

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по выполнению лабораторных работ
по дисциплине «Техническая защита информации»
для студентов направления подготовки
10.03.01 «Информационная безопасность»
Направленность (профиль)
«Организация и технологии защиты информации (по отрасли или в сфере профессиональной
деятельности)»

Ставрополь

2026

СОДЕРЖАНИЕ

Раздел №1	6
Лабораторная работа 1. Место технической защиты информации в государственной системе защиты информации в РФ. Характеристика информации и информационных процессов как предмета технической	6
Лабораторная работа 2. Термины, определения и основы методологии в области технической защиты информации	6
Лабораторная работа 3. Характеристика технических каналов утечки информации, возникающих за счет побочных электромагнитных излучений и наводок ...	6
Раздел №2	34
Лабораторная работа 4. Характеристика угроз безопасности информации в автоматизированных информационных системах	34
Лабораторная работа 5. Исследование сигнальных демаскирующих признаков радиоэлектронных средств	34
Лабораторная работа 6. Акустические каналы утечки речевой информации	34
Раздел №3	51
Лабораторная работа 7. Характеристика технических каналов утечки информации, возникающих за счет побочных электромагнитных излучений и наводок ..	51
Лабораторная работа 8. Специально создаваемые радиоэлектронные технические каналы утечки информации.....	51
Лабораторная работа 9. Акустические каналы утечки речевой информации	51

ВВЕДЕНИЕ

1. Цель и задачи освоения дисциплины (модуля)

«Техническая защита информации» является формирование набора общекультурных и профессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность». Формируемые в рамках дисциплины компетенции способствуют решению профессиональных задач по защите информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях, а также приобретение набора общекультурных и общепрофессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».

Формируемые в рамках дисциплины компетенции способствуют решению профессиональных задач по защите информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях, а также приобретение набора общекультурных и общепрофессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Техническая защита информации относится к дисциплинам обязательной части.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ОПК-4 Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности;	ИД-3 ОПК-4 Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	в совершенстве анализирует физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности
ОПК-11 Способен проводить эксперименты по заданной методике и обработку их результатов;	ИД-1 ОПК-11 Показывает понимание сущности проведения экспериментов по заданной методике и обработку их результатов	-формулирует сущность проведения экспериментов по заданной методике и обработку их результатов; -выделяет целесообразные методики для проведения экспериментов; -демонстрирует уверенное

		использование процедур обработки результатов проведенных экспериментов
	ИД-2ОПК-11 Демонстрирует способность к реализации проведения экспериментов по заданной методике и обработку их результатов	-демонстрирует способность и проведения экспериментов по заданной методике и обработку их результатов; -уверенно выбирает заданные методики проведения экспериментов; -применяет методы обработки результатов экспериментов
ОПК-2.1 Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба;	ИД-1ОПК-2.1 Показывает понимание сущности анализа функционального процесса объекта защиты и его информационных составляющих	-демонстрирует понимание сущности анализа функционального процесса объекта защиты и его информационных составляющих; -формулирует сущность анализа функционального процесса объекта защиты и его информационных составляющих; -оперирует понятиями процесса анализа функционального процесса объекта защиты и его информационных составляющих
	ИД-2ОПК-2.1 Выявляет возможные источники информационных угроз, их возможные цели, пути реализации и предполагаемый ущерб	-выделяет возможные источники информационных угроз, их возможные цели, пути реализации и предполагаемый ущерб; -анализирует возможные источники информационных угроз, их возможные цели, пути реализации и предполагаемый ущерб;

		-оперирует понятиями возможных источников информационных угроз, их возможными целями, путями реализации;
--	--	--

РАЗДЕЛ № 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Тема № 4. ИССЛЕДОВАНИЕ СИГНАЛЬНЫХ ДЕМАСКИРУЮЩИХ ПРИЗНАКОВ РАДИОЭЛЕКТРОННЫХ СРЕДСТВ

ЛАБОРАТОРНЫЕ РАБОТЫ № 1 – 3.

Тема 1: место технической защиты информации в государственной системе защиты информации в рф. Характеристика информации и информационных процессов как предмета технической.

Тема 2: Термины, определения и основы методологии в области технической защиты информации.

Тема 3: Характеристика технических каналов утечки информации, возникающих за счет побочных электромагнитных излучений и наводок.

Подтема: исследование сигнальных демаскирующих признаков радиоэлектронных средств.

Время – 6 часов.

Формируемые компетенции: ОПК-4, ОПК-11, ОПК-2.1.

УЧЕБНЫЕ ВОПРОСЫ:

1. Определение вероятности обнаружения радиоэлектронного средства аппаратурой радиотехнической разведки.
2. Моделирование сигналов радиопередатчиков.
3. Исследование сигнальных демаскирующих признаков работы радиопередатчиков.

СОДЕРЖАНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

Вводная часть

Известно, что основной объем охраняемой информации в настоящее время добывается негласно с помощью современных технических средств радиоэлектронной разведки. Этому способствуют высокие уровни развития технологий в различных областях техники, позволяющие создавать высокоэффективные автономные автоматические средства добывания информации в портативном, миниатюрном и сверхминиатюрном исполнении. Широкий класс создаваемых портативных устройств дает возможность использования разнообразных способов их применения с учетом различных ограничений по территориальной доступности (внутри кабинета или служебного помещения, на охраняемой территории учреждения или закрытого объекта, за пределами охраняемой территории объекта и т.п.).

Радиоэлектронная разведка базируется на временном или спектральном анализе перехватываемых сигналов. Технология радиоразведки (РР) при этом сводится к следующему:

- перехват (регистрация) сигнала;

- обработка (анализ) перехваченных сигналов;
- восстановление информации, содержащейся в перехваченных сигналах, и ее анализ.

Однако радиоразведке, как правило, предшествует радиотехническая разведка (РТР) по получению информации о параметрах радиосигналов (сигнальных признаках), поскольку для согласования радиоприемника разведывательного средства с передатчиком сигнала необходимо знать его параметры.

Следовательно, задача защиты сигнальной признаковой информации решается, прежде всего, путем проведения мероприятий по предотвращению процедур обнаружения и распознавания радиоэлектронных средств (РЭС) по их признакам.

Таким образом, для обеспечения защиты информации, циркулирующей в технических средствах обработки, хранения и передачи информации, необходимо знать и уметь выявлять сигнальные демаскирующие признаки этих РЭС, а также оценивать возможности средств РТР по обнаружению функциональных и опасных сигналов.

Исходя из этого, в первом учебном вопросе с помощью математической модели исследуется величина вероятности обнаружения РЭС по мощности излучаемого сигнала аппаратурой РТР, а во втором вопросе путем технологии схмотехнического моделирования в программе «Electronics Workbench» исследуются демаскирующие признаки модулированных сигналов.

ВОПРОСЫ, ПОДЛЕЖАЩИЕ ИССЛЕДОВАНИЮ

1. Определение вероятности обнаружения радиоэлектронного средства аппаратурой радиотехнической разведки

Оценка возможностей радиоразведки по отношению к конкретному РЭС включает два этапа:

1) Определение возможности добывания разведанных об объекте с помощью различных технических средств разведки (ТСР) в заданных условиях.

2) Определение качества этих данных.

Для оценки возможностей ТСР используются следующие показатели:

- вероятность обнаружения РЭС;
- вероятность распознавания РЭС;
- дальность действия технических средств разведки (ТСР);
- точность определения местоположения РЭС и ошибки измерения его параметров;
- вероятность ошибки воспроизведения перехваченных сообщений.

Вероятность обнаружения является количественным показателем возможности получения разведданных рассматриваемым средством разведки в заданных условиях. **Вероятность обнаружения сигнала характеризует** возможность ТСР за определенный временной интервал наблюдения при фиксированной (допустимой) вероятности ложного обнаружения (ложной тревоги $P_{лт}$) осуществлять выделение сигнала на фоне шума, действующего на входе приемного устройства, без определения параметров сигнала. Числовое значение этого показателя при его сопоставлении с нормативным уровнем позволяет оценить степень опасности средств разведки в конкретной разведывательной ситуации и исключить из дальнейшего рассмотрения неопасные средства разведки.

Расчет вероятности обнаружения конкретного РЭС связан с выявлением средств разведки, с помощью которых возможно добывание разведданных о нем и исключением из дальнейшего рассмотрения средств разведки, с помощью которых в заданных условиях никаких данных получить нельзя.

После выявления средств разведки, обеспечивающих обнаружение РЭС, проводится оценка качества добываемых разведданных. При этом различные по характеру разведданные оцениваются различными показателями.

Вероятность распознавания является количественным показателем достаточности добываемых разведданных для классификации РЭС по типам или их описания.

Под дальностью действия систем разведки понимается максимальное расстояние между приемником ТСР и передатчиком РЭС, при котором обнаружение и измерение координат РЭС осуществляется с заданными вероятностями правильного обнаружения и ложной тревоги ($W_{по}$ и $W_{лт}$) или измерение его параметров с заданной среднеквадратической погрешностью.

Определение местоположения и величин ошибок измерения параметров объекта является количественным показателем точности и достоверности разведданных, получаемых в виде числовых характеристик РЭС. Этот **показатель характеризует** степень соответствия между измеренными и действительными значениями параметров РЭС и для всех параметров определяется как средний квадрат разности между этими значениями.

Расчет ошибок измерения параметров РЭС позволяет оценить возможность использования полученных разведданных для аналитического определения тактико-технических характеристик РЭС, для идентификации РЭС по их известным сигнальным демаскирующим признакам, для выявления индивидуальных признаков и поэкземплярного распознавания РЭС, а также оценить возможность правильной привязки разнородных радиоданных к конкретным РЭС.

Вероятность ошибки воспроизведения перехваченных сообщений **служит** количественным показателем достоверности сообщений, полученных в процессе радиоперехвата. В зависимости от вида сообщения **в качестве показателя вероятности (достоверности) используется** либо

среднеквадратическое отклонение перехваченного сообщения от переданного, либо вероятность ошибки, характеризующая процент неверно воспроизведенных элементов сообщения (слов, цифр, букв). При расчете этих показателей наряду с пространственно-энергетическими условиями приема сигнала учитываются особенности его обработки при восстановлении передаваемого сообщения.

Для каждого типа аппаратуры используются только определенные показатели. Для проведения оценки возможности аппаратуры необходимы данные по объекту разведки, по аппаратуре разведки, по условиям ведения разведки.

Рассмотрим подробнее общий подход к оценки возможностей разведки по вероятности обнаружения.

Обнаружением РЭС с помощью аппаратуры разведки называется процесс принятия решения о наличии или отсутствии РЭС в данной области пространства в результате приема и обработки его сигналов.

Прием сигналов всегда происходит на фоне помех того или иного вида (собственные шумы приемника, радишумы космического пространства, отражение от гидрометеоров, земной поверхности и др.). Наличие помех приводит к искажению передаваемых сигналов и к возникновению ошибок в оценке обстановки. **При обнаружении возможны четыре ситуации.**

Во-первых, если РЭС действительно имеется и сигналы поступают при наличии помех, то по данным разведки наблюдателем **могут быть приняты два решения**: первое – **РЭС есть** и второе – **РЭС нет**. **Первый случай** (т.е. принятие решения о том, что РЭС есть при наличии РЭС в действительности) **называется правильным обнаружением РЭС**. **Второй случай** (принятие решения об отсутствии РЭС в то время, как РЭС есть) **называется пропуском РЭС**. Возможность неопределенного ответа - "неизвестно, есть ли РЭС или его нет" - исключается.

Во-вторых, если объекта нет, то при наличии помех также **возможны два решения**: **РЭС есть** и **РЭС нет**. В этом случае принятие решения о наличии объекта (когда его в действительности нет) называется **ложной тревогой**, а решение об отсутствии объекта – **правильным необнаружением**.

Пропуск РЭС и ложная тревога являются ошибками при обнаружении РЭС. Так как в общем случае сигналы и помехи являются случайными функциями времени, то принятие того или иного решения носит случайный характер. Поэтому **возможность возникновения перечисленных ситуаций принято характеризовать соответствующими вероятностями**: вероятностью правильного обнаружения $W_{по}$, пропуска $W_{пр}$, ложной тревоги $W_{лт}$ и правильного необнаружения $W_{пн}$.

Правильное обнаружение и пропуск РЭС (при наличии объекта в действительности) образуют полную группу несовместимых событий, поэтому

$$W_{no} + W_{np} = 1. \quad (1)$$

Точно так же ложная тревога и правильное необнаружение образуют полную группу несовместимых событий при отсутствии РЭС

$$W_{лт} + W_{пн} = 1. \quad (2)$$

Рассмотренные четыре вероятности являются условными, т.к. они характеризуют события, происходящие при условии наличия или отсутствия РЭС. В реальных условиях работы станции разведки мы не можем заранее знать, имеются ли РЭС в просматриваемой области пространства или их там нет.

Обозначим вероятность наличия РЭС в интересующий нас области пространства через $W(P)$, а вероятность отсутствия РЭС через $W(O)$.

Четыре указанных события также составляют полную группу несовместимых событий, поэтому

$$W(P) \cdot W_{по} + W(P) \cdot W_{пр} + W(O) \cdot W_{лт} + W(O) \cdot W_{пн} = 1, \quad (3)$$

где:

$W(P) \cdot W_{по}$ – безусловная вероятность правильного обнаружения РЭС,

$W(P) \cdot W_{пр}$ – безусловная вероятность пропуска РЭС,

$W(O) \cdot W_{лт}$ – безусловная вероятность ложной тревоги обнаружения РЭС,

$W(O) \cdot W_{пн}$ – безусловная вероятность правильного необнаружения РЭС.

Оптимальным устройством обнаружения будет такое устройство, с помощью которого может быть достигнуто лучшее (по сравнению с другими) значение выбранного критерия при прочих равных условиях. Наиболее употребляемыми являются три критерия: критерий идеального наблюдателя, критерий Неймана-Пирсона, критерий последовательного анализа.

В соответствии с **критерием идеального наблюдателя** оптимальное устройство обнаружения должно обеспечивать минимум суммарной безусловной вероятности ошибок обнаружения, т.е.

$$W_{ош} = W(P) \cdot W_{пр} + W(O) \cdot W_{лт} \quad \min. \quad (4)$$

Критерий идеального наблюдателя применяется для систем радиосвязи, когда вероятности $W(P)$ и $W(O)$ известны априори. Относительная частота появления ошибок определяется априорными вероятностями $W(P)$ и $W(O)$ соответственно. Поэтому средняя вероятность общей (суммарной) ошибки равна

$$W_{ош} = W(P) \cdot W_{пр} + W(O) \cdot W_{лт}, \quad (5)$$

а вероятность правильного обнаружения сигнала равна $W_{по} = 1 - W_{пр}$.

В соответствие с **критерием Неймана-Пирсона**, оптимальное устройство характеризуется максимумом разности

$$W_{по} - W_{лт} \quad \max, \text{ при } W_{лт} \leq (W_{лт})_{\text{доп}}. \quad (6)$$

Следовательно, оптимальный характер критерия Неймана-Пирсона

состоит в том, что он максимизирует вероятность правильного обнаружения при фиксированной вероятности ложной тревоги.

В приемном устройстве, с помощью которого производится обнаружение сигналов, осуществляется определение апостериорных вероятностей различных сообщений (например, сообщение – есть РЭС или его нет) и указание в качестве решения на то сообщение, вероятность которого больше остальных. Основными характеристиками устройства, используемыми для обнаружения сигналов, являются рабочие характеристики приемника.

Рабочая характеристика приемника (обнаружителя) представляет зависимость $W_{по}$ от отношения сигнал/шум на входе обнаружителя (q) для заданного значения $W_{лт}$.

На рис. 1 представлены соответствующие зависимости для обнаружителя, описываемого соотношением

$$W_{по} = \frac{q - \bar{\mathcal{O}}(1 - W_{\bar{\mathcal{O}}})}{\sqrt{1 + q}}, \quad (7)$$

где $\bar{\mathcal{O}}(1 - W_{\bar{\mathcal{O}}})$ - интеграл вероятности для случая узкополосного импульсного сигнала.

Таким образом, рассчитав соотношение сигнал/шум в точке приема и зная $W_{лт}$, можно определить $W_{по}$.

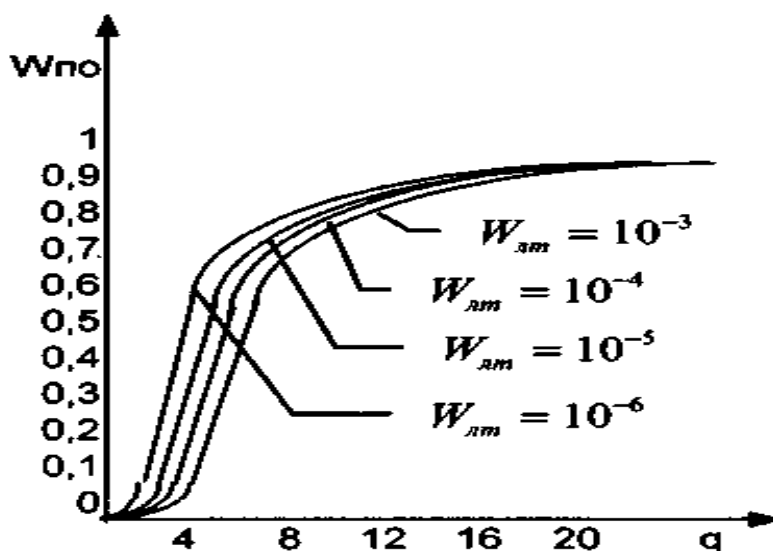


Рис. 1 – Зависимость вероятности правильного обнаружения от отношения сигнал/шум

Итак, в качестве показателя для оценки возможностей средств радиоразведки по перехвату информации наиболее часто используется вероятность обнаружения сигнала средством разведки P_o .

Методика расчета вероятности обнаружения аппаратурой РТР

Для расчета вероятности обнаружения W_o излучения РЭС аппаратурой РТР необходимы следующие исходные данные (при этом рассматривается только случай прямой видимости, например, УКВ радиосвязь, сотовая телефония).

1. Данные по объекту обнаружения, т.е. РЭС:
 - мощность передатчика РЭС ($P_{изл}$);
 - коэффициент направленного действия (КНД) антенны РЭС в направлении аппаратуры разведки (G_o);
 - длина волны излучения (λ).
2. Данные по аппаратуре радиотехнической разведки:
 - вероятность ложной тревоги ($W_{лт}$);
 - предельная чувствительность приемника ($P_{пр}$);
 - КНД антенны приемника ($G_{пр}$).
3. Данные по условиям ведения разведки:
 - дальность между РЭС и приемником РТР (D).

При наличии перечисленных исходных данных расчет производится в следующем порядке.

Предварительно определяется эквивалентная мощность передатчика РЭС ($P_{изл}^{э\kappa\upsilon}$) и эквивалентная чувствительность разведывательного приемника ($P_{пр}^{э\kappa\upsilon}$)

$$P_{изл}^{э\kappa\upsilon} = P_{изл} \cdot G_o, \quad P_{пр}^{э\kappa\upsilon} = \frac{P_{пр}}{G_{пр}}, \quad (8)$$

Затем рассчитывается вероятность W_o по формулам

$$W_o = W_{лт}^{\frac{1}{1+0,5 \cdot r^2}}, \quad r^2 = \frac{\lambda^2}{64 \cdot \pi^2} \cdot \frac{P_{изл}^{э\kappa\upsilon}}{P_{пр}^{э\kappa\upsilon} \cdot D^2}, \quad (9)$$

Дальность действия технических средств разведки

При ведении пассивной РЭР (РР и РТР) радиосигнал от объекта разведки (излучателя) распространяется к разведывательному приемнику. В этом случае мощность радиосигнала на входе приемника определяется формулой

$$P_{с\kappa} = \frac{P_{изл} \cdot G_o \cdot S_{эф}}{4\pi \cdot D^2}, \quad (10)$$

где: $P_{изл}$ – мощность излучателя; G_o – коэффициент усиления антенны; $S_{эф}$ – эффективная площадь приемной антенны $S_{эф} \approx (0.5 \div 0.7) \times S_{геом}$; $S_{геом}$ – геометрическая площадь приемной антенны; D – расстояние до разведываемого объекта.

Для средств разведки этот сигнал наблюдается на фоне естественных и внутренних шумов приемника. При этом мощность шума определяется как

$$P_{ш} = N_o \times \Delta f_{пр},$$

где N_0 – спектральная плотность шума; Δf_{np} – полоса пропускания приемника.

Для требуемого отношения q_0 сигнал/шум на выходе приемника максимальная дальность действия средства разведки равно

$$D_{\max} = \frac{1}{2} \sqrt{\frac{P_{\text{изл}} \cdot G_0 \cdot S_{\text{эф}}}{\pi \cdot q_0 \cdot \alpha_{\text{п}} \cdot \Delta f_{np} \cdot N_0}}, \quad (11)$$

где: $\alpha_{\text{п}}$ – потери в отношении сигнал/шум в тракте приемника.

Реальная дальность действия средств разведки меньше $D_{\max}$, что обусловлено поглощением энергии излучения при распространении радиоволн в атмосфере. Реальная дальность действия уменьшается по сравнению с $D_{\max}$ в $\sqrt{0.5\alpha}$ раз, где $\alpha_{\text{пг}}$ – коэффициент поглощения сигнала в атмосфере.

Содержание практической работы, выполняемой студентами в ходе занятия

1. Описание лабораторного оборудования:

– ПЭВМ с программным математическим редактором «Mathcad Professional», версия 14 и программным редактором схематического моделирования «Electronics Workbench», версия 5.12.

2. Требования безопасности при выполнении работы:

I. Перед началом выполнения лабораторной работы:

1. Изучить оборудование и рабочее место.
2. Получить разрешение к выполнению лабораторных работ от руководителя занятий или лаборанта.

II. Во время выполнения лабораторных работ:

Убедиться, что на измерительных приборах переключатели установлены в исходном положении ручек, на минимальное напряжение и максимальные пределы измерения.

Включать питающие напряжения и собранные схемы только после разрешения руководителя занятий или лаборанта и предупреждения всех работающих.

Проверять наличие питающих напряжений и проводить измерения электрических величин только с помощью соответствующих измерительных приборов, одной рукой, после установки на них максимально ожидаемого результата и рода измеряемой величины.

ВНИМАНИЕ!

- Не прикасаться к открытым токоведущим частям, проводникам, клеммам и зажимам, не облакачиваться на приборы, не прикасаться к батареям, не отвлекаться от измерений, не производить изменений в схеме и не оставлять без наблюдения цепь, находящуюся под напряжением.
- При работе с катушками индуктивности и конденсаторами не трогать их и соединительные провода, так как вследствие резонанса могут возникнуть большие токи и напряжение.
- При обнаружении неисправностей в измерительных приборах **немедленно** отключить источники питания и доложить об этом руководителю занятий или лаборанту.

III. По окончании выполнения лабораторных работ:

1. Докладывать руководителю занятий или лаборанту о завершении работ.

2. Обесточить собранные схемы, разобрать их (если это предусмотрено) и выключить контрольно-измерительные приборы.
3. Привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

ПРИ РАБОТЕ ЗАПРЕЩАЕТСЯ:

- производить самостоятельное включение автоматов защиты, заменять предохранители, устранять неисправности и повреждения;
- проводить какие-либо переключения, соединения, не предусмотренные инструкциями по выполнению лабораторных работ.

ПРИ АВАРИЙНЫХ СИТУАЦИЯХ И НЕСЧАСТНЫХ СЛУЧАЯХ:

- немедленно отключить автоматы защиты, доложить руководителю занятий и действовать согласно его указаний;
- при поражении электрическим током оказать первую помощь в соответствии с принятой методикой до прибытия врача.

ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ:

- лица, нарушившие требования инструкции отстраняются от выполнения лабораторных работ и допускаются только после сдачи зачета по правилам и мерам безопасности;
- при выводе из строя приборов и оборудования лаборатории по вине лица, проводившего работы и в случае нарушения требования инструкции, они несут материальную ответственность в соответствии с действующим законодательством РФ.

3. Задание для работы

1) Составить и отладить программу методики расчета вероятности обнаружения в «Mathcad Professional».

2) Исследовать зависимость вероятности обнаружения РЭС от мощности излучения.

3) Исследовать зависимость вероятности обнаружения РЭС от КНД приемной антенны.

4) Исследовать зависимость вероятности обнаружения РЭС от длины волны.

