МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по выполнению практических работ
по дисциплине
ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки	10.03.01 Информационная безопасность
Направленность (профиль)	Комплексная защита объектов информатизации
Квалификация выпускника	Бакалавр
Форма обучения	Очная
Учебный план	2020 г.

Пятигорск 2020 г.

Введение

Дисциплина «Техническая защита информации» относится к вариативной части блока 1 Б.28. Ее освоение происходит в 5 и 6 семестрах ОП ВО подготовки бакалавра направления 10.03.01 «Информационная безопасность». Для изучения данной дисциплины необходимы знания, навыки и компетенции, полученные при изучении дисциплины «Основы информационной безопасности». Полученные в ходе изучения данной дисциплины знания, навыки и компетенции пригодятся при изучении дисциплины «Комплексная система защиты информации на предприятии», «Многоканальные цифровые системы передачи и средства их защиты».

Главной целью методических рекомендаций для студентов по организации самостоятельной работы по дисциплине «Техническая защита информации» является развитие умений и навыков, необходимых для практического применения знаний по технической защите информации при решении профессиональных задач. Данные методические рекомендации способствуют достижению этой цели.

В результате освоения содержания дисциплины «Техническая защита информации» студент должен знать: способы несанкционированного доступа к конфиденциальной информации на объекты информатизации; программно-аппаратные и технические средства защиты информации; современные концепции защиты объектов информации. Студент должен владеть: навыками проведения технико-экономического обоснования проектных решений; навыками работы в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации; уметь: применять комплексный подход к обеспечению информационной безопасности объекта защиты; формировать предложения по оптимизации комплекса технических средств, применяемых в процессе защищаемого объекта и его информационных составляющих; проводить технические расчёты основных тактико-технических характеристик проектируемых систем охраны объектов.

Методические рекомендации для студентов по организации самостоятельной работы по дисциплине «Техническая защита информации» составлены в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования, рабочим учебным планом и рабочей программой дисциплины «Техническая защита информации».

СОДЕРЖАНИЕ

Практическое занятие № 1.

Тема: Разработка пространственной модели объекта информационной защиты. Описание угроз утечки информации по техническим каналам.

Цель: Изучить основы организации технической защиты информации на объектах информатизации и в выделенных помещениях, ознакомиться с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники, ознакомиться с техническими каналами утечки акустической (речевой) информации.

В результате выполнения практического занятия студент должен **знать**: угрозы информационной безопасности объектов информатизации; современные концепции защиты объектов информации. Студент должен **уметь**: проводить анализ исходных данных для проектирования систем защиты выделенных помещений; проводить технические расчёты основных тактико-технических характеристик проектируемых систем защиты выделенных помещений.

Предлагаемые студенту задания позволяют проверить компетенции ПК-1, ПК-4, ПК-5, К-12, ПК-13.

Актуальность темы: Работа систем защиты выделенных помещений в значительной мере определяется качеством оценки защищённости информации от утечки по техническим каналам, выбора и применения средств защиты. Применяемые в системах средства защиты призваны обеспечить эффективную защиту конфиденциальной информации.

Теоретическая часть:

Пространственная модель представляет собой подробное описание выделенного помещения, инженерных конструкций, коммуникаций и средств связи, характеристику и основные параметры электронных устройств, находящихся на объекте защиты, а также технических средств безопасности. Пространственная модель объекта – это модель пространственных зон с указанным месторасположением источников защищаемой информации.

Предусматривается пространственная характеристика по таким элементам как:

- Этаж, граница КЗ на ситуационном плане
- Соседние помещения, название, толщина стен
- Помещение над потолком, название, толщина перекрытий
- Помещение под полом, название, толщина перекрытий
- Количество окон, наличие штор на окнах
- Двери (кол-во, одинарные, двойные)
- Вентиляционные отверстия, места размещения, размеры отверстий
- Батареи отопления, типы, куда выходят трубы
- Цепи электропитания
- Телефон
- Электрические часы
- Бытовые радиосредства
- Бытовые электроприборы
- ПЭВМ
- Технические средства охраны
- Телевизионные средства наблюдения

- Пожарная сигнализация
- Другие средства

Описание элементов сопровождаются функциональной, конструктивной и технической характеристиками.

Для объекта защиты, назначенного преподавателем из приложения В, разработать пространственную модель объекта информационной защиты – табличное описание пространственных зон с указанием месторасположения источников защищаемой информации. При составлении модели использовать в качестве образца таблицу П.1, приложения А.

Описание угроз утечки информации по техническим каналам.

Рассматривается актуальность угроз утечки информации по техническим каналам. Источником угрозы безопасности информации является ОСВТ и физические явления, являющиеся причиной возникновения угрозы безопасности информации. За счет реализации технических каналов утечки информации возникают следующие угрозы безопасности:

- угроза утечки акустической (речевой) информации;
- угроза утечки видовой информации;
- угроза утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН);
- угроза утечки акустической информации по каналу АЭП.

Устранение угрозы утечки видовой информации возможно без применения технических средств защиты, поэтому детально разберем остальные угрозы. Количественные результаты оценки утечки информации по каналам, полученные при проведении специальных исследований, приведены в приложении А, таблицы П.2, П.3. Измерения напряжения в канале НЧ АЭП проводились на контактах всех устройств ВТСС в рабочем режиме и в режиме холостого хода. При проведении измерений было выявлено превышение показателей противодействия относительно нормированных показателей.

Предоставленные результаты специальных исследований служат исходными данными для разработки технического решения по обеспечению защиты конфиденциальной информации от утечки по техническим каналам.

Вопросы:

1. Построить пространственную модель выделенного помещения.
2. Описать угрозы утечки информации по техническим каналам.
3. Оформить результаты специальных исследований.

Список литературы, рекомендуемый к использованию по данной теме:

Перечень основной литературы:

1. Технические средства и методы защиты информации: учеб.пособие / под ред. А.П. Зайцева, А.А. Шелупанова. – [4-е изд., испр. и доп.]. – Москва : Горячая линия-Телеком, 2016. – 616 с.
2. Хорев А.А. Техническая защита информации: учеб. пособие для студентов ву-зов. В 3-х т. М.: НПЦ «Аналитика», 2017.

Перечень дополнительной литературы:

1. Разработка системы технической защиты информации: учебное пособие [Элек-тронный ресурс]/ В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. – 2-е изд., стер. – М.: Флинта, 2014. – URL:http://biblioclub.ru/index.php?page=book&id=93349.

2. Чипига, А.Ф. Информационная безопасность автоматизированных систем: учеб. пособие/ А. Ф. Чипига- М.: Гелиос АРВ, 2013.

Приложение А.

Таблица П.1. Пространственная модель защищаемого объекта

№ эл.	Наименование элемента пространственной зоны	Характеристики пространственной зоны
1	2	5
1.	Название выделенного помещения,	№ 1*
2.	Класс защищённости АС (на основании требований РД Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации", 1992г.)	Класс 1Г
3.	Этаж	1
4.	Контролируемая зона	Контролируемая зона (КЗ) объекта проходит по ограждающим конструкциям, потолку и полу помещения для переговоров
5.	Количество окон, наличие штор, количество фрамуг, размеры (мм)	2 окна, на всех окнах жалюзи; окна выходят на проезжую часть улицы со зданиями
6.	Двери: количество и из какоко материала изготовлены	1 дверь; стальная, усиленная
7.	Стены здания: толщина, материал	Перегородки: кирпичная кладка 65 см, облицовка. Перекрытие: монолитное
8.	Вентиляционные отверстия: места размещения, размеры	15х20см
9.	Система отопления	1 чугунная батарея вдоль окон, трубы стальные. Все трубы выведены к теплоцентрали.
№ эл.	**Наименование элемента пространственной зоны**	**Характеристики пространственной зоны**
1	2	5
	Цепи электропитания	Количество вводов линий 220В: две линии. Цепь электропитания подключена к городской сети напряжением 220 В, частотой 50 Гц.

10.		Электро-щитовая находится в глубине здания около служебного помещения. К цепи электропитания подключены все кабинеты и помещения. Всего 2 розетки. Критические узлы подключены к источникам бесперебойного питания.
11.	Телефон	1 шт. 2-х жильный кабель (RJ – 11) от мини-АТС
12.	Радиотрансляция	Отсутствует
13.	Электрические часы	Отсутствует
14.	Бытовые радиосредства, теле-, аудио- и видеотехника	Согласно индивидуального задания
15.	Система охраны	Имеется, автономная
16.	СКУД	Имеется, автономная
17.	Система пожарной сигнализации	Имеется
18.	Компьютерная система	1 ноутбук и 1 принтер имеют соединение через коммутатор HUB, размещенный в коридоре второго этажа; имеется соединение с сетью Интернет
* - здесь и далее поля, выделенные красным, для заполнения согласно индивидуального задания		

Таблица П.2. Результаты виброакустических исследований без САЗ

№	**Место исследования**	**Отношение Сигнал/шум**	**Разборчивость речи W**
Акустика			
1	Дверь	+	+
2	Вент. канал	+	-
Виброакустика			
3	Стены	+	+
4	Окно (рамы/стёкла)	+	+
5	Перекрытие нижнего этажа	+	-
6	Перекрытие верхнего этажа	+	-
7	Система отопления	+	-

Таблица П.3. Выписка из Протокола специальных исследований основного технического средства (монитор) по ПЭМИН

R2воз, м	**r1, м**	**r1', м**
75	3,9	0,9

где:

R2 - минимальный радиус зоны вокруг технического средства обработки информации (объекта), в пределах которого возможен перехват побочных электромагнитных излучений и последующее восстановление содержащейся в них информации.

