой справки-аннотации – при словесной разборчивости менее 40…50%. При словесной разборчивости менее 20…30% значительно затруднено установление даже предмета ведущегося разговора, а при словесной разборчивости меньше 10% это практически невозможно даже при использовании современной техники фильтрации помех [17]. Значения показателя словесной разборчивости в зависимости от целей защиты приведены в табл. 4.

4. Значения показателя словесной разборчивости в зависимости от целей защиты

Цель защиты	Потенциальные технические каналы утечки информации	Критерий эффективности W
Скрытие факта ведения переговоров в выделенном помещении	Прямой акустический, акустовибрационный, акустооптический, акустоэлектрический, акустоэлетромагнитный	$W \le 0{,}1$
Скрытие предмета переговоров в выделенном помещении		$W \le 0{,}2 \ldots 0{,}3$
Скрытие содержания переговоров в выделенном помещении		$W \le 0{,}3 \ldots 0{,}4$
Скрытие содержания переговоров в выделенном помещении	Прямой акустический без применения технических средств (непреднамеренное прослушивание)	$W \le 0{,}4 \ldots 0{,}6$

Анализ источников [26] позволил сделать вывод о том, что для оценки разборчивости, речевой коммуникации и секретности переговоров используются качественные характеристики, представленные на рис. 14.

Для определения параметров, необходимых для расчета коэффициента словесной разборчивости, требуется провести измерения ограждающих конструкций по акустическому каналу. На рисунке 15 изображены основные варианты размещения датчиков при измерениях ограждающих конструкций.

При проведении измерений составляющие элементы измерительного комплекса размещаются следующим образом [4, 34]:

– излучатель тест-сигнала должен находиться в 1,0 м от исследуемого объекта в контролируемом помещении на высоте 1,5 м от пола;

Рис. 14. Оценочные значения разборчивости, речевой коммуникации и секретности переговоров

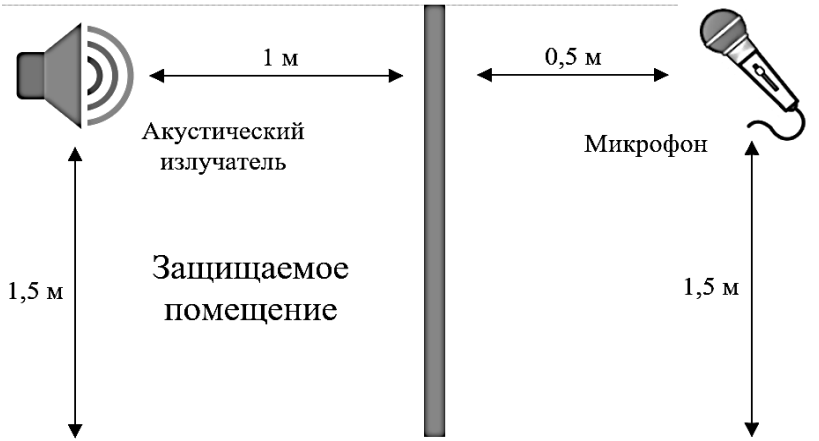


Рис. 15. Схема размещения датчиков при измерениях словесной разборчивости речи основных ограждающих и инженерных конструкций

– микрофонное устройство в 1,0 м от ограждающей конструкции за пределами помещения. В случае, когда есть уверенность, что на контролируемом объекте нет «слабых» мест, достаточно провести одно или два измерения вдоль конструкции. При наличии подозрений на дефекты (отверстия, трещины) и т.д. необходимо увеличивать количество проводимых измерений.

При измерениях перекрытий пола и потолка присутствуют некоторые нюансы. Излучатель тест-сигнала размещается аналогично предыдущему варианту, над полом защищаемого помещения, а микрофон размещается под потолком в помещении этажом ниже, на удалении 0,5 м. При этом ориентация микрофона осуществляется по нормали к плоскости потолка и направлена вверх. Если в защищаемом помещении имеется фальшпотолок, то в любом случае микрофон размещается в 0,5 м от потолка помещения. На рисунке 17 изображены основные варианты размещения датчиков при измерениях перекрытий пола и потолка [7, 8 – 10].

Перед постановкой активной акустической помехи нужно провести расчет коэффициента словесной разборчивости и, основываясь на полученных значениях, проводить регулировку мощности акустического шума. Применение этого способа позволит подобрать значение оптимального уровня излучения генератора акустического шума, уменьшив его мощность с максимальной на достаточную.

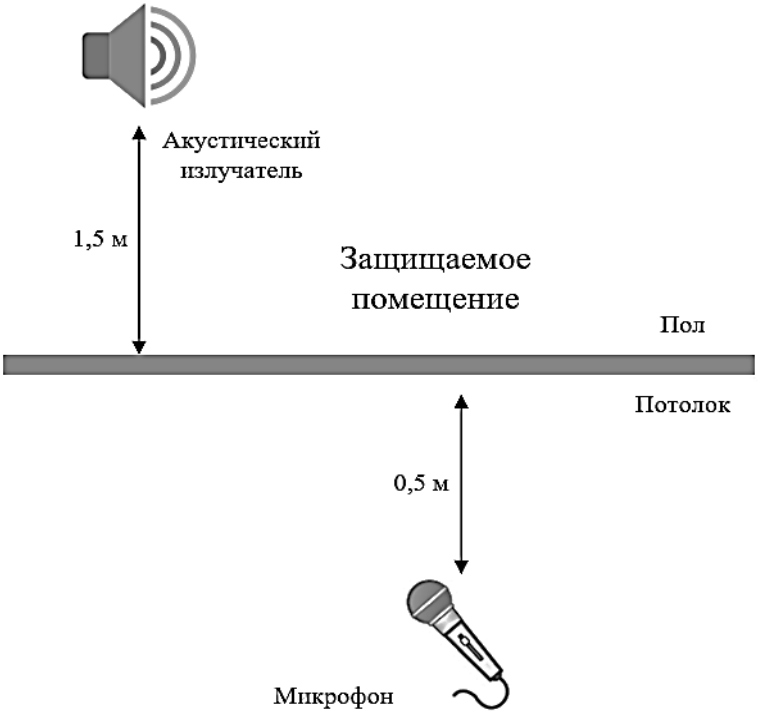


Рис. 16. Схема размещения датчиков при измерениях перекрытий

Для снятия показателей, необходимых для расчета коэффициента словесной разборчивости, требуется провести измерения ограждающих конструкций (стен, перекрытий потолка и пола) по акустическому каналу. Для замера элементы измерительного комплекса размещаются следующим образом. Излучатель тест-сигнала (колонка) в 1,0 м от конструкции в контролируемом помещении на высоте 1,5 м от пола, микрофон в 1,0 м от ограждающей конструкции за пределами помещения. Когда есть уверенность, что в ограждающей конструкции нет «слабых» мест, достаточно одного-двух замеров вдоль стены [18]. Если есть подозрения на трещины, проходы (отверстия) и т.д., необходимо увеличивать число контрольных точек [28].

В процессе исследования были получены оригинальные результаты по возможности адаптации СЗИ по акустическому каналу утечки на основе динамического мониторинга характеристики защищенности.

Максимальный уровень шума, который может генерировать средство защиты, не всегда является необходимым. Предложенный метод конфигурирования уровня излучения средства защиты обеспечивает решение этой проблемы: позволяет использовать прибор эффективно (с точки зрения обеспечения безопасности), но не превышая необходимый минимум.

3.2. ПОДСИСТЕМА ФОРМИРОВАНИЯ ПОМЕХ СПЕЦИАЛЬНОГО ТИПА

Одним из опасных каналов утечки конфиденциальной информации является акустический канал. Опасность заключается в возможности получить обсуждаемую в помещении информацию множествами способов – от прямого подслушивания до использования сложных технических устройств, снимающих информацию с твердых поверхностей и способных не только записать ее, но и даже передать за пределы контролируемой зоны.

Для реализации защиты от подобных утечек существует не меньшее количество средств защиты. Одним из вариантов защиты является обеспечение повышенной звукоизоляции помещения, что поможет избежать прямой утечки информации. Однако такой способ не всегда полностью обеспечивает конфиденциальность, поэтому активно используют средства активной защиты – генераторы шума.

Однако появляется новая проблема, использование зашумления должно быть контролируемое, такое, чтобы обеспечивать максимально эффективное использование излучаемых помех, но при том же приносить как можно меньше дискомфорта людям, работающим в помещении. Для решения этой проблемы предложено использовать методы

оценки разборчивости речи, которые помогут понять, какой уровень излучения генераторов является достаточным. Это решение избавит от необходимости слепо использовать максимально зашумление и сделает защиту более щадящей для людей при той же эффективности.

Точную настройку амплитудно-частотных характеристик тракта маскирующего сигнала невозможно выполнить, используя простейшие системы активной акустической защиты помещений.

В реальных условиях даже тщательная регулировка системы активной защиты не спасает присутствующих в помещении людей от дискомфорта из-за навязчивых фоновых шумов. Соответственно эти негативные воздействия вызывают повышенную утомляемость персонала, а длительное воздействие может привести к депрессиям и другим расстройствам нервной системы [12, 19].

Показателем эффективности мер защиты от утечки информации в общем случае является наличие или отсутствие за пределами контролируемой зоны сигналов утечки, доступных для перехвата и анализа их техническими средствами.

Для количественной оценки эффективности проведенных мер необходимо осуществить формализацию показателя эффективности с учетом возможностей выполнения измерений сигналов утечки, размеров и топологии контролируемой зоны и нормативных требований по закрытию каналов утечки.

При решении вопроса о выборе показателей эффективности в работе [6] рекомендуется руководствоваться следующими основными положениями:

– выбранный показатель должен отражать основное назначение системы, а также соответствовать цели проводимого исследования;

– используемый показатель должен быть критичен по отношению к параметрам, определяющим его значение;

– показатель должен быть наглядным и по-возможности просто определяемым;

– показатель должен давать возможность учета всех факторов, определяющих эффективность системы, иначе говоря, должен быть конструктивным (удобным для пользователя);

– частные показатели не должны противоречить общему показателю эффективности системы.