5) Исследовать зависимость вероятности обнаружения РЭС от вероятности ложной тревоги.

6) Составить и отладить программу расчета дальности обнаружения РЭС в «Mathcad Professional».

7) Исследовать зависимость дальности обнаружения РЭС от мощности шума.

8) Произвести индивидуальные исследования, используя исходные данные согласно варианту, указанному преподавателем.

9) Оформить отчет о проделанной работе в соответствии с требованиями, изложенными в описании работы.

4. Порядок выполнения работы

Задание 1.1. Составить и отладить программу методики расчета вероятности обнаружения в «Mathcad Professional».

1) В редакторе «Mathcad Professional» ввести формулы (8) – (9), описывающие методику расчета вероятности обнаружения РЭС для аппаратуры РТР.

2) Ввести исходные данные, приведенные в таблице 1, для которых вероятность обнаружения РЭС W_o должна равняться 0,9. Сравнивая полученный результат с требуемым, убедится в правильности введенных формул методики.

Таблица 1 – Исходные данные.

$P_{изл}$, Вт	G_o	λ , м	D , м	$W_{ЛТ}$	$P_{пр}$, Вт	$G_{пр}$
2	1	0,33	$6,4 \times 10^3$	10^{-3}	2×10^{-12}	10

Задание 1.2. Исследовать зависимость вероятности обнаружения РЭС от мощности излучения.

1) Изменить дальность между передатчиком РЭС и приемником ТСП, установив ее равной 3×10^3 м.

2) Рассчитать значения W_o при мощности передатчика, равной 0,1 Вт; 0,5 Вт; 1 Вт; 1,5 Вт; 2 Вт; 3 Вт; 5 Вт.

3) Построить и проанализировать график зависимости вероятности обнаружения РЭС от мощности излучения.

Задание 1.3. Исследовать зависимость вероятности обнаружения РЭС от КНД приемной антенны, имеющей нормированную диаграмму направленности, представленную на рис. 2.

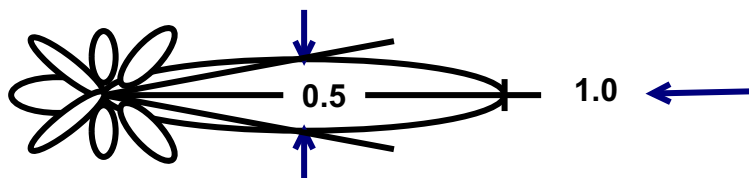


Рис. 2 – Диаграмма направленности приемной антенны

1) Установить изначальные исходные данные.

2) Рассчитать значения W_o при КНД приемной антенны, равной:

– 0,1 (т.е. антенна ориентирована на РЭС минимумом диаграммы направленности);

– 2 (т.е. антенна ориентирована на РЭС задним лепестком диаграммы);

– 3 (т.е. антенна ориентирована на РЭС передним боковым лепестком диаграммы);

– 5 (т.е. антенна ориентирована на РЭС под углом, соответствующим 0,5 максимального уровня диаграммы);

– 10 (т.е. антенна точно ориентирована на РЭС основным лепестком по максимуму диаграммы).

3) Построить и проанализировать график зависимости вероятности обнаружения РЭС от КНД приемной антенны.

Задание 1.4. Исследовать зависимость вероятности обнаружения РЭС

от длины волны.

- 1) Установить изначальные исходные данные.
- 2) Рассчитать значения W_o при длинах волн, соответствующих частотам 450 МГц, 900 МГц, 1800 МГц, 2400 МГц, 5000 МГц, 10000 МГц.
- 3) Построить и проанализировать график зависимости вероятности обнаружения РЭС от значений длины волны.

Задание 1.5. Исследовать зависимость вероятности обнаружения РЭС от вероятности ложной тревоги.

- 1) Установить изначальные исходные данные.
- 2) Рассчитать значения W_o при значениях вероятности ложной тревоги $W_{лт}$, равных 10^{-12} ; 10^{-9} ; 10^{-6} ; 10^{-5} ; 10^{-4} ; 10^{-3} ; 10^{-2} ; 10^{-1} .
- 3) Построить и проанализировать график зависимости вероятности обнаружения РЭС от значений вероятности ложной тревоги.

Задание 1.6. Составить и отладить программу расчета дальности обнаружения РЭС в «Mathcad Professional».

- 1) В редакторе «Mathcad Professional» ввести формулы (10) – (11), описывающие методику расчета дальности обнаружения РЭС для аппаратуры РТР.

- 2) Установить изначальные исходные данные, предназначенные для предыдущей методики.

- 3) Ввести дополнительные исходные данные, приведенные в таблице 2, для которых максимальная дальность обнаружения РЭС $D_{\max}$ должна равняться 6 км. Сравнивая полученный результат с требуемым, убедится в правильности введенных формул методики.

Таблица 2 – Дополнительные исходные данные.

$S_{\text{ГЕОМ}}, \text{м}^2$	q_o	$N_o, \text{Вт/Гц}$	$\Delta f_{\text{пр}}, \text{Гц}$	$\alpha_{\text{П}}$
0,64	10	10^{-15}	84000	2

Задание 1.7. Исследовать зависимость дальности обнаружения РЭС от мощности шума.

- 1) Рассчитать значения $D_{\max}$ от величин мощности шума, пропорциональных ширине полосы пропускания приемника, равной 3100 Гц, 15000 Гц, 84000 Гц, 200000 Гц.

- 2) Построить и проанализировать график зависимости дальности обнаружения РЭС от значений мощности шума.

- 3) Рассчитать максимальную мощность излучения передатчика, при которой РЭС может быть обнаружено только в пределах контролируемой зоны, равной 0,5 км.

Задание 1.8. Произвести индивидуальные исследования, используя исходные данные из таблицы 3 согласно варианту, указанному преподавателем. В ходе этих исследований рассчитать:

- зависимость вероятности обнаружения РЭС от изменения его мощности излучения при заданной длине волны;
- зависимости вероятности обнаружения РЭС от изменения длины

волны при заданной мощности излучения;

- значение максимальной дальности обнаружения РЭС средствами РТР от мощности шума, создаваемой в заданной полосе пропускания;

- значение максимальной мощности излучения передатчика, при которой РЭС может быть обнаружено только в пределах контролируемой зоны для полосы пропускания 81200 Гц.

Таблица 3 – Исходные данные для индивидуального задания.

<i>№ варианта</i>	<i>$P_{изл}$, Вт</i>	<i>f, МГц</i>	<i>Δf_{np}, Гц</i>	<i>$D_{кз}$, м</i>
1.	1	890	4000	900
2.	1,2	895	7000	800
3.	1,4	905	12500	700
4.	1,5	910	14000	600
5.	1,7	915	20000	750
6.	1,8	935	22500	850
7.	0,9	940	25000	950
8.	0,8	945	42000	550
9.	0,75	950	56000	1000
10.	0,7	960	80000	650
11.	0,6	955	100000	1050
12.	1,3	885	120000	1100

Задание 1.9. Оформить отчет о выполнении лабораторной работы. В отчете отобразить:

- тему и цель работы, порядок ее выполнения;
- математическую модель (методику), на базе которой проводилось лабораторные исследования;

- графики зависимости вероятности обнаружения РЭС от изменения его мощности излучения, КНД приемной антенны, длины волны и вероятности ложной тревоги;

- графики зависимости максимальной дальности обнаружения РЭС средствами РТР от мощности шума;

- значение максимальной мощности излучения передатчика, при которой РЭС может быть обнаружено только в пределах контролируемой зоны.

- по результатам работы сделать выводы о влиянии сигнальных демаскирующих признаков и параметров РЭС на вероятность их обнаружения W_0 .

Задание 4.10. Защитить отчет по первой части проделанной лабораторной работы.

2 – 3. Моделирование и исследование сигнальных демаскирующих признаков работы радиопередатчиков

Краткие теоретические или справочно-информационные материалы

Распознавание радиоэлектронных средств (РЭС) осуществляется по их сигнальным демаскирующим признакам. Для уяснения этого рассмотрим понятие сигнала и классификацию сигналов.

Под **сигналом** понимается распространяющийся в пространстве носитель с информацией, содержащейся в значениях его физических параметров. К ним относятся: электромагнитные поля и электрический ток от созданных человеком источников сигналов, таких как радиоэлектронные средства, устройства и приборы.

Классификация сигналов представлена на рис. 3.



Рис. 3 – Классификация сигналов

К аналоговым сигналам относятся сигналы, уровень (амплитуда) которых может принимать произвольные значения в определенном для сигнала интервале. Амплитуда простого и достаточно распространенного в природе гармонического сигнала изменяется по синусоидальному закону:

$$s(t) = A \sin(\omega t + \varphi), \quad (12)$$

где A – амплитуда, $\omega = 2\pi f$ – круговая частота колебания, φ – фаза колебания. Частота f измеряется в Гц и называется линейной.

Большинство аналоговых сигналов имеют более сложную форму. Периодические (повторяющиеся через время T_n – период) сигналы произвольной формы могут быть представлены в соответствии с формулой Фурье в виде суммы гармонических колебаний:

$$s(t) = C_0 + \sum_{k=1}^n C_k \cos(k\omega t - \varphi_k), \quad (13)$$

где C_0 – постоянная составляющая сигнала; C_k – амплитуда k -й гармоники сигнала ($k=1, 2, \dots, n$); k и φ_k – частота и фаза k -й гармоники сигнала.

Ряд Фурье представляет собой математическую модель периодического сигнала, также как любой цвет может быть разложен на составляющие красного, зеленого и синего цветов.

Совокупность гармонических составляющих сигнала образуют его спектр. Амплитуда каждой спектральной составляющей характеризует энергию соответствующей гармоники основной частоты сигнала. Чем выше скорость изменения амплитуды сигнала, тем больше в его спектре высокочастотных гармоник. Разность между максимальной и минимальной частотами спектра сигнала, между которыми сосредоточено основная часть, например, 95% энергии, называется **шириной спектра ΔF** . Графическое изображение спектра периодического сигнала представлено на рис. 4.

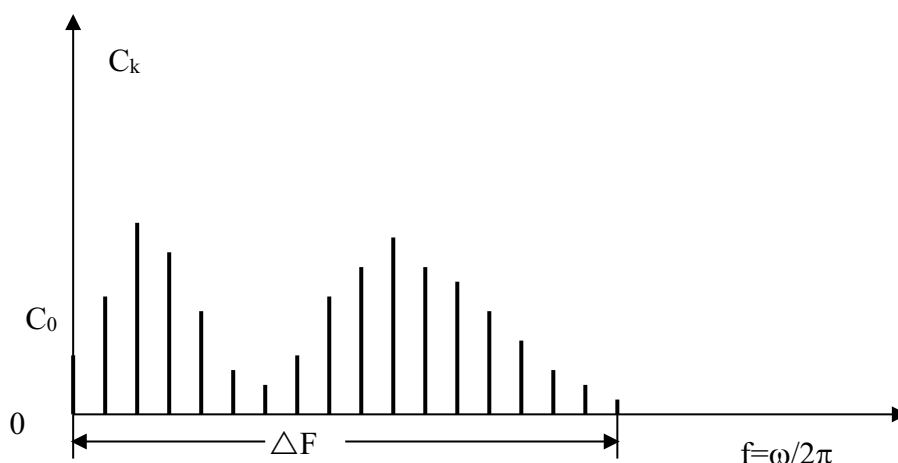


Рис. 4 – Спектр периодического многотонального аналогового сигнала

Частоты составляющих спектра непериодического аналогового сигнала непрерывно меняются. При наблюдении спектра такого сигнала на экране анализатора спектра положение и уровень различных спектральных составляющих непрерывно меняются, и спектр выглядит как сплошной.

В соответствии с изменением амплитуды аналогового сигнала меняется его энергия или мощность (так как мощность пропорциональна квадрату амплитуды). В зависимости от времени измерения энергии сигнала различают среднюю и мгновенную мощность. Десятичный логарифм отношения максимальной мощности сигнала к минимальной называется **динамическим диапазоном сигнала**.

Таким образом, **аналоговый сигнал описывается набором параметров, являющихся его признаками**. К ним относятся:

- частота или диапазон частот;
- фаза сигнала;
- длительность сигнала;
- амплитуда или мощность сигнала;
- ширина спектра сигнала;
- динамический диапазон сигнала.

У дискретных сигналов амплитуда имеет конечный, заранее определенный набор значений. Наиболее широко применяется двоичный

(бинарный) дискретный сигнал: в ЭВМ, в телеграфии, при передаче данных. Информационные сигналы, циркулирующие в ЭВМ IBM PC, имеют два уровня амплитуды: низкий (L-уровень, 0 В) и высокий (H-уровень, 5 В). Осциллограмма бинарного сигнала показана на рис. 5.

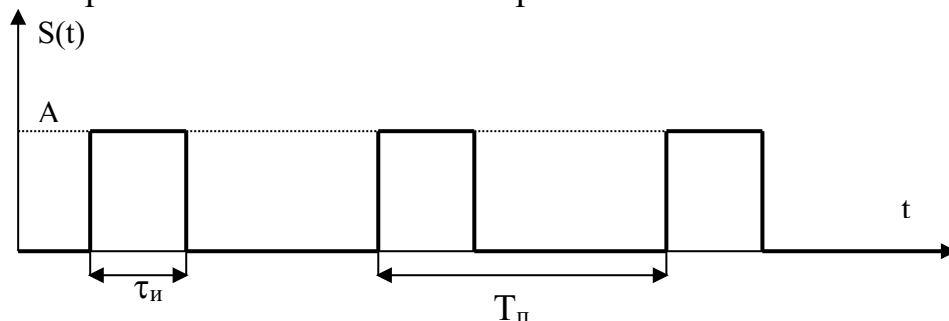


Рис. 5 – Осциллограмма бинарного сигнала

Дискретный сигнал характеризуется следующими параметрами:

- амплитудой A или мощностью P ;
- длительностью импульса τ_n ;
- периодом T_n или частотой $F_n = 1/T_n$ повторения импульсов (для периодических дискретных сигналов);
- шириной спектра сигнала F_C ;
- скважностью импульсов $= T_n / \tau_n$.

Спектр дискретного периодического сигнала содержит бесконечное количество убывающих по амплитуде гармоник. Для бинарного периодического сигнала фрагмент спектра показан на рис. 6.

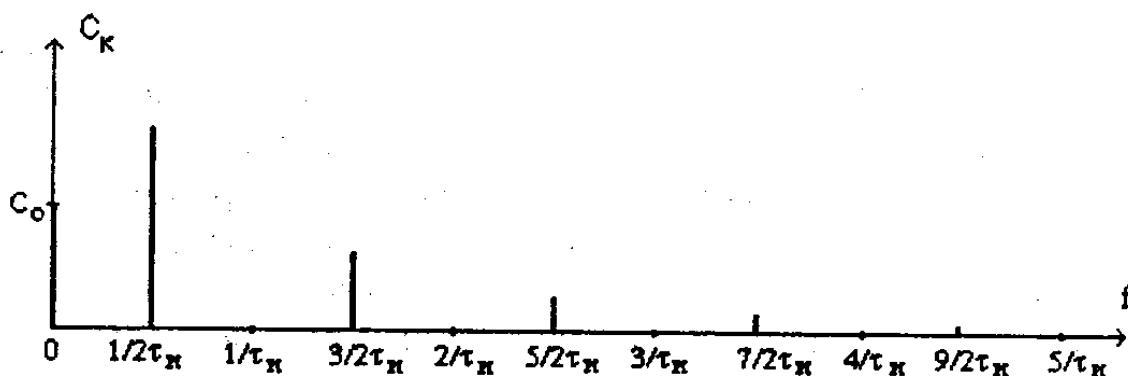


Рис. 6 – Спектр бинарного периодического сигнала со скважностью 2

Он характеризуется следующими свойствами:

- форма огибающей спектра описывается функцией $|\sin x / x|$;
- амплитуда гармоник C_k имеет нулевое значение в точках k / τ_n , $k=1,2,\dots$;
- в области частот спектра $(0-1/\tau_n)$ располагаются -1 гармоник;
- постоянная составляющая сигнала равна $A/2$.

Учитывая, что большая часть энергии сигнала сосредоточена в области частот $0-1/\tau_n$, *ширина спектра бинарного периодического сигнала*

приблизительно оценивается по формуле: $F = 1/\tau$.

При прохождении дискретных сигналов по реальным электрическим цепям радиотехнических средств с ограниченной полосой пропускания их форма искажается и крутизна склона импульса уменьшается. Прямоугольный импульс приобретает колоколообразную форму. В результате этого размывается граница между формой аналогового и дискретного сигналов. Искажения формы и уменьшение амплитуды импульсных сигналов в проводах кабелей ограничивают дальность их передачи, например, для обеспечения межмашинного обмена данными в локальных сетях.

По физической природе сигналы могут быть акустическими, электрическими, магнитными, электромагнитными (**в радиодиапазоне — радиосигналы**), корпускулярными (*в виде потоков элементарных частиц*) и материально-вещественными, например, пахучие добавки в газ подают сигнал об его утечке.

Сигналы по виду передаваемой информации делятся на речевые, телеграфные, телекодовые, факсимильные, телевизионные, о радиоактивных излучениях и условные. Телеграфные и телекодовые сигналы используются для передачи буквенно-цифровой информации с низкой и высокой скоростью соответственно. Факсимильные и телевизионные сигналы обеспечивают передачу неподвижных и подвижных изображений. Сигналы радиоактивных излучений являются демаскирующими признаками радиоактивных веществ. Условные сигналы несут информацию, содержание которой предварительно определено между ее источником и получателем, например, горшок с цветком на подоконнике в литературных произведениях о разведчиках — о провале явки.

Вид информации, содержащей в сигнале, изменяет его демаскирующие признаки: форму, ширину спектра, частотный и динамический диапазон. Например, стандартный речевой сигнал, передаваемый по телефонной линии, имеет ширину спектра 300 – 3400 Гц, звуковой – 16 – 20000 Гц, телевизионный – 6 – 8 МГц и т. д. Произведение $B = F_{\Sigma}$ с называется базой сигнала. Если $B \approx 1$, то сигнал узкополосный, при $B \gg 1$ – сигнал широкополосный.

По времени проявления сигналы могут быть регулярными, время появления которых получателю информации известно, например, сигналы точного времени, и случайные, когда это время неизвестно. Статистические характеристики проявления случайных сигналов во времени могут представлять собой достаточно информативные демаскирующие признаки источников, прежде всего, об их принадлежности и режимах функционирования. Например, появление в помещении радиосигнала во время ведения в нем разговоров может с достаточно высокой вероятностью служить демаскирующим признаком закладного устройства с акустическим автоматом.

В данной лабораторной работе исследуются сигнальные демаскирующие признаки наиболее часто применяемых сигналов, к которым

относятся амплитудно-модулированные, квадратурно-модулированные, частотно-модулированные, амплитудно-манипулированные, частотно-модулированные и фазомодулированные сигналы.

Приведенные сигналы подробно рассмотрены в лекции №4, за исключением гауссовского частотно-манипулированного сигнала с минимальным сдвигом (GMSK), который рассмотрим здесь.

В цифровой сотовой связи в стандарте GSM используется *гауссовская манипуляция с минимальным сдвигом* (Gaussian Minimum Shift Keying – GMSK). Это разновидность частотной модуляции, предназначенные для передачи дискретных (цифровых) сигналов. Английский термин Shift Keying, переводится обычно как манипуляция, в буквальном смысле означает переключение сдвигом или переключение скачком, т.е. дискретное переключение. При этом термин «минимальный сдвиг» относится к сдвигу частоты.

Суть гауссовской манипуляции состоит в следующем. Несущая частота дискретно – через интервалы времени, кратные периоду T битовой модулирующей последовательности, - принимает значения одну из двух значений частоты

$$f_H = f_0 - F/4 \text{ или } f_B = f_0 + F/4, \quad (14)$$

где: f_0 – центральная частота используемого частотного канала, $F=1/T$ – частота битовой последовательности.

Минимально возможным разнесом частот, при котором обеспечивается ортогональность колебаний частот f_B и f_H , т.е. разность фаз, равная π , является равным

$$\Delta f = f_B - f_H = F/2. \quad (15)$$

Поскольку модулирующая частота в этом случае равна $F/2$, а девиация частоты $F/4$, индекс частотной модуляции составляет

$$m = \left(\frac{F/4}{F/2} \right) = 0.5. \quad (16)$$

Термин «гауссовская» соответствует дополнительной фильтрации модулирующей битовой последовательности относительно узкополосным гауссовским фильтром. Преимущество данного вида модуляции в том, что он имеет минимальный уровень излучения на боковых и зеркальных частотах, то есть не мешает другим пользователям радиоэфира, поскольку имеет минимальную ширину спектра. При этом плотность информации – 1 бит на символ или на герц.

Содержание практической работы, выполняемой студентами в ходе занятия

1. Описание лабораторного оборудования:

– ПЭВМ с программным редактором схематического моделирования «Electronics Workbench» (EWB), версия не ниже 5.12.

2. Требования безопасности при выполнении работы приведены на стр. 8.

3. Задание для работы

- 1) Исследовать сигнальные демаскирующие признаки амплитудно- и частотно-модулированных сигналов.
- 2) Исследовать сигнальные демаскирующие признаки квадратурного амплитудно-модулированного сигнала.
- 3) Исследовать сигнальные демаскирующие признаки манипулированных сигналов.
- 4) Исследовать сигнальные демаскирующие признаки GMSK сигнала.
- 5) Составить отчет о проделанной работе в соответствии с требованиями, изложенными в описании работы.

4. Порядок выполнения работы

Задание 2.1. Исследовать сигнальные демаскирующие признаки амплитудно- и частотно-модулированных (АМ и ЧМ) сигналов.

- 1) Запустить программу EWB и собрать схему, приведенную на рис. 7.

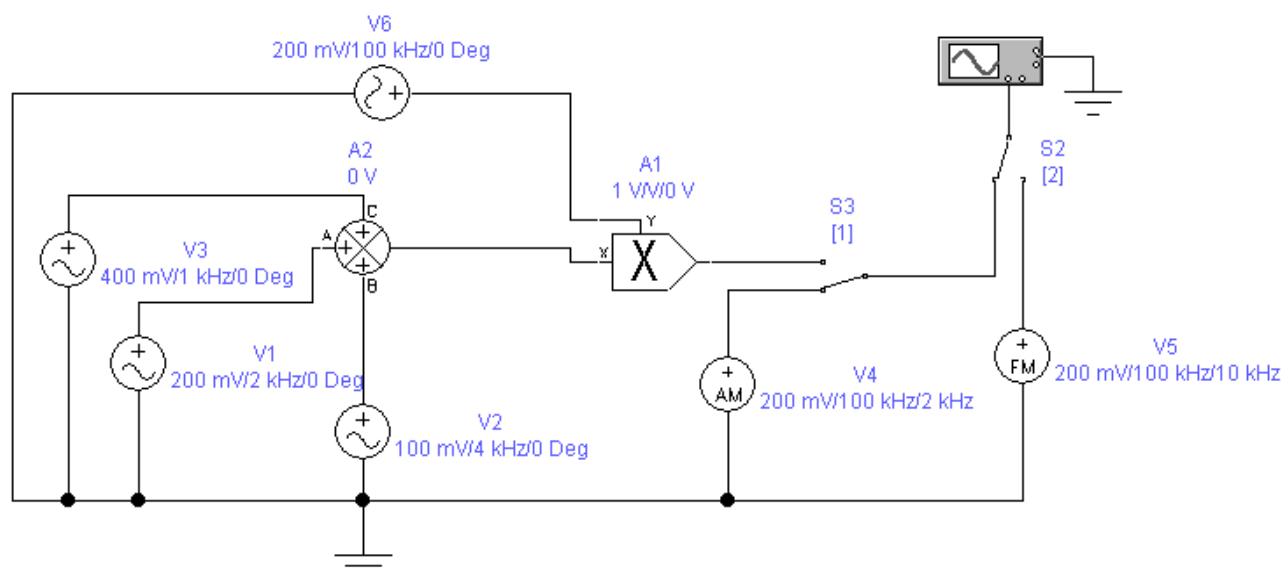


Рис. 7 – Схема исследования АМ и ЧМ сигналов

- 2) Установить параметры элементов схемы в соответствии с величинами, указанными на рис. 7. Схема исследования, приведенная на рис. 7, содержит модели:

- источника однотонового амплитудно-модулированного сигнала (V4);
- источника однотонового частотно-модулированного сигнала (V5);
- источника многотонового речеподобного сигнала, составленного из трех генераторов переменного синусоидального напряжения (V1, V2, V3) и сумматора напряжений (A2);
- генератора несущего высокочастотного колебания (V6);
- балансного модулятора (умножитель A1).