Зона 1 (r1) - минимальный радиус зоны вокруг ОТСС, в пределах которого уровень наведенного от ОТСС информативного сигнала в сосредоточенных антеннах* превышает допустимое (нормированное) значение.

Зона 1' (r1') - минимальный радиус зоны вокруг ОТСС, в пределах которого уровень наведенного от ОТСС информативного сигнала в распределенных антеннах** превышает допустимое (нормированное) значение.

Примечание:

* - Сосредоточенная случайная антенна представляет собой компактное техническое средство (например, телефонный аппарат, громкоговоритель радиотрансляционной сети, датчик пожарной сигнализации и т.д.), подключенное к линии, выходящей за пределы контролируемой зоны.

** - К распределенным случайным антеннам относятся случайные антенны с распределенными параметрами: кабели, провода, металлические трубы и другие токопроводящие коммуникации, выходящие за пределы контролируемой зоны.

Практическое занятие № 2.

Тема: Разработка системы активной защиты речевой информации по акустическому и виброакустическому каналу.

Цель: Изучить основы организации технической защиты информации на объектах информатизации и в выделенных помещениях, ознакомиться с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники, ознакомиться с техническими каналами утечки акустической (речевой) информации.

В результате выполнения практического занятия студент должен **знать**: методику расстановки средств активной защиты речевой информации от утечки по акустическому, виброакустическому каналам; современные концепции защиты объектов информации. Студент должен **уметь**: проводить анализ исходных данных для проектирования систем защиты выделенных помещений; проводить технические расчёты основных тактико-технических характеристик проектируемых систем защиты выделенных помещений.

Предлагаемые студенту задания позволяют проверить компетенции ПК-1, ПК-4, ПК-5, К-12, ПК-13.

Актуальность темы: Работа систем защиты выделенных помещений в значительной мере определяется качеством оценки защищённости информации от утечки по техническим каналам, выбора и применения средств защиты. Применяемые в системах средства защиты призваны обеспечить эффективную защиту конфиденциальной информации.

Теоретическая часть:

Система виброакустической защиты (СВАЗ)

Проектирование системы защиты акустической речевой информации, как и любой другой, должно опираться на исходные данные. В рассматриваемой задаче проектирования системы защиты информации от утечки по виброакустическим каналам такими изысканиями являются предварительное экспертное обследование помещения.

Исходя из характеристик материала, геометрических размеров ограждающей конструкции и известного среднего радиуса действия того или иного типа излучателей, для каждой ограждающей конструкции можно определить необходимое ориентировочное количество каждого типа и моделей излучателей для создания эффективного зашумления. В итоге ориентировочно может быть определено общее число каждого типа излучателей, требуемое для зашумления всех ограждающих конструкций, коммуникаций и прилегающих пространств помещения в целом. Исходя из этого количества, могут быть сформулированы требования к количеству независимых каналов и нагрузочной способности базового блока СВАЗ, т.е. определена ориентировочная конфигурация СВАЗ в целом, включающая:

- тип и модель базового блока;
- тип излучателей (пассивные излучатели или генераторы-излучатели);
- общее число акустических излучателей;
- общее число вибрационных легких излучателей;
- общее число вибрационных тяжелых излучателей.

В качестве средства активной защиты информации от утечки по техническим каналам предлагается использовать Комплекс (3095) технических средств защиты информации (ТСЗИ) (СВАЗ, ПЭМИН, размыкатели), локальное проводное управление, производства ООО "Анна". Комплекс служит для защиты выделенного помещения и должен иметь возможность включения и выключения уполномоченным пользователем с помощью единого пульта управления, находящегося в выделенном помещении.

Схема комплекса представлена на рис.2.

Рисунок 2 - Схема комплекса "3095"

Состав комплекса представлен в Приложении Б, таблице П.4.

Методика расстановки САЗ

На основе имеющегося опыта большинство различных ситуаций, встречающихся при создании систем защиты информации от утечки по виброакустическим каналам, можно

свести к следующим типовым задачам создания вибрационных и акустических зашумляющих полей на различных конструкциях:
- вибрационное зашумление окна;
- акустическое зашумление пространства за окном.
- вибрационное зашумление массивных ограждающих конструкций (стена, межкомнатная перегородка, двери, люки и т.п.) и жестких архитектурных конструкций;
- вибрационное зашумление инженерных коммуникаций круглого сечения (труб);
- акустическое и вибрационное зашумление смежных замкнутых объемов (смежных помещений, входных тамбуров, воздуховодов систем вентиляции и кондиционирования и т.п.).

1 Акустическое зашумление

1) Очень эффективным решением для зашумления элементов окна является применение аудиогенераторов-излучателей «СА-4Б». Такое применение акустических излучателей возможно для окон, конструкция которых позволяет их размещать между рамами окна. Пример такого применения аудиоизлучателей представлен на рис. 4.

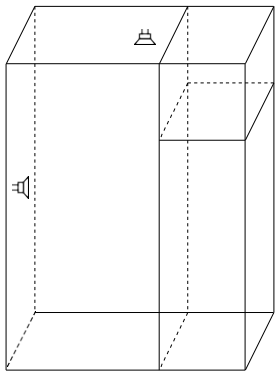

Рисунок 4 - Пример применения аудиоизлучателей для окна

Условные обозначения:

- Генераторы-акустоизлучатели "СА-4Б1"

Рисунок 5 - Генераторы-акустоизлучатели "СА-4Б1"

Суть такого решения заключается в следующем. Акустический шумовой сигнал, создаваемый аудиоизлучателями, распространяясь в замкнутом пространстве сравнительно небольшого объема, многократно отражается от конструкций окна. При этом он очень эффективно возбуждает в них вибрации, особенно в протяженных жестких конструкциях, которыми являются большие стекла. Дополнительно такое решение может использоваться в случаях, когда звукоизоляция окна не обеспечивает необходимого

ослабления акустического сигнала при его распространении за пределы помещения, и требуется создание акустической шумовой помехи в пространстве за окном.

2) Дверные проемы, в том числе и оборудованные тамбурами, также являются источниками повышенной опасности и в случае недостаточной звукоизоляции также нуждаются в применении активных методов защиты. Акустические излучатели систем зашумления в этом случае желательно располагать снаружи тамбура, вблизи дверной коробки со стороны смежного помещения. При таком размещении колонок системы зашумления (САЗ) «просачивающийся сигнал» имеет наименьшую величину, для его зашумления нужна минимальная мощность шума, как правило, уже не мешающая персоналу. А в защищаемое помещение шум вообще не проникает. Контроль выполнения норм защиты информации в этом случае, проводится вблизи внешней поверхности внешней (по отношению к защищаемому помещению) двери тамбура.

Рисунок 6 – Размещение акустического излучателя у дверного проёма с одним створом.

При отсутствии в конструкции двери порога независимо от площади проёма рекомендуется установка не менее 4-х излучателей на уровнях 1,5 и 0,5 м от уровня пола (см. рисунок 7). Акустические излучатели могут размещаться как открыто, на плоскости ограждающей конструкции, так и полускрыто, в стенных нишах, закрытых декоративными решётками и затянутых радиотканью.

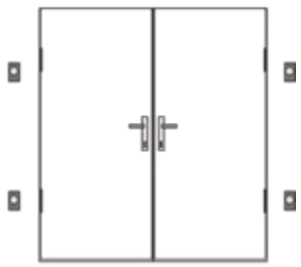

Рисунок 7 - Вариант размещения акустических излучателей для защиты дверного проёма с двумя створами.

3) При защите систем вентиляции наилучшим местом размещения колонки системы активной защиты является короб (канал) вентиляции на расстоянии не менее 1,5 м в

глубину от плоскости его выхода в ВП. При таком размещении шум колонки не слышен в выделенном помещении, а защищенность достигается при невысоких уровнях громкости колонки.

Очень эффективным является размещение колонки в отдельном кожухе,

«пристыкованном» к коробу вентиляции в том месте, где от него выполнен отвод в защищаемое выделенное помещение. Естественно, в стенке короба, там, где закреплен кожух с колонкой, должны быть проделаны отверстия для прохода звука. При таком размещении колонку легко извлечь для ремонта, очистки от пыли, она не уменьшает своими габаритами сечение вентиляционного канала и не мешает нормальному воздухообмену.