На этой основе осуществлен синтез речеподобной помехи для защиты от несанкционированного прослушивания.

Известно, что для защиты от несанкционированного прослушивания в средствах активной защиты стремятся использовать помеховые колебания с повышенным маскирующим действием и стохастически-

ми свойствами, затрудняющими шумоочистку полезных сигналов. Такими являются акустические колебания, подобные речевым сообщениям не только по временным и спектральным характеристикам, но и по восприятию на слух. Общее представление системы активной защиты от несанкционированного прослушивания приведено на рис. 17.

Обобщенная схема акустической (акустовибрационной) защиты содержит три основных компонента: подсистема создания акустических (акустовибрационных) помех, подсистема контроля эффективности помех и подсистема управления.

При использовании речеподобных сигналов (РПС) в качестве помех их следует называть речеподобными помехами (РПП). Для активной защиты речи от несанкционированного прослушивания применяются помехи самого различного рода [16, 20].

Генерирование помех данного типа проводится различными способами, наиболее подходящими для имитации акустического проявления речи. При этом, как правило, отсутствуют необходимые разъяснения – достижение какого именно сходства с РС является целью формирования РПП в каждом отдельном случае.

Рис. 17. Общее представление системы активной защиты от несанкционированного прослушивания

В работах [16, 20, 37, 38] содержится несколько определений РПП и описаний способов их формирования. В работах [4, 37] маскирующий сигнал «создают из исходного маскируемого сигнала путем модуляции шумовым сигналом моментов пересечения нуля маскируемым сигналом». Отмечается, что: «…модуляцию моментов пересечения нуля речевого сигнала можно производить путем фазовой модуляции речевого сигнала шумовым».

В работе [16] упоминаются «речевой хор», состоящий из суммы нескольких речевых сигналов, и «речеподобный шум, алгоритм синтеза которого теоретически обоснован, представлен аналитическим выражением, адаптирован под первые три форманты интегрального формантного спектра».

В работах [3, 14] маскирующее речевое сообщение именуется как «шумовая речеподобная помеха (шум с огибающей амплитудного спектра, подобной речевому сигналу)». Отмечается, что: «В соответствии с требованиями Государственной технической комиссии при Президенте Российской Федерации генератор помех должен формировать шумовые колебания в диапазоне частот от 175 до 5600 Гц». По сведениям работ [1, 14, 17] для маскирования РПС речеподобной помехой «…специалистами в основном предлагается создание трех видов такой помехи»:

– речеподобная помеха формируется из фрагментов речи трех дикторов радиовещательных станций при примерно равных уровнях смешиваемых сигналов (первый вид);

– речеподобная помеха формируется из одного доминирующего речевого сигнала или музыкального фрагмента и смеси фрагментов радиопередач с шумом (второй вид);

– речеподобная помеха формируется из фрагментов скрываемого речевого сигнала при многократном их наложении с различными уровнями (третий вид).

В системах активной защиты речевой информации в помещениях для переговоров в качестве маскирующих сигналов возможно использование речеподобных сигналов и речевых последовательностей, сформированных с учетом лингвистических особенностей языка и статистических характеристик встречаемости фонем в данном языке, а также длины слов и предложений.

Формирование речеподобных сигналов можно выполнить компиляционным методом по базе структурных единиц речи. В результате сформированные таким образом речеподобные сигналы сохраняют все оттенки речи определенного диктора, и их весьма сложно отличить от информационных сигналов этого же диктора.

Качество синтезируемого помехового сигнала возможно повысить, используя экспоненциальные сплайн-функции на границах перехода от одной фонемной структуры к другой и наложение окончания одной фонемной структуры на начало другой. При этом будет происходить некоторое более быстрое затухание амплитуд колебаний окончания одной фонемной структуры и увеличение амплитуды начала второй фонемной структуры. Такой механизм компиляционного синтеза речи позволит устранить скачки сигнала на границах фонемных структур. Для этого нужна база фонемных структурных единиц речи с несколько увеличенными сегментами во временной области.

Сравнительный анализ методов сегментации речи показывает, что для формирования фонемных структурных единиц речи для синтеза компиляционным методом наиболее удобным является метод сегментации, использующий динамическое программирование. Для этого необходимо иметь запись слитной речи, размеченной на фонемные структурные элементы и содержащей все необходимые фонемные структурные единицы.

Так как фонетические базы структурных элементов речи в начале и в конце содержат переходные области, то при синтезе речи следует использовать сплайны для переходных областей. Рекомендуется использовать «сшивание» аллофонов при компиляционном синтезе речи. Переходной участок окончания предшествующего аллофона, умноженный на убывающую функцию, изменяющуюся от 1 до 0, накладывается на переходной участок последующего аллофона, умноженный на возрастающую функцию от 0 до 1.

В работах [4, 38] предложен способ синтеза РПС, формируемого по случайному закону и по своим основным временным, спектральным характеристикам и восприятию на слух максимально подобного РПС, но не содержащего смысловой информации. В работе [19] для формирования РПС предложен алгоритм, основанный на управлении системой синтеза речи по тексту. Временные характеристики длительностей пауз между фоноабзацами, фразами и синтагмами составляют обычно примерно 0,3; 0,8 и 1,5 с. Эти величины являются среднестатистическими для русского языка.

Соответствие спектральных характеристик РПП характеристикам РПС обеспечивается применением выбранной базы аллофонов, которая формируется из реальных речевых сообщений диктора. Фонетические особенности сообщений русского языка учитываются использованием условных вероятностей слогов.

Алгоритм функционирования данного способа формирования представлен на рис. 18.

Наиболее эффективным считается третий тип речеподобного шума. Он создается из фрагментов разговора людей с различным тембром голоса путем многократного наложения его фрагментов друг на друга с разными уровнями интенсивности сигнала и вырезания пауз между определенными словами. Чрезвычайно важно, на каком языке осуществляются переговоры собеседников, так как различные языки имеют свои отличительные особенности и звуки, например, подобный генератор, работающий на китайском языке, будет практически бесполезен для европейца. Получившаяся в результате этого процесса помеха озвучивается динамиком-колонкой.

Шум смешивается с информационным сигналом, отражается от стен, потолка и предметов интерьера и попадает в микрофон прослушивающего устройства. Таким образом, получается непрерывный процесс генерации очень эффективного речеподобного шума. Получив запись защищенного разговора, злоумышленник не сможет разобрать его содержание даже с помощью специального программного обеспечения.

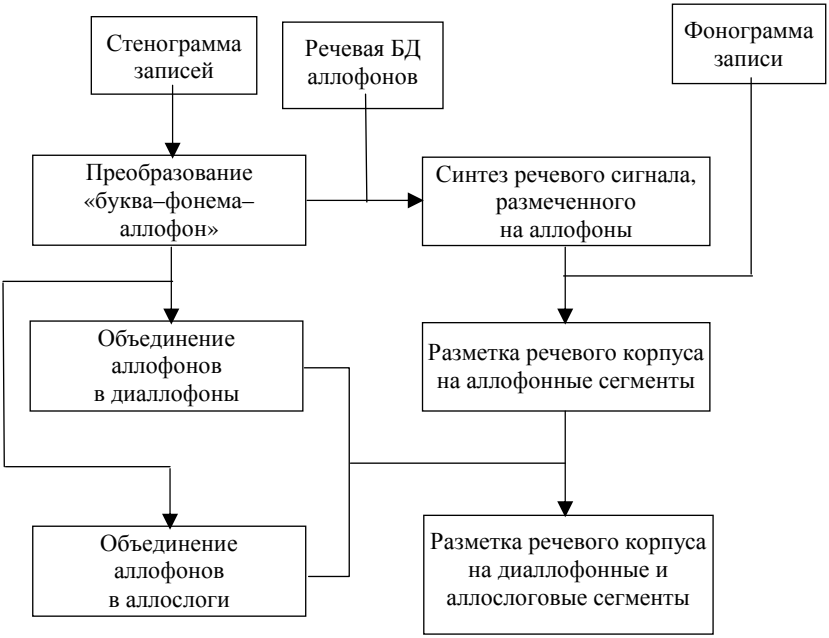


Рис. 18. Алгоритм формирования РПП на основе аллофонов

Речеподобный шум создают из исходного речевого сигнала путем его фазовой модуляции шумовым сигналом, что приводит к разрушению формантной структуры исходного речевого сигнала.

Для разработки алгоритма формирования речеподобной помехи используем гармоническую модель речевого сигнала, описанную в работах [37, 38].

Согласно этой модели любой звук $U(t)$ можно представить в виде

$$S(t) = \sum_{p=1}^{N} U_p(t) \sin\left[2\pi p \int_0^t F_0(\tau) d\tau + \Phi_p(t) \right] + r(t),$$

где $F_0(t)$ – мгновенная частота основного тона звука; $U_p(t)$ – амплитуда p-й гармонической составляющей звука; $\Phi_p(t)$ – фаза p-й гармонической составляющей звука; N – число энергетически значимых гармонических составляющих звука; $r(t)$ – шумовая составляющая звука; $t \in [0, T]$, $\tau \in [0, t]$, T – время анализа звука.

С учетом данного описания звукового сигнала математическая модель речеподобной реверберационной помехи может быть представлена выражением [38]

$$S_{\text{РПП}}(t) = \sum_{j=1}^{6} \sum_{p=1}^{N} U_{pj}(t) \sin\left[2\pi p \int_0^{t-t_j} F_0(\tau) d\tau + \Phi_{pj}(t) \right] + \sum_{j=1}^{6} r_j(t),$$

где j – количество каналов в генераторе РПП; t_j – интервалы задержки исходного сигнала в каналах генератора.

В защищаемом помещении размещается микрофон для приема акустических колебаний, возникающих при разговоре. Сигнал с микрофона поступает на синтезатор речеподобной помехи и воспроизводится посредством акустической системы. Места установки соответствующих устройств и процесс попытки съема акустического сигнала приведены на рис. 19 [27].