- 3) Провести исследование однотонового амплитудно-

модулированного сигнала. Для этого выполнить следующие действия:

- переключатель S3 (клавиша 1) установить в нижнее положение, а переключатель S2 (клавиша 2) – в левое положение, тем самым подключив выход источника (V4) АМ сигнала к входу осциллографа;
- включить осциллограф и настроить его для регистрации АМ сигнала;
- измерить параметры и отобразить в отчете временную диаграмму или осциллограмму однотонового АМ сигнала;
- измерить и вычислить коэффициент (глубину) модуляции, воспользовавшись формулой

$$M_{AM} = \frac{U_{max} - U_{min}}{U_{max} + U_{min}}; \quad (17)$$

- сравнить вычисленный и установленные коэффициенты модуляции, определив относительную погрешность;
- получить и измерить спектр однотонового АМ сигнала с помощью симулятора Фурье анализа, установив в нем номер выходного узла схемы, подключенного к осциллографу, основную частоту (Fundamental frequency), равную 1 КГц, и число гармоник (Number of harmonics), равное 200;
- отобразить в отчете спектр (частотное представление) однотонового АМ сигнала;
- определить, как влияет на вид диаграммы и спектра однотонового АМ сигнала изменение частоты модулирующего (информационного, низкочастотного) сигнала;
- определить, как влияет на вид диаграммы и спектра однотонового АМ сигнала изменение коэффициента модуляции, последовательно устанавливая его равным 0,25; 0,5, 0,75 и 1;
- сделать выводы о том, какими сигнальными демаскирующими признаками обладают однотоновые АМ сигналы.

4) Провести исследование многотонового амплитудно-модулированного сигнала. Для этого выполнить следующие действия:

- переключатель S3 (клавиша 1) установить в верхнее положение, а переключатель S2 (клавиша 2) – в левое положение, тем самым подключив выход балансного модулятора (A1), как источника многотонового АМ сигнала, к входу осциллографа;
- включить осциллограф и настроить его для регистрации АМ сигнала;
- измерить и отобразить в отчете временную диаграмму или осциллограмму многотонового АМ сигнала;
- получить и измерить спектр многотонового АМ сигнала с помощью симулятора Фурье анализа, установив в нем номер выходного узла схемы, подключенного к осциллографу, основную частоту (Fundamental frequency), равную 1 КГц, и число гармоник (Number of harmonics), равное 200;

– отобразить в отчете спектр (частотное представление) многотонального АМ сигнала;

– определить, как влияет на вид диаграммы и спектра многотонального АМ сигнала изменение амплитуды и частоты модулирующего (информационного, низкочастотного) сигнала, меняя значения амплитуды напряжения и частоты колебания генераторов (V1, V2, V3);

– сделать выводы о том, какими сигнальными демаскирующими признаками обладают однотоновые АМ сигналы.

5) Провести исследование однотонового частотно-модулированного сигнала. Для этого выполнить следующие действия:

– установить переключатель S2 (клавиша 2) – в правое положение, тем самым подключив выход источника (V5) ЧМ сигнала к входу осциллографа;

– включить осциллограф и настроить его для регистрации ЧМ сигнала;

– измерить параметры и отобразить в отчете временную диаграмму или осциллограмму однотонового ЧМ сигнала;

– измерить и вычислить девиацию частоты F и индекс модуляции, воспользовавшись формулой

$$M_{\times M} = \frac{\Delta F}{F_f} = \frac{F_{\max} - F_{\min}}{2 \cdot F_f}; \quad (18)$$

– сравнить вычисленный и установленные индексы модуляции, определив относительную погрешность;

– получить и измерить спектр однотонового ЧМ сигнала с помощью симулятора Фурье анализа, установив в нем номер выходного узла схемы, подключенного к осциллографу, основную частоту (Fundamental frequency), равную 1 КГц, и число гармоник (Number of harmonics), равное 400;

– отобразить в отчете спектр (частотное представление) однотонового ЧМ сигнала;

– определить, как влияет на вид диаграммы и спектра однотонового ЧМ сигнала изменение частоты модулирующего (информационного, низкочастотного) сигнала;

– определить, как влияет на вид диаграммы и спектра однотонового ЧМ сигнала изменение индекса модуляции, последовательно устанавливая его равным 1; 2,4; 5; 10 и 100;

– сделать выводы о том, какими сигнальными демаскирующими признаками обладают однотоновые ЧМ сигналы.

6) Сделать выводы по проделанной работе, сравнив демаскирующие признаки АМ и ЧМ сигналов.

Задание 2.2. Исследовать сигнальные демаскирующие признаки квадратурного амплитудно-модулированного (КАМ) сигнала.

1) Открыть новый файл программы EWB и собрать схему, приведенную на рис. 8.

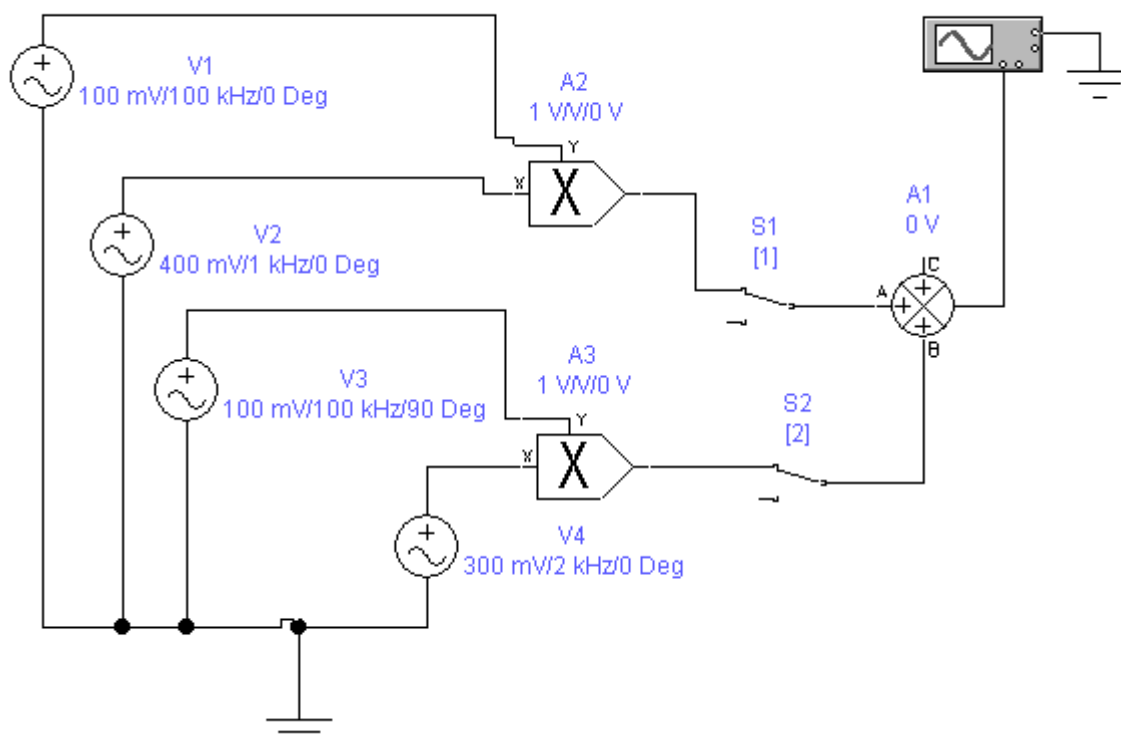


Рис. 8 – Схема исследования КАМ сигналов

2) **Установить параметры элементов схемы** в соответствии с величинами, указанными на рис. 8. Схема исследования, приведенная на рис. 8, содержит модели:

- источника однотоновых низкочастотных (модулирующих, управляющих) сигналов (V2 и V4);
- генераторов несущих высокочастотных колебаний (V1 и V3), имеющих одинаковую частоту колебаний, но сдвинутых по фазе относительно друг друга на 90° ;
- балансных модуляторов (умножители A2 и A3);
- сумматора напряжения (A1).

3) **Провести исследование квадратурного амплитудно-модулированного сигнала.** Для этого выполнить следующие действия:

- переключатели S1 (клавиша 1) и S2 (клавиша 2) установить в верхнее положение, тем самым подключив выходы балансных АМ модуляторов (A2 и A3) к входу сумматора (A1), выход которого подключен к входу осциллографа;
- включить осциллограф и настроить его для регистрации КАМ сигнала;
- измерить параметры и отобразить в отчете временную диаграмму или осциллограмму КАМ сигнала;
- получить и измерить спектр КАМ сигнала с помощью симулятора Фурье анализа, установив в нем номер выходного узла схемы, подключенного к осциллографу, основную частоту (Fundamental frequency), равную 1 КГц, и число гармоник (Number of harmonics), равное 200;
- отобразить в отчете спектр (частотное представление) КАМ

сигнала;

- сравнить внешний вид диаграммы и спектра КАМ сигнала с АМ сигналами, его составляющими; для этого, подключая по очереди с помощью переключателей S1 и S2 только один балансный модулятор к сумматору A1 и отключая другой, получить диаграммы и спектры АМ сигналов;

- определить, как влияет на вид диаграммы и спектра КАМ сигнала изменение частоты одного из модулирующих (информационных, низкочастотных) сигналов, последовательно устанавливая ее равной 500, 1000, 2000, 3000 и 4000 Гц;

- определить, как влияет на вид диаграммы и спектра КАМ сигнала изменение амплитуды одного из модулирующих (информационных, низкочастотных) сигналов, последовательно устанавливая его равным 100, 200, 300 и 400 мВ;

- сделать выводы о том, какими сигнальными демаскирующими признаками обладают КАМ сигналы.

Задание 2.3. Исследовать сигнальные демаскирующие признаки манипулированных сигналов.

1) ***Открыть новый файл программы EWB и собрать схему, приведенную на рис. 9.***

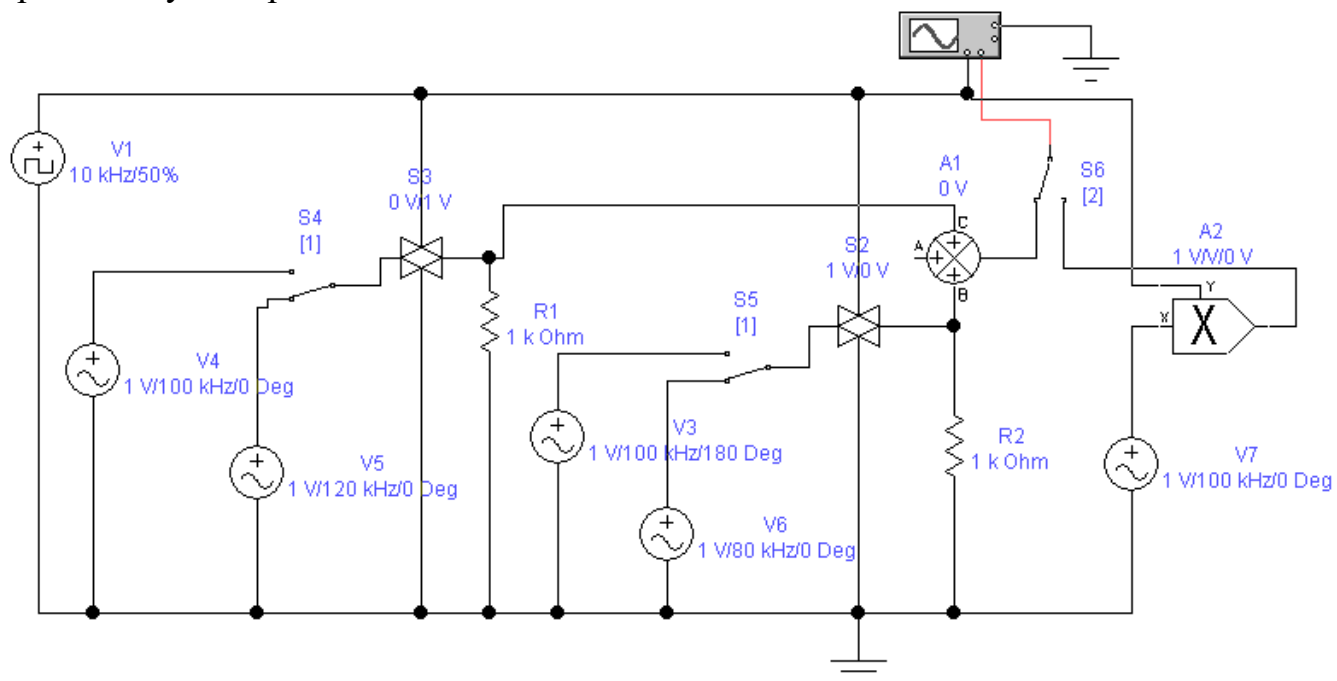


Рис. 9 – Схема исследования манипулированных сигналов

2) ***Установить параметры элементов схемы*** в соответствии с величинами, указанными на рис. 9. Схема исследования, приведенная на рис. 9, содержит модели:

- амплитудного модулятора (манипулятора), состоящего из балансного модулятора (A2), генератора несущего колебания (V7) и источника битовой последовательности на базе генератора тактовых импульсов (V1);

- частотного модулятора (манипулятора), состоящего из аналоговых

ключей (S3 и S2), нагруженных соответственно на сопротивления R1 и R2, сумматора напряжений (A2), генераторов несущих колебания (V5 и V6) и источника битовой последовательности на базе генератора тактовых импульсов (V1);

– фазового модулятора (манипулятора), состоящего из аналоговых ключей (S3 и S2), нагруженных соответственно на сопротивления R1 и R2, сумматора напряжений (A2), генераторов несущих колебания (V4 и V3) и источника битовой последовательности на базе генератора тактовых импульсов (V1).

3) Провести исследование амплитудно-манипулированного (АМн) сигнала. Для этого выполнить следующие действия:

– установить переключатель S6 (клавиша 2) в правое положение, тем самым подключив выход балансного АМ модулятора (A2) ко второму входу осциллографа;

– включить осциллограф и настроить его для АМн сигнала;

– измерить параметры и отобразить в отчете временную диаграмму или осциллограмму АМн сигнала;

– получить и измерить спектр АМн сигнала с помощью симулятора Фурье анализа, установив в нем номер выходного узла схемы, подключенного к второму входу осциллографа, основную частоту (Fundamental frequency), равную 1 КГц, и число гармоник (Number of harmonics), равное 200;

– отобразить в отчете спектр (частотное представление) АМн сигнала;

– определить, как влияет на вид диаграммы и спектра АМн сигнала изменение частоты битовой последовательности, последовательно устанавливая ее величину, равную 25%, 50 % и 75%;

– определить, как влияет на вид диаграммы и спектра АМн сигнала изменение амплитуды модулирующей битовой последовательности, устанавливая ее равной 0,5; 1 и 2 В;

– сделать выводы о том, какими сигнальными демаскирующими признаками обладают АМн сигналы.

4) Провести исследование частотно-манипулированного (ЧМн) сигнала. Для этого выполнить следующие действия:

– установить переключатель S6 (клавиша 2) в левое положение, а переключатели S4 и S5 (клавиша 2) в нижнее положение, тем самым соединив частотный манипулятор и подключив его выход (выход сумматора A1) ко второму входу осциллографа;

– включить осциллограф и настроить его для ЧМн сигнала;

– измерить параметры и отобразить в отчете временную диаграмму или осциллограмму ЧМн сигнала;

– получить и измерить спектр ЧМн сигнала с помощью симулятора Фурье анализа, установив в нем номер выходного узла схемы, подключенного к второму входу осциллографа, основную частоту (Fundamental frequency), равную 1 КГц, и число гармоник (Number of harmonics), равное 200;

- отобразить в отчете спектр (частотное представление) ЧМн сигнала;
- определить, как влияет на вид диаграммы и спектра ЧМн сигнала изменение частоты несущих колебаний, последовательно устанавливая их величины, равные 80 и 120 КГц, 85 и 115 КГц, 90 и 110 КГц;
- определить, как влияет на вид диаграммы и спектра ЧМн сигнала изменение частоты битовой последовательности, последовательно устанавливая ее величину, равную 25%, 50 % и 75%;
- определить, как влияет на вид диаграммы и спектра ЧМн сигнала изменение частоты модулирующей битовой последовательности, устанавливая ее равной 10 КГц, 16 КГц, 20 КГц;
- сделать выводы о том, какими сигнальными демаскирующими признаками обладают ЧМн сигналы.

5) Провести исследование фазово-манипулированного (ФМн) сигнала. Для этого выполнить следующие действия:

- установить переключатель S6 (клавиша 2) в левое положение, а переключатели S4 и S5 (клавиша 2) в верхнее положение, тем самым соединив фазовый манипулятор и подключив его выход (выход сумматора A1) ко второму входу осциллографа;
- включить осциллограф и настроить его для ФМн сигнала;
- измерить параметры и отобразить в отчете временную диаграмму или осциллограмму ФМн сигнала;
- получить и измерить спектр ФМн сигнала с помощью симулятора Фурье анализа, установив в нем номер выходного узла схемы, подключенного к второму входу осциллографа, основную частоту (Fundamental frequency), равную 1 КГц, и число гармоник (Number of harmonics), равное 200;
- отобразить в отчете спектр (частотное представление) ФМн сигнала;
- определить, как влияет на вид диаграммы и спектра ФМн сигнала изменение фазы несущих колебаний, последовательно устанавливая величину фазы генераторов (V4 и V3), равные 315 и 45 градусов, 270 и 90 градусов, 180 и 180 КГц;
- определить, как влияет на вид диаграммы и спектра ФМн сигнала изменение частоты битовой последовательности, последовательно устанавливая ее величину, равную 25%, 50 % и 75%;
- определить, как влияет на вид диаграммы и спектра ФМн сигнала изменение частоты модулирующей битовой последовательности, устанавливая ее равной 10 КГц, 16 КГц, 20 КГц;
- сделать выводы о том, какими сигнальными демаскирующими признаками обладают ФМн сигналы.

Задание 2.4. Исследовать сигнальные демаскирующие признаки GMSK сигнала.

- 1) **Открыть новый файл программы EWB и собрать схему, приведенную на рис. 10.**

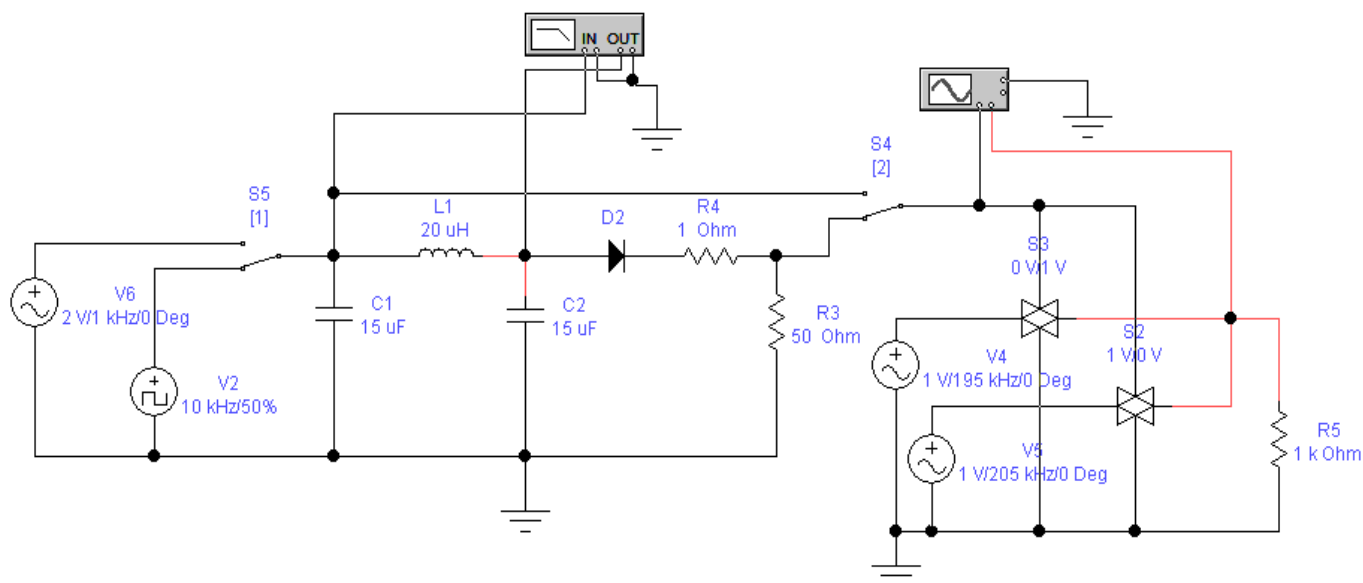


Рис. 10 – Схема исследования GMSK сигнала

2) **Установить параметры элементов схемы** в соответствии с величинами, указанными на рис. 10. Схема исследования, приведенная на рис. 10, содержит модели:

- источника битовой последовательности на базе генератора тактовых импульсов (V2);
- гауссовского фильтра нижних частот (ФНЧ) на базе элементов C1, C2 и L1;
- последовательного диодного ограничителя на базе элементов D2, R4, R3, ограничивающего сигнал ниже нулевого уровня и тем самым, формирующего колоколообразные импульсы;
- частотного модулятора (манипулятора) с индексом модуляции 0,5, состоящего из аналоговых ключей (S3 и S2), нагруженных на сопротивление R5, генераторов несущих колебания (V4 и V5).

3) **Провести исследование GMSK сигнала с индексом 0,5.** Для этого выполнить следующие действия:

- установить переключатель S5 (клавиша 1) в верхнее положение, тем самым подключив к входу гауссовского фильтра генератор синусоидального напряжения;
- включить построитель АЧХ и измерить АЧХ фильтра нижних частот, настроив вертикальную развертку в пределах $I = -80$ дБ, $F = 30$ дБ, а горизонтальную развертку – $I = 1$ кГц, $F = 1$ МГц;
- измерить параметры ФНЧ и отобразить в отчете его АЧХ;
- установить переключатель S5 (клавиша 2) в нижнее положение, тем самым подключив к входу гауссовского фильтра источник битовой последовательности;
- установить переключатель S4 (клавиша 2) в верхнее положение, тем самым подключив выход источника битовой последовательности к первому входу осциллографа и входу частотного манипулятора;
- включить осциллограф и настроить его для измерения битовой

последовательности и ее ЧМн сигнала;

- измерить параметры и отобразить в отчете временную диаграмму или осциллограмму битовой последовательности и ее ЧМн сигнала;

- получить и измерить ширину спектра ЧМн сигнала битовой последовательности с помощью симулятора Фурье анализа, установив в нем номер выходного узла схемы, подключенного к второму входу осциллографа, основную частоту (Fundamental frequency), равную 1 КГц, и число гармоник (Number of harmonics), равное 200;

- отобразить в отчете спектр (частотное представление) ЧМн сигнала битовой последовательности;

- установить переключатель S4 (клавиша 2) в нижнее положение, тем подключив выход гауссовского фильтра к первому входу осциллографа и входу частотного манипулятора;

- измерить параметры и отобразить в отчете временную диаграмму или осциллограмму гауссовской битовой последовательности и ее GMSK сигнала;

- получить и измерить ширину спектра GMSK сигнала с помощью симулятора Фурье анализа, установив в нем номер выходного узла схемы, подключенного к второму входу осциллографа, основную частоту (Fundamental frequency), равную 1 КГц, и число гармоник (Number of harmonics), равное 200;

- сравнить ширину спектров исследуемых сигналов;

- сделать выводы о том, какими сигнальными демаскирующими признаками обладают GMSK сигналы.