Такое размещение обеспечивает защищённость и не мешает воздухообмену (рисунок 8).

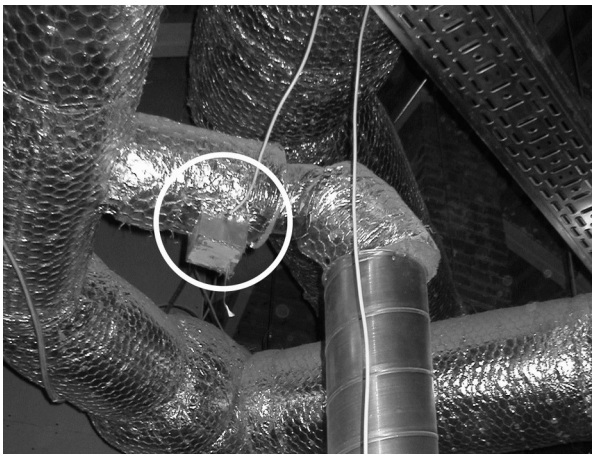

Рисунок 8 – Размещение акустического излучателя вне воздуховода

4) акустическое и вибрационное зашумление смежных замкнутых объемов. Для этих целей ЗАО «АННА» предлагаются Генераторы-акустоизлучатели "СА-4Б".

Рисунок 9 - Генераторы-акустоизлучатели "СА-4Б"

Вибрационное зашумление

1) Вибрационное зашумление массивных ограждающих конструкций и жестких архитектурных конструкций. Такие элементы, как правило, сделаны из материалов, характеризующихся высокими плотностью, массой и модулем упругости. Поэтому в данной задаче предпочтительным является применение тяжелых генераторов-вибровозбудителей "СВ-4Б1".

2) Особым случаем применения тяжелых генераторов-вибровозбудителей "СВ-4Б1" является зашумление различных инженерных коммуникаций круглого сечения.

3) Одной из наиболее часто решаемых задач является задача вибрационного зашумления элементов остекления окна. Для решения этой задачи ООО «АННА» предлагает

применение легких генераторов-вибровозбудителей "СВ-4Б". Легкие генераторы-вибровозбудители "СВ-4Б" обычно применяют на окнах, конструкция которых позволяет наклеивать их прямо на стекло, как показано на рис. 10.

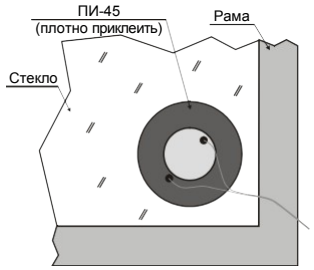

Рисунок 10 – Крепление генераторов-вибровозбудителей "СВ-4Б" на стекло

Определение мест установки, типов и количества излучателей.

а) Акустика. Ориентировочное количество аудиогенераторов-излучателей "СА-4Б"/"СА-4Б1" может быть определено исходя из следующих норм:

1) один "СА-4Б" на каждый вентиляционный канал,

2) один "СА-4Б1" на дверной тамбур или входную дверь;

2) один "СА-4Б" на каждые 8...12 м2 надпотолочного пространства или других пустот.

б) Виброакустика. Для оценки необходимого количества виброгенераторов-излучателей "СВ-4Б"/ "СВ-4Б1" необходимо исходить из следующих норм:

1) при установке на стену – один "СВ-4Б1" на каждые 15...25 м^2 площади поверхности стены (при этом излучатели должны устанавливаться на уровне половины высоты стены при высоте стены менее 5 м или на высоте от пола помещения не менее 2.5 м при высоте стены 5 м и более, далее – через каждые 5 м высоты);

2) при установке на потолок (пол) – один "СВ-4Б1" на каждые 15...25 м2 плиты перекрытия;

3) при установке на оконный переплет - один "СВ-4Б1" на каждое окно или раздельную раму;

4) при установке на дверь – один "СВ-4Б1" на каждое полотно двери;

5) при установке на трубы систем водо-, тепло- или газоснабжения – один "СВ-4Б1" на каждую отдельную трубу перед выходом из помещения.

6) Ориентировочное количество "СВ-4Б" определяется из расчета: один "СВ-4Б" на каждый элемент остекления.

Вопросы:

1. Подобрать средства активной защиты. Описать состав комплекса защиты.
2. Нарисовать схему расстановки средств защиты при акустическом зашумлении.
3. Нарисовать схему расстановки средств защиты при вибрационном зашумлении.

Список литературы, рекомендуемый к использованию по данной теме:

Перечень основной литературы:

1. Технические средства и методы защиты информации: учеб.пособие / под ред. А.П. Зайцева, А.А. Шелупанова. – [4-е изд., испр. и доп.]. – Москва : Горячая линия-Телеком, 2016. – 616 с.

2. Хорев А.А. Техническая защита информации: учеб. пособие для студентов ву-зов. В 3-х т. М.: НПЦ «Аналитика», 2017.

Перечень дополнительной литературы:

1. Разработка системы технической защиты информации: учебное пособие [Элек-тронный ресурс]/ В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. – 2-е изд., стер. – М.: Флинта, 2014. – URL:http://biblioclub.ru/index.php?page=book&id=93349.
2. Чипига, А.Ф. Информационная безопасность автоматизированных систем: учеб. пособие/ А. Ф. Чипига- М.: Гелиос АРВ, 2013.

Приложение Б.

Таблица П.4. Состав комплекса.

Обозначение на схеме	**Полное наименование (комментарии)**	**ID**
	электропитание и управление	
Блок питания и управления	"Соната-ИП4.1" ("Соната-ИП4.3"), универсальный блок питания и управления	309 (312)
	Система виброакустической защиты (СВАЗ)	
СА-4Б	"СА-4Б". Генератор-акустоизлучатель	956
СА-4Б1	"СА-4Б1". Генератор-акустоизлучатель большой мощности	955
СВ-4Б	"СВ-4Б". Генератор-вибровозбудитель	938
СВ-4Б1	"СВ-4Б1". Генератор-вибровозбудитель пониженной шумности	937
	Система защиты от утечек за счет побочных электромагнитных излучений и наводок	
	(ПЭМИН)	
Соната-Р3.1*)	"Соната-Р3.1 Средство активной защиты информации от утечек за счет ПЭМИН (кл2)	232
Соната-Р3*)	"Соната-Р3" Средство активной защиты информации от утечек за счет ПЭМИН (кл1)	233
Соната-РС3	"Соната-РС3" Средство активной защиты информации от утечки за счет наводок информативного сигнала на сети электропитания и заземления	240
	Система защиты технических средств связи (ТСС) от утечек за счет электроакустических преобразований	
Соната-ВК4.1	Размыкатель телефонной линии "Соната-ВК4.1"	975
Соната-ВК4.2	Размыкатель линий оповещения и сигнализации "Соната- ВК4.2"	976
Соната-ВК4.3	Размыкатель линий компьютерной сети "Соната-ВК4.3"	977
	Блоки сопряжения с внешними устройствами**)	
Соната-ДУ4.1	Соната-СК4.1. Силовой коммутатор нагрузок 220 В большой мощности, обратная связь, сухой контакт	530

Соната-ДУ4.2	"Соната-СК4.2", адаптер электропривода (окон), сухой контакт	531
	Устройство дистанционного управления	
Проводной пульт управления	"Соната-ДУ4.1" ("Соната-ДУ4.3"), пульт управления комплексом ТСЗИ	523 (528)

*) Выбор устройства активной защиты информатизации от утечки каналам ПЭМИН Соната-Р3 или Соната-Р3.1 зависит от требований к защите помещения (класс 1 или класс 2).

Практическое занятие № 3.

Тема: Разработка системы защиты от утечек за счет побочных электромагнитных излучений и наводок.

Цель: Изучить основы организации технической защиты информации на объектах информатизации и в выделенных помещениях, ознакомиться с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники, ознакомиться с техническими каналами утечки акустической (речевой) информации.

В результате выполнения практического занятия студент должен **знать**: угрозы информационной безопасности объектов информатизации; современные концепции защиты объектов информации. Студент должен **уметь**: проводить анализ исходных данных для проектирования систем защиты выделенных помещений; проводить технические расчёты основных тактико-технических характеристик проектируемых систем защиты выделенных помещений.

Предлагаемые студенту задания позволяют проверить компетенции ПК-1, ПК-4, ПК-5, К-12, ПК-13.

Актуальность темы: Работа систем защиты выделенных помещений в значительной мере определяется качеством оценки защищённости информации от утечки по техническим каналам, выбора и применения средств защиты. Применяемые в системах средства защиты призваны обеспечить эффективную защиту конфиденциальной информации.