Модель синтезатора речеподобной помехи приведена на рис. 20.

Вычислительный эксперимент по моделированию генератора РПП осуществлен с применением математического пакета *Matlab*.

Модель синтезатора речеподобной помехи собрана на базе стандартных объектов среды визуального проектирования *Simulink*, входящей в состав пакета *Matlab*.

Источником речевого сигнала для формирования речеподобной помехи служит микрофон, установленный в помещении (рис. 21). В состав синтезатора входят формирователь речеподобной помехи и акустомат.

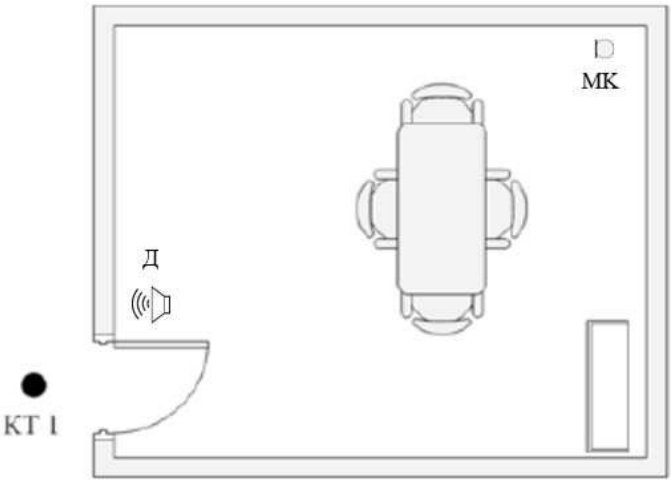


Рис. 19. Положение контрольной точки съема информации и формирователя РПП в выделенном помещении

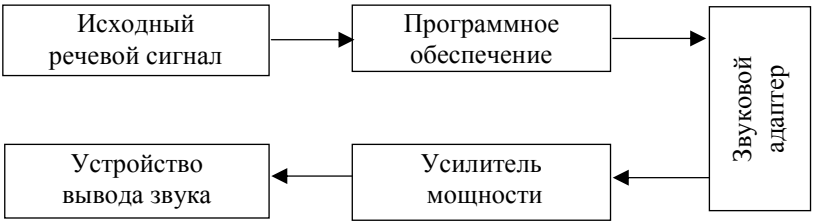


Рис. 20. Модель синтезатора речеподобной помехи

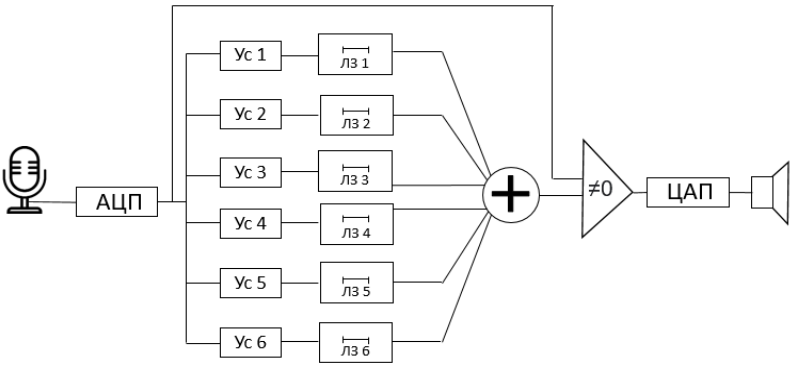


Рис. 21. Процесс формирования речеподобной реверберационной помехи

Формирователь речеподобной помехи представляет собой несколько каналов преобразования исходного сигнала путем усиления (ослабления) и задержки на определенный интервал времени (рис. 22).

Реализация модели синтезатора речеподобной помехи с шестью каналами формирователя в среде *Simulink* представлена на рис. 23 [38].

Исследования, проведенные на разработанной модели, показали, что временные характеристики линий задержки каналов формирования для устранения пауз между фоноабзацами, фразами и синтагмами должны составлять соответственно 0,3; 0,5; 0,8; 1,1; 1,3 и 1,5 с соответственно. Эти величины являются среднестатистическими для русского языка [14].

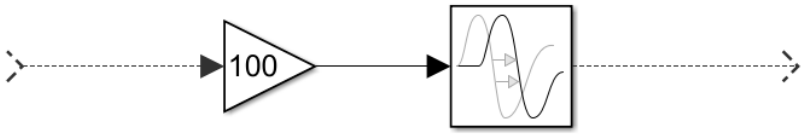


Рис. 22. Канал преобразования исходного сигнала

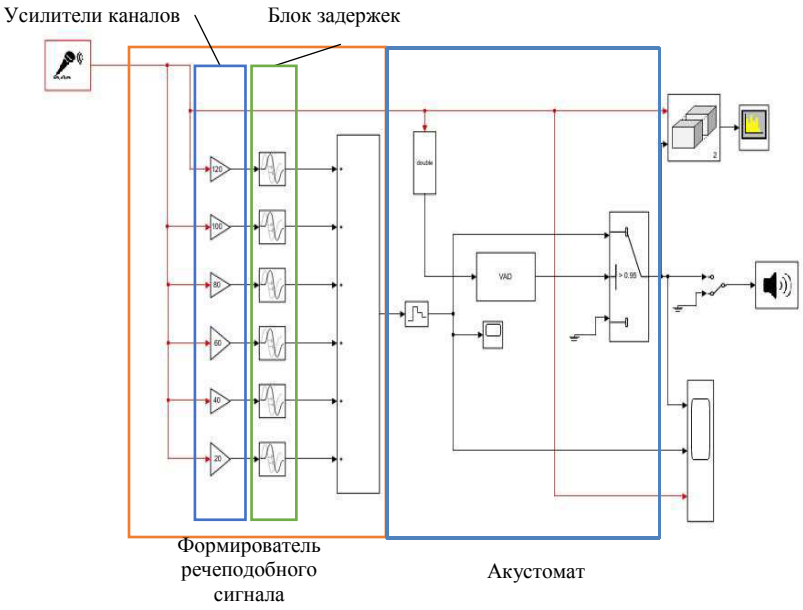


Рис. 23. Модель синтезатора речеподобной помехи с шестью каналами формирователя

Коэффициенты усиления каналов подбираются посредством измерения уровня словесной разборчивости автоматически.

Исследования модели показали, что увеличение количества каналов приводит к изменению как спектра генерируемой помехи, так и ее амплитуды. Эти изменения заметны при переходе от трехканальной схемы (рис. 24) к четырехканальной (рис. 25).

Исследования синтезированной речеподобной помехи позволило получить вероятностные характеристики распределения ее амплитуды, которые представлены в виде гистограммы на рис. 26.

В ходе исследования модели получены спектры речевого сигнала и синтезированной генератором речеподобной помехи (рис. 27), а также временные диаграммы речеподобной реверберационной помехи и ее смеси с исходным речевым сигналом (рис. 28). Результат моделирования показывает достаточную схожесть данных спектров.