4) *Провести исследование GMSK сигнала с индексом 0,3.* Для этого выполнить следующие действия:

- рассчитать, воспользовавшись выражениями (14) – (16), частоту манипуляции, девиацию частоты, нижнюю и верхнюю частоты несущих колебаний манипулятора для частоты битовой последовательности, равной 24 КГц;

- с учетом полученных результатов изменить частоту битовой последовательности, нижнюю и верхнюю частоты генераторов несущих колебаний;

- установить переключатель S5 (клавиша 1) в верхнее положение, тем самым подключив к входу гауссовского фильтра генератор синусоидального напряжения;

- изменяя одновременно емкости C1 и C2, с помощью построителя АЧХ настроить резонанс ФНЧ на частоту битовой последовательности;

- отобразить в отчете новую АЧХ ФНЧ;

- установить переключатель S5 (клавиша 2) в нижнее положение, тем самым подключив к входу гауссовского фильтра источник битовой последовательности;

- установить переключатель S4 (клавиша 2) в нижнее положение, тем подключив выход гауссовского фильтра к первому входу осциллографа и входу частотного манипулятора;

- измерить параметры и отобразить в отчете временную диаграмму или осциллограмму гауссовской битовой последовательности и ее GMSK сигнала;

- получить и измерить ширину спектра GMSK сигнала с помощью симулятора Фурье анализа, установив в нем номер выходного узла схемы, подключенного к второму входу осциллографа, основную частоту (Fundamental frequency), равную 1 КГц, и число гармоник (Number of harmonics), равное 200;

- сравнить ширину спектров исследуемых сигналов;

- сделать выводы о том, какими сигнальными демаскирующими признаками обладают GMSK сигналы.

Задание 2.5. Составить отчет о проделанной работе. В отчете отобразить:

- тему и цель работы, порядок ее выполнения;

- принципиальные схемы исследования;

- временные диаграммы сигналов для различных видов модуляции и манипуляции;

- спектры сигналов для различных видов модуляции и манипуляции;

- требуемые расчеты, и полученные зависимости в виде таблиц или графиков;

- сделанные по результатам работы выводы.

Задание 2.6. Защитить отчет по второй части, проделанной лабораторной работы.

**Задание обучаемым для самостоятельной учебной работы
при подготовке к лабораторной работе:**

1. Закрепить и углубить знания, полученные на лекции, для этого изучить конспект лекций и рекомендуемую литературу.
2. Изучить методические указания к лабораторной работе и подготовить отчет по лабораторной работе согласно методическим указаниям.

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1-3

Тема № 5. ИССЛЕДОВАНИЕ ИСТОЧНИКОВ ОПАСНЫХ СИГНАЛОВ

ЛАБОРАТОРНЫЕ РАБОТЫ № 4-6.

Тема 1: Характеристика угроз безопасности информации в автоматизированных информационных системах.

Тема 2: Исследование сигнальных демаскирующих признаков радиоэлектронных средств

Тема 3: Акустические каналы утечки речевой информации

Подтема: Исследование источников опасных сигналов

Время – 6 часов.

Формируемые компетенции: ОПК-4, ОПК-11, ОПК-2.1.

УЧЕБНЫЕ ВОПРОСЫ:

- 1. Исследование побочных электрических сигналов, возникающих за счет эффекта акустоэлектрического преобразования.**
- 2. Моделирование физического эффекта паразитной генерации высокочастотных сигналов.**
- 3. Исследование физического эффекта паразитной генерации высокочастотных сигналов.**

СОДЕРЖАНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

Вводная часть

Существует большая группа источников информации, таких как основные и вспомогательные технические средства и системы, от которых могут распространяться несанкционированные сигналы с защищаемой информацией и которые возникают случайно, или создаются злоумышленниками. Так как эти сигналы несут угрозу безопасности информации, то их условно называют опасными.

Все многообразие типов технических средств, выступающих в роли источников опасных сигналов, по физической природе их возникновения делится на следующие группы (классы):

- акустоэлектрические преобразователи;
- излучатели низкочастотных сигналов;
- излучатели высокочастотных сигналов;
- паразитные связи и наводки.

Опасные сигналы в виде электромагнитных излучений и электрических наводок в проводах и линиях коммуникаций, несмотря на их небольшой уровень, могут распространяться за пределы контролируемой зоны организации и быть перехвачены злоумышленниками.

Следовательно, бакалавры по направлению информационной безопасности должны владеть методами и средствами выявления угроз безопасности в автоматизированных информационных системах путем моделирования источников опасных сигналов, измерения их величины и оценки угрозы. Для достижения этой цели в первом учебном вопросе исследуются побочные электрические сигналы, возникающие за счет эффекта акустоэлектрического преобразования, во втором вопросе – эффект паразитной генерации высокочастотных сигналов.

Проверка подготовленности обучаемых к лабораторной работе

Перечень контрольных вопросов:

- 1) Источники опасных сигналов в радиоэлектронных средствах.
- 2) Высокочастотные и низкочастотные побочные излучения в технических средствах и системах.
- 3) Принцип возникновения паразитной генераций усилителей.
- 4) Виды паразитных связей между цепями технических средств и систем.
- 5) Взаимная индукция (определение).
- 6) Переходное затухание, его единицы измерения.
- 7) Причины возникновения взаимной индукции.
- 8) Принципы наведения ЭДС: за счет магнитного поля или электромагнитной волны.
- 9) Причины и порядок применения нагрузочных сопротивлений.

ВОПРОСЫ, ПОДЛЕЖАЩИЕ ИССЛЕДОВАНИЮ

1. Исследование побочных электрических сигналов, возникающих за счет эффекта акустоэлектрического преобразования

Краткие теоретические или справочно-информационные материалы

Побочные наводки, возникающие за счет наличия преобразовательных акустоэлектрических элементов в цепях различных технических устройств, находящихся в выделенном помещении, опасны тем, что ими может воспользоваться злоумышленник без проникновения в помещение (или охраняемую зону), без установки специальных подслушивающих устройств.

Подобные каналы утечки информации наиболее часто возникают на основе так называемых акустоэлектрических преобразователей.

Акустоэлектрический преобразователь – это устройство, преобразующее акустическую энергию (т.е. энергию упругих волн в воздушной среде) в электромагнитную энергию в схемах тех устройств, в которых находится акустоэлектрические преобразователи.

Одним из наиболее распространенных представителей акустоэлектрических преобразователей являются электродинамические громкоговорители (см. рис. 1).

Эти динамики предназначены для преобразования электрических сигналов в акустические. Однако они являются классическим примером принципа взаимности, то есть обладают обратным микрофонным эффектом, являясь одновременно достаточно хорошими акустоэлектрическими преобразователями.

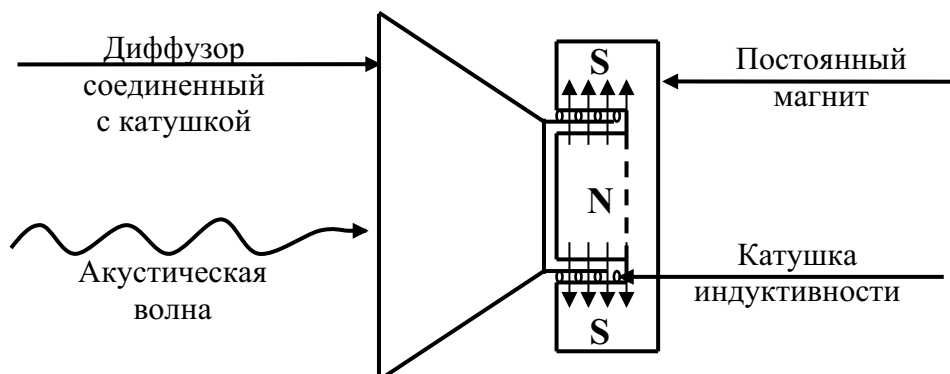


Рис. 1 – Схема электродинамического громкоговорителя

Воздействие акустических сигналов на диффузор динамика (см. рис. 1) приводит к преобразованию акустической энергии в механическую и изменению положения катушки в магнитном поле, что приводит к появлению опасного электрического сигнала в катушке динамика, напряжение которого равно

$$U_{oc} = P_{ак} B L S / Z_{мех} \quad (1)$$

где $P_{ак}$ – акустическое давление информативного сигнала; B – магнитная индукция; L – длина проводника катушки, движущегося в магнитном поле B ; S – площадь поверхности диффузора динамика; $Z_{мех}$ – механическое сопротивление системы динамика.

Достаточно большая площадь диффузора динамика обеспечивает подобным преобразователям достаточно высокую чувствительность к акустическому воздействию (2 – 3 мВ/Па) и сравнительно равномерную амплитудно-частотную характеристику для речевого сигнала.

Опасные сигналы на концах катушки достигают величин в 5 -15 мВ. Этой величины достаточно для распространения наведенных сигналов за пределы помещения, здания и даже территории. Поэтому неработающие, но непосредственно подключенные к радиотрансляционной сети громкоговорители могут выполнять функцию микрофона и передавать информацию разговоров в помещении на достаточно большое расстояние.

Содержание практической работы, выполняемой студентами в ходе занятия

1. Описание лабораторного оборудования:

- учебно-действующий макет акустоэлектрических преобразователей;
- осциллограф GOS-620FQ;
- генератор НЧ сигналов GOS-810;
- блок питания;
- элементы коммутации;

– эмулятор лабораторного оборудования для исследования эффекта акустоэлектрического преобразования.

Учебно-действующий макет (см. рис. 2) представляет собой линейку расположенных рядом друг с другом динамиков с разной площадью диффузоров и внутренними сопротивлениями, вдоль которых на специальной каретке перемещается источник сигнала (излучающий динамик), на который подается входной сигнал с генератора звуковой частоты. Для контроля сигнал одновременно подаётся и на осциллограф.

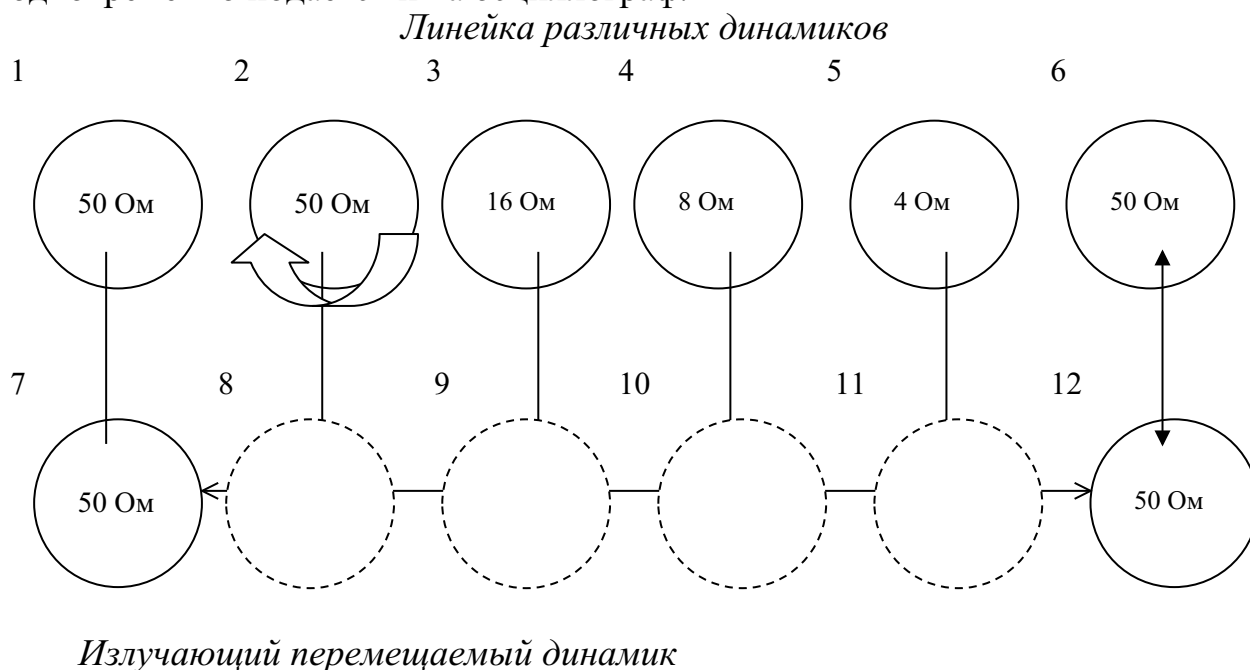


Рис. 2 – Учебно-действующий макет акустоэлектрических преобразователей

Излучающий динамик имеет внутреннее сопротивление, равное 50 Ом, и диаметр диффузора – 2,8 см. Он перемещается относительно приемных динамиков с помощью специальной каретки, ручка которой размещена с правой стороны макета.

Макет содержит ряд приемных динамиков, один из которых имеет диаметр диффузора, равный 2,8 см, второй – 4 см, а остальные – 5 см. Поскольку промышленностью выпускаются динамики с внутренним электрическим сопротивлением, равным 50, 16, 8 и 4 Ом, то данный макет содержит всю эту линейку динамиков.

На 2-м динамике слева имеется возможность изменять угол прихода звуковой волны путем вращения принимающего динамика. Крайний справа динамик имеет возможность перемещаться, обеспечивая изменение расстояние от источника сигнала (излучающего динамика) до приемника, с помощью каретки, ручка которой размещена на верхней крышке макета.

Подключение того или иного приемного динамика осуществляется за счет переключателей ТВ1, ТВ2, ТВ3, ТВ4. С выхода динамиков сигнал через усилитель низкой частоты ($K_{yc} = 70$) подается на осциллограф для измерения его величины.

2. Требования безопасности при выполнении работы:

I. Перед началом выполнения лабораторной работы:

3. Изучить оборудование и рабочее место.
4. Получить разрешение к выполнению лабораторных работ от руководителя занятий или лаборанта.

II. Во время выполнения лабораторных работ:

Убедиться, что на измерительных приборах переключатели установлены в исходном положении ручек, на минимальное напряжение и максимальные пределы измерения.

Включать питающие напряжения и собранные схемы только после разрешения руководителя занятий или лаборанта и предупреждения всех работающих.

Проверять наличие питающих напряжений и проводить измерения электрических величин только с помощью соответствующих измерительных приборов, одной рукой, после установки на них максимально ожидаемого результата и рода измеряемой величины.

ВНИМАНИЕ!

- Не прикасаться к открытым токоведущим частям, проводникам, клеммам и зажимам, не облокачиваться на приборы, не прикасаться к батареям, не отвлекаться от измерений, не производить изменений в схеме и не оставлять без наблюдения цепь, находящуюся под напряжением.
- При работе с катушками индуктивности и конденсаторами не трогать их и соединительные провода, так как вследствие резонанса могут возникнуть большие токи и напряжение.
- При обнаружении неисправностей в измерительных приборах **немедленно** отключить источники питания и доложить об этом руководителю занятий или лаборанту.

III. По окончании выполнения лабораторных работ:

1. Докладать руководителю занятий или лаборанту о завершении работ.
2. Обесточить собранные схемы, разобрать их (если это предусмотрено) и выключить контрольно-измерительные приборы.
3. Привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

ПРИ РАБОТЕ ЗАПРЕЩАЕТСЯ:

- | |
|--|
| <ul style="list-style-type: none">• производить самостоятельное включение автоматов защиты, заменять предохранители, устранять неисправности и повреждения;• проводить какие-либо переключения, соединения, не предусмотренные инструкциями по выполнению лабораторных работ. |
|--|

ПРИ АВАРИЙНЫХ СИТУАЦИЯХ И НЕСЧАСТНЫХ СЛУЧАЯХ:

- | |
|---|
| <ul style="list-style-type: none">• немедленно отключить автоматы защиты, доложить руководителю занятий и действовать согласно его указаний;• при поражении электрическим током оказать первую помощь в соответствии с принятой методикой до прибытия врача. |
|---|

ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ:

- лица, нарушившие требования инструкции отстраняются от выполнения лабораторных работ и допускаются только после сдачи зачета по правилам и мерам безопасности;
- при выводе из строя приборов и оборудования лаборатории по вине лица, проводившего работы и в случае нарушения требования инструкции, они несут материальную ответственность в соответствии с действующим законодательством РФ.

3. Задание для работы

10) Собрать схему исследования.

11) Исследовать зависимость величины опасного сигнала от площади диффузора акустоэлектрического преобразователя (динамика)

12) Исследовать зависимость величины опасного сигнала от интенсивности входного акустического сигнала.

13) Исследовать зависимость величины опасного сигнала от расстояния между источником акустического сигнала и акустоэлектрическим преобразователем.

14) Исследовать зависимость величины опасного сигнала от угла прихода звуковой волны φ .

15) Исследовать зависимость величины опасного сигнала от величины электрического сопротивления акустоэлектрического преобразователя.

16) Оформить отчет о проделанной работе в соответствии с требованиями, изложенными в описании работы.

4. Порядок выполнения работы

Задание 1.1. Собрать схему исследования.

Для проведения исследований необходимо:

1) Собрать блок-схему согласно рис. 3, соединив гнездо «ВХОД» макета с выходом генератора GOS-810 и входом 1-го канала осциллографа GOS-620FQ, а гнездо «ВЫХОД» макета – с входом 2-го канала осциллографа;

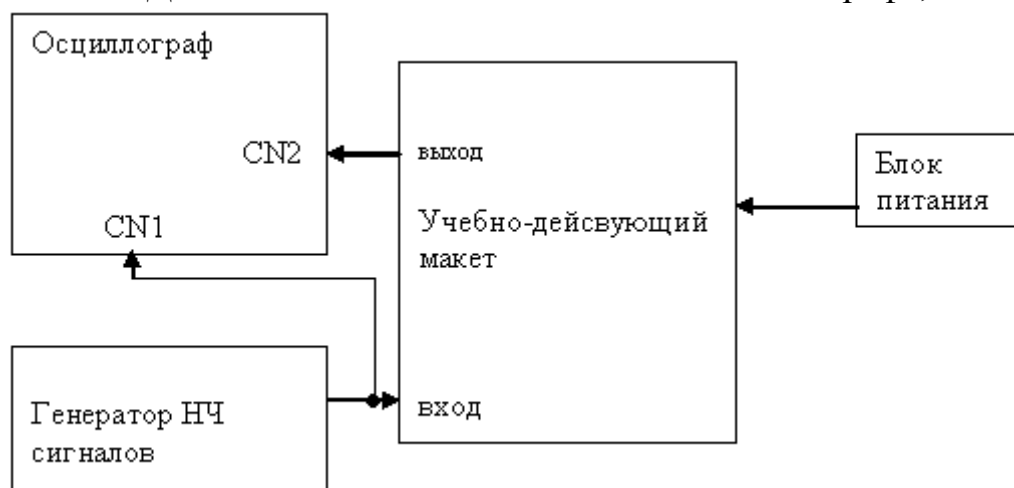


Рис 3 – Блок-схема для проведения исследований

2) Установить переключатели макета ТВ 1,2,3,4 в среднее положение.
3) На блоке питания выставить напряжение 9 В, выход блока питания подключить к гнезду макета «Питание 9В».

4) Установить на генераторе НЧ GOS-810 ручку «AMPLITYDE» в крайнее левое положение.

5) Включить питание на осциллографе и генераторе НЧ.

6) Каретку перемещения излучающего динамика на макете (ручка справа) установить в крайнее левое положение, а ручку изменения расстояния между динамиками (излучающим и приемным) на тыльной стороне макета выдвинуть на максимальное расстояние.

7) На генераторе НЧ ручкой «FREQANCE» установить частоту выходного сигнала $F_c = 1500$ Гц, а переключателем «ATTENUATOR» и ручкой «AMPLITYDE» - напряжение $U_c = 10$ мВ, контролируя его величину на экране осциллографа по 1-му каналу.

Задание 1.2. Исследовать зависимость величины опасного сигнала от площади диффузора акустоэлектрического преобразователя (динамика).

Для этого произвести следующие действия (операции):

- 1) Установить переключатели макета ТВ1 и ТВ3 в верхнее положение, а ТВ 4 – в нижнее.
- 2) Каретку перемещения излучающего динамика на макете (ручка справа) установить в крайнее левое положение.
- 3) По второму каналу осциллографа измерить величину опасного сигнала U_c для динамика с диаметром диффузора $d = 5$ см.
- 4) Переключатели ТВ 3 и ТВ4 установить в среднее положение.
- 5) Переместить каретку перемещения динамика на макете (ручка справа) вправо во второе положение, ТВ 3,4 установить в верхнее положение.
- 6) Измерить величину опасного сигнала U_c при $d = 4$ см.
- 7) Переключатели ТВ 3 ,4 установить в среднее положение.
- 8) Переместить каретку в крайнее правое положение, переключатель ТВ3 установить в нижнее, ТВ4 – в верхнее положение.
- 9) Измерить величину сигнала U_c при $d = 2,8$ см.
- 10) Измеренные значения опасных сигналов занести в таблицу 1.

Таблица 1.



Диаметр (см)	5,0	4,0	2,8
Площадь (см ²)	19,6	12,6	6,2
U_c (мВ)			

- 11) По результатам измерений построить график зависимости величины опасного сигнала U_c от площади диффузора S динамика.
- 12) Сделать вывод по результатам проделанной работы.

Задание 1.3. Исследовать зависимость величины опасного сигнала от интенсивности входного акустического сигнала.

Для этого произвести следующие действия (операции):

- 1) Переключатели макета ТВ1 и ТВ4 установить в верхнее положение, а ТВ 3 – в нижнее.
- 2) По второму каналу осциллографа измерить величину опасного сигнала U_c для значения входного сигнала $U_B = 10$ мВ.
- 3) Изменяя напряжение входного сигнала U_B с помощью ручки «AMPLITUDE» НЧ генератора с шагом 5мВ в интервале от 10 мВ до 30 мВ, измерить значения амплитуды опасного сигнала U_c по второму каналу осциллографа.
- 4) Измеренные значения занести с таблицу 2.

Таблица 2.

U_B (мВ)	10	15	20	25	30
U_c (мВ)					
J_B (мВт/см ²)					



- 5) Рассчитать величину интенсивности входного акустического сигнала J_B

по формулам:

$$J_B = P_B/S \text{ (мВт/см}^2\text{)}, \text{ где } P_B = U_B^2/R. \quad (2)$$

при условии, что сопротивление динамиков $R=50$ Ом, а площадь диффузора $d = 2,8$ см.

6) По результатам измерений и расчетов построить график зависимости напряжения опасного сигнала U_c от интенсивности входного акустического сигнала.

7) Сделать вывод по результатам проделанной работы.

Задание 1.4. Исследовать зависимость величины опасного сигнала от расстояния между источником акустического сигнала и акустоэлектрическим преобразователем.

Для этого произвести следующие действия (операции):

1) Выставить напряжение опасного сигнала U_c равное 10 мВ.

2) Переключатель TIME/DIV по 2 каналу осциллографа установить в положение 0,2.

3) Ручку на задней стенке макета переместить вперед до упора, при этом расстояние между источником звука (излучающим динамиком) и приемным динамиком L равно 5мм.

4) Установить переключатель ТВ3 в нижнее положение, а ТВ4 – в верхнее.

5) Изменяя ручкой расстояние между источником звука и приемным динамиком через 5 мм, каждый раз измерить по 2 каналу осциллографу величину опасного сигнала U_c .

6) Измеренные значения занести в таблицу 3.



Таблица 3.

Расстояние L (мм)	5	10	15	20	25	30
U_c (мВ)						

7) По результатам измерений построить график зависимости величины сигнала U_c от расстояния L до источника звука.

8) Сделать вывод по результатам проделанной работы.

Задание 1.5. Исследовать зависимость величины опасного сигнала от угла прихода звуковой волны φ .

Для этого произвести следующие действия (операции):

1) Переместить каретку с излучающим динамиком во второе положение.

2) Установить переключатели ТВ3 и ТВ4 в верхнее положение.

3) Последовательно измерить по второму каналу осциллографа величину напряжения опасного сигнала U_c при углах 0° , 15° , 30° , 45° , 60° , 75° , 90° .

4) Измеренные значения занести в таблицу 4.



Таблица 4

Угол φ (град)	0	15	30	45	60	75	90
U_c (мВ)							

5) По результатам измерений построить график зависимости величины сигнала U_c от угла прихода звуковой волны φ .

6) Сделать вывод по результатам проделанной работы.

Задание 1.6. Исследовать зависимость величины опасного сигнала от величины электрического сопротивления акустоэлектрического преобразователя.

Для этого произвести следующие действия (операции):

- 1) Вернуть угол прихода звуковой волны равный 0° .
- 2) Измерить величину напряжения опасного сигнала U_c при $R_{дин} = 50$ Ом.
- 3) Перевести переключатель ТВ 2 в верхнее положение.
- 4) Измерить U_c при $R_{дин} = 16$ Ом.
- 5) Перевести переключатели ТВ2, ТВ3 и ТВ4 в среднее положение, переместить каретку перемещения динамиков в положение 3.
- 6) Установить переключатели ТВ3 и ТВ4 в нижнее положение.
- 7) Измерить U_c при $R_{дин} = 8$ Ом.
- 8) Установить переключатель ТВ2 в нижнее положение.
- 9) Измерить U_c при $R_{дин} = 4$ Ом.
- 10) Измеренные значения занести в таблицу 5.