Теоретическая часть:

Естественные каналы утечки информации образуются за счёт побочных электромагнитных излучений, возникающих при обработке информации СВТ (электромагнитные каналы утечки информации), а также вследствие наводок информативных сигналов в линиях электропитания и заземления СВТ, соединительных линиях ВТСС и посторонних проводниках (электрические каналы утечки информации).

В **электромагнитных каналах утечки информации** носителем информации являются электромагнитные излучения (ЭМИ), возникающие при обработке информации техническими средствами. Основными причинами возникновения электромагнитных каналов утечки информации в ТСОИ являются побочные электромагнитные излучения, возникающие вследствие протекания информативных сигналов по элементам ТСОИ.

Причинами возникновения **электрических каналов утечки информации** являются наводки информативных сигналов (под которыми понимаются токи и напряжения в токопроводящих элементах), вызванные побочными электромагнитными излучениями, ёмкостными и индуктивными связями.

Наводки информативных сигналов могут возникнуть:

- в линиях электропитания ТСОИ;
- в линиях электропитания и соединительных линиях ВТСС;
- в цепях заземления ТСОИ и ВТСС;

- в посторонних проводниках (металлических трубах систем отопления, водоснабжения, металлоконструкциях и т.д.).

Основными источниками возникновения ПЭМИ при работе СВТ являются:

- Процессор, шина данных процессора и цепи питания.
- Контроллеры и мост чипсета.
- Модули памяти и шина данных.
- Инверторы питания перечисленных выше устройств.
- HDD и шины IDE (ATA) и SATA.
- CD и шина IDE (ATA).
- Видеокарта и шина AGP или E-PCI.
- COM порт и внешние подключения по нему.
- LTP порт и внешние подключения по нему.
- USB порт.
- VGA и другие виды портов, предназначенные для подключения мониторов.
- Беспроводные сетевые адаптеры IEEE 802 для локальных сетей.

Рис 3.1 Основные источники возникновения ПЭМИ при работе СВТ

Понятие **Электромагнитная наводка.** Электромагнитная наводка – передача (индуцирование) электрических сигналов из одного устройства (цепи) в другое, непредусмотренная схемными или конструктивными решениями и возникающая за счет паразитных электромагнитных связей. Электромагнитные наводки могут приводить к утечке информации по токопроводящим коммуникациям, имеющим выход за пределы контролируемой зоны.

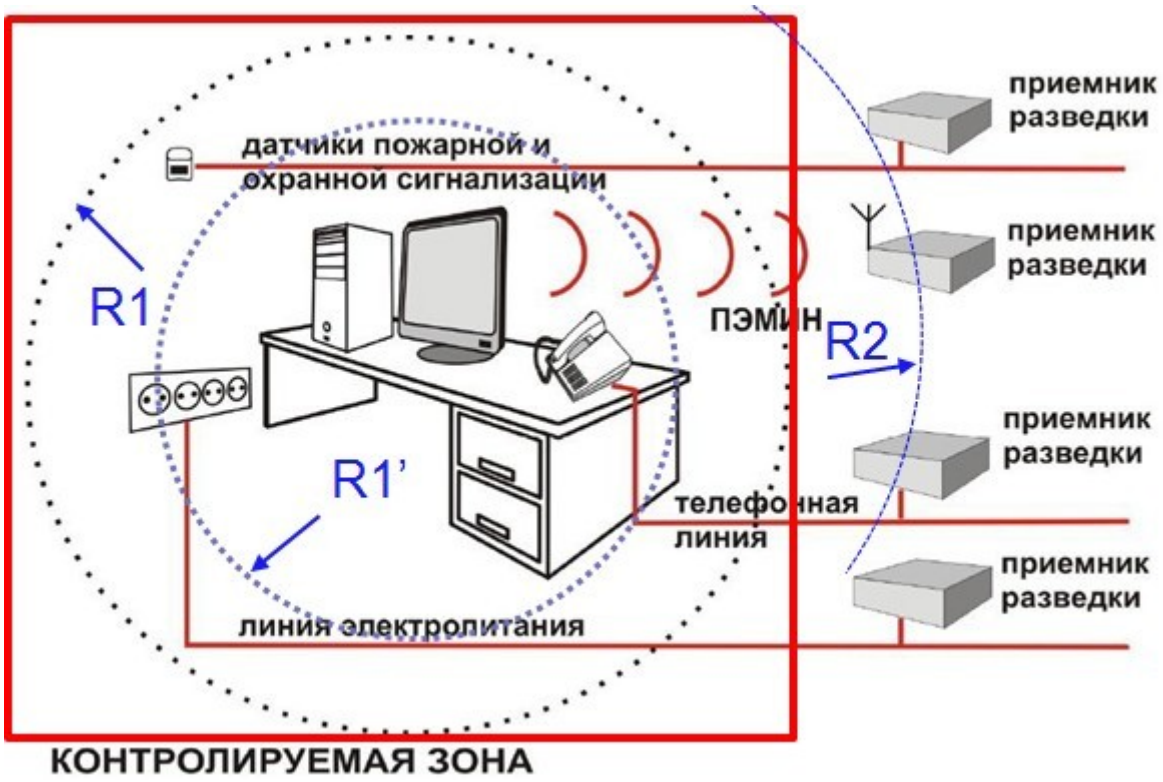

Рис 3.2 Радиусы опасных зон для перехвата информативных сигналов

В зависимости от физических причин возникновения наводки информативных сигналов можно разделить на:

- наводки информативных сигналов в электрических цепях ТСОИ, вызванные информативными ПЭМИ ТСОИ;
- наводки информативных сигналов в соединительных линиях ВТСС и посторонних проводниках, вызванные информативными ПЭМИ ТСОИ;
- наводки информативных сигналов в электрических цепях ТСОИ, вызванные внутренними ёмкостными и индуктивными связями (“просачивание” информативных сигналов в цепи электропитания через блоки питания ТСОИ);
- наводки информативных сигналов в цепях заземления ТСОИ, вызванные информативными ПЭМИ ТСОИ, а также гальванической связью схемной (рабочей) земли и блоков ТСОИ.

Отсюда:

- **r1** - минимальный радиус зоны для устройства ВТСС, линии которых имеют выход за границы контролируемой зоны.
- **r1'** - минимальный радиус зоны для линий и кабелей ВТСС, имеющие выход за границы контролируемой зоны.

Система защиты от утечек за счет побочных электромагнитных излучений и наводок (ПЭМИН). Реализация пассивных методов защиты, основанных на применении экранирования и фильтрации, приводит к ослаблению уровней побочных электромагнитных излучений и наводок (опасных сигналов) ТСПИ и тем самым к уменьшению отношения опасный сигнал/шум (с/ш), рисунок 11. Однако в ряде случаев, несмотря на применение пассивных методов защиты, на границе контролируемой зоны отношение с/ш превышает допустимое значение. В этом случае применяются активные

меры защиты, основанные на создании помех средствам разведки, что также приводит к уменьшению отношения с/ш.