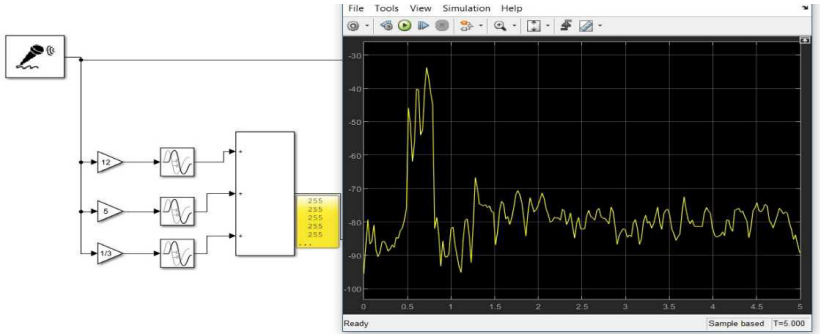


Рис. 24. Трехканальная схема синтезатора речеподобной помехи

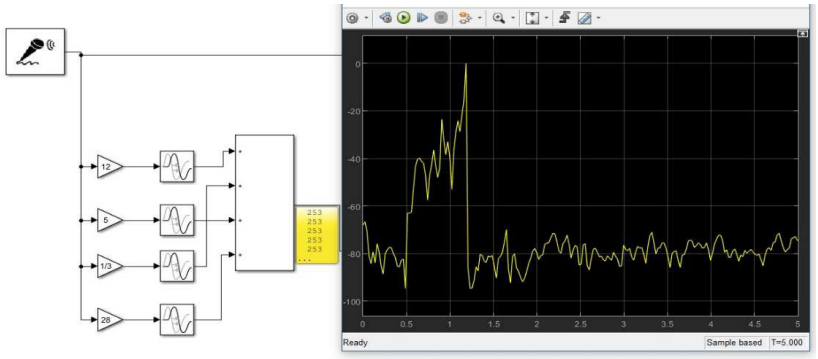


Рис. 25. Четырехканальная схема синтезатора речеподобной помехи

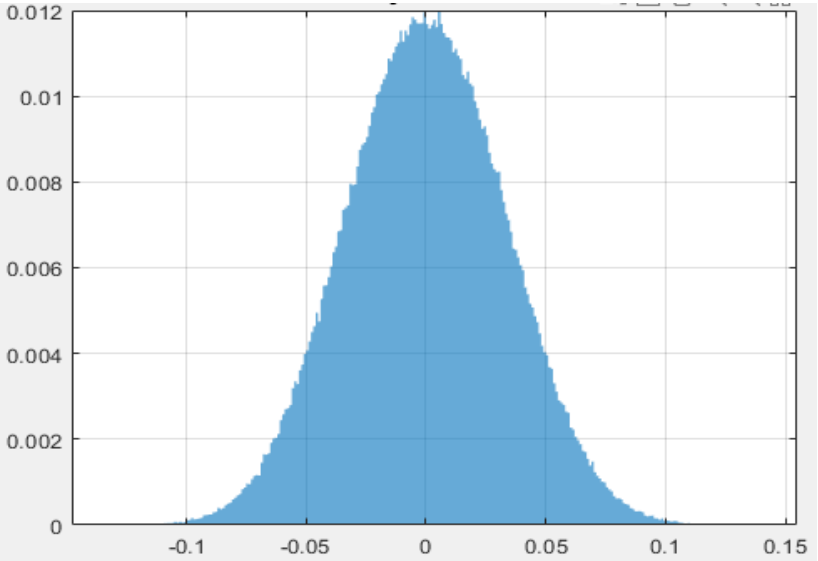


Рис. 26. Относительная вероятность амплитуды речеподобного сигнала

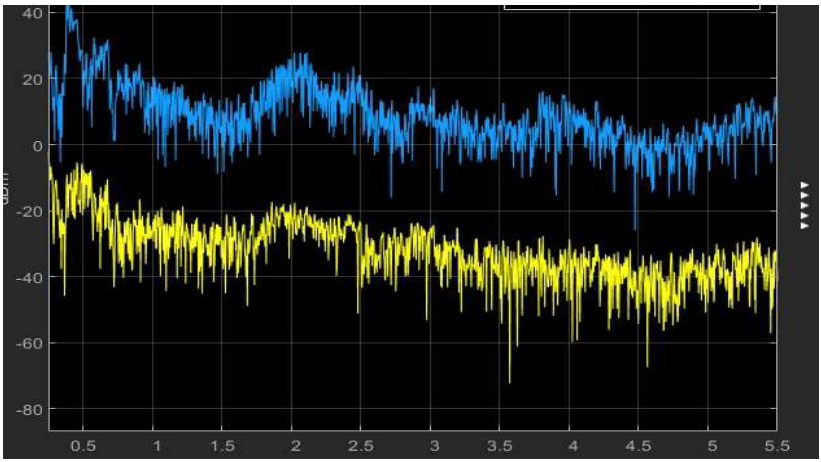


Рис. 27. Спектры речевого сообщения и речеподобной помехи

Спектральный состав речи в значительной степени зависит от пола, возраста и индивидуальных особенностей говорящего. Для различных людей отклонение уровней сигналов, измеренных в октавных полосах, от типовых уровней может составлять до 6 дБ.

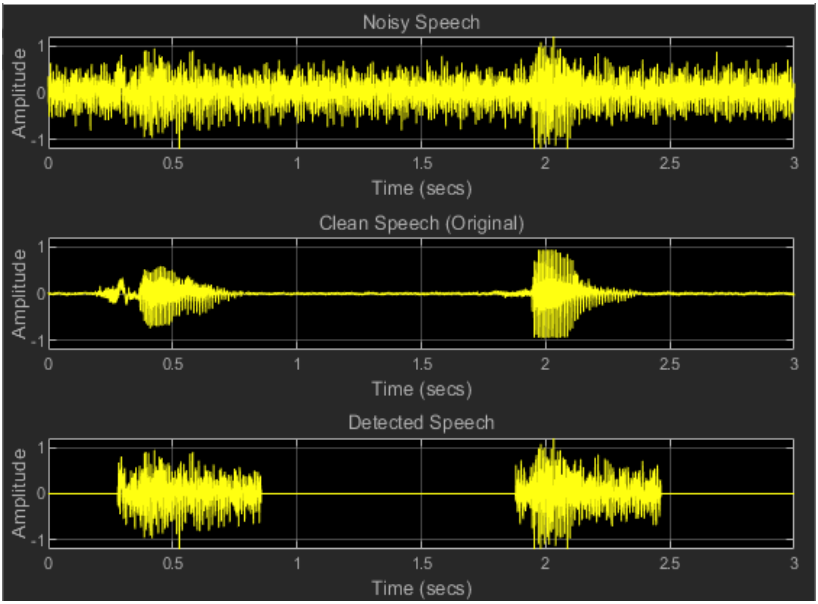


Рис. 28. Результаты моделирования генератора речеподобной помехи (речеподобная помеха, речевое сообщение, сигнал акустомата)

Первая и седьмая октавные полосы являются малоинформативными, поэтому наиболее часто для оценки возможностей средств акустической разведки уровни речевого сигнала измеряют только в пяти (2 – 6) октавных полосах [37, 38]. На рисунке 29 показаны различия в энергетических характеристиках РПП и «розового» шума.

Исследования полученной модели синтезатора речеподобной помехи показали, что уровень РПП при одинаковых показателях словесной разборчивости значительно ниже.

Эффективность формируемой с применением предложенных метода и модели речеподобной помехи подтверждена экспериментально.

Исследования разработанной модели синтезатора речеподобной помехи проведены с использованием артикуляционного и инструментально-расчетного методов [14, 17, 26].

Для проведения экспериментальных исследований использована лабораторная установка, включающая: ноутбук *1* с установленной программой генерации речеподобной помехи; акустическую систему *2*; анализатор спектра – шумомер и цифровой диктофон *3* (рис. 30).

Контрольная точка располагалась за дверью, в месте возможной установки закладных устройств. Дверной проем не был оборудован

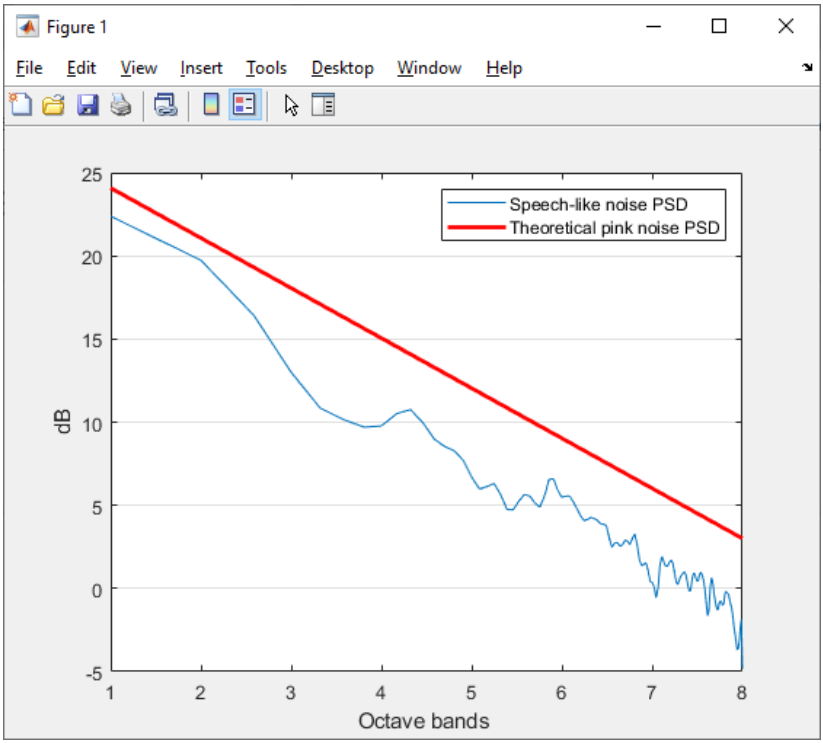


Рис. 29. Энергетические характеристики РПП и «розового» шума

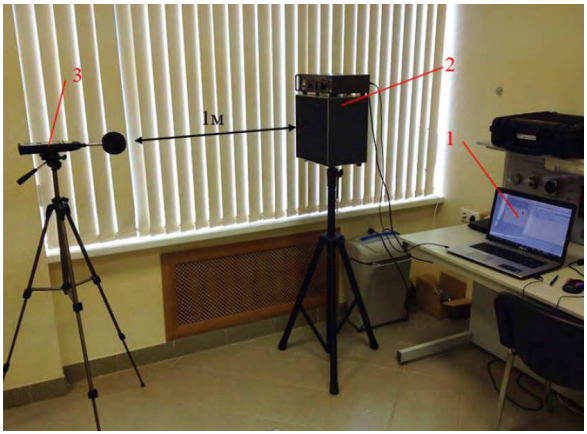


Рис. 30. Схема экспериментальных исследований

тамбуром, уплотнителем и резиновыми проставками. Звукоизоляция проема на частоте 1000 Гц составляла 33 дБ.

Интегральный уровень тестового сигнала выбран организацией-лицензиатом равным типовой речи со средним уровнем громкости. В качестве генератора белого шума использовалась Соната-АВ.

Оценка эффективности речеподобной помехи проводились в два этапа. На первом этапе проводилась оценка эффективности речеподобной помехи методом артикуляционных испытаний в соответствии с ГОСТ 16600–72.

С использованием специальной программы на жесткий диск ноутбука были записаны 10 фраз из артикуляционных таблиц ГОСТ 16600–72 (тест 19), которые использовались в качестве тестового сигнала. Фразы, используемые в исследовании, приведены в табл. 5.

На звуковую карту ноутбука подавался тестовый сигнал и формируемая речеподобная помеха. Уровень помехи и уровень сигнала регулировались с помощью микшера громкости. С линейного выхода звуковой карты ноутбука сигналы (тестовый сигнал, помеховый сигнал,

5. Фразы, используемые в исследовании, согласно ГОСТ 16600–72

№	Фраза
1	Суховей уменьшил урожай
2	У юнги широкие плечи
3	Конфеты подарил друг
4	На заводе появилась техника
5	Тишина воцарилась в зале
6	Ветер помогал перебежке
7	Ребенок ходит в ясли
8	Танцовщица устроилась в цирк
9	План утверждают в области
10	Диктора поразило сообщение

а также смесь сигнала и помехи) подавались на вход усилителя акустической системы. Принятый микрофоном сигнал обрабатывался и производилось измерение уровня словесной разборчивости.

Процедура измерения уровня словесной разборчивости представлена на рис. 31.