Таблица 5.

$R_{дин}$ (Ом)	50	16	8	4
U_c (мВ)				

11) По результатам измерений построить график зависимости величины сигнала U_c от сопротивления динамика $R_{дин}$.

12) Сделать вывод по результатам проделанной работы.

Задание 1.7. Оформить отчет о выполнении лабораторной работы.

В отчете отобразить:

- тему и цель работы, порядок ее выполнения;
- математическую модель (методику), на базе которой проводилось лабораторные исследования;
- графики зависимости вероятности обнаружения РЭС от изменения его мощности излучения, КНД приемной антенны, длины волны и вероятности ложной тревоги;
- графики зависимости максимальной дальности обнаружения РЭС средствами РТР от мощности шума;
- значение максимальной мощности излучения передатчика, при которой РЭС может быть обнаружено только в пределах контролируемой зоны.
- по результатам работы сделать выводы о влиянии сигнальных демаскирующих признаков и параметров РЭС на вероятность их обнаружения W_o .

Задание 1.8. Защитить отчет по первой части проделанной лабораторной работы.

2 - 3. Моделирование и исследование физического эффекта паразитной генерации высокочастотных сигналов

Краткие теоретические или справочно-информационные материалы

Паразитная генерация может возникнуть при определенных условиях в усилителях и логических элементах дискретной техники. Логический элемент рассматривается в данном контексте как усилитель с очень высоким коэффициентом усиления.

Математическую модель усилителя независимо от числа каскадов усиления можно представить в виде комплексной передаточной функции $K_{yc}(\omega)e^{j\varphi_{yc}(\omega)}$, где $K_{yc}(\omega)$ и $\varphi_{yc}(\omega)$ - зависящие от частоты $\omega = 2\pi f$ коэффициент усиления и фаза выходного сигнала по отношению к входному.

В усилителе фаза выходного сигнала для нечетного числа каскадов усиления изменяется на 180° , а при четном числе каскадов совпадает с фазой входного сигнала.

Поскольку между элементами усилителя всегда существуют емкостные, индуктивные и гальванические паразитные связи, то на входе усилителя наряду с усиливаемым внешним сигналом присутствуют сигналы, проникшие во входные цепи через паразитную обратную связь, в том числе с выхода усилителя. Паразитную обратную связь можно также представить математической моделью $K_{oc}(\omega)e^{j\varphi_{oc}(\omega)}$.

Обобщенная математическая модель усилителя с обратной связью представлена на рис. 4.

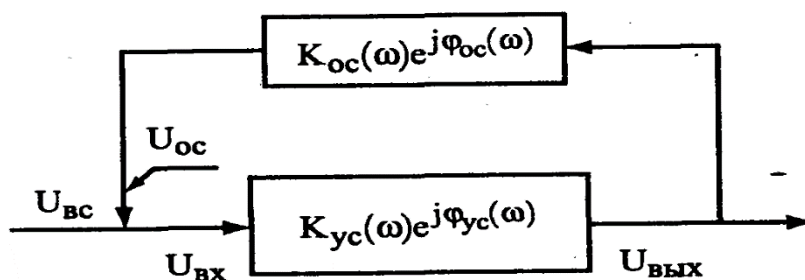


Рис. 4 – Модель усилителя с обратной связью

Связь между выходом и входом усилителя описывается уравнением:

$$U_{\text{вых}} = (U_{\text{вс}} + U_{\text{ос}}) K_{yc}(\omega)e^{j\varphi_{yc}(\omega)} = [U_{\text{вс}} + U_{\text{вых}} K_{oc}(\omega)e^{j\varphi_{oc}(\omega)}] K_{yc}(\omega)e^{j\varphi_{yc}(\omega)}. \quad (3)$$

Режим усиления переходит в режим генерации, когда выходной сигнал достигает максимального значения и поддерживается на этом уровне независимо от $U_{\text{вх}}$. Это условие выполняется при нулевом значении знаменателя указанного выше выражения. Следовательно, *для возникновения режима генерации необходимо выполнить два условия:*

$$1) K_{oc}(\omega) = 1/K_{yc}(\omega);$$

$$2) \varphi_{oc}(\omega) = -\varphi_{yc}(\omega).$$

Первое условие определяет минимально необходимую для возникновения паразитной генерации величину коэффициента паразитной обратной связи. Чем выше коэффициент усиления усилителя, тем меньший коэффициент паразитной обратной связи создает предпосылки для возникновения генерации. Например, если $K_{oc} = 10$, то для возникновения генерации необходимо проникновение 0,1 части выходного сигнала на вход усилителя. Для усилителя с $K_{yc} = 100$ достаточно поступления на его вход 0,01 части выходного сигнала. Эта зависимость объясняет возможность паразитной генерации в логических элементах дискретной техники. Высокий коэффициент усиления логического элемента и высокая частота спектральных составляющих фронта дискретного сигнала создают благоприятные условия для возникновения паразитной генерации в логических элементах.

Второе условие предусматривает, что изменение фазы сигнала обратной связи должно быть противоположно величине фазового сдвига усилителя. Это означает, что фазы внешнего сигнала и сигнала обратной связи должны быть приблизительно равными. **Обратная связь**, при которой фаза сигнала на входе усилителя совпадает с фазой сигнала обратной связи, **называется** положительной, а когда фазы этих сигналов противоположные – отрицательной. Если положительная обратная связь способствует паразитной генерации, то отрицательная, наоборот, повышает стабильность работы усилителя, но за счет некоторого снижения напряжения на выходе усилителя. Поэтому в усилителях с высоким коэффициентом усиления для исключения паразитной генерации создают между каскадами отрицательную обратную связь, а также применяют комплекс мер по уменьшению паразитных связей. С этой целью при монтаже пользуются короткими экранированными провода, элементы входных и выходных цепей разносят на максимально возможное расстояние, экранируют трансформаторы усилителей, в цепи питания предварительных каскадов устанавливают RC-фильтры низких частот, усилительные каскады размещают в одну линию и др.

Опасность паразитной генерации состоит также в том, что она часто возникает на частотах выше рабочего диапазона и без специальных исследований не обнаруживается. Действительно, с ростом частоты обрабатываемых сигналов уменьшаются значения паразитных емкостных и индуктивных сопротивлений между каскадами. В результате этого увеличиваются K_{oc} и сдвиг фазы сигналов, прошедших через паразитные связи. Поэтому возможность выполнения условий генерации в усилителе на частотах, превышающих верхнюю частоту рабочего диапазона частот усилителя, повышается. Хотя на этой частоте полезные сигналы на вход усилителя не подаются, но на его входе присутствуют сигналы, обусловленные тепловым шумом и проникшие через паразитную обратную связь. Любая шумовая реализация на входе усиливается усилителем и частично возвращается через паразитную обратную связь на его вход. При равенстве фаз величина суммарного сигнала на входе усилителя повышается, что приводит к росту

сигнала на выходе усилителя. Следствием этого является увеличение сигнала U и дальнейшее увеличение сигнала на входе усилителя и т.д. Происходит лавинообразный процесс нарастания амплитуды сигнала на входе и выходе усилителя, завершаемый процессом непрерывной генерации на резонансной частоте. Поэтому не рекомендуется, например, применять в усилителях низкой частоты высокочастотные транзисторы, которые усиливают шумы с частотами выше верхней границы рабочего диапазона частот.

Паразитная генерация усилителя или логического элемента *создает угрозу информации*, если происходит его модуляция паразитного высокочастотного колебания информационными сигналами. Это явление возникает в случае, если цепи паразитного генератора содержат акустоэлектрические преобразователи или в них попадают опасные сигналы от других случайных акустоэлектрических преобразователей усилителя.

Содержание практической работы, выполняемой студентами в ходе занятия

1. Описание лабораторного оборудования:

– ПЭВМ с программным редактором схематического моделирования «Electronics Workbench» (EWB), версия не ниже 5.12.

2. Требования безопасности при выполнении работы приведены на стр. 5.

3. Задание для работы

- 1) Исследовать эффект паразитной генерации на транзисторном усилителе.
- 2) Исследовать эффект паразитной генерации на операционном усилителе.
- 3) Исследовать эффект паразитной генерации на логических элементах.
- 4) Составить отчет о проделанной работе в соответствии с требованиями, изложенными в описании работы.

4. Порядок выполнения работы

Задание 2.1. Исследовать эффект паразитной генерации на транзисторном усилителе.

- 1) ***Запустить программу EWB и собрать схему***, приведенную на рис. 5.
- 2) ***Установить параметры элементов схемы*** в соответствии с величинами, указанными на рис. 5. Схема исследования, содержит:
 - источник гармонического напряжения (сигнала) на элементе V3;
 - источник электропитания в виде аккумуляторной батареи V4;
 - транзисторный усилитель, собранный на биполярном транзисторе Q1, резисторах R1 – R4 и конденсаторах C5, C9;
 - колебательного контура, состоящего из катушки индуктивности L1, и конденсаторов C6, C7;
 - цепь обратной положительной связи, образуемая за счет паразитной емкости C8.

Усилитель и колебательный контур имеет гальваническую связь через общий (заземляющий) провод. Колебательный контур и паразитный конденсатор подключаются к усилителю с помощью переключателей S1 и S2,

управляемых клавишей «Пробел».

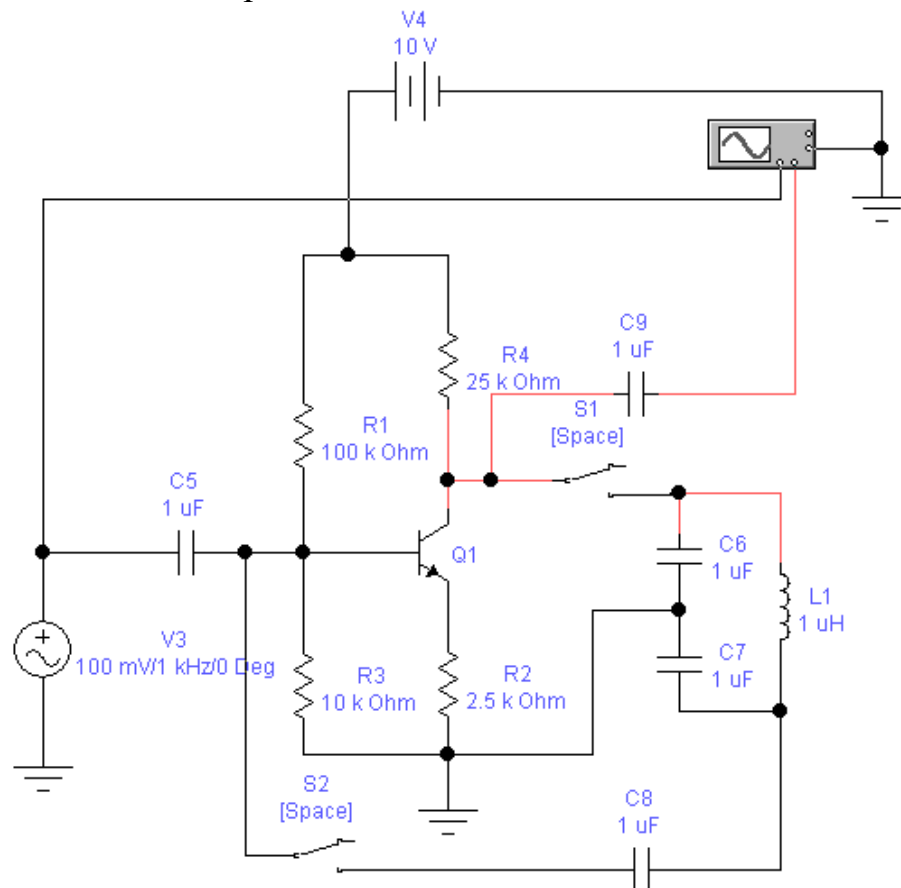


Рис. 5 – Схема исследования эффекта паразитной генерации на транзисторном усилителе

3) **Включить эмулятор EWB**, убедиться в работоспособности схемы. Для этого двойным щелчком **открыть осциллограф**, и его **настроить** на регистрацию отображения аналогового входного и выходного усиленного сигналов.

4) **Измерить** с помощью осциллографа **частоту** входного и усиленного выходного сигналов.

5) **Определить коэффициент усиления** транзисторного усилителя, предварительно измерив амплитуды напряжения входного и выходного сигналов.

6) **Отобразить в отчете осциллограммы** входного и усиленного выходного сигналов.

7) **Сделать выводы** о работе усилителя.

8) Нажав клавишу «Пробел» с помощью переключателей S1 и S2, **сымитировать** образование паразитных емкостей, которые подключают колебательный контура к коллекторной цепи и к цепи базы усилителя, образуя **паразитную цепь положительной обратной связи**.

9) **Произвести** с помощью осциллографа **наблюдение эффекта паразитной генерации**.

10) **Отобразить в отчете осциллограммы** входного и выходного сигналов усилителя.

- 11) **Измерить** с помощью осциллографа **частоту выходного сигнала**.
- 12) **Сделать выводы** по результатам проделанной работы.

Задание 2.2. Исследовать эффект паразитной генерации на операционном усилителе.

- 1) **Запустить программу EWB** и собрать схему, приведенную на рис. 6.

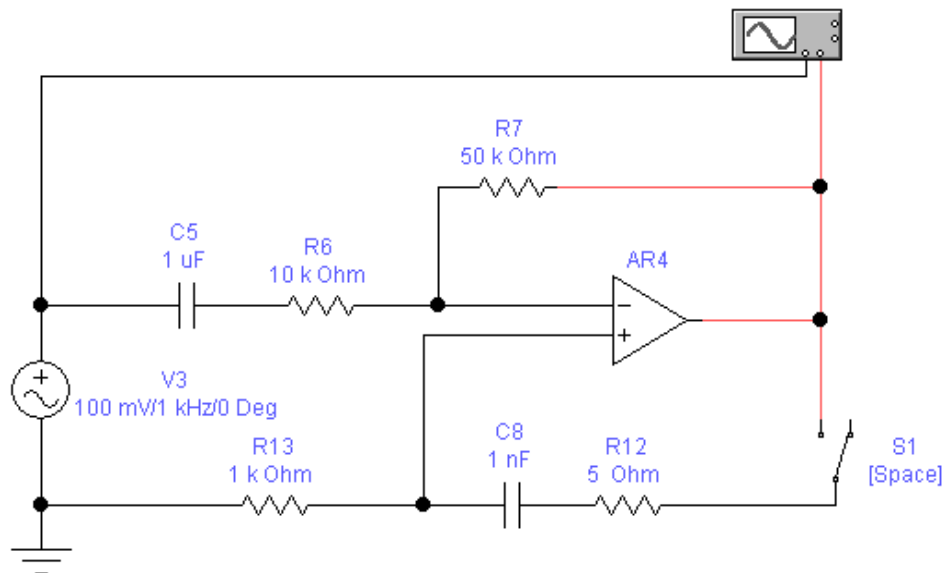


Рис. 6 – Схема исследования эффекта паразитной генерации на операционном усилителе

- 2) **Установить параметры элементов схемы** в соответствии с величинами, указанными на рис. 6. Схема исследования, содержит:

- источник гармонического напряжения (сигнала) на элементе V3;
- усилитель, собранный на операционном усилителе AR4, резисторах R6, R7, R13 и конденсаторе C5;
- цепь обратной положительной связи, образуемой за счет сопротивления R12 и емкости C8.

Цепь обратной положительной связи подключается к усилителю с помощью переключателя S1, управляемого клавишей «Пробел».

- 3) **Включить эмулятор EWB**, убедиться в работоспособности схемы. Для этого двойным щелчком **открыть осциллограф**, и его **настроить** на регистрацию отображения аналогового входного и выходного усиленного сигналов.

- 4) **Измерить** с помощью осциллографа **частоту** входного и усиленного выходного сигналов.

- 5) **Определить коэффициент усиления** операционного усилителя, предварительно измерив амплитуды напряжения входного и выходного сигналов.

- 6) **Отобразить в отчете осциллограммы** входного и усиленного выходного сигналов.

- 7) **Сделать выводы** о работе усилителя.

- 8) Нажав клавишу «Пробел» с помощью переключателя S1,

сымитировать образование паразитной емкости, которая образует **паразитную цепь положительной обратной связи**.

9) **Произвести** с помощью осциллографа **наблюдение эффекта паразитной генерации**.

10) **Отобразить в отчете осциллограммы** входного и выходного сигналов усилителя.

11) **Измерить** с помощью осциллографа **частоту выходного сигнала**.

12) **Изменить параметры элементов** цепи R12, R13 и C8 в соответствии с указанным преподавателем вариантом (см. табл. 6), и **повторить выполнение пунктов 8 – 11** задания.

Таблица 6 – Индивидуальные исходные данные для задания 2.2.

№ варианта	R12, Ом	C8, нФ	R13, Ом
1.	5	5	900
2.	5	120	10
3.	5	4	900
4.	5	115	10
5.	3	3	900
6.	3	110	10
7.	3	2	900
8.	3	95	10
9.	2	0,5	900
10.	2	90	10
11.	2	0,2	900
12.	2	80	10

13) **Сделать выводы** по результатам проделанной работы.

Задание 2.3. Исследовать эффект паразитной генерации на логических элементах.

1) **Запустить программу EWB и собрать схему**, приведенную на рис. 7.

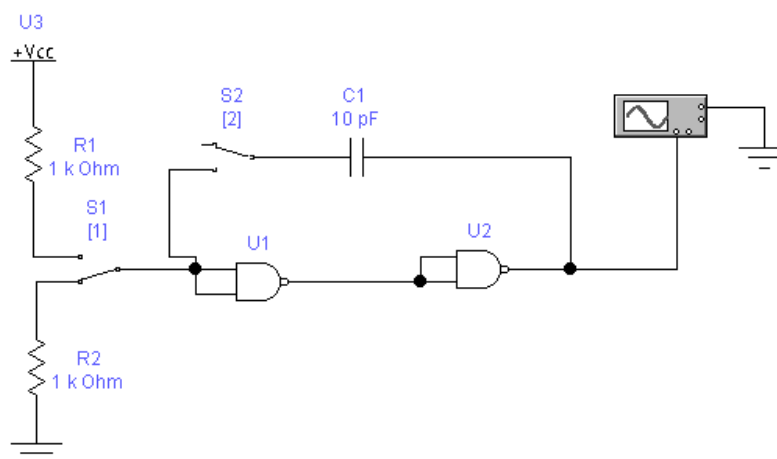


Рис. 7 – Схема исследования эффекта паразитной генерации на логических элементах

2) **Установить параметры элементов схемы** в соответствии с величинами, указанными на рис. 7. Схема исследования, содержит:

- источник постоянного напряжения U_3 величиной – 5 В;
- логические элементы 2 И-НЕ U_1 и U_2 , соединенные последовательно в виде инверторов;
- сопротивления R_1 и R_2 для подачи на вход логического элемента U_1 потенциала логической единицы и потенциала логического нуля соответственно, которые подключаются с помощью переключателя S_1 , управляемого клавишей «1»;
- паразитную емкость C_1 , подключаемую в цепь обратной положительной связи с помощью переключателя S_2 , управляемого клавишей «2».

3) **Включить эмулятор EWB**, убедиться в работоспособности схемы. Для этого двойным щелчком **открыть осциллограф**, и его **настроить** на регистрацию отображения дискретных сигналов.

4) **Произвести** с помощью осциллографа **наблюдение цифровых сигналов**, переключая переключатель S_1 с помощью клавиши «1».

5) **Отобразить в отчете осциллограммы** цифровых сигналов.

6) **Сделать выводы** о работе логических элементов.

7) Нажав клавишу «2» с помощью переключателя S_2 , **сымитировать** образование паразитной емкости, которая образует **паразитную цепь положительной обратной связи**.

8) **Произвести** с помощью осциллографа **наблюдение эффекта паразитной генерации**.

9) **Отобразить в отчете осциллограмму** выходного цифрового сигнала.

10) **Измерить** с помощью осциллографа **частоту выходного сигнала**.

11) **Изменяя параметры паразитной емкости C_1** , устанавливая ее последовательно 1 пФ, 10 пФ, 100 пФ и 1000 пФ, измерить частоту паразитной генерации. Определить, как зависит частота паразитной генерации от величины паразитной емкости.

12) **Сделать выводы** по результатам проделанной работы.

Задание 2.4. Составить отчет о проделанной работе. В отчете отобразить:

- тему и цель работы, порядок ее выполнения;
- принципиальные схемы исследования;
- полученные временные диаграммы (осциллограммы) входных и выходных сигналов, сигналов паразитной генерации;
- произведенные измерения и полученные зависимости;
- сделанные по результатам работы выводы.

Задание 2.5. Защитить отчет по второй части, проделанной

лабораторной работы.

**Задание обучаемым для самостоятельной учебной работы
при подготовке к лабораторной работе:**

3. Закрепить и углубить знания, полученные на лекции, для этого изучить конспект лекций и рекомендуемую литературу.
4. Изучить методические указания к лабораторной работе №2 и подготовить отчет по лабораторной работе согласно методическим указаниям.

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1-3

РАЗДЕЛ № 3. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ СРЕДСТВАМИ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И АВТОМАТИЗИРОВАННЫМИ СИСТЕМАМИ

**Тема № 8. МОДЕЛИРОВАНИЕ И ИССЛЕДОВАНИЕ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ, ВОЗНИКАЮЩИХ ЗА СЧЕТ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ И НАВОДОК
ЛАБОРАТОРНЫЕ РАБОТЫ № 7-9.**

Тема 1: Характеристика технических каналов утечки информации, возникающих за счет побочных электромагнитных излучений и наводок.

Тема 2: Специально создаваемые радиоэлектронные технические каналы утечки информации

Тема 3: Акустические каналы утечки речевой информации

Подтема: Моделирование и исследование технических каналов утечки информации, возникающих за счет побочных электромагнитных излучений и наводок

Время – 6 часов.

Формируемые компетенции: ОПК-4, ОПК-11, ОПК-2.1.

УЧЕБНЫЕ ВОПРОСЫ:

- 1. Моделирование электромагнитных каналов утечки информации, возникающих от технических средств передачи, хранения, обработки и отображения информации (ТСПИ).**
- 2. Исследование электромагнитных каналов утечки информации, возникающих от технических средств передачи, хранения, обработки и отображения информации (ТСПИ).**
- 3. Моделирование и исследование электрических каналов утечки информации, наводимых в линиях электропитания и заземления ТСПИ, соединительных линиях ВТСС и посторонних проводниках.**

СОДЕРЖАНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

Вводная часть

Каждое средство вычислительной техники (техническое устройство АИС) потенциально может образовывать различные каналы утечки информации. Это обусловлено взаимосвязями технических средств, с одной стороны, с объектами внешней среды, а с другой – результатами проявления физических эффектов, входящих в их состав. Проведение физического анализа путем моделирования систем позволяет выявить потенциальные каналы утечки информации.

В ходе данной лабораторной работы проводится моделирование и исследование электромагнитных каналов утечки информации, создаваемых от

технических средств передачи, хранения, обработки и отображения информации (ТСПИ), а также электрических каналов утечки информации, наводимых в линиях электропитания и заземления ТСПИ, соединительных линиях ВТСС и посторонних проводниках.

Проверка подготовленности обучаемых к лабораторной работе

Перечень контрольных вопросов:

- 1) Сравнительная характеристика электромагнитного и электрического каналов утечки информации.
- 2) Структурная схема электромагнитного канала утечки информации, возникающего за счет побочных электромагнитных излучений СВТ.
- 3) Структурная схема электрического канала утечки информации, возникающего за счет наводок от побочных электромагнитных излучений СВТ.
- 4) Причины возникновения ПЭМИ в средствах вычислительной техники.
- 5) Причинами возникновения наводок информационных сигналов от СВТ.
- 6) Условия возникновения электромагнитного канала утечки информации.
- 7) Условия возникновения электрического канала утечки информации.
- 8) Сравнительная характеристика опасных зон R_2 и r_1 .