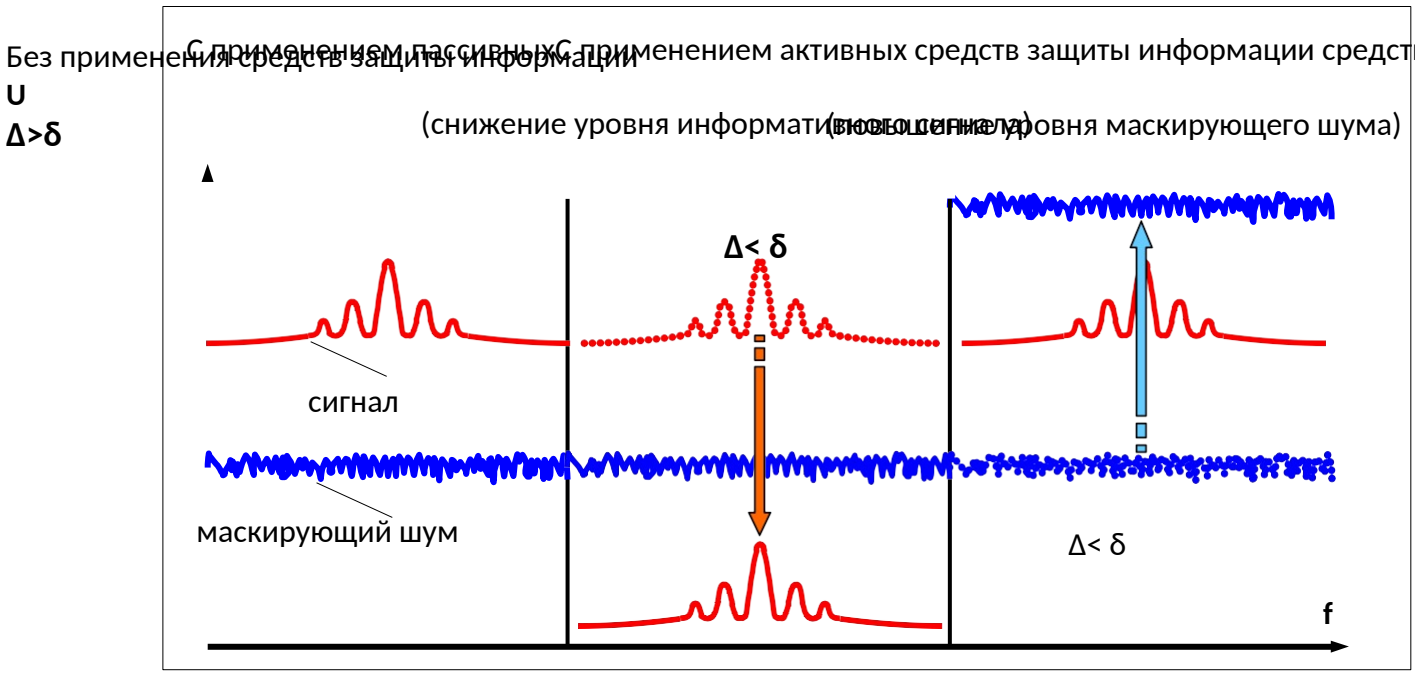

Рисунок 3.3 - Физические основы пассивных и активных методов защиты информации

1. Для исключения перехвата побочных электромагнитных излучений по электромагнитному каналу используется **пространственное зашумление**, схема представлена на рисунке.

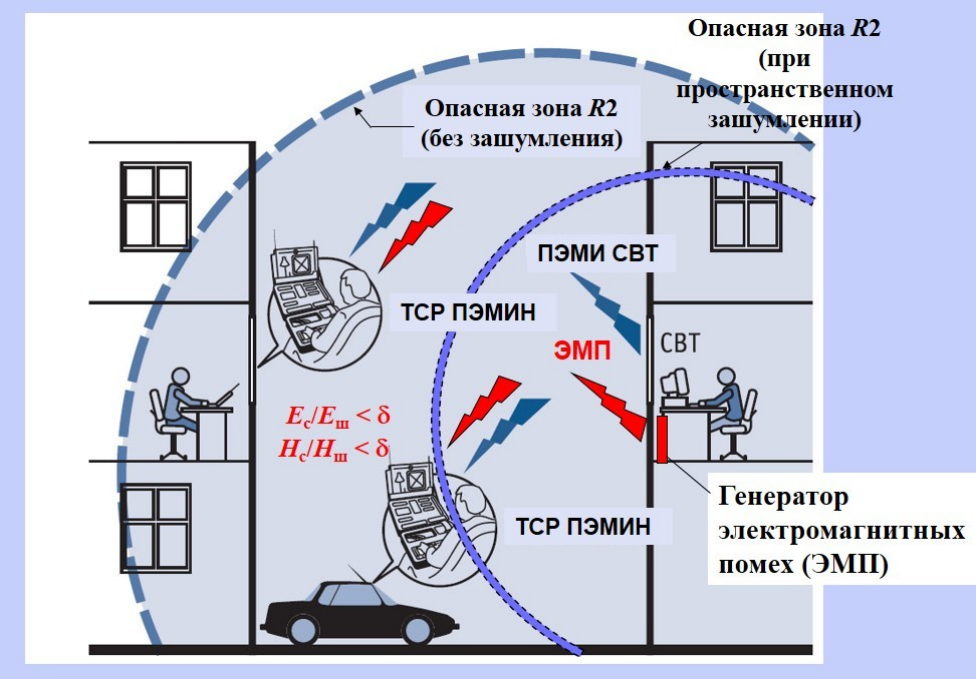

Рис 3.4– схема пространственного электромагнитного зашумления

К системе пространственного зашумления, применяемой для создания маскирующих электромагнитных помех, предъявляются следующие требования:

• система должна создавать электромагнитные помехи в диапазоне частот возможных побочных электромагнитных излучений ТСПИ;

• создаваемые помехи не должны иметь регулярной структуры, генерируемый шум должен иметь нормальное распределение плотности вероятности мгновенных значений амплитуд компонентов E (H, U) по отношению к нормальному (Гауссовскому) шуму не ниже заданных;

• уровень создаваемых помех (как по электрической, так и по магнитной составляющей поля) должен обеспечить отношение с/ш на границе контролируемой зоны меньше допустимого значения во всем диапазоне частот возможных побочных электромагнитных излучений ТСПИ;

• система должна создавать помехи как с горизонтальной, так и с вертикальной поляризацией (поэтому выбору антенн для генераторов помех уделяется особое внимание).

В настоящее время в основном применяются системы пространственного зашумления, использующие помехи типа "белый шум", то есть излучающие широкополосный шумовой сигнал (как правило, с равномерно распределенным энергетическим спектром во всем рабочем диапазоне частот), существенно превышающий уровни побочных электромагнитных излучений. Такие системы применяются для защиты широкого класса технических средств: электронно-вычислительной техники, систем звукоусиления и звукового сопровождения, систем внутреннего телевидения и т.д.

2. Защита объектов ВТСС от утечки информации, возникающей за счет наводок побочных электромагнитных излучений, достигается: установкой помехоподавляющих фильтров в цепях электропитания ТСПИ, диэлектрических вставок в инженерные коммуникации и экраны кабелей электропитания, а также использованием систем **линейного электромагнитного зашумления.**

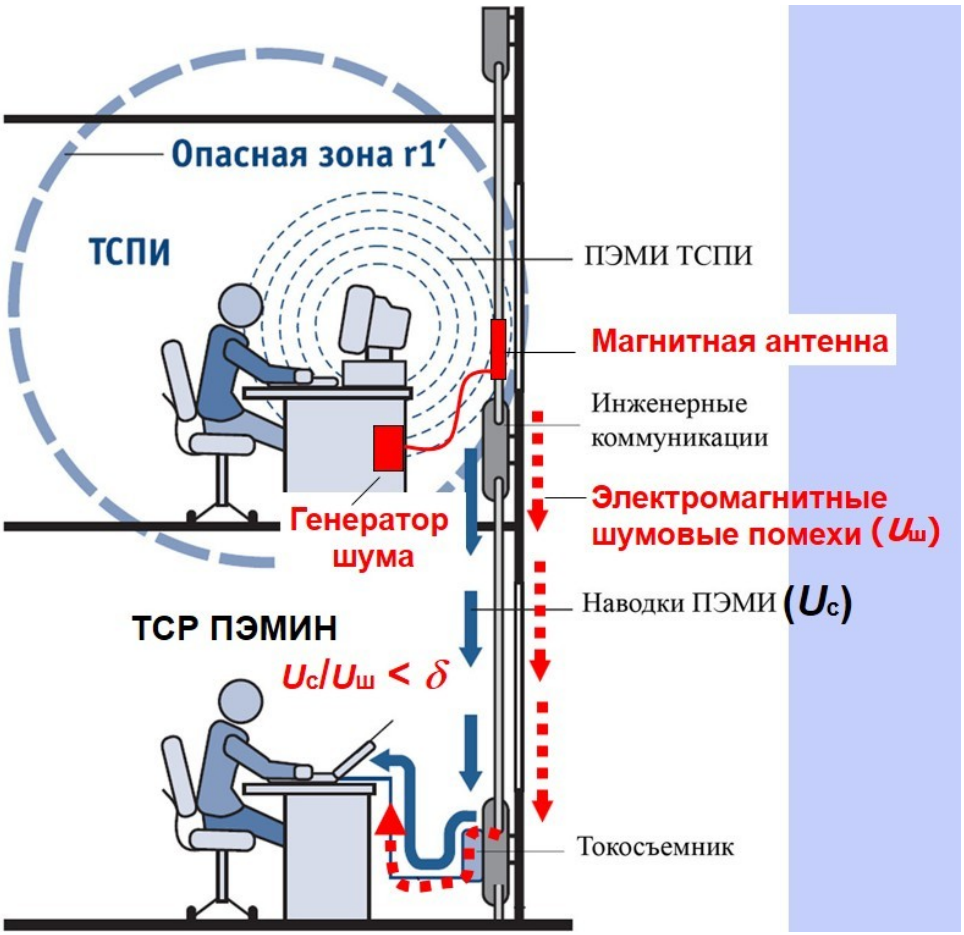

Рис 3.5 – Схема создания шумовых помех в системе отопления

Генератор шума «ГШ-1000У» предназначен для маскировки побочных информативных электромагнитных излучений и наводок персональных компьютеров, компьютерных сетей и комплексов в диапазоне частот 0,1-1800 МГц путем формирования и излучения в окружающее пространство маскирующего электромагнитного поля шума. Внешний вид устройства представлен на рисунке 3.6.