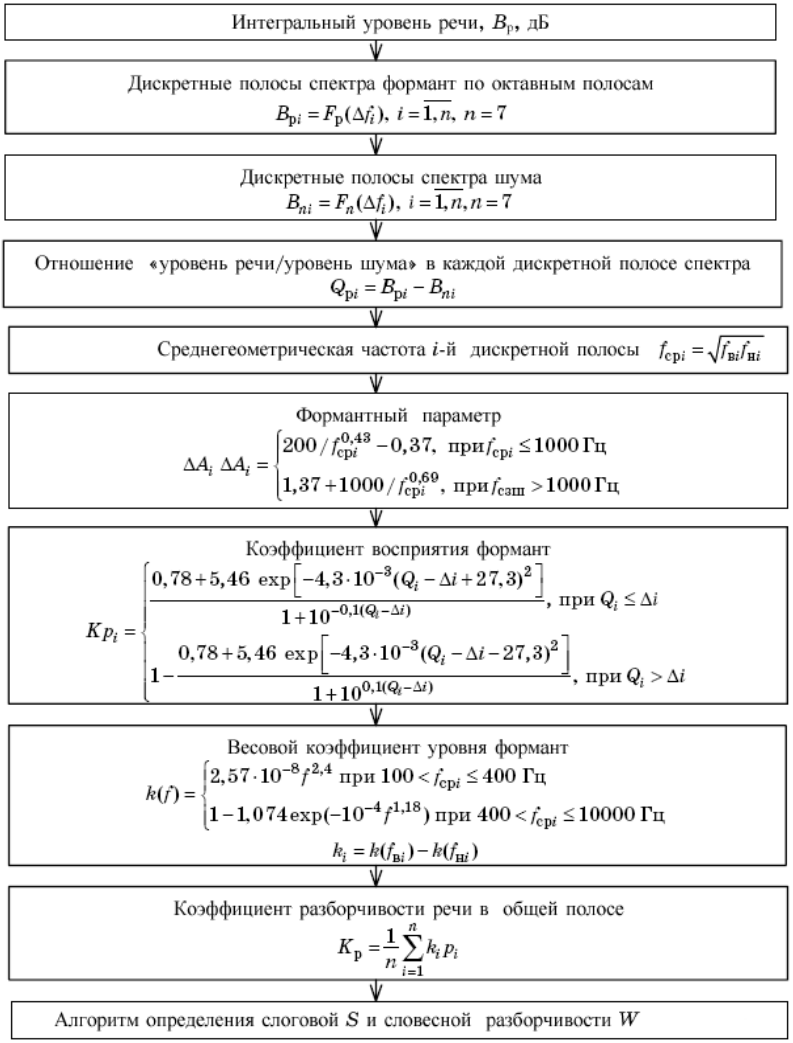


Рис. 31. Процедура измерения уровня словесной разборчивости

6. Измеренные уровни сигналов и помех

Средняя частота октавной полосы, Гц	Уровень сигнала, дБ	Уровень «сигнал + шум» при различных отношениях сигнал/шум, дБ					
		–5	0	5	10	15	20
125	53,3	63,6	58,6	52,7	49,6	42,1	38,8
250	63,1	69,5	66,1	60,5	56,1	50,4	45,4
500	65,5	73,2	68,7	63,0	60,3	53,3	49,0
1000	61,1	66,4	61,6	56,1	51,5	46,5	41,0
2000	56,7	69,1	64,8	59,4	55,8	49,1	44,4
4000	54,6	67,4	62,0	55,1	52,3	46,0	41,5
8000	56,5	65,8	69,3	53,3	49,8	43,7	39,0

Уровень помехи, уровень сигнала и уровень внешнего шума измерялись шумомером (табл. 6).

С помощью цифрового диктофона сделаны восемь аудиозаписей: запись помехи, запись сигнала и 6 записей «сигнал + помеха», где разница между сигналом и помехой соответственно составляла –5; 0; 5; 10; 15 и 20 дБ.

На рисунке 32 представлены осциллограмма аудиозаписи формируемой речеподобной помехи и осциллограмма аудиозаписи «сигнал + + помеха», которая предоставлялась для прослушивания аудиторам.

Полученные аудиозаписи «сигнал + помеха» предоставлялись для прослушивания субъектам, которые не знали слов, которые использовались в качестве тестовых сигналов. Субъектам предоставлялась возможность многократного прослушивания записей и их отрезков. Услышанные слова заносились в таблицу, по которой рассчитывался процент правильно понятых слов (табл. 7).

Результаты, представленные в табл. 7, показывают, что уже при отношении сигнал/помеха менее 5 дБ словесная разборчивость становится менее 11%, что исключает возможность установления предмета разговора.

На втором этапе проводилась оценка эффективности речеподобной помехи инструментально-расчетным методом. В качестве исходных данных для расчета использовались измеренные уровни сигналов и помех в октавных полосах, приведенные в табл. 7.

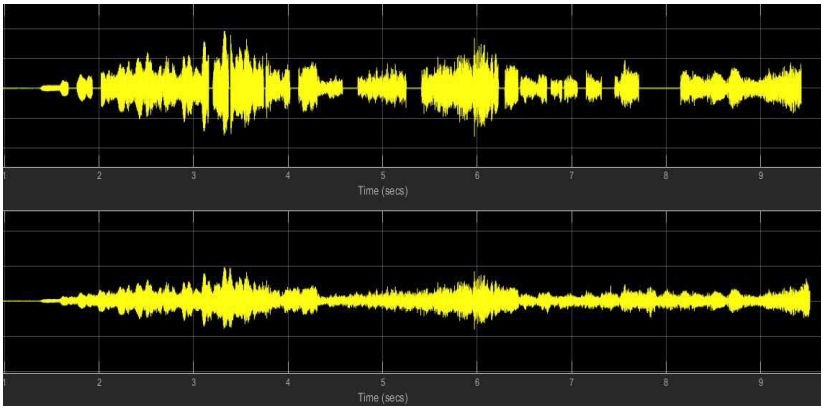


Рис. 32. Осциллограммы формируемой смеси речевого сигнала и речеподобной помехи

7. Результаты оценки словесной разборчивости артикуляционным методом

Номер эксперимента	Словесная разборчивость W, %, при отношении сигнал/шум q, дБ					
	–5	0	5	10	15	20
1	5	24	45	65	78	86
2	3	22	34	62	75	83
3	7	29	50	70	82	93
4	2	19	38	6	72	85
5	3	21	33	65	78	88
Средняя разборчивость речи	4	23	40	65	77	87

Расчет словесной разборчивости речи W инструментально-расчетным методом (ИРМ) проводился по стандартной методике. Результаты расчетов приведены в табл. 8 и на рис. 33.

Анализ результатов, представленных в табл. 7, показывает, что они имеют высокую корреляцию с результатами расчетов. Сравнение результатов оценки словесной разборчивости при использовании

8. Результаты оценки словесной разборчивости ИРМ

Отношение сигнал/шум, дБ	Словесная разборчивость *W*, %
–5	38
0	68
5	84
10	91
15	95
20	98

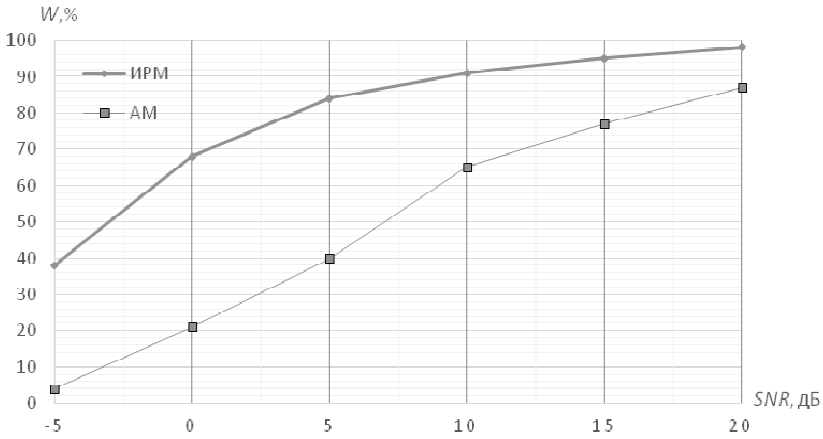


Рис. 33. Результаты оценки словесной разборчивости в зависимости от отношения сигнал/шум

речеподобной помехи артикуляционным и инструментально-расчетным методами показывает, что они существенно отличаются. Так, например, при отношении сигнал/помеха, равном 5 дБ, словесная разборчивость, полученная артикуляционным методом, составляет 40%, а полученная инструментально-расчетным методом – 84%. Такое различие возникает, вероятно, из-за того, что используемая для расчета словесной разборчивости речи методика не учитывает особенностей восприятия человеком речи в условиях помехи, формируемой из звуков этой же речи.

9. Сравнительная таблица зависимости словесной разборчивости от уровня интегральной помехи

Вид помехи	*W*, %	Интегральный уровень помехи
«Розовый» шум (программная реализация)	10	63,17
Речеподобная реверберационная помеха (модель)	10	61
«Белый» шум (Соната-АВ)	10	69,49

Таблица 9 – сравнительная таблица эффективности применения «речеподобных» шумовых помех по сравнению с «белым» шумом. При словесной разборчивости, равной 10% (при данном значении невозможно установить предмет ведущегося в помещении разговора даже при проведении операции шумоочистки), интегральный уровень помехи «белый» шум составил 69,49 дБ, тогда как речеподобного шума 61 дБ. Из рассмотренных шумовых помех наиболее эффективной оказалась комбинированная речеподобная помеха: поочередное изменение уровня и тональности сигнала. «Белый» шум оказался наиболее громким по сравнению с другими маскирующими шумовыми помехами.

3.3. ПОДСИСТЕМА ФОРМИРОВАНИЯ УПРАВЛЯЮЩЕЙ ИНФОРМАЦИИ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОГО КОМПЛЕКСА

Для решения задачи синтеза НИК необходимо количественно определить все параметры, характеризующие защищенность объектов при воздействии различных угроз, и оценить эффективность различных используемых средств защиты при воздействии тех или иных угроз.

После того как каждый из указанных параметров определен, формулируется задача выбора оптимального решения.