ВОПРОСЫ, ПОДЛЕЖАЩИЕ ИССЛЕДОВАНИЮ

1 - 2. Моделирование и исследование электромагнитных каналов утечки информации, возникающих от технических средств передачи, хранения, обработки и отображения информации (ТСПИ)

Краткие теоретические или справочно-информационные материалы

Утечка информации по электромагнитному каналу осуществляется посредством перехвата электромагнитных излучений радиодиапазона, создаваемых от элементов технических средств. Эти излучения могут быть функциональными и побочными. С помощью этого канала может быть осуществлен перехват функциональных сигналов радиостанций и систем связи, радиолокационных и радионавигационных систем, систем телеуправления, средств радиотелефонной связи, мониторов ПЭВМ, радиозакладок различного типа, переговоров внутри помещений предприятия с помощью беспроводных служебных систем связи и др.

Перехват информации по радиоканалам имеет ряд преимуществ по сравнению с другими каналами утечки информации, а именно:

- отсутствует непосредственный контакт с источником информации;
- на прием сигналов не влияет ни время года, ни время суток;
- информация получается в реальном масштабе времени;
- перехват информации реализуется скрытно;
- источник информации не имеет сведений о процессе перехвата;

—дальность перехвата ограничивается только особенностями распространения соответствующего диапазона радиоволн и возможностями источника информации.

Классификация радиоканалов утечки информации приведена на рис. 1. При этом утечка информации по радиоканалу может происходить как без преобразования информационного сигнала, так и с его преобразованием, т.е. с помощью радиозакладок, осуществляющих преобразование акустических информационных сигналов в радиоизлучения. В данной лабораторной работе рассматриваются только электромагнитные каналы утечки без преобразования информационного сигнала, создающие условия для перехвата функциональных радиосигналов или побочных электромагнитных излучений.

Перехват информационных излучений реализуется на основе использования разнообразных радиоприемных средств, средств анализа и регистрации информации.



Рис. 1 – Классификация электромагнитных каналов (радиоканалов) утечки информации

Перехват сигналов связных радиостанций

Электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться естественным образом с использованием стандартных технических средств.

Упрощенная структура типового комплекса средств перехвата сигналов связанных радиостанций включает (см. рис. 2):

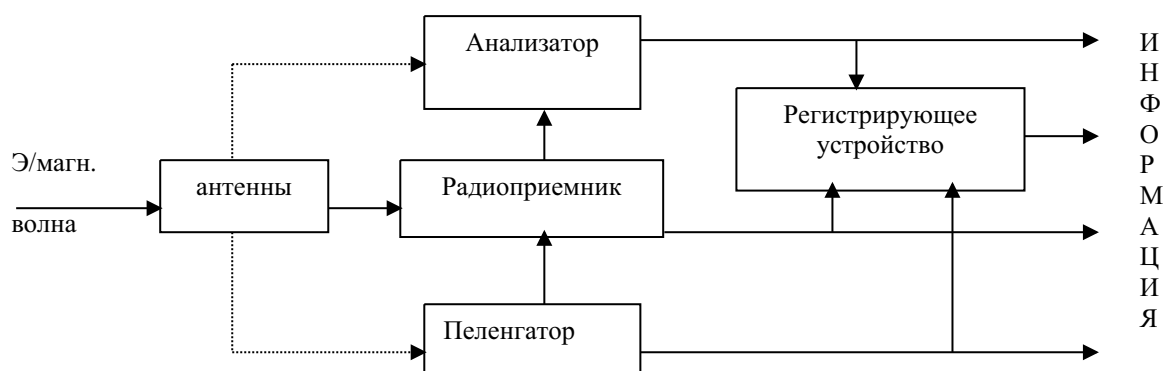


Рис. 2 – Структура комплекса средств перехвата

1) **приемные антенны** – предназначены для преобразования электромагнитной волны в электрические сигналы, амплитуда, частота и фаза которых соответствуют аналогичным характеристикам электромагнитной волны;

2) **радиоприемник** обеспечивает поиск и селекцию радиосигналов по частоте, усиление и демодуляцию (детектирование) выделенных сигналов, их усиление и обработку;

3) **анализаторы технических характеристик сигналов** определяют параметры сигналов: частотные, временные, энергетические, виды модуляции, структуру кодов и др.;

4) **радиопеленгатор** позволяет определить направление на источник электромагнитного излучения и его координаты;

5) **регистрирующее устройство** обеспечивает запись сигналов для документирования и последующей обработки.

Для перехвата радиосигналов связанных радиостанций используют различные типы приемников или радиокомплексы. Так, например, используются приемные устройства AR-3000A, AR-5000, APK-ЦТ, Winradio 3100i-DSP, радиокомплексы OSC-5000, APK-MK1, APK-Д1, APK-ПК-П, R9000-DM-20 (профессиональный радиоприемник – многофункциональный комплекс).

Перехват радиотелефонных сигналов

Для перехвата радиосигналов со сложной структурой, применяемой в сотовой, пейджинговой и других видах мобильной связи, созданы специальные приемные комплексы. Например, система контроля использования служебных радиотелефонов сотовой связи стандарта NMT-450 TТС-1 (фирма «Нелк») позволяет обнаруживать и сопровождать по частоте входящие и исходящие звонки абонентов сотовой связи, осуществлять слежение по частоте за каналом во время телефонного разговора, вести одновременно автоматическую запись разговора на диктофон и т.д. В комплексе используются ПЭВМ и два приемника AR-3000 А.

Для перехвата сообщений сотовых телефонов созданы автоматизированные станции перехвата сотовых систем связи. В состав станций входят: портативный

компьютер, спецдемолятор, приемное устройство, управляемое компьютером. Достаточно на экране компьютера задать номер интересующего абонента и комплекс будет автоматически записывать входящие переговоры, определять номера звонящих к контролируемому абоненту, сопровождать мобильный объект при переходе из соты в соту. Аналогичные системы существуют и для радиотелефонов отечественной системы «Алтай».

Обработка перехваченного радиосигнала осуществляется с помощью средств технического анализа. К ним относятся: Stabilock 4051, Stabilock 4032, HP 8920 A/D и др.

Для перехвата факсимильных передач применяются специальные комплексы типа 4600-FAX-INT, ФАКС-02, FAX MANAGER и др. Обеспечивают автоматический перехват в реальном масштабе времени любого числа страниц, передаваемых по факсу со скоростью от 300 до 9600 бит/с, запись факсимильного сообщения и служебной информации, вывод их на печать.

Перехват пейджинговых передач осуществляется комплексами АРК-Д1, АРК-ПК с использованием программного обеспечения СМО-ДЕМ, которое реализует следующие функции:

- программа настройки приемника на частоты, предварительно внесенные в файл пейджерных радиостанций;
- прием сообщений, передаваемых в формате PJCSAG со скоростями передачи 512, 1200 или 2400 Бод;
- автоматическое распознавание скорости и полярности передачи;
- регистрация сообщений (сохранение на диске), ручное декодирование и анализ принятых сообщений, оперативный просмотр принятых сообщений, поиск сообщения по шаблону (во всех таблицах кодировки);
- накопление в базе данных информации об абонентах и ее обновление;
- прием сообщений всех абонентов (режим «Обнаружение»);
- сохранение содержимого экрана в файле.

Радиомаяки

Радиомаяки позволяют осуществлять перехват информации о составе технических средств и местах их установки. Такая информация является важной, так как позволяет установить, какие средства обработки и передачи информации устанавливаются в помещениях контролируемой зоны. Кроме того, приобретаемая и устанавливаемая техника может содержать закладные устройства, управляемые дистанционно. Подготовка по организации канала утечки информации включает и процедуру локализации «меченых» технических средств. Для этого могут использоваться радиосигнальные маяки.

Радиосигнальные маяки устанавливаются, например, в упаковку, что позволяет контролировать места размещения закупленных средств вычислительной техники. В системный блок встраиваются дополнительные устройства, которые собираются из стандартных модулей, используемых в ПК, и устанавливаются таким образом, чтобы иметь доступ к выходной или вводимой информации. Передача сигналов маяка на пункт прослушивания осуществляется по радиоканалу.

Побочные электромагнитные излучения

Помимо функциональных сигналов от ТСПИ носителями информации в электромагнитных каналах утечки информации являются побочные электромагнитные излучения (ПЭМИ), возникающие при обработке информации техническими средствами.

Побочным электромагнитным излучением (ПЭМИ) ТСПИ называется нежелательное радиоизлучение, возникающее в результате нелинейных процессов в блоках ТСПИ.

Основными причинами возникновения электромагнитных каналов утечки информации в ТСПИ являются:

- побочные электромагнитные излучения, возникающие вследствие протекания информативных сигналов по элементам ТСПИ;
- модуляция информативным сигналом побочных электромагнитных излучений высокочастотных генераторов ТСПИ (на частотах работы высокочастотных генераторов);
- модуляция информативным сигналом паразитного электромагнитного излучения ТСПИ (например, возникающего вследствие самовозбуждения усилителей низкой частоты).

Паразитным электромагнитным излучением ТСПИ называется побочное радиоизлучение, возникающее в результате самовозбуждения генераторных или усилительных блоков ТСПИ из-за паразитных связей. Наиболее часто такие связи возникают ***за счёт случайных преобразований отрицательных обратных связей*** (индуктивных или ёмкостных) ***в паразитные положительные***, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов. Частота автогенерации (самовозбуждения) лежит в пределах рабочих частот нелинейных элементов усилителей (например, полупроводниковых приборов). В ряде случаев паразитное электромагнитное излучение модулируется информативным сигналом (*модуляцией называется процесс изменения одного или нескольких параметров электромагнитного излучения (например, амплитуды, частоты или фазы)* в соответствии с изменениями параметров информативного сигнала, воздействующих на него.

В средствах вычислительной техники ПЭМИ возникают при следующих режимах обработки информации:

- вывод информации на экран монитора;
- ввод данных с клавиатуры;
- запись информации на накопители;
- чтение информации с накопителей;
- передача данных в каналы связи;
- вывод данных на периферийные печатные устройства – принтеры, плоттеры; запись данных от сканера на магнитный носитель и т.д.

При каждом режиме работы СВТ возникают ПЭМИ, имеющие свои характерные особенности. Диапазон возможных частот побочных электромагнитных излучений СВТ может составлять от 10 кГц до 2 ГГц.

Для перехвата побочных электромагнитных излучений СВТ *используются* специальные стационарные, перевозимые и переносимые приёмные устройства, которые называются техническими средствами разведки побочных электромагнитных излучений и наводок (ТСР ПЭМИН).

Типовой комплекс разведки ПЭМИ включает: специальное приёмное устройство, ПЭВМ (или монитор), специальное программное обеспечение и широкодиапазонную направленную антенну. В качестве примера на рис. 3 приведён внешний вид одного из таких комплексов.



Рис. 3. Комплекс перехвата побочных электромагнитных излучений СВТ:
а) специальное приёмное устройство PKI2715 (дальность перехвата ПЭМИ от 10 до 50 м); б) широкополосная направленная антенна R&SHB 007 (диапазон частот от 80 МГц до 1,3 ГГц, коэффициент усиления 5-7 дБ)

Средства разведки ПЭМИ могут устанавливаться в близлежащих зданиях или машинах, расположенных за пределами контролируемой зоны объекта (рис. 4).



Рис. 4 – Перехват ПЭМИ от средств вычислительной техники техническими средствами разведки

Наиболее опасным (с точки зрения утечки информации) режимом работы СВТ является вывод информации на экран монитора. Учитывая широкий спектр ПЭМИ видеосистемы СВТ ($\Delta F_c > 100$ МГц) и их незначительный уровень,

перехват изображений, выводимых на экран монитора ПЭВМ, является довольно трудной задачей.

Дальность перехвата ПЭМИ современных СВТ, как правило, не превышает 30-50 м.

Качество перехваченного изображения значительно хуже качества изображения, выводимого на экран монитора ПЭВМ (рис. 5).

Особенно трудная задача – перехват текста, выводимого на экран монитора и написанного мелким шрифтом (рис. 6).

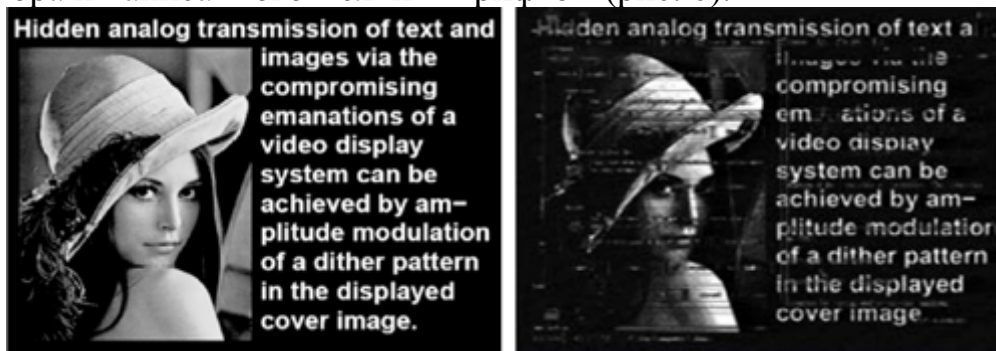


Рис. 5 – Тестовое изображение, выведенное на экран монитора (а) и изображение, перехваченное средством разведки ПЭМИ (б)

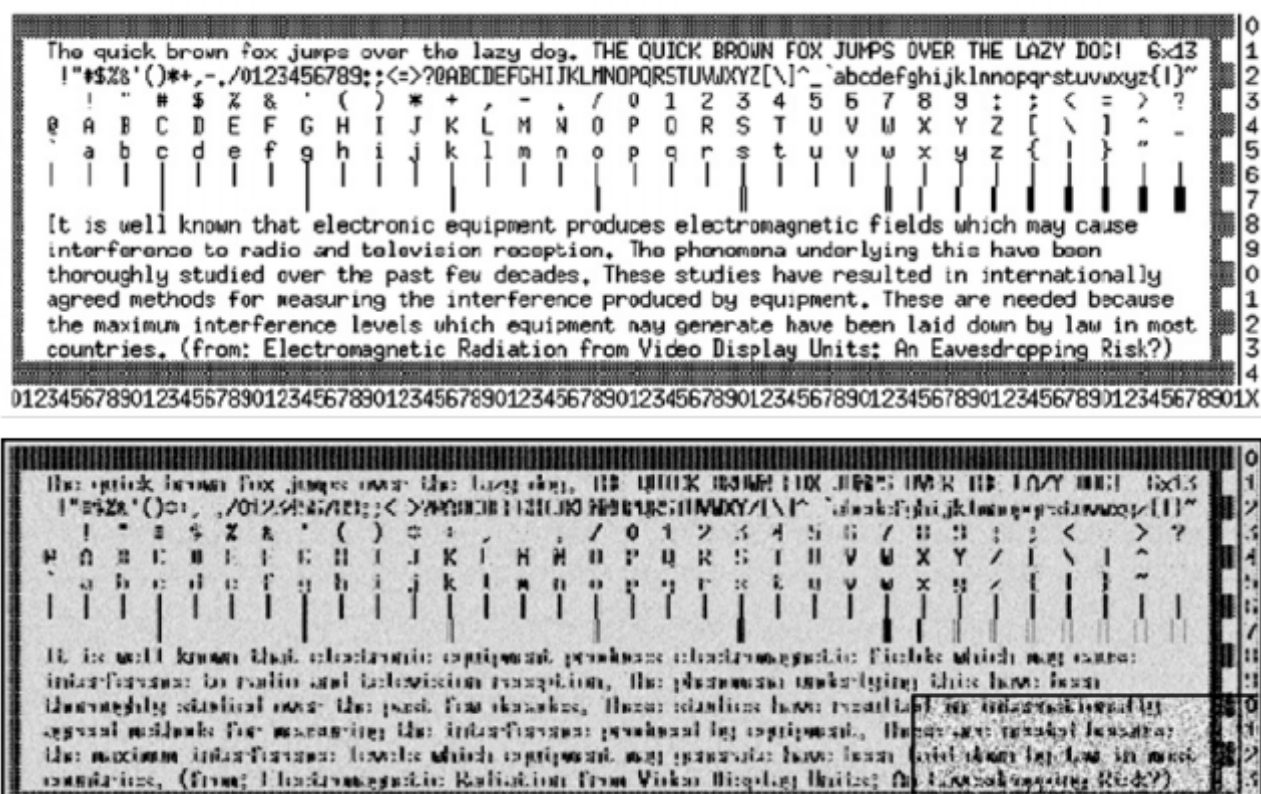


Рис. 6 – а) Исходный текст, выведенный на экран монитора (режим работы VGA монитора 800×600, 75Hz, размер букв 6х13 пикселей);
б) текст, перехваченный средством разведки ПЭМИ ($\Delta f_{\text{пр}} = 200$ МГц)

В качестве показателя оценки эффективности защиты информации от утечки по техническим каналам используется вероятность правильного обнаружения информативного сигнала (P_0) приёмным устройством средства

разведки. В качестве критерия обнаружения наиболее часто используется критерий «Неймана-Пирсона». В зависимости от решаемой задачи защиты информации пороговое значение вероятности обнаружения информативного сигнала может составлять от 0,1 до 0,8, полученное при вероятности ложной тревоги от 10^{-3} до 10^{-5} .

Зная характеристики приёмного устройства и антенной системы средства разведки, можно рассчитать допустимое (нормированное) значение напряжённости электромагнитного поля, при котором вероятность обнаружения сигнала приёмным устройством средства разведки будет равна некоторому (нормированному) значению ($P_o = P_n$).

Пространство вокруг ТСПИ, на границе и за пределами которого напряжённость электрической (Е) или магнитной (Н) составляющей электромагнитного поля не превышает допустимого (нормированного) значения ($E \leq E_n$; $H \leq H_n$), называется опасной зоной 2 (R2).

Зона R2 для каждого СВТ определяется инструментально-расчётным методом при проведении специальных исследований СВТ на ПЭМИ и указывается в предписании на их эксплуатацию или сертификате соответствия.

Таким образом, для возникновения электромагнитного канала утечки информации необходимо выполнение двух условий (рис.7):

1) Расстояние от СВТ до границы контролируемой зоны должно быть менее зоны R2 ($R_{кз} < R2$).

2) В пределах зоны R2 возможно размещение стационарных или перевозимых (переносимых) средств разведки ПЭМИН.

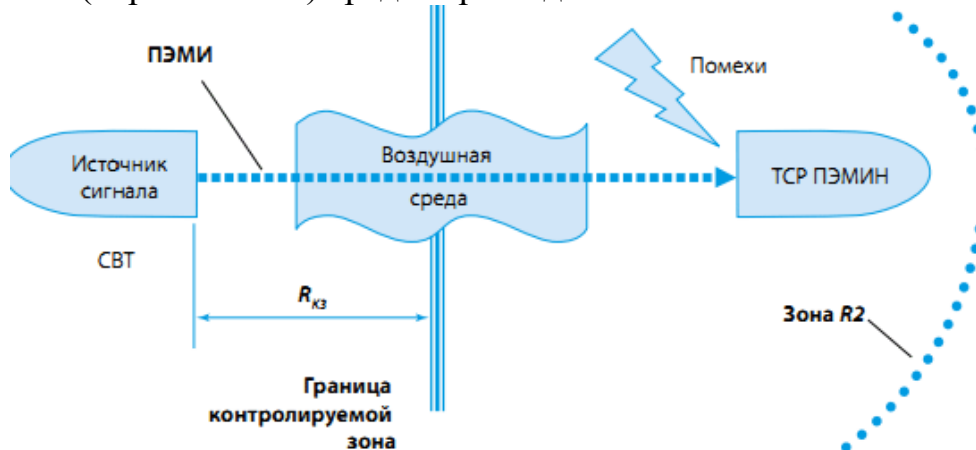


Рис.7 – Схема электромагнитного технического канала утечки информации, возникающего за счёт ПЭМИ от СВТ

Исследование технических каналов утечки информации возможно двумя методами: инструментально-расчетным и схемотехнического моделирования с помощью ЭВМ.

Первый метод требует наличия дорогостоящего оборудования, что затрудняет его использование в образовательном процессе. Тогда как проектирование радиоэлектронных средств технического канала утечки информации с применением ЭВМ требует описания этих объектов на языке математики в виде, удобном для его алгоритмической реализации.

Математическое описание проектируемого объекта называют математической моделью. По способу получения математические модели радиотехнических объектов делят на физические и формальные. Физические модели получают на основе изучения физических закономерностей функционирования проектируемого объекта, так что структура уравнений и параметры модели имеют ясное физическое толкование. Формальные модели получают на основе измерения и установления связи между основными параметрами объекта в тех случаях, когда физика работы его известна недостаточно полно. Как правило, формальные модели требуют большого числа измерений и по своей природе являются локальными, справедливыми вблизи тех режимов, в которых производились измерения. Такие модели называют моделями «черного ящика».

В современных системах автоматизированного проектирования формирование системы уравнений математической модели проектируемого объекта выполняется автоматически с помощью ЭВМ на базе типовых электрических моделей.

Понятие электрической модели включает либо систему уравнений, связывающих напряжения и токи в электрической схеме, являющейся моделью объекта, либо саму электрическую схему, составленную из базовых элементов (резисторов, конденсаторов), на основе которой можно в ЭВМ получить систему уравнений, связывающих напряжения и токи в модели объекта.

Для моделирования технических каналов утечки информации удобнее всего применять информационные технологии, обеспечивающие решение задач схемотехнического проектирования. В качестве программного редактора такой информационной технологии схематического моделирования используется «Electronics Workbench» (EWB), содержащий большую библиотеку радиоэлектронных компонентов, контрольно-измерительные приборы, максимально приближенные к промышленным образцам, имеющий простой легко усвояемый интерфейс.

Рассмотрим процесс схемотехнического моделирования с использованием EWB на примере моделирования электромагнитного технического канала утечки информации (ТКУИ), возникающего за счёт ПЭМИ от средств вычислительной техники (СВТ). Для моделирования ТКУИ в EWB необходимо структурные элементы канала заместить абстракциями в виде типовых элементов, имеющихся в библиотеке компонентов программы. Для этого детализируем схему канала, представив ее в виде, как показано на рис 8.

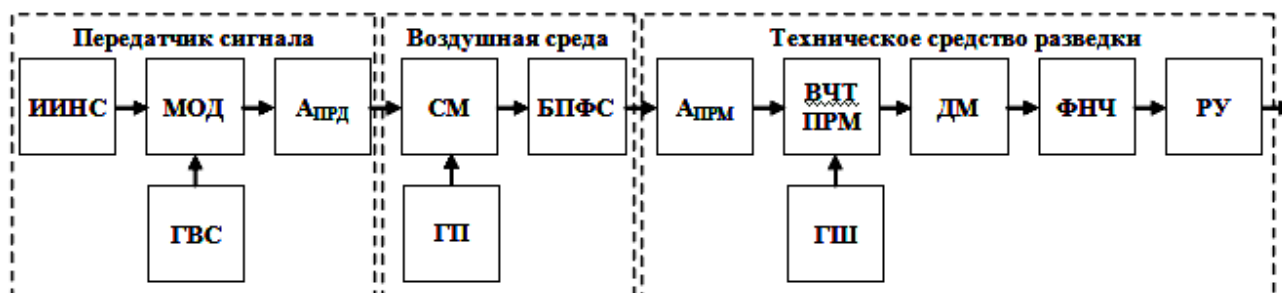


Рис.8 – Функциональная схема электромагнитного технического канала утечки информации, возникающего за счёт ПЭМИ от СВТ

Схемотехническая модель передатчика (источника) сигнала содержит (см. рис. 8):

- источник информационного низкочастотного сигнала (ИИНС);
- генератор высокочастотного сигнала (ГВС), генерирующий несущее колебание;
- модулятор (МОД), т.е. нелинейный преобразователь, формирующий радиосигнал;
- передающую антенну ($A_{\text{прд}}$), осуществляющую преобразование электрического сигнала в электромагнитное поле.

Для моделирования воздушной среды используются (см. рис. 8):

- генератор помех (ГП), имитирующий естественные или преднамеренные помехи;
- аналоговый сумматор (СМ), формирующий аддитивную смесь сигнала и помехи;
- блок передаточной функции среды (БПФС), имитирующий ослабление и частотные искажения радиосигнала в воздушной среде распространения.

Техническое средство разведки моделируется в виде (см. рис. 8):

- приемной антенны ($A_{\text{прм}}$), осуществляющей преобразование радиосигнала, распространяющего в виде электромагнитной волны, в электрический сигнал;
- генератора шума (ГШ), имитирующего наличие внутренних (тепловых) шумов приемника;
- высокочастотного тракта приемника (ВЧПРМ), осуществляющего частотную селекцию и линейное преобразование (усиление) смеси принятого радиосигнала и внутренних шумов;
- демодулятора (ДМ), осуществляющего детектирование сигнала; фильтра низких частот (ФНЧ), предназначенного для выделения низкочастотного информационного сигнала;
- решающего устройства (РУ), осуществляющего распознавание символов информационного сигнала.