Рисунок 3.6 – внешний вид генератора шума ГШ-1000У

Дополнительно имеет 4 независимых коаксиальных выхода некоррелированного напряжения шума, к которым можно подключать:

- устройства ввода маскирующего напряжения шума (например, ответвитель «Дух») в сети электропитания, заземления, инженерные коммуникации и т.д.;
- дополнительные выносные антенны.

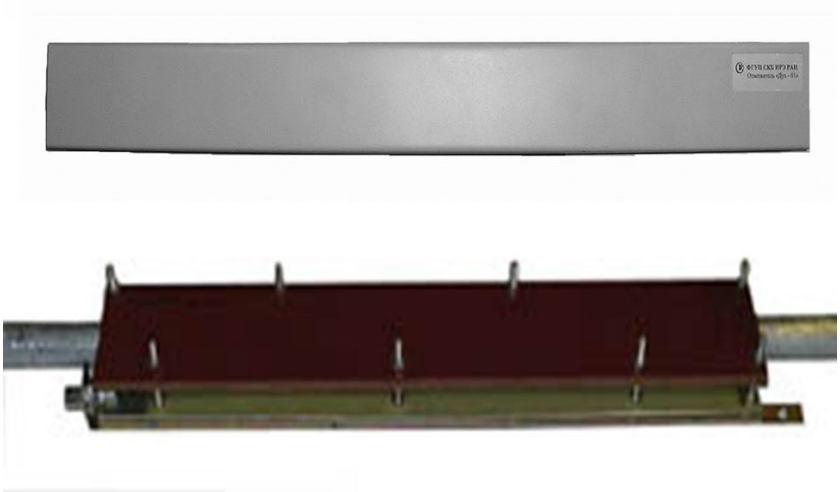

Рис 3.7 Внешний вид и способ крепления ответвителя «Дух»

Средство активной защиты информации "Соната-Р3.1" предназначено для защиты информации от утечки за счет побочных электромагнитных излучений и наводок на линии электропитания и заземления, линии проводной связи и токоведущие проводные коммуникации. "Соната Р3.1" обеспечивает защиту путем излучения в окружающее пространство электромагнитное поля шума, а также инжекции шумовых токов в линии сети электропитания и заземления.

Изделие может быть включено в состав комплекса ТСЗИ. В этом случае управление его работой и контроль режима работы (исправности) будет осуществляться от пульта управления "Соната-ДУ4.1" в комплексе с блоком питания "Соната-ИП4.х" (Комплекс 3095).

 Соната-Р3.1	 Соната-Р3.1 с дополнительной

	антенной

Рисунок 3.8 – Внешний вид устройства "Соната-Р3.1"

Рисунок 3.9 – Внешний вид Пульта управления "Соната-ДУ 4.2"

Средство активной защиты информации от утечки за счет наводок информативного сигнала на цепи заземления и электропитания "Соната-РС3" (далее Изделие) предназначено для защиты информации, содержащей сведения, составляющие государственную тайну и иной информации с ограниченным доступом, обрабатываемой техническими средствами и системами, от утечки за счет наводок информативного сигнала на цепи заземления и электропитания и может устанавливаться в выделенных помещениях до 1 категории включительно.

Рисунок 3.10 – Внешний вид устройства «Соната-РС3» спереди и сзади

Особенности конструкции устройств позволяют получать эффективные и недорогие решения при оборудовании объекта вычислительной техники с большим количеством средств вычислительной техники (СВТ).

Вариант установки устройства «Соната-РС3» на объекте ВП с одним вводом линии 220В на рис. 3.11.

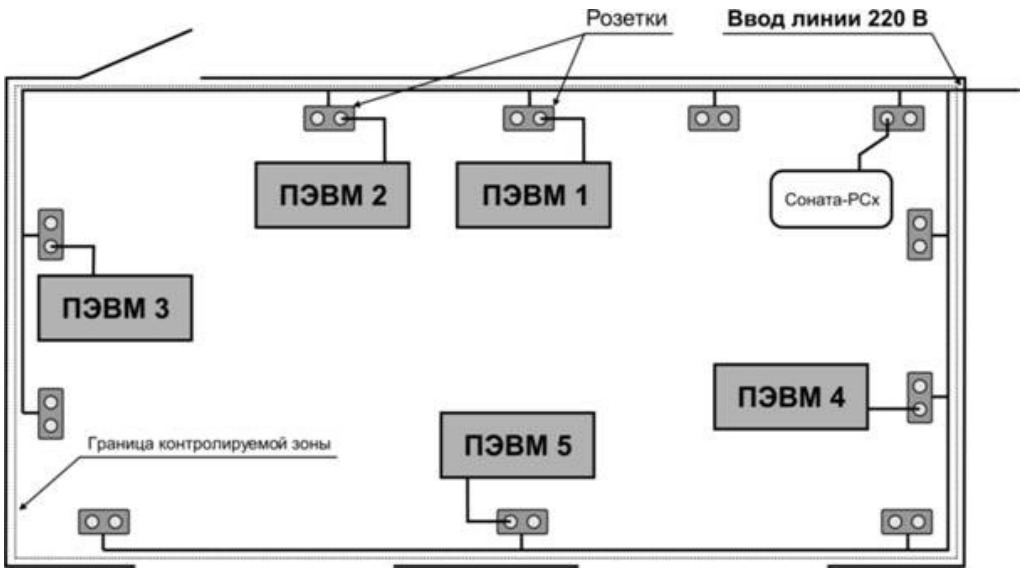

Рисунок 3.11 - Вариант установки устройства «Соната-РС3» на объекте ВП с одним вводом линии 220В

Вариант установки устройства «Соната-РС3» на объекте ВП с двумя вводами линий 220В на рис. 3.12.

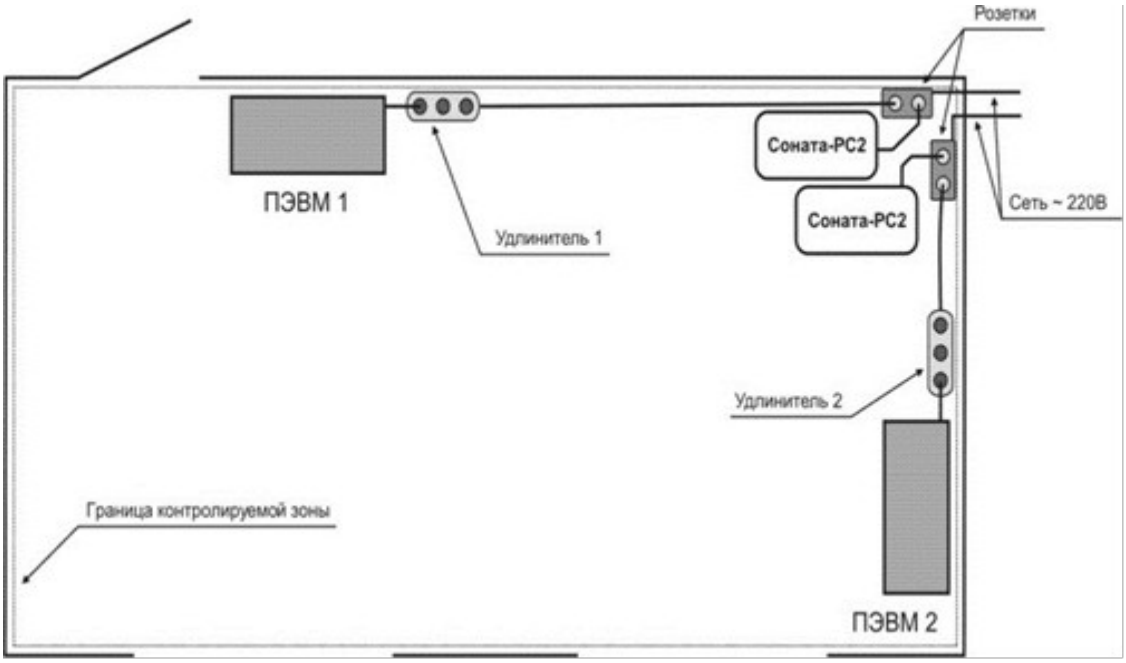

Рисунок 3.12 - Вариант установки устройств «Соната-РС3» на объекте ВП с двумя вводами линий 220В

Вопросы:

1. Описать системы защиты от утечек за счет побочных электромагнитных излучений и наводок (ПЭМИН).
2. Подобрать средства для пространственного зашумления.
3. Подобрать средства для линейного зашумления.
4. Нарисовать схему расстановки средств защиты от утечек за счет ПЭМИН.

Список литературы, рекомендуемый к использованию по данной теме:

Перечень основной литературы:

1. Технические средства и методы защиты информации: учеб.пособие / под ред. А.П. Зайцева, А.А. Шелупанова. – [4-е изд., испр. и доп.]. – Москва : Горячая линия-Телеком, 2016. – 616 с.
2. Хорев А.А. Техническая защита информации: учеб. пособие для студентов ву-зов. В 3-х т. М.: НПЦ «Аналитика», 2017.