Когда все параметры оценены количественно, она превращается в задачу многокритериальной оптимизации, которая может быть решена математическими методами (линейное, векторное, динамическое программирование).

Критерий оптимальности $I = \text{extr}(Y, Y_{\text{тр}})$ формулируется на основе целевой функции $L(Y, Y_{\text{тр}})$, включающей систему используемых показателей Y и требуемых значений таких показателей $Y_{\text{тр}}$, а также указания по поиску ее экстремума (min, max, min max, max min и др.).

Возможно использование следующих основных видов целевых функций: простая $L = (Y - Y_{тр})$; модульная $L = |Y - Y_{тр}|$; квадратичная $L = (Y - Y_{тр})^2$.

Помимо указанных выше технических параметров, при синтезе НИК параметрами могут выступать стоимость, срок сохранности конфиденциальности информации, время работы и др.

Наличие множества таких различных показателей и зачастую противоречивых критериев оптимальности порождает проблему многокритериальной (векторной) оптимизации процесса функционирования НИК.

Задача оптимизации по векторному критерию состоит в поиске решений, удовлетворяющих экстремуму одновременно всех компонент векторного критерия оптимальности.

Существует несколько основных путей решения данной задачи: поиск компромиссных решений, оптимальных по Парето; поиск решений, оптимальных в смысле обобщенного скалярного критерия, полученного путем свертки (скаляризации) всех компонент векторного критерия оптимальности; поиск по одному выбранному главному показателю при условии, что остальные показатели удовлетворяют системе ограничений, заданных в виде неравенств, и поиск, основанный на ранжировании показателей по важности (лексикографический метод и метод последовательных уступок).

Подсистема формирования управляющих воздействий выполняет непрерывный контроль состояния системы защиты конфиденциальной информации, проверку соответствия показателей защищенности допустимым значениям и обеспечивает оперативное подключение новых средств защиты в ситуациях, способных привести к нарушению безопасности конфиденциальной информации.

3.4. ВЕРИФИКАЦИЯ РАЗРАБОТАННОГО ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА

Подключение и размещение аппаратных средств защиты стоит выполнять по инструкции производителя. Основываясь на его рекомендациях, удастся достичь оптимального уровня защиты помещения с имеющимся комплексом технических средств. Необходимые инструкции доступны на сайте производителя и подбираются в зависимости от конкретной модели устройства.

На рисунке 15 представлены основные варианты размещения датчиков записи звука при измерениях основных ограждающих и инженерных конструкций. Существуют особенности при измерениях перекрытий пола и потолка. В таком случае излучатель и микрофон размещаются в соответствии со схемой, представленной на рис. 30.

Установка программного обеспечения «ИСИДОРА» не требуется, так как программа является портативной, активация заключается в запуске соответствующего исполняемого файла. Программу следует запускать на устройстве, к которому уже подключен блок управления и питания средств защиты. Пользовательский интерфейс приложения продемонстрирован на рис. 34.

Запуск записи и анализа звука осуществляется нажатием кнопки «Включить микрофон» (рис. 35). При наведении на эту или любую последующую кнопку появится всплывающая подсказка. Повторное нажатие выключит функцию.

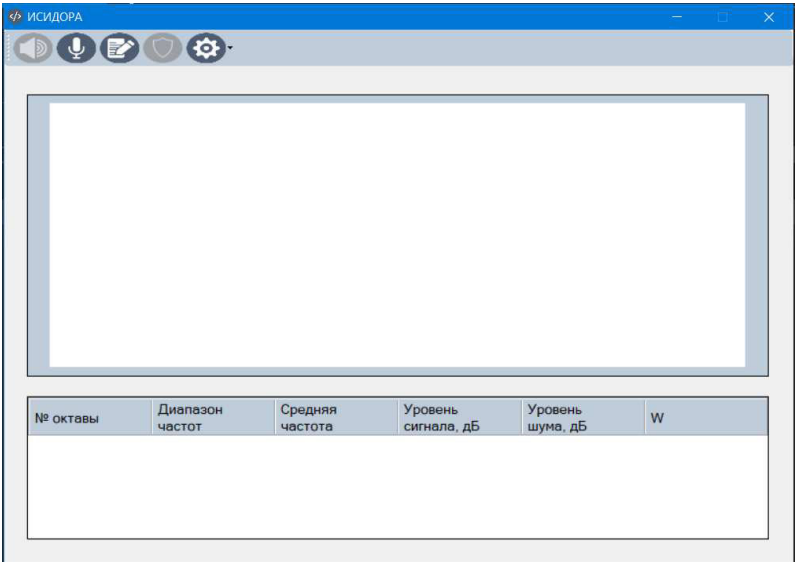


Рис. 34. Пользовательский интерфейс программы «ИСИДОРА»

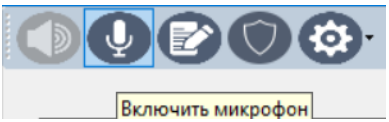


Рис. 35. Кнопка «Включить микрофон»

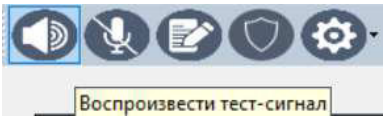


Рис. 36. Кнопка «Воспроизвести тест-сигнал»

Режим тестирования включается нажатием кнопки «Воспроизвести тест-сигнал» (рис. 36). До включения записи звука данный функционал заблокирован.

Воспроизведение тест-сигнала отобразится на спектре отдельными всплесками на каждой анализируемой октаве. Наблюдать этот процесс можно на графике спектра (рис. 37).

Результаты расчетов отображены на таблице результатов (рис. 38).

Помимо этого, нажатие на кнопку «История измерений», представленную на рис. 39, выводит результаты измерений, проведенных в последний запуск программы.

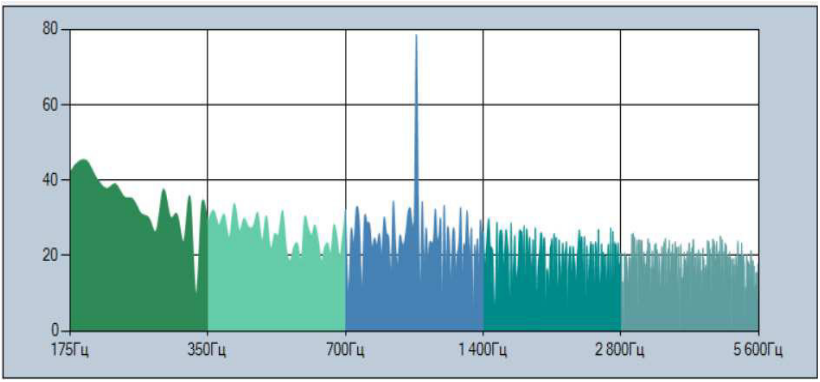


Рис. 37. Всплеск уровня сигнала на графике спектра

№ октавы	Диапазон частот	Средняя частота	Уровень сигнала, дБ	Уровень шума, дБ	W
1	175-350	250	36,683	36,355	0,292
2	350-700	500	37,431	30,403	0,292
3	700-1400	1000	45,713	26,279	0,292
4	1400-2800	2000	43,818	26,351	0,292

Рис. 38. Результаты расчета уровня словесной разборчивости

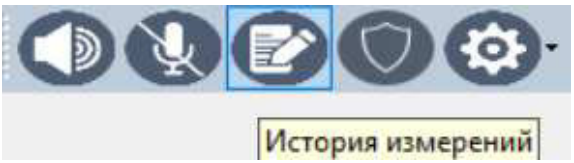


Рис. 39. Кнопка «История измерений»

Для начала автонастройки генератора активной помехи можно исключить предварительный запуск вычисления словесной разборчивости, так как этот режим включает в себя предварительный расчет. Кнопка включения режима отображена на рис. 40. Результатом настройки будет являться либо сообщение об успешности операции с указанием выбранного уровня излучения, либо сообщение об ошибке.

Нажатие кнопки «Настройки» предоставляет доступ для дополнительных настроек работы программы (рис. 41). К таким относятся: настройка выбора количества анализируемых октав, настройки отображения спектра и уровней шума, изменение относительно величины перевода амплитуды сигнала в децибелы.

Для верификации программного продукта проведем эксперимент, сравнивающий теоретически рассчитанный коэффициент словесной разборчивости и практически полученный посредством использования программного обеспечения «ИСИДОРА».

Для оценки возможностей средств акустической речевой разведки необходимо определить места возможного размещения датчиков аппаратуры акустической разведки или места возможного прослушивания речи и для них рассчитать отношения сигнал/шум в октавных полосах, затем – словесную разборчивость речи *W*.

Если рассчитанное значение словесной разборчивости речи не превышает установленного нормированного значения, считается, что перехват разговоров, ведущихся в выделенном помещении, техническими средствами акустической разведки невозможен.

Рис. 40. Кнопка «Автонастройка генератора шума»

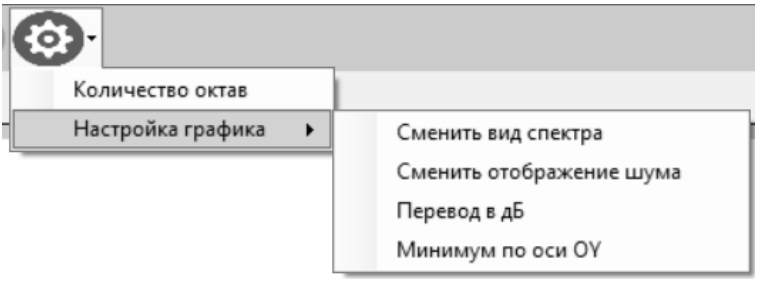


Рис. 41. Кнопка «Настройки»

Если рассчитанное значение словесной разборчивости речи выше установленного нормированного значения, необходимо применять меры по защите выделенного помещения от утечки речевой информации по прямому акустическому каналу.

Ослабление акустических сигналов осуществляется путем звукоизоляции помещений, которая направлена на локализацию источников акустических сигналов внутри них. Звукоизоляция оценивается величиной ослабления акустического сигнала и обеспечивается с помощью архитектурных и инженерных решений, а также применением специальных строительных и отделочных материалов.