В программе EWB в качестве ИИНС могут использоваться: источник гармонического (синусоидального) напряжения; источники амплитудно-модулированных или частотно-модулированных сигналов; генераторы импульсного напряжения.

Генератор импульсного напряжения V1 (см. рис. 11), формирующий меандр, позволяет имитировать битовую последовательность данных, поскольку при большой выборке данных логические нули и единицы в битовой последовательности будут распределены примерно поровну. Высокочастотный несущий сигнал создается с помощью источник гармонического (синусоидального) напряжения V2.

Модулятор и демодулятор в EWB реализуются соответственно с помощью

аналогового умножителя A2 и аналогового делителя A4 с управляемыми коэффициентами передачи.

Эквивалентная электрическая схема передающей и приемной антенны представляет собой последовательный колебательный контур, содержащий активное сопротивление, индуктивность и емкость, соответственно элементы R4, L1, C3 и R6, L2, C4. Эквивалентная электрическая схема антенны представлена на рис. 9.

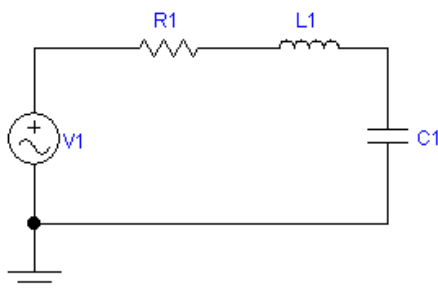


Рис. 9 – Эквивалентная электрическая схема антенны

Передающая характеристика воздушной среды моделируется с помощью RC фильтра нижних частот (элементы R5, C6), характеризующего пропускную способность среды, и масштабирующего звена A1, в котором реализуется ослабление радиосигнала в среде. Моделирование аддитивной смеси радиосигнала и помехи (шума), имеющейся в среде или во входных цепях приемника, осуществляется с помощью сумматоров напряжений A3 и A5 соответственно.

Генераторы помех и шума могут быть смоделированы с помощью источников частотно-модулированных сигналов (V3, V4) путем задания большой модулирующей частоты близкой к несущей частоте и очень большого индекса модуляции, например как приведено на рис. 10 (а). Осциллограмма полученного шумоподобного сигнала представлена на рис. 10 (б).

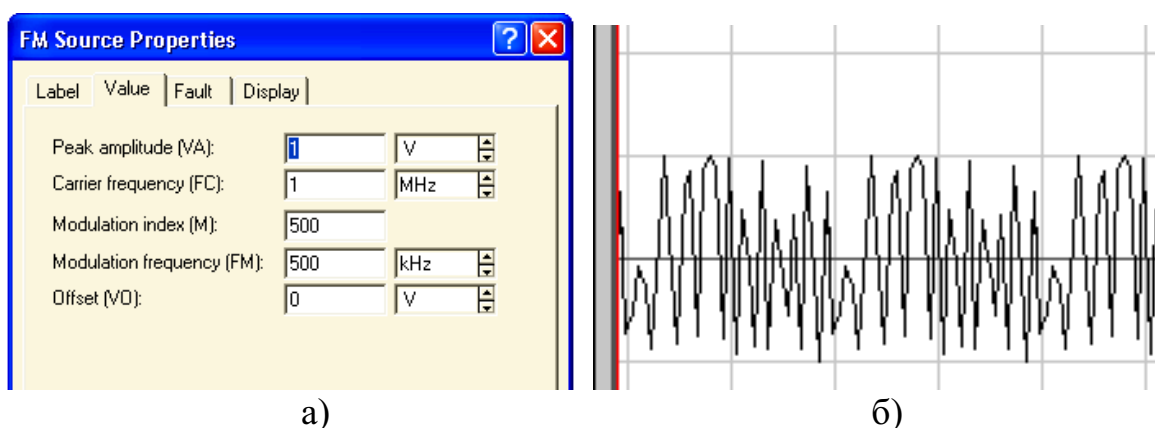


Рис. 10 – Пример моделирования генератора помех (шума) на базе источника ЧМ-сигнала:

- а) Параметры источника ЧМ-сигнала;
- б) осциллограмма шумоподобного сигнала

Простейший ФНЧ, находящийся в приемнике ТСП, реализуется с помощью

RC фильтра (элементы R1, C1). Решающее устройство строится на основе управляемого ограничителя напряжения (VR1) и источников опорного напряжения (V5, V6).

Результат схемотехнического моделирования в программе EWB представлен на рисунке 11.

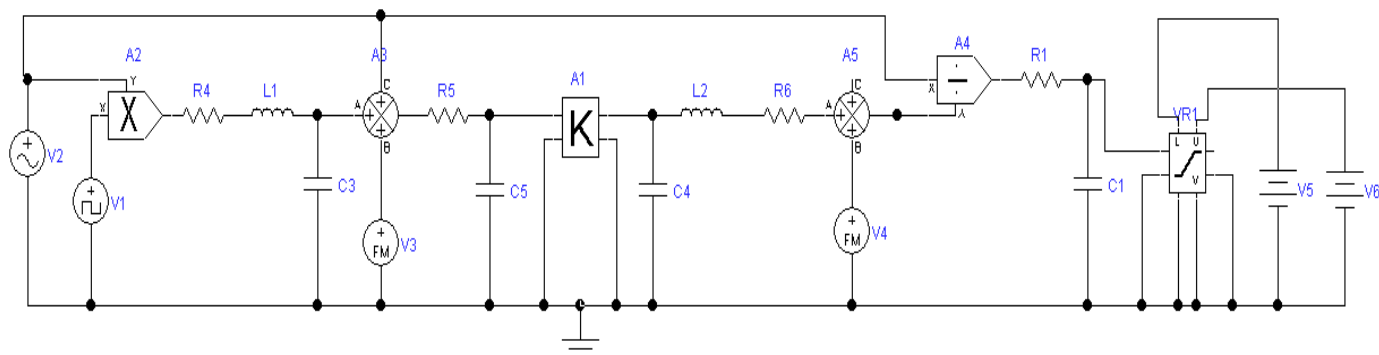


Рис. 11 – Схемотехническая модель электромагнитного ТКУИ в программе EWB

Разработанная модель позволяет исследовать электромагнитный ТКУИ путем представления структурных элементов канала эквивалентными базовыми компонентами из библиотеки EWB, которые автоматически описываются системами математических уравнений. Изменением их параметров, можно адекватно смоделировать любой электромагнитный ТКУИ с учетом конкретных условий обстановки и оценить величину угрозы безопасности информации.

Содержание практической работы, выполняемой студентами в ходе занятия

1. Описание лабораторного оборудования:

- ПЭВМ на каждого обучающегося;
- программный редактор схематического моделирования «Electronics Workbench» (EWB), версия не ниже 5.12.

2. Требования безопасности при выполнении работы:

3. Задание для работы

17) Смоделировать электромагнитный технический канал утечки информации, возникающий за счёт ПЭМИ от СВТ, в программе EWB.

18) Исследовать эквивалентную электрическую схему замещения электромагнитного ТКУИ, возникающего за счёт ПЭМИ от СВТ.

19) Смоделировать и исследовать электромагнитный технический канал утечки информации, возникающий за счёт ПЭМИ при передаче цифрового видеосигнала.

20) Оформить и защитить отчет по первой части проделанной лабораторной работы.

4. Порядок выполнения работы

Задание 1.1. Смоделировать электромагнитный технический канал утечки информации в программе EWB. Для этого необходимо:

- 1) Собрать электрическую схему замещения, приведенную на рис. 12.

2) Ввести параметры элементов, как указано на рис. 12, и отладить схему до работоспособного состояния, получив по первому каналу последовательность радиоимпульсов, а по второму каналу – битовую последовательность видеоимпульсов. Для этого установить переключатели S1 и S2 в верхнее положение, переключатель S3 – в левое положение, а переключатель S4 – в правое.

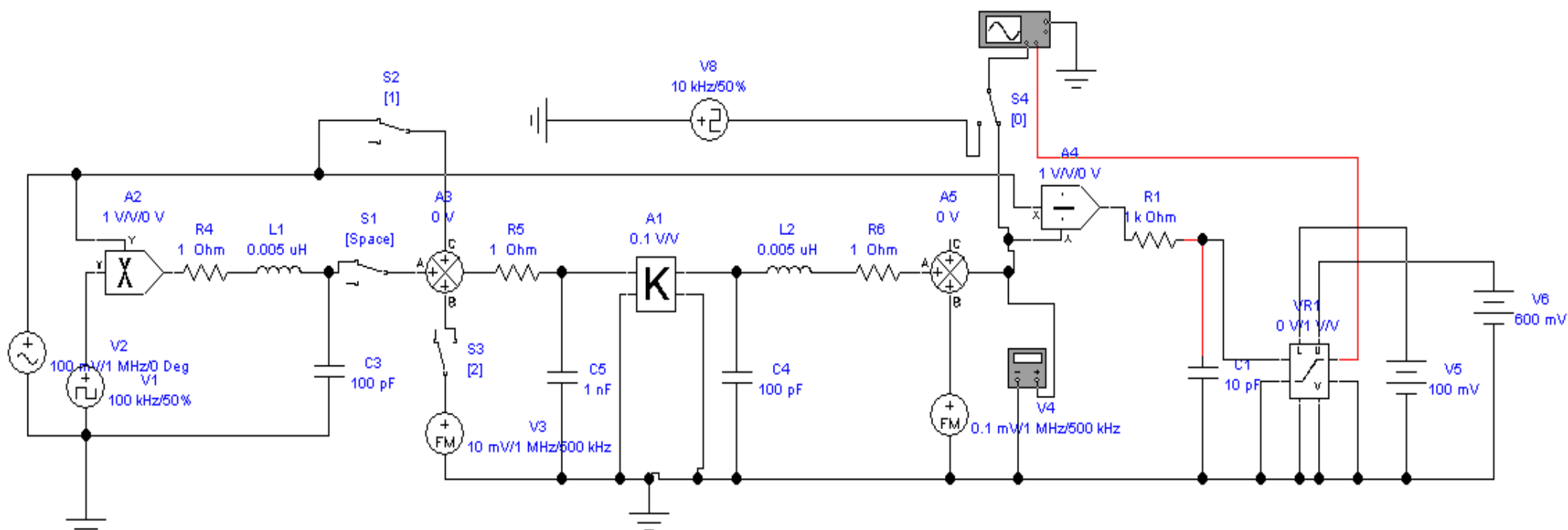


Рис. 12 – Электрическая схема замещения электромагнитного технического канала утечки информации

Пример правильно полученных осциллограмм приведен на рис. 13.

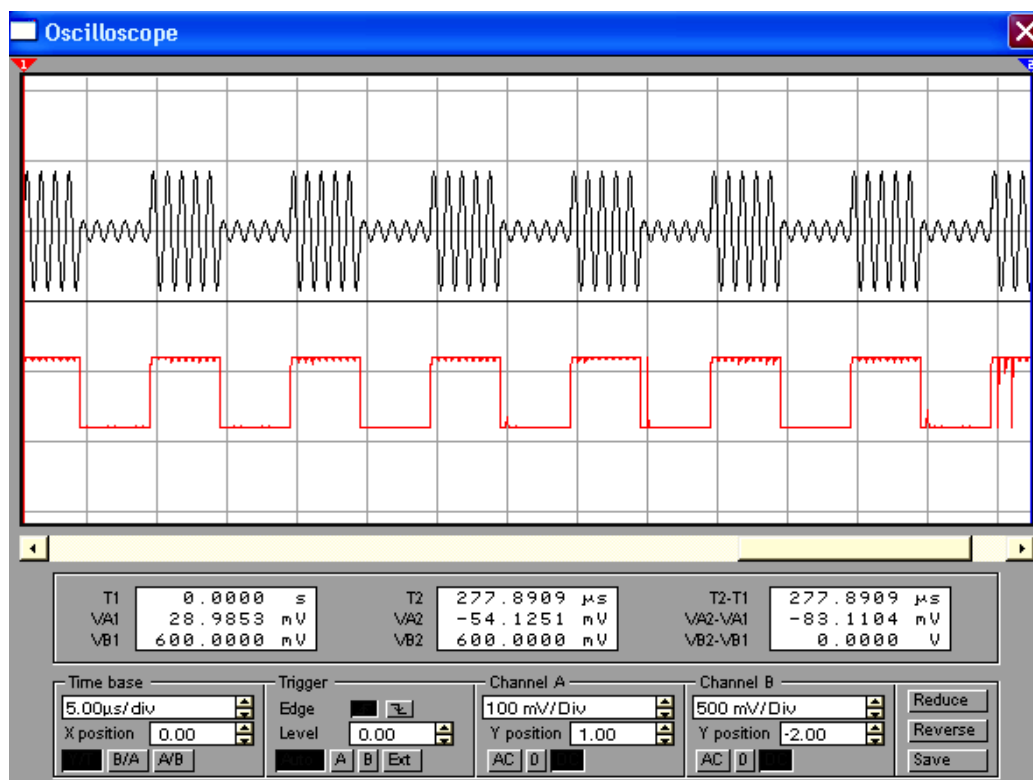


Рис. 13 – Осциллограммы последовательности радиоимпульсов и битовой последовательности видеоимпульсов

3) Сравнивая функциональную схему электромагнитного технического канала утечки информации, приведенную на рис. 8, и смоделированную схему, составить схемы замещения для всех функциональных элементов канала.

4) Сделать выводы по результатам проделанной работы.

Задание 1.2. Исследовать эквивалентную электрическую схему замещения электромагнитного ТКУИ, возникающего за счёт ПЭМИ от СВТ. Для этого необходимо выполнить следующие операции:

1) Оценить угрозу утечки компьютерных данных, возникающую за счет наличия данного канала. Для этого необходимо выполнить следующие операции:

- установить переключатель S4 в левое положение, подключив к первому каналу осциллографа генератор тактовых импульсов V8, формирующий синхроимпульсы большой длительности, в которую укладывается последовательность из 10 бит.

- запустить симулятор EWB, и дать схеме проработать 30 секунд, после чего отключить симулятор;

- произвести подсчет количества ошибочно принятых символов в битовой последовательности, содержащей 100 символов, отображаемых по второму каналу осциллографа, при этом студент выступает в роли решающего устройства технического средства разведки. Для этого, продвигая горизонтальную прокрутку осциллографа, посчитать количество искаженных

бит $B_{ош}$ по критерию идеального наблюдателя. Под искаженным битом понимается такой бит, у которого помеха искажает амплитуду импульса на величину не менее половины амплитуды импульса. На приведенном примере (см. рис. 13) искаженными битами являются 10 бит и последний 15 бит;

- определить вероятность правильного приема $P_{пр}$ перехваченных символов, воспользовавшись формулой

$$P_{пр} = \frac{1 - B_{ош}}{B};$$

- сделать выводы по результатам проделанной работы.

2) Определить зависимость вероятности правильного приема символов от отношения сигнал/помеха на входе приемника, для этого необходимо:

- отключить источник сигнала, переведя переключатели S1 и S2 в нижнее положение, нажав клавишу «1»;

- подключить источник помех, переведя переключатель S3 в правое положение, нажав клавишу «2»;

- установить в источнике V3 напряжение помехи, создаваемое генератором помех, равное 1 мВ;

- включить симулятор и измерить с помощью мультиметра напряжение помехи на входе приемника, результат измерения занести в таблицу 1;

- далее, изменяя напряжение помехи в пределах от 10 мВ до 50 мВ с шагом 10 мВ, повторить предыдущие два пункта работы, занести измеренные данные в таблицу 1;

Таблица 1 – Измеренные и расчетные данные

U _{ГП} , мВ	1	10	20	30	40	50
U _П , мВ						
U _С , мВ						
h = U _С / U _П						
P _о						

- подключить источник сигнала, нажав клавишу «Пробел, отключить генератор помех, нажав клавишу «1»;

- включить симулятор и измерить с помощью мультиметра напряжение сигнала на входе приемника, занести измеренные данные в таблицу 1;

- рассчитать величину отношения сигнал/помеха на входе приемника, рассчитанные данные занести в таблицу 1.

- одновременно подключить источник сигнала и генератор помех;

- последовательно устанавливая величины напряжения помехи, приведенные табл. 1, запуская кратковременно симулятор, произвести подсчет количества ошибочно принятых символов в битовой последовательности, содержащей более 50 символов, отображаемых по второму каналу осциллографа, а также расчет вероятности правильного приема P_о перехваченных символов, результаты занести в таблицу 1;

- построить в отчете график зависимости вероятности правильного приема символов от отношения сигнал/помеха на входе приемника;

- сделать выводы по результатам проделанной работы.

3) Определить зависимость вероятности правильного приема от коэффициента ослабления среды (относительного расстояния от источника сигнала до разведывательного приемника), для этого необходимо:

- подключить источник сигнала, нажав клавишу «Пробел, отключить генератор помех, нажав клавишу «1»;

- установить коэффициент ослабления среды распространения в масштабирующем звене схемы, равным 0,1, имитируя определенное расстояние между источником сигнала и разведывательным приемником;

- запустив кратковременно симулятор, произвести подсчет количества ошибочно принятых символов в битовой последовательности, содержащей более 50 символов, отображаемых по второму каналу осциллографа, а также расчет вероятности правильного приема P_0 перехваченных символов, результаты занести в таблицу 2;

- изменяя коэффициент ослабления от величины 0,09 до 0,01 с шагом 0,02 (т.е. имитируя увеличение расстояния между источником сигнала и разведывательным приемником), произвести подсчет количества ошибочно принятых символов в битовой последовательности, содержащей более 50 символов, отображаемых по второму каналу осциллографа, а также расчет вероятности правильного приема P_0 перехваченных символов, результаты занести в табл. 2;

- построить в отчете график зависимости вероятности правильного приема символов от величины коэффициента ослабления среды (относительного расстояния от источника сигнала до разведывательного приемника);

- сделать выводы по результатам проделанной работы.

4) Сделать выводы по результатам выполненного задания.

Задание 1.3. Смоделировать и исследовать электромагнитный технический канал утечки информации, возникающий за счёт ПЭМИ при передаче цифрового видеосигнала. Для этого необходимо выполнить следующие операции:

1) Моделирование источника сигнала.

Источником сигнала является либо цифровая видеокамера, либо видеоадаптер компьютера.

Компонентный телевизионный видеосигнал представляется в цифровой форме в соответствии с Рекомендацией ITU-R 601. Эта рекомендация устанавливает правила раздельной дискретизации, квантования и кодирования сигнала яркости Y и двух цветоразностных сигналов $R-Y$ (Cr) и $B-Y$ (Cb). Частота дискретизации для яркостного сигнала Y установлена равной 13,5 МГц, для цветоразностных сигналов - 6,75 МГц, т.е. частота дискретизации яркостного сигнала в 2 раза больше частоты дискретизации цветоразностных сигналов. Если взять, как принято, в качестве условной (базовой для иерархии цифровых стандартов) единицы частоту 3,375 МГц, то частоты дискретизации яркостного и двух цветоразностных сигналов будут находиться в соотношении 4:2:2, которое и дает часто используемое название стандарта. При таких значениях

частот дискретизации можно практически преобразовать без искажений в цифровую форму сигнал яркости в полосе до 5,75 МГц, а цветоразностные сигналы – в полосе до 2,75 МГц (надо помнить о запасном интервале между граничной частотой сигнала и половиной частоты дискретизации). Стандарт 4:2:2 используется в качестве базового стандарта.

Частоты дискретизации представляют гармоники строчной частоты, что обеспечивает неподвижную ортогональную структуру отсчетов ТВ изображения. Величинам 13,5 и 6,75 МГц кратна, как частота строчной развертки стандарта телевизионного разложения 625/50, так и частота развертки стандарта 525/60. Собственно, выбор в качестве базовой именно частоты 3,375 МГц во многом связан с соображениями кратности с частотами строчной развертки двух мировых стандартов разложения. Это важно потому, что позволило ввести единый мировой стандарт цифрового кодирования компонентного видеосигнала, при котором в активной части строки содержится 720 отсчетов яркостного сигнала и по 360 – каждого цветоразностного. Различие в системах 625/50 и 525/60 заключается в разном числе строк и несколько отличающейся длительности интервала гашения. Полная скорость передачи цифрового компонентного видеосигнала составляет $10 \times 13,5 + 10 \times 6,75 + 10 \times 6,75 = 270$ Мбит/с.

Однако на практике расчет скорости видеопотока производится несколько иначе. Сохраняется только активная часть строки видеосигнала. Рассчитываются следующие составляющие: количество пикселей в кадре для яркостной компоненты $= 720 \times 576 = 414\,720$; количество пикселей в кадре для каждой цветностной компоненты $= 360 \times 576 = 207\,360$; число битов в кадре $= 10 \times 414\,720 + 10 \times 207\,360 \times 2 = 8294400 = 8,29$ Мбит; и скорость передачи данных (BR) $= 8,29 \times 25 = 207,36$ Мбит/с.

Таким образом, источник сигнала может быть схемотехнически смоделирован с помощью источника импульсных напряжений (генератора таковых импульсов), формирующего меандр, который позволяет имитировать цифровой видеосигнал в виде битовой последовательности данных, поскольку при большой выборке данных логические нули и единицы в битовом потоке будут распределены примерно поровну. Исходя из ранее изложенного, с учетом округления, в качестве источника видеопотока выбираем генератор тактовых импульсов с частотой 100 МГц.

2) Моделирование распределенной антенны.

Распределенной антенной излучающей ПЭМИ является видеокабель.

В теории антенно-фидерных устройств установлено, что эквивалентная электрическая схема передающей антенны может быть представлена в виде последовательного колебательного контура, содержащего активное сопротивление, индуктивность и емкость, как показано на рис. 9.

Для того чтобы окончательно решить задачу моделирования кабеля осталось определить параметры активного сопротивления, индуктивности и емкости. Для этого необходимо воспользоваться справочными данными, в которых указываются значения распределенных параметров кабеля, а именно: погонное сопротивление (Ом/м); погонная емкость (пФ/м); погонная

индуктивность (нГн/м).

3) Собрать электрическую схему замещения, приведенную на рис. 13.

Данная схема представляет собой схемотехническую модель канала утечки, возникающего при передаче цифрового видеосигнала по видеокабелю. Будем считать, что в данном канале характеристики приемника технического средства разведки согласованы с характеристиками излучаемого сигнала, т.е. приемник осуществляет прием сигналов без искажений. Также введем допущение, что приемник позволяет корректировать принятый сигнал для его лучшего обнаружения и распознавания. Для этого приемник содержит схемы коррекции в виде генераторов гармонических напряжений.

Установить параметры элементов, как указано на рис. 13, и отладить схему, получив требуемый сигнал по второму каналу осциллографа.