Перечень дополнительной литературы:

1. Разработка системы технической защиты информации: учебное пособие [Элек-тронный ресурс]/ В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. – 2-е изд., стер. – М.: Флинта, 2014. – URL:http://biblioclub.ru/index.php?page=book&id=93349.
2. Чипига, А.Ф. Информационная безопасность автоматизированных систем: учеб. пособие/ А. Ф. Чипига- М.: Гелиос АРВ, 2013.

Практическое занятие № 4.

Тема: Разработка системы защиты технических средств связи (ТСС) от утечек за счет электроакустических преобразований.

Цель: Изучить основы организации технической защиты информации на объектах информатизации и в выделенных помещениях, ознакомиться с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники, ознакомиться с техническими каналами утечки акустической (речевой) информации.

В результате выполнения практического занятия студент должен **знать**: угрозы информационной безопасности объектов информатизации; современные концепции защиты объектов информации. Студент должен **уметь**: проводить анализ исходных данных для проектирования систем защиты выделенных помещений; проводить технические расчёты основных тактико-технических характеристик проектируемых систем защиты выделенных помещений.

Предлагаемые студенту задания позволяют проверить компетенции ПК-1, ПК-4, ПК-5, К-12, ПК-13.

Актуальность темы: Работа систем защиты выделенных помещений в значительной мере определяется качеством оценки защищённости информации от утечки по техническим каналам, выбора и применения средств защиты. Применяемые в системах средства защиты призваны обеспечить эффективную защиту конфиденциальной информации.

Теоретическая часть:

Проектирование системы защиты акустической речевой информации, как и любой другой, должно опираться на исходные данные.

На рисунке 1 показана схема расположения линий ВТСС со стороны окна. Измерения напряжения в канале НЧ АЭП проводились на контактах всех устройств ВТСС в рабочем режиме и в режиме холостого хода.

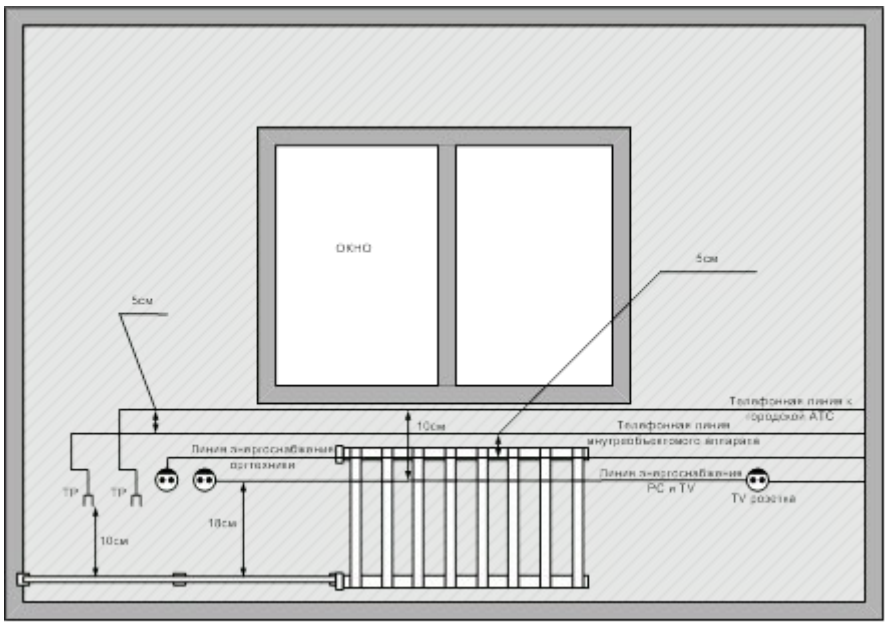

Рисунок 1 – Схема расположения линий ВТСС со стороны окна

При проведении измерений было выявлено превышение показателей противодействия относительно нормированных показателей.

Система защиты технических средств связи (ТСС) от утечек за счет электроакустических преобразований**.**

Технические меры сводятся к включению в линию связи специальных устройств локализации микрофонного эффекта. Размыкатели слаботочных линий “Соната-ВК4.1” предназначены для защиты информации от утечки за счет акустоэлектрических преобразований и ВЧ-навязывания по телефонным линиям, “Соната-ВК4.2” по соединительным линиям систем оповещения и сигнализации, а “Соната-ВК4.3” по линиям компьютерных сетей.

Рисунок 16 – Внешний вид устройства Соната-ВК4.2

Таблица 5. Основные технические характеристики размыкателей “Соната-ВКх”

Параметр	**Соната-ВК4.1**	**Соната-ВК4.2**	**Соната-ВК4.3**
Проводность линии	4 - х		8-ми
Параметры коммутируемой линии	Аналоговая телефонная линия	Коммутируемое напряжение/сила тока/мощность, не более – 125В/2А/30Вт(30В*А)	Кабельные линии (UTPи аналоги) компьютерной сети стандарта Ethernet10/100

Размыкатели "Соната-ВК4.1", "Соната-ВК4.2", "Соната-ВК4.3" могут применяться с блоком питания и управления "Соната-ИП4.х" совместно с пультом управления и в составе комплексов ТСЗИ.

Вопросы:

1. Описать систему защиты от утечек за счет АЭП.
2. Подобрать устройства локализации микрофонного эффекта.
3. Нарисовать схему расстановки средств защиты от утечек за счет АЭП.

Список литературы, рекомендуемый к использованию по данной теме:

Перечень основной литературы:

1. Технические средства и методы защиты информации: учеб.пособие / под ред. А.П. Зайцева, А.А. Шелупанова. – [4-е изд., испр. и доп.]. – Москва : Горячая линия-Телеком, 2016. – 616 с.

2. Хорев А.А. Техническая защита информации: учеб. пособие для студентов ву-зов. В 3-х т. М.: НПЦ «Аналитика», 2017.
Перечень дополнительной литературы:
1. Разработка системы технической защиты информации: учебное пособие [Элек-тронный ресурс]/ В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. – 2-е изд., стер. – М.: Флинта, 2014. – URL:http://biblioclub.ru/index.php?page=book&id=93349.
2. Чипига, А.Ф. Информационная безопасность автоматизированных систем: учеб. пособие/ А. Ф. Чипига- М.: Гелиос АРВ, 2013.

Практическое занятие № 5.

Тема: Расчет максимально возможного количества элементов комплекса ТСЗИ, подключаемых к блоку питания и управления, подбор кабеля.

Цель: Изучить основы организации технической защиты информации на объектах информатизации и в выделенных помещениях, ознакомиться с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники, ознакомиться с техническими каналами утечки акустической (речевой) информации.

В результате выполнения практического занятия студент должен **знать**: угрозы информационной безопасности объектов информатизации; современные концепции защиты объектов информации. Студент должен **уметь**: проводить анализ исходных данных для проектирования систем защиты выделенных помещений; проводить технические расчёты основных тактико-технических характеристик проектируемых систем защиты выделенных помещений.
Предлагаемые студенту задания позволяют проверить компетенции ПК-1, ПК-4, ПК-5, К-12, ПК-13.
Актуальность темы: Работа систем защиты выделенных помещений в значительной мере определяется качеством оценки защищённости информации от утечки по техническим каналам, выбора и применения средств защиты. Применяемые в системах средства защиты призваны обеспечить эффективную защиту конфиденциальной информации.
Теоретическая часть:
Расчет максимально возможного количества элементов комплекса ТСЗИ, подключаемых к изделиям "Соната-ИП4.х".
Блоки электропитания и управления "Соната-ИП4.1", "Соната-ИП4.2" и "Соната-ИП4.3" предназначены для:
1) электропитания и управления подключаемыми к выходу «Нагрузка» элементами системы активной акустической и вибрационной защиты акустической речевой информации "Соната-АВ" модель 4Б (Системы) в ходе ее эксплуатации;
2) управления подключаемыми к выходу «Нагрузка» средств активной защиты информации от утечки за счёт ПЭМИН ("Соната-Р3", "Соната-Р3.1", "Соната-РС3");
3) автоматический контроль исправности и режимов работы подключенных к нему устройств;
4) настройки (установки интегрального уровня, корректировки спектра и т.п.) изделий, перечисленных в п.1 и п.2, и считывания из них служебной информации (состояние счетчика наработки, код ошибки при отказе, индивидуальный адрес и т.п.), при инсталляции (проверке) комплекса технических средств защиты информации.

Для выполнения п.3 и п.4. изделия "Соната-ИП4.1", "Соната-ИП4.2" и "Соната-ИП4.3"необходимо подключить к управляющей ПЭВМ.