Воспользуемся справочными значениями звукоизоляции тестируемого объекта. В качестве тестового помещения используем учебную аудиторию. Потенциальное место утечки – стандартная дверь со стеклянной вставкой.

Воспользуемся справочным материалом коэффициентов звукопоглощения различных материалов для определения необходимого для эксперимента показателя (табл. 10).

Примем громкость разговора в помещении равной уровню громкого разговора в офисе – 60 дБ.

Опираясь на справочный коэффициент звукопоглощения, за пределы помещения выйдет лишь часть информации [13]. Вычислим уровень сигнала на каждой анализируемой частоте и запишем в табл. 11.

Для достижения равных условий вычислений статически зададим обусловленные данные программе. Уровнем естественного шума в помещении будет считаться тихий звук в 35 дБ.

10. Коэффициенты звукопоглощения материалов

Материал или конструкция	Коэффициент звукопоглощения при частоте звука, Гц				
	250	500	1000	2000	4000
Деревянная дверь со стеклянной вставкой	0,20	0,10	0,05	0,04	0,05

11. Потенциальный уровень сигнала за пределами помещения

Частота сигнала, Гц	250	500	1000	2000	4000
Уровень сигнала за пределами помещения	48	54	57	58	57

Результат расчета можно увидеть на рис. 42. Программа вычислила, что при заданных условиях коэффициент словесной разборчивости будет равен значению 0,563.

Вернем настройку программного обеспечения на автоматический режим измерений. Установив излучатель тест-сигналов и микрофон согласно рекомендуемой схеме, проведем программный расчет коэффициента словесной разборчивости. Результат вычислений представлен на рис. 43.

Вычислено, что коэффициент словесной разборчивости при реальном тестировании в заданном помещении приблизительно равен теоретическому расчету. Программный результат вычисления коэффициента словесной разборчивости равен 0,556. С учетом небольшой погрешности, допускаемой при реализации подобных инструментально-расчетных методик, эксперимент можно считать успешным, а измерения, производимые программой, – верными.

Однако стоит отметить, что полученный коэффициент словесной разборчивости не соответствует требованиям безопасности. Пусть минимальным уровнем, необходимым для обеспечения безопасности речевой информации, будет считаться показатель, равный 0,3. Так как шумоизоляция помещения не удовлетворяет требованиям безопасности, необходимо ввести дополнительные меры, подключив средства активной акустической помехи.

№ октавы	Диапазон частот	Средняя частота	Уровень сигнала, дБ	Уровень шума, дБ	W
1	175-350	250	48	35	0,563
2	350-700	500	54	35	0,563
3	700-1400	1000	57	35	0,563
4	1400-2800	2000	58	35	0,563
5	2800-5600	4000	57	35	0,563

Рис. 42. Результат расчета коэффициента словесной разборчивости при использовании справочных данных

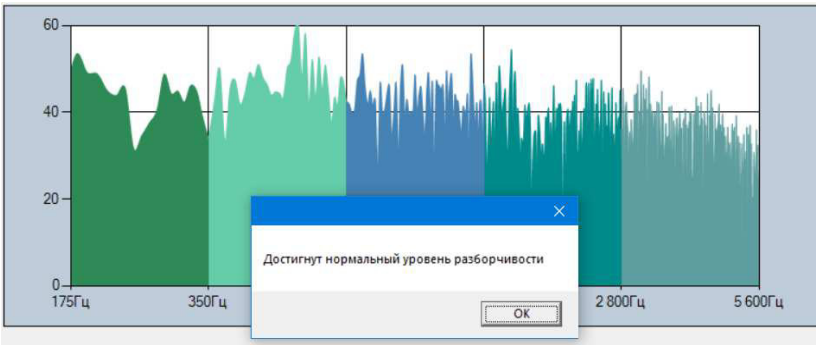
№ октавы	Диапазон частот	Средняя частота	Уровень сигнала, дБ	Уровень шума, дБ	W
1	175-350	250	55,527	39,313	0,566
2	350-700	500	58,748	29,061	0,566
3	700-1400	1000	58,323	43,724	0,566
4	1400-2800	2000	64,817	44,277	0,566
5	2800-5600	4000	61,953	38,106	0,566

Рис. 43. Результат расчета коэффициента словесной разборчивости при использовании программного обеспечения «ИСИДОРА»

В качестве устройств воспользуемся генератор-акустоизлучателем «Соната-СА-65М», представленным на лабораторном стенде. Подключив средство защиты к блоку питания и управления «Соната-ИП3», соединим устройство с компьютером. Запустив автонастройку генератора, остается дождаться окончания выполнения работы программы. На рисунке 44 отображен результат настройки.

Руководство по эксплуатации программно-аппаратного комплекса сводится к двум отдельным разделам: инструкции аппаратной и программной части. Из-за отсутствия строгих ограничений по используемым аппаратным средствам нельзя привести единые рекомендации к настройке и размещению средств защиты, поэтому для получения таких инструкций следует обратиться к производителю средств защиты. Руководство по эксплуатации программного обеспечения «ИСИДОРА» мы представили в этом разделе, детально описывая использование всех возможностей программы.

Верификация научно-исследовательского комплекса была построена на сравнении результатов вычислительного эксперимента и теоретических расчетов характеристик НИК. Результат проведения вычислительного эксперимента показал приблизительно равный теоретическим расчетам результат, что является доказательством верности работы НИК.



№ октавы	Диапазон частот	Средняя частота	Уровень сигнала, дБ	Уровень шума, дБ	W
1	175-350	250	51,753	69,441	0,109
2	350-700	500	58,181	50,945	0,109
3	700-1400	1000	33,852	49,094	0,109
4	1400-2800	2000	59,003	42,052	0,109
5	2800-5600	4000	48,535	41,314	0,109

Рис. 44. Результат работы режима автонастройки генератора шума

Помимо этого, была протестирована функция адаптивной настройки генератора шума «Соната-СА-65М». Для обеспечения словесной разборчивости, равной 0,3, программа настроила средство активной защиты на второй уровень излучения. Такой уровень не мешает нахождению и работе в помещении и позволяет снизить коэффициент словесной разборчивости до 0,109, что является хорошим результатом, ведь при словесной разборчивости, равной 10%, практически невозможно установление предмета ведущегося разговора, даже при использовании современной техники фильтрации помех.

ЗАКЛЮЧЕНИЕ

Значительные финансовые потери многие компании ежегодно несут вследствие утечки конфиденциальной информации. На борьбу с данной проблемой выделяют внушительные материальные средства, предпринимают различные меры защиты, вместе с тем зачастую не уделяют должного внимания техническим каналам утечки речевой информации, что является существенной ошибкой. Повышение уровня защиты конфиденциальной информации является полезным вложением, способным сберечь в разы больше собственной стоимости. Этот факт обуславливает актуальность этой работы, конечным продуктом которой является усовершенствованный программно-аппаратный комплекс защиты речевой информации от утечки по акустическому каналу.

В ходе исследования были систематизированы причины формирования технических каналов утечки. Детально проанализированы прямой акустический, акустовибрационный и оптико-электрический каналы.

Основными средствами защиты речевой информации от утечки по данным каналам является звукоизоляция помещений, поиск закладных устройств и активная акустическая маскировка. Основу средств маскировки составляют генераторы помех. На практике наиболее широкое применение нашли генераторы шумовых колебаний. Применение данного метода позволяет снизить отношение сигнал/шум на входе технического средства разведки за счет увеличения уровня помехи.

Однако акустические помехи, создаваемые техническими средствами защиты информации, не должны приносить существенный дискомфорт присутствующим в помещении участникам диалога. Возникает проблема приведения мощности акустической помехи к оптимальному уровню, удовлетворяющему и требованиям защищенности помещения, и комфортному ведению разговора.

Сравнительный анализ существующих методик оценки разборчивости речи показал, что для решения задачи исследования помещения на предмет утечки информации по речевому каналу эффективным решением будет использование инструментально-расчетного метода. Данный метод основывается на версии формантного метода Н. Б. Покровского, при котором числовое значение словесной разборчивости рассчитывается на основе измерения отношения уровней речевого сигнала и шума в местах предполагаемой утечки речевой информации.

При обнаружении недостаточной защищенности помещения и решении использования средства активной защиты информации выявили необходимость проведения настройки устройства на оптимальный уровень излучения. Настройка основана на методе перебора доступных уровней излучения СЗИ в поисках минимально возможного из обеспечивающих

необходимый уровень защиты. Эта тактика делает настройку прибора автоматической, что добавляет удобство в работу пользователя.

В ходе работы были разработаны и реализованы модель и программно-аппаратный комплекс, в полной мере обеспечивающие решение поставленных задач: вычисление коэффициента словесной разборчивости, позволяющего оценить уровень защищенности помещения, адаптивная настройка средств активной защиты информации. Аппаратная часть комплекса представлена в виде минимально необходимого набора средств защиты, состоящего из генератора акустических помех, виброгенераторов, обеспечивающих защиту от утечки по акустовибрационному каналу и предотвращающих съем информации оптикоэлектронными методами. Поставщиком аппаратных средств защиты была выбрана зарекомендовавшая себя отечественная компания «Анна». Данная компания производит весь требуемый набор продуктов, позволяя собрать комплекс под конкретные цели потребителя. Деятельность производителя лицензирована, а сама продукция сертифицирована.

Для верификации программно-аппаратного комплекса было проведено сравнение реальных результатов работы программы с теоретически рассчитанными для заданной экспериментальной обстановки. Результат работы вычислительной программы показал приблизительно равный теоретическим расчетам результат, что можно принять как доказательство верности работы программы.

Помимо этого, была протестирована функция адаптивной настройки генератора шума «Соната-СА-65М». С помощью программы удалось привести уровень разборчивости речи за пределами помещения к показателю, равному 0,109, что является хорошим результатом, ведь при словесной разборчивости, равной 10%, практически невозможно установление предмета ведущегося разговора, даже при использовании современной техники фильтрации помех. Результат работы может использоваться как программно-аппаратный комплекс защиты акустической информации в помещениях офисного типа. Особенностью продукта является наличие свойства адаптивности акустических генераторов шума под происходящие в помещении изменения акустической обстановки.

Таким образом, создание на основе разработанной методологии построения научно-исследовательских комплексов мониторинга характеристик защищенности корпоративной информации макета программно-аппаратного комплекса для исследования и нейтрализации каналов утечки речевой информации обеспечивает расширение теоретических знаний и практики применения СЗИ в области технологий построения научно-исследовательских комплексов мониторинга характеристик защищенности конфиденциальной информации и получения новых экспериментальных данных о процессах формирования и их применения.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев, В. В. Сравнительная характеристика методов разборчивости речи / В. В. Алексеев, А. В. Яковлев, М. В. Моисеева // XXVIII Междунар. науч.-техн. конф. «Современные технологии в задачах управления, автоматики и обработки информации». – М. : Изд-во «НИЯУ «МИФИ», 2019. – С. 85–86.

2. Авдеев, В. Б. Методические основы защищенности акустической речевой информации от ее утечки по каналам линейного и нелинейного высокочастотного облучения / В. Б. Авдеев // Специальная техника. – 2013. – № 5. – С. 16 – 25.

3. Бузов, Г. А. Защита от утечки информации по техническим каналам : учебное пособие / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. – М. : Горячая линия – Телеком, 2005. – 415 с.

4. Бутов, Ю. И. Совершенствование методов технической защиты информации в режимных учебных аудиториях и оценка их эффективности / Ю. И. Бутов, А. И. Колезнев, О. А. Скляр // Инфокоммуникационные технологии. – 2007. – № 3. – С. 150 – 152.

5. Ворона, В. А. Способы и средства защиты информации от утечки по техническим каналам / В. А. Ворона, В. О Костенко // Computational nanotechnology. – 2016. – № 3. – С. 208 – 223.

6. Гавриленко, А. В. Сравнительный анализ некоторых методов оценки разборчивости речи / А. В. Гавриленко, В. С. Дидковский, А. Н. Продеус // Акустический симпозиум «Консонанс-2007». – 2007. – С. 54 – 65.

7. Генератор-аудиоизлучатель «Соната-СА-65М» [Электронный ресурс]. – URL : http://www.geroltd.ru/Catalog/Sredsv_zash/Acusto_shum/Sonata-CA-65M.html (дата обращения: 20.02.2020).

8. Генератор-виброизлучатель «Соната-СВ-45М» [Электронный ресурс]. – URL : http://www.geroltd.ru/Catalog/Sredsv_zash/Acusto_shum/Sonata-CB-45M.html (дата обращения: 20.02.2020).

9. Генератор-виброизлучатель «Соната-СП-45М» [Электронный ресурс]. – URL : http://www.geroltd.ru/Catalog/Sredsv_zash/Acusto_shum/Sonata-CP-45M.html (дата обращения: 20.02.2020).

10. Герасименко, В. А. Защита информации в автоматизированных системах обработки данных : в 2 кн. Кн. 1. / В. А. Герасименко. – М. : Энергоатомиздат, 1994. – 400 с.

11. Герасименко, В. Г. Методы защиты акустической речевой информации от утечки по техническим каналам / В. Г. Герасименко, Ю. Н. Лаврухин, В. И. Тупота. – М. : РЦИБ Факел, 2008. – 256 с.

12. Голошубов, К. С. Исследование проведения проверки по выполнению норм эффективности защиты речевой информации от утечки по акустическому каналу / К. С. Голошубов, А. А. Ложечкин, А. П. Жук. – Ставрополь : Северо-Кавказский федер. ун-т, 2015. – 136 с.

13. ГОСТ 31295.1–2005. Шум. Затухание звука при распространении на местности. Ч. 1. Расчет поглощения звука атмосферой. – Введ. 2007-01-01. – М. : Стандартинформ, 2006. – 39 с.

14. ГОСТ Р 50840–95. Передача речи по трактам связи. Методы оценки качества, разборчивости и узнаваемости. – М. : Изд-во стандартов, 1996. – 234 с.

15. Дворянкин, С. В. Обоснование критериев эффективности защиты речевой информации / С. В. Дворянкин, Ю. К. Макаров, А. А. Хорев // Защита информации. Инсайд. – 2007. – № 2. – С. 18 – 25.

16. Дидковский, В. С. Акустическая экспертиза каналов речевой коммуникации / В. С. Дидковский, М. В. Дидковская, А. Н. Продеус. – Киев : Имэкс-ЛТД, 2008. – 420 с.

17. Железняк, В. К. Некоторые методические подходы к оценке эффективности защиты речевой информации / В. К. Железняк, Ю. К. Макаров, А. А. Хорев // Специальная техника. – 2000. – № 4. – С. 39 – 45.

18. Иванов, А. В. Методика оценки защищенности речевой информации от утечки по техническим каналам с учетом форсирования речи : автореф. … канд. техн. наук: 05.13.19 / А. В. Иванов. – Новосибирск, 2015. – 22 с.

19. Козлов, С. Н. Защита информации: устройства несанкционированного съема информации и борьба с ними / С. Н. Козлов. – М. : Академический проект, 2018. – 286 с.

20. Корепанов, А. Г. Оценка защищенности помещений от утечки речевой информации / А. Г. Корепанов, А. В. Михеев // Материалы Всероссийской ежегодной научно-практической конференции «Общество, наука, инновации» (НПК-2013) – 2013. – С. 1455 – 1459.

21. Кузнецов, В. И. Акустические свойства связной речи / В. И. Кузнецов, Л. В. Бондарко, В. М. Леонов. – СПб. : Санкт-Петербургский гос. ун-т, 1996. – 53 с.

22. Лыньков, Л. М. Основы защиты информации и управления интеллектуальной собственностью / Л. М. Лыньков, В. Ф. Голиков, Т. В. Борботько. – Минск : БГУИР, 2013. – 243 с.

23. Моляков, А. С. Технические каналы утечки акустической информации / А. С. Моляков // Аспирант и соискатель. – 2006. – № 6. – С. 176 – 178.

24. Паршин, К. А. Оценка уровня информационной безопасности на объекте информатизации. Информатика и вычислительная техника, информационные системы и технологии : учебное пособие / К. А. Паршин. – М. : ФГБОУ «Учебно-методический центр по образованию на железнодорожном транспорте», 2015. – 95 с.

25. Перегудов, Ф. И. Введение в системный анализ / Ф. И. Перегудов, Ф. П. Тарасенко. – М. : Высшая школа, 1989. – 361 с.

26. Покровский, Н. Б. Расчет и измерение разборчивости речи / Н. Б. Покровский. – М. : Гос. изд-во литературы по вопросам связи и радио, 1962. – 392 с.

27. Свидетельство о государственной регистрации программы для ЭВМ 2019667587. Российская Федерация. Измерительная система дополненной реальности. – Акустика (ИСИДОРА) / Машкова О. С., Савилова У. А., Шибков Д. А., Яковлев А. В., Яковлева Д. А. ; заявитель и правообладатель Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный технический университет». – № 2019666736 ; заявл. 17.12.2019 ; опубл. 25.12.2019. – 1 с.

28. Системный подход к построению программно-аппаратного комплекса для подготовки специалистов по информационной безопасности / В. В. Алексеев, В. А. Гриднев, А. В. Яковлев, О. С. Машкова, У. А. Савилова, Д. А. Шибков, Д. А. Яковлева // Вестник Тамбовского государственного технического университета. – 2021. – Т. 27, № 1. – С. 20 – 30.

29. Смирнов, В. И. Оценки защищенности речевой информации в выделенном помещении с помощью инструментально-расчетного метода / В. И. Смиронов // Кибернетика и программирование. – 2012. – № 2. – С. 18 – 24.

30. Соната-ИП3 (исп. 305, исп. 307, исп. 308) – Блок электропитания и управления комплексом ТСЗИ [Электронный ресурс]. – URL : http://deep-electronics.ru/catalog/tekhnicheskie-sredstva-zashchity-informatsii/zashchita-informatsii-ot-utechki-po-tekhnicheskim-kanalam/po-akusticheskomu-kanalu/sonata-ip3-isp-305-307-308/ (дата обращения: 20.02.2020).

31. Средства акустической и вибрационной защиты акустической информации ООО «Анна» [Электронный ресурс]. – URL : http://www.npoanna.ru/#/cat/2 (дата обращения: 20.04.2021).

32. Хорев, А. А. Оценка возможностей средств акустической (речевой) разведки / А. А. Хорев // Специальная техника. – 2009. – № 4. – С. 49 – 63.

33. Хорев, А. А. Техническая защита информации. Т. 1: Технические каналы утечки информации / А. А. Хорев. – М. : Аналитика, 2008. – 436 с.

34. Хорев, А. А. Способ и алгоритм формирования речеподобной помехи / А. А. Хорев // Вестник Воронежского государственного университета. Сер. Системный анализ и информационные технологии. – Воронеж, 2017. – № 1. – С. 57 – 67.

35. Царегородцев, А. В. Методы и средства защиты информации в государственном управлении / А. В. Царегородцев, М. М. Тараскин. – М. : Проспект, 2017. – 205 с.

36. Юдин, Е. Я. Защита от шума : справочник проектировщика / Е. Я. Юдин. – М. : Стройиздат, 1974. – 134 с.

37. Яковлев, В. А. Защита информации на основе кодового зашумления. Ч. 1: Теория кодового зашумления / В. А. Яковлев. – СПб. : Военная академия связи им. С. М. Буденного, 1993. – 246 с.

38. Model of a speech-like interference generator for speech information protection / V. V. Alekseev, A. V. Yakovlev, M. V. Moiseeva, A. A. Tikhomirova // IOP Conf. Series : Materials Science and Engineering. – 2021. – Vol. 537. – P. 062043.

СОДЕРЖАНИЕ