Рисунок 17 - Соната-ИП4.1. Вид спереди

Нормальная работа комплекса ТСЗИ во всех режимах будет гарантирована, если соблюдаются следующие условия:

1) суммарный максимальный ток потребления $I_{макс}$ элементов комплекса ТСЗИ, подключенных к изделию "Соната-ИП4.х", не превышает нагрузочной способности последнего *1,5 А*;

2) падение напряжения *U* на проводах, соединяющих нагрузки и изделие "Соната-ИП4" не превышает *2 В;*

3) количество элементов комплекса ТСЗИ, *логически* подключенных к 1 изделию "Соната-ИП4.х", не превышает *100* шт.

Справочные данные по некоторым типам элементов комплекса ТСЗИ приведены в приложении В, таблицах П.6, П.7..

Расчет падения напряжения на проводах U производится по формуле:

$$U= R_{пр}*I_{макс} \quad (1)$$

Пример расчета. Медный кабель сечением 0,5 мм^2, длина 25м, акустоизлучатели: "СА-4Б1" – 2 шт., "СА-4Б" – 2шт., вибровозбудители: "СВ-4Б" – 5 шт., "СВ-4Б1" - 5 шт. По формуле (1):

$I_{макс}$ = 2*0,25+(2+5+5)*0,03=0,86 < 1,5А.

U = 2,2*0,86=1,892< 2В.

Для получения более подробной информации необходимо обратиться на сайт производителя оборудования [5].

Вопросы:

1. Описать технические характеристики по применяемым типам элементов комплекса.
2. Подобрать блоки электропитания и управления САЗ.
3. Расчет максимально возможного количества элементов комплекса ТСЗИ.

Список литературы, рекомендуемый к использованию по данной теме:

Перечень основной литературы:

1. Технические средства и методы защиты информации: учеб.пособие / под ред. А.П. Зайцева, А.А. Шелупанова. – [4-е изд., испр. и доп.]. – Москва : Горячая линия-Телеком, 2016. – 616 с.

2. Хорев А.А. Техническая защита информации: учеб. пособие для студентов ву-зов. В 3-х т. М.: НПЦ «Аналитика», 2017.
Перечень дополнительной литературы:
3. Разработка системы технической защиты информации: учебное пособие [Элек-тронный ресурс]/ В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. – 2-е изд., стер. – М.: Флинта, 2014. – URL:http://biblioclub.ru/index.php?page=book&id=93349.
4. Чипига, А.Ф. Информационная безопасность автоматизированных систем: учеб. пособие/ А. Ф. Чипига- М.: Гелиос АРВ, 2013.
5. Рекомендации по расчету максимального возможного количества элементов комплекса ТСЗИ, подключаемых к изделиям "Соната-ИП4.х" и подбору кабеля. [Электронный ресурс]/ URL:http://www.npoanna.ru/Content.aspx?name=info.cable-lines.

Приложение В

Таблица П.6. Типовые значения сопротивления Rпр некоторых кабелей.

Материал жил (сечение)	Длина кабеля			
	10м	25м	50м	100м
Медь (сечение 1,5 кв мм)	0,35 Ом	0,9 Ом	1,7 Ом	3,4 Ом
Медь (сечение 0,75 кв мм)	0,7 Ом	1,8 Ом	3,4 Ом	6,8 Ом
Медь (сечение 0,5 кв мм)	0,9 Ом	2,2 Ом	4,35 Ом	8,7 Ом
Медь (сечение 0,2кв мм)	2 Ом	5 Ом	10 Ом	20 Ом
Медь (сечение 0,12кв мм)	3,3 Ом	8,25 Ом	16,5 Ом	33 Ом

Таблица П.7. Значение максимального тока, потребляемого от источника электропитания.

№	**Издел ие**	**Максимальный ток потребления элемента ТСЗИ, А**
1	Акустоизлучатель "СА-4Б"	0,03
2	Акустоизлучатель БМ "СА-4Б1"	0,25
3	Вибровозбудитель "СВ-4Б"	0,03
4	Вибровозбудитель ПШ "СВ-4Б1"	0,03
5	"Соната-СК4.1", "Соната-РС3", "Соната-Р3.1"	Менее 0,001*)
6	"Соната-СК4.2"	0,1
7	Пульт управления "Соната-ДУ4.1" (локальный)	0,06
8	"Соната-ВК4.1"	0,05
9	"Соната-ВК4.2"	0,06
10	"Соната-ВК4.3"	0,07
11	Пульт управления "Соната-ДУ4.1" (комплекс)	0,06

* Примечание: изделия имеют собственный источник электропитания от сети 220В.

Практическое занятие № 6.

Тема: Обеспечение оперативного контроля исправности, режима работы и контроля состава комплекса.

Цель: Изучить основы организации технической защиты информации на объектах информатизации и в выделенных помещениях, ознакомиться с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники, ознакомиться с техническими каналами утечки акустической (речевой) информации.

В результате выполнения практического занятия студент должен **знать**: угрозы информационной безопасности объектов информатизации; современные концепции защиты объектов информации. Студент должен **уметь**: проводить анализ исходных данных для проектирования систем защиты выделенных помещений; проводить технические расчёты основных тактико-технических характеристик проектируемых систем защиты выделенных помещений.

Предлагаемые студенту задания позволяют проверить компетенции ПК-1, ПК-4, ПК-5, К-12, ПК-13.

Актуальность темы: Работа систем защиты выделенных помещений в значительной мере определяется качеством оценки защищённости информации от утечки по техническим каналам, выбора и применения средств защиты. Применяемые в системах средства защиты призваны обеспечить эффективную защиту конфиденциальной информации.

Теоретическая часть:

Система мониторинга событий информационной безопасности (СМИБ) предназначена для автоматизации процесса сбора и анализа информации о событиях безопасности, поступающих из различных источников. В качестве таких источников могут выступать средства защиты информации, общесистемное и прикладное ПО, телекоммуникационное обеспечение и др. СМИБ включает в себя следующие компоненты:

- **программно-техническая часть** – реализуется на основе продуктов по мониторингу событий безопасности класса SIEM (Security Information and Event Management);
- **документационная часть** - включает в себя набор документов, описывающих основные процессы, связанные с выявлением и реагированием на инциденты безопасности;
- **кадровая составляющая** - подразумевает выделение сотрудников, ответственных за работу с СМИБ.

Программно-техническая часть СМИБ включает следующие компоненты:

- агенты мониторинга, предназначенные для сбора информации, поступающей от различных источников событий, включающих в себя средства защиты, общесистемное и прикладное ПО, телекоммуникационное обеспечение и др.;
- сервер событий, обеспечивающий централизованную обработку информации о событиях безопасности, которая поступает от агентов. Обработка осуществляется в соответствии с правилами, которые задаются администратором безопасности;
- хранилище данных, содержащее результаты работы системы, а также данные, полученные от агентов;

- консоль управления системой, позволяющая в реальном масштабе времени просматривать результаты работы системы, а также управлять её параметрами.

Важной задачей, которая должна решаться в процессе внедрения, является определение тех инцидентов, которые будут выявляться в процессе работы СМИБ. Для этого выполняются следующие действия:

- определение типов основных инцидентов ИБ;
- определение списка событий, которые ведут к инциденту ИБ;
- определение источника инцидента ИБ;
- определение и приоритезация рисков, связанных с инцидентами ИБ.

Для удаленного контроля и управления комплексом ТСЗИ необходимо специализированное рабочее место АРМ оператора мониторинга и управления с СПО “ИНСПЕКТОР” пример представлен на рисунке 17.

Рисунок 17 – АРМ оператора

СПО “СПЕКТР” позволяет осуществлять мониторинг информационной безопасности всех необходимых ресурсов в режиме реального времени, получая информацию как на уровне средств защиты, так и на уровне сетевых ресурсов, приложений и баз данных, что позволяет построить комплексную систему мониторинга и управления событиями информационной безопасности.

Вопросы:

1. Определить задачи, решаемые системой мониторинга событий информационной безопасности.
2. Подобрать программно-техническую часть системы мониторинга событий информационной безопасности.
3. Описать систему мониторинга событий информационной безопасности.

Список литературы, рекомендуемый к использованию по данной теме:

Перечень основной литературы:

1. Технические средства и методы защиты информации: учеб.пособие / под ред. А.П. Зайцева, А.А. Шелупанова. – [4-е изд., испр. и доп.]. – Москва : Горячая линия-Телеком, 2016. – 616 с.
2. Хорев А.А. Техническая защита информации: учеб. пособие для студентов ву-зов. В 3-х т. М.: НПЦ «Аналитика», 2017.

Перечень дополнительной литературы:

1. Разработка системы технической защиты информации: учебное пособие [Электронный ресурс]/ В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. – 2-е изд., стер. – М.: Флинта, 2014. – URL:http://biblioclub.ru/index.php?page=book&id=93349.
2. Чипига, А.Ф. Информационная безопасность автоматизированных систем: учеб. пособие/ А. Ф. Чипига- М.: Гелиос АРВ, 2013.