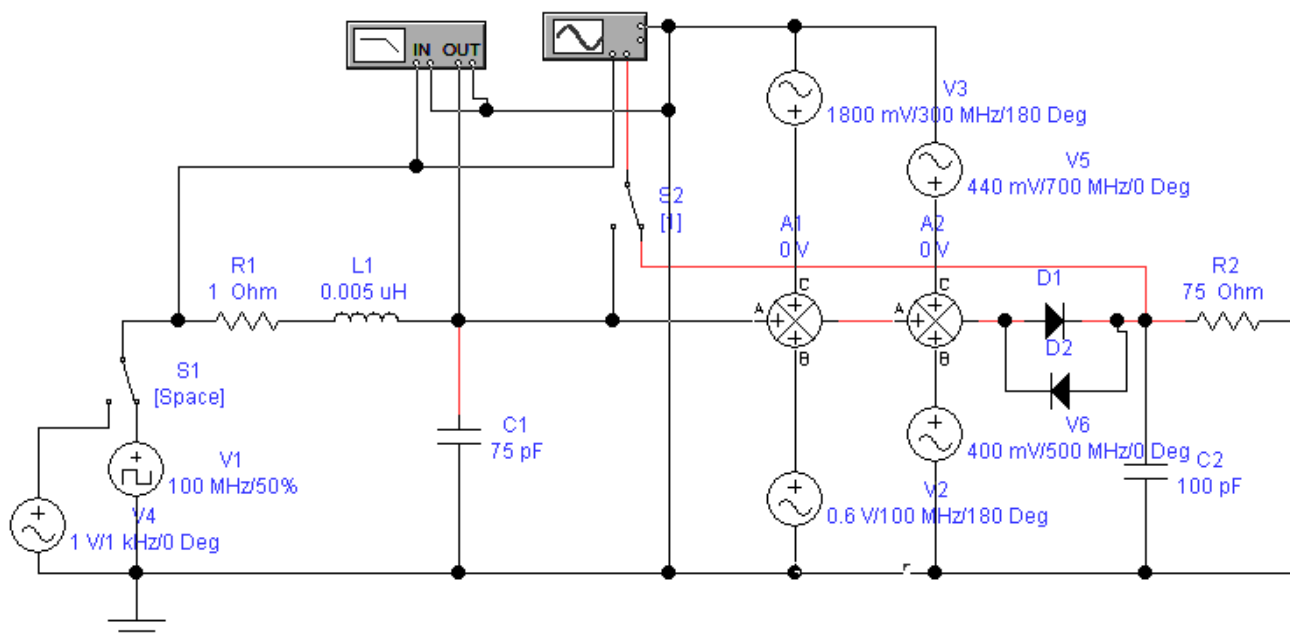


Рис. 13 – Электрическая схема замещения электромагнитного ТКУИ, возникающего за счёт ПЭМИ при передаче цифрового видеосигнала

5) Провести измерение амплитудно-частотной характеристики колебательной системы, имитирующей передающую антенну, для этого:

- подключить к входу последовательного колебательного контура источник гармонического напряжения путем нажатия клавиши «Пробел»;
- измерить с помощью измерителя АЧХ (Bode Plotter) АЧХ контура и определить его резонансную частоту и полосу пропускания по уровню 0,7 (-3 дБ);
- сделать выводы по результатам проделанной работы.

6) Исследовать параметры излучаемого видеосигнала (ПЭМИ), для этого необходимо:

- подключить к входу излучающей колебательной системе (антенне) источник видеосигнала, нажав клавишу «Пробел», а ко входу – второй канал осциллографа;

- зарегистрировать с помощью осциллографа и отобразить в отчете передаваемый видеосигнал (по первому каналу) и излучаемый видеосигнал (по второму каналу), измерить их параметры частоту и амплитуду;
- определить за счет каких физических явлений и эффектов произошло искажение излучаемого видеосигнала;
- зарегистрировать с помощью Фурье-анализатора и отобразить в отчете спектры передаваемого видеосигнала и излучаемого видеосигнала, установив номера необходимых узлов схемы, частоту первой гармоники – 100 МГц и число гармоник – 200;
- измерить с помощью Фурье-анализатора частоты (F) и амплитуды (S1(F) и S2(F)) гармоник с первой по седьмую, как передаваемого, так и излучаемого видеосигнала, результаты измерений занести в таблицу 3;

Таблица 3 – Измеренные и рассчитанные данные

Параметры гармоник	Номер гармоники						
	1	2	3	4	5	6	7
Частота F, МГц							
Амплитуда передаваемого видеосигнала, S1(F), мВ							
Амплитуда излучаемого видеосигнала, S2(F), мВ							
Разность амплитуд, $\Delta S(F)$, мВ							

- рассчитать разность амплитуд гармоник между передаваемым и излучаемым видеосигналами, $\Delta S(F) = S1(F) - S2(F)$, результаты расчета занести в таблицу 3;

- определить изменения амплитуд, каких гармоник привели к существенному искажению излучаемого сигнала (ПЭМИ);

- сделать выводы по результатам проделанной работы.

7) Исследовать возможность распознавания видеосигнала после перехвата его ПЭМИ с помощью технических средств разведки, с этой целью:

- установить параметры корректирующих генераторов таким образом, чтобы с их помощью устранить разность амплитуд $\Delta S(F)$ для четырех гармоник, внесших наиболее существенный вклад в искажение излученного видеосигнала; при этом если разность $\Delta S(F)$ положительная, то в генераторе начальная фаза должна быть равна 0 градусов, т.е. корректирующий сигнал – синфазен с корректируемым, если разность $\Delta S(F)$ отрицательная, то в генераторе начальная фаза должна быть равна 180 градусов, т.е. корректирующий сигнал должен быть в противоположенной фазе с корректируемым сигналом;

- подключить ко второму каналу осциллографа выход приемника, нажав клавишу «1», запустить симулятор и зарегистрировать с помощью осциллографа и отобразить в отчете откорректированный видеосигнал;
- сравнить откорректированный видеосигнал с исходным передаваемым видеосигналом и сделать вывод о возможности его распознавания.

8) Самостоятельно выполнить данное задание для других исходных данных (см. таблицу 4) по варианту указанному преподавателем. После корректировки принятого видеосигнала при необходимости провести сглаживание его высокочастотных колебаний подбором величины конденсатора C_2 .

Таблица 4 – Исходные данные для самостоятельного исследования.

№ варианта	Скорость цифрового видеопотока	Характеристики видеокабеля
1.	400 Мбит/с	$R = 2 \text{ Ом}, L = 0.005 \text{ мкГн}, C = 50 \text{ пФ}$
2.	540 Мбит/с	$R = 2 \text{ Ом}, L = 0.005 \text{ мкГн}, C = 50 \text{ пФ}$
3.	160 Мбит/с	$R = 1 \text{ Ом}, L = 0.004 \text{ мкГн}, C = 150 \text{ пФ}$
4.	120 Мбит/с	$R = 1 \text{ Ом}, L = 0.004 \text{ мкГн}, C = 150 \text{ пФ}$
5.	140 Мбит/с	$R = 2 \text{ Ом}, L = 0.05 \text{ мкГн}, C = 100 \text{ пФ}$
6.	100 Мбит/с	$R = 2 \text{ Ом}, L = 0.05 \text{ мкГн}, C = 100 \text{ пФ}$
7.	400 Мбит/с	$R = 2 \text{ Ом}, L = 0.05 \text{ мкГн}, C = 50 \text{ пФ}$
8.	540 Мбит/с	$R = 2 \text{ Ом}, L = 0.05 \text{ мкГн}, C = 50 \text{ пФ}$
9.	160 Мбит/с	$R = 1 \text{ Ом}, L = 0.01 \text{ мкГн}, C = 80 \text{ пФ}$
10.	120 Мбит/с	$R = 1 \text{ Ом}, L = 0.01 \text{ мкГн}, C = 80 \text{ пФ}$
11.	140 Мбит/с	$R = 2 \text{ Ом}, L = 0.05 \text{ мкГн}, C = 150 \text{ пФ}$
12.	100 Мбит/с	$R = 2 \text{ Ом}, L = 0.05 \text{ мкГн}, C = 150 \text{ пФ}$

9) Сделать выводы по результатам выполненного задания.

Задание 1.4. Оформить и защитить отчет по первой части проделанной лабораторной работы.

1) В отчете отобразить:

- тему и цель работы, порядок ее выполнения, задания исследований;
- исследуемые схемотехнические модели каналов утечки информации;
- измеряемые осциллограммы сигналов и их спектры;
- таблицы с результатами измерений и расчетов;
- полученные графики зависимостей;
- выводы по результатам проделанной работы и выполнения заданий.

2) Защитить отчет по первой части проделанной лабораторной работы.

3. Моделирование и исследование электрических каналов утечки информации, наводимых в линиях электропитания и заземления ТСПИ, соединительных линиях ВТСС и посторонних проводниках

Краткие теоретические или справочно-информационные материалы

Электрические каналы утечки информации связаны с перехватом информационных сигналов, проходящих по электрическим цепям различного назначения.

Они могут возникать за счет:

- утечки из электрических сетей связи;
- утечки информационных сигналов в цепях электропитания технических средств обработки информации;
- утечки информационных сигналов в цепь заземления технических средств обработки информации.

Классификация электрических каналов утечки информации приведена на рис. 5.1.

Наибольшее внимание уделяется электрическим цепям связи: проводным, кабельным. Получили распространение как контактные, так и бесконтактные способы подключения.

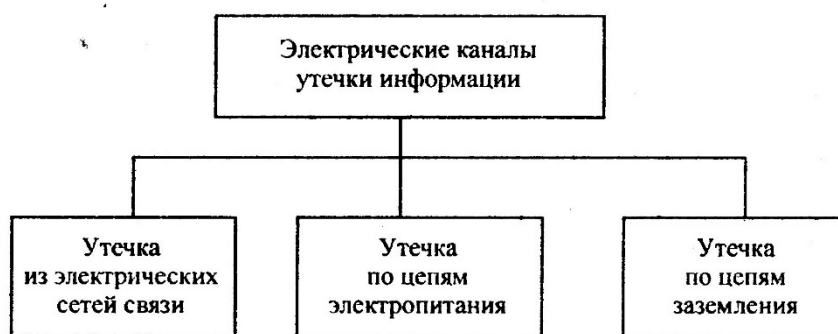


Рис. 5.1. Классификация электрических каналов утечки информации

Появление информационных сигналов в цепях электропитания технических средств, связанных с обработкой и передачей информации, чаще всего обусловлено тем, что они подключены к общим линиям питания.

В любом радиотехническом изделии имеется собственный блок питания, преобразующий входное напряжение от электросети в требуемые для работы напряжения постоянного или переменного тока. Опасный сигнал может при определенных условиях проникать через цепи питания прибора в сеть электропитания помещения, затем через силовой щит, распределительное устройство за пределы здания.

Электрический ток, потребляемый другим техническим средством, может содержать переменную составляющую информационному сигналу, который, как правило, значительно отличается от частоты электросети 50 Гц. С помощью фильтров информационный сигнал может быть выделен, усилен, обработан и записан.

В цепях питания конечных каскадов усилителей ток, потребляемый аппаратурой, изменяется в соответствии с изменением сигнала на входе усилителей. В результате в цепи питания появляются составляющие

информационного сигнала в диапазоне спектра огибающей 0-40 Гц. Исследования разборчивости огибающей речевого сигнала (двузначных чисел) показывают, что она достаточно высокая в указанной полосе частот и составляет 70%. Таким образом, если цепи питания выходят за пределы контролируемой зоны, то имеется реальная возможность перехвата информации.

Информационный электрический сигнал по цепям электропитания может передаваться от закладок, устанавливаемых в технических средствах обработки информации в линиях связи.

Информативное электрическое поле в контуре заземления возникает при подключений к нему оборудования для обеспечения электробезопасности обслуживающего персонала и снижения уровня помех. В этом случае токи речевого сигнала вследствие асимметрии трактов передачи информации будут протекать в контуре заземления. Опасный электрический сигнал может быть перехвачен как в заземляющем проводе, так и в «потенциальной» зоне вокруг заземления. Перехват информации во втором случае может быть осуществлен путем расположения одного из электродов аппаратуры разведки в зоне «нулевого» потенциала и перемещения другого электрода в «потенциальной» зоне заземления.

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.).

В зависимости от причин возникновения наводки информативных сигналов можно разделить на [1, 5, 9]:

а) наводки информативных сигналов в электрических цепях ТСОИ, вызванные информативными побочными и (или) паразитными электромагнитными излучениями ТСОИ;

б) наводки информативных сигналов в соединительных линиях ВТСС и посторонних проводниках, вызванные информативными побочными и (или) паразитными электромагнитными излучениями ТСОИ;

в) наводки информативных сигналов в электрических цепях ТСОИ, вызванные внутренними ёмкостными и (или) индуктивными связями («просачивание» информативных сигналов в цепи электропитания через блоки питания ТСОИ);

г) наводки информативных сигналов в цепях заземления ТСОИ, вызванные информативными ПЭМИ ТСОИ, а также гальванической связью схемной (рабочей) земли и блоков ТСОИ.

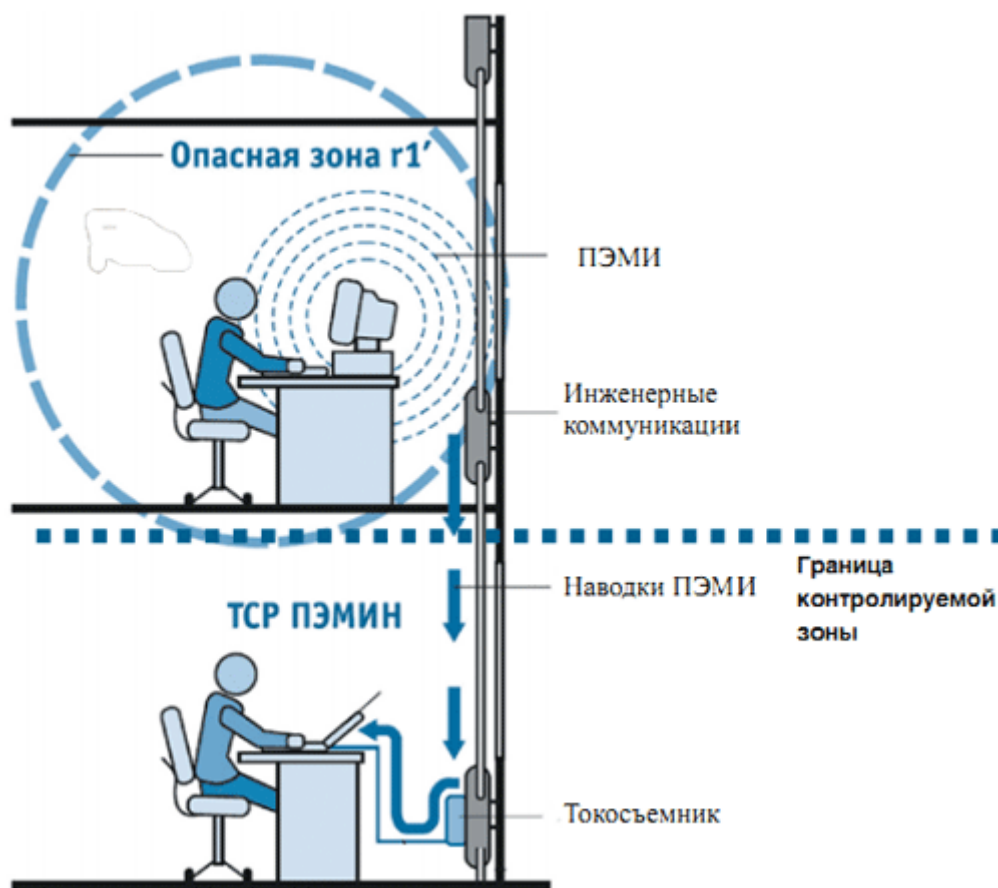


Рис. 8. Перехват наводок информативных сигналов с инженерных коммуникаций техническим средством разведки ПЭМИН

Различные вспомогательные технические средства, их соединительные линии, а также линии электропитания, посторонние проводники и цепи заземления выполняют роль случайных антенн, при подключении к которым средств разведки возможен перехват наведённых информативных сигналов (рис. 8).

Случайные антенны могут быть сосредоточенными и распределёнными.

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

К распределённым случайным антеннам относятся случайные антенны с распределёнными параметрами: кабели, провода, металлические трубы и другие токопроводящие коммуникации, выходящие за пределы контролируемой зоны. Уровень наводимых в них сигналов в значительной степени зависит не только от мощности излучаемых сигналов, но и расстояния до них от ТСОИ.

При распространении по случайной антенне наведённый информативный сигнал затухает. Коэффициент затухания информативного сигнала можно рассчитать или определить экспериментально. При известных коэффициенте усиления случайной антенны, её чувствительности и характеристиках приёмного устройства легко рассчитать значение наведённого информативного

сигнала, при котором вероятность его обнаружения приёмным устройством средства разведки будет равна нормированному значению ($P_0 = P_{\Pi}$).

Пространство вокруг ТСОИ, на границе и за пределами которого уровень наведённого от ТСОИ информативного сигнала в сосредоточенных антеннах не превышает допустимого (нормированного) значения ($U = U_n$), называется опасной зоной 1 (r_1), а в распределённых антеннах – опасной зоной 1' (r_1') [1, 7].

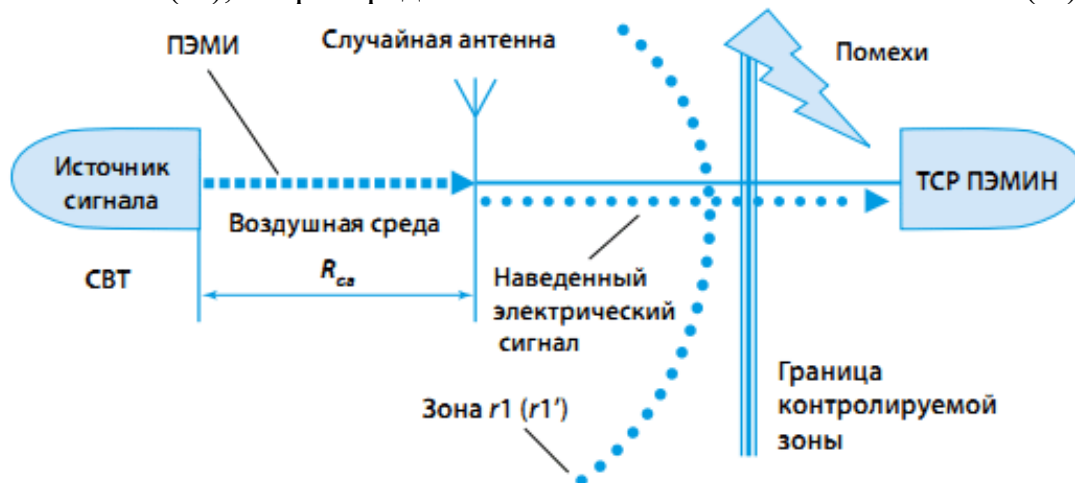


Рис. 9. Схема технического канала утечки информации, возникающего за счёт наводок побочных электромагнитных излучений СВТ в случайных антеннах (схема электрического канала утечки информации)

В отличие от зоны R2 размер зоны r_1 (r_1') зависит не только от уровня побочных электромагнитных излучений ТСОИ, но и от длины случайной антенны (от помещения, в котором установлено ТСОИ до места возможного подключения к ней средства разведки).

Зоны r_1 и r_1' для каждого СВТ определяются инструментально-расчётным методом, и их значения указываются в предписании на их эксплуатацию СВТ.

Для возникновения электрического канала утечки информации необходимо, чтобы (рис. 9):

- соединительные линии ВТСС, линии электропитания, посторонние проводники и т.д., выполняющие роль случайных антенн, выходили за пределы контролируемой зоны объекта;
- расстояние от СВТ до случайной сосредоточенной антенны было менее r_1 , а расстояние до случайной распределённой антенны было менее r_1' ;
- была возможность непосредственного подключения к случайной антенне за пределами контролируемой зоны объекта средств разведки ПЭМИН.

Появление информативных сигналов в цепи электропитания СВТ возможно как за счёт ПЭМИ, так и при наличии внутренних паразитных ёмкостных и (или) индуктивных связей выпрямительного устройства блока питания СВТ.

Наводки информативных сигналов в цепях заземления СВТ также могут быть обусловлены гальванической связью схемной (рабочей) земли и блоков СВТ.

В случае нахождения трансформаторной подстанции или заземлителя контура заземления за пределами контролируемой зоны объекта, при подключении к ним средства разведки ПЭМИН возможен перехват наведённых в них информативных сигналов (рис. 10).

Схемы технических каналов утечки информации, возникающих за счёт наводок информативных сигналов в линиях электропитания и заземления СВТ, приведены на рис. 11 и 12 соответственно.

Содержание практической работы, выполняемой студентами в ходе занятия

1. Описание лабораторного оборудования:

– ПЭВМ с программным редактором схематического моделирования «Electronics Workbench» (EWB), версия не ниже 5.12.

2. Требования безопасности при выполнении работы

3. Задание для работы

1). Самостоятельно смоделировать и провести исследование электрического канала утечки информации, возникающего путем наводки информационного сигнала в линию электропитания ТСПИ за счет гальванической паразитной связи.

2). Самостоятельно смоделировать и провести исследование электрического канала утечки информации, возникающего путем наводки информационного сигнала в соединительную линию ВТСС за счет емкостной паразитной связи.

3). Самостоятельно смоделировать и провести исследование электрического канала утечки информации, возникающего путем наводки информационного сигнала в цепь заземления ТСПИ за счет индуктивной паразитной связи.

3). Самостоятельно смоделировать и провести исследование электрического канала утечки информации, возникающего путем наводки от высокочастотного ПЭМИ информационного сигнала в посторонних проводниках.

5) Составить отчет о проделанной работе в соответствии с требованиями, изложенными в описании работы.

4. Порядок выполнения работы аналогичен предыдущим исследованиям.

5. ЗАЩИТИТЬ ОТЧЕТ ПО ВТОРОЙ ЧАСТИ, ПРОДЕЛАННОЙ ЛАБОРАТОРНОЙ РАБОТЫ.

Задание обучаемым для самостоятельной учебной работы при подготовке к лабораторной работе:

5. Закрепить и углубить знания, полученные на лекции, для этого изучить конспект лекций и рекомендуемую литературу.

6. Изучить методические указания к лабораторной работе №2 и подготовить отчет по лабораторной работе согласно методическим указаниям.

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1-3

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по выполнению практических работ
по дисциплине «Техническая защита информации»
для студентов направления подготовки
10.03.01 «Информационная безопасность»
Направленность (профиль)
«Организация и технологии защиты информации (по отрасли или в сфере профессиональной
деятельности)»

Ставрополь

2026

СОДЕРЖАНИЕ

Раздел № 6.....	77
Способы и средства выявления электронных устройств негласного получения информации	77
Практические занятия № 1-4.....	77
Раздел № 7.....	102
Способы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.....	102
Практические занятия № 5-8.....	102
Раздел № 8.....	113
Способы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам	113
Практические занятия № 9-13.....	113
Раздел № 9.....	129
Организация технической защиты информации	129
Практические занятия № 14-18.	129

1. Цель и задачи освоения дисциплины (модуля)

«Техническая защита информации» является формированием набора общекультурных и профессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность». Формируемые в рамках дисциплины компетенции способствуют решению профессиональных задач по защите информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях, а также приобретение набора общекультурных и общепрофессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ОПК-4 Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности;	ИД-3ОПК-4 Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	в совершенстве анализирует физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности
ОПК-11 Способен проводить эксперименты по заданной методике и обработку их результатов;	ИД-1ОПК-11 Показывает понимание сущности проведения экспериментов по заданной методике и обработку их результатов	-формулирует сущность проведения экспериментов по заданной методике и обработку их результатов; -выделяет целесообразные методики для проведения экспериментов; -демонстрирует уверенное использование процедур обработки результатов проведенных экспериментов
	ИД-2ОПК-11 Демонстрирует способность к реализации проведения экспериментов по заданной методике и обработку их результатов	-демонстрирует способность и проведения экспериментов по заданной методике и обработку их результатов; -уверенно выбирает заданные методики

		проведения экспериментов; -применяет методы обработки результатов экспериментов
ОПК-2.1 Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба;	ИД-1ОПК-2.1 Показывает понимание сущности анализа функционального процесса объекта защиты и его информационных составляющих	-демонстрирует понимание сущности анализа функционального процесса объекта защиты и его информационных составляющих; -формулирует сущность анализа функционального процесса объекта защиты и его информационных составляющих; -оперирует понятиями процесса анализа функционального процесса объекта защиты и его информационных составляющих
	ИД-2ОПК-2.1 Выявляет возможные источники информационных угроз, их возможные цели, пути реализации и предполагаемый ущерб	-выделяет возможные источники информационных угроз, их возможные цели, пути реализации и предполагаемый ущерб; -анализирует возможные источники информационных угроз, их возможные цели, пути реализации и предполагаемый ущерб; -оперирует понятиями возможных источников информационных угроз, их возможными целями, путями реализации;

РАЗДЕЛ № 6. СПОСОБЫ И СРЕДСТВА ВЫЯВЛЕНИЯ ЭЛЕКТРОННЫХ УСТРОЙСТВ НЕГЛАСНОГО ПОЛУЧЕНИЯ ИНФОРМАЦИИ

Тема № 28. ПРИНЦИПЫ ПОСТРОЕНИЯ И РАБОТЫ ПРОГРАММНО-АППАРАТНЫХ КОМПЛЕКСОВ ПОИСКА УСТРОЙСТВ НЕГЛАСНОГО СЪЕМА ИНФОРМАЦИИ

Практические занятия № 1 – 4.

Тема: Принципы построения и работы клавиатуры «с2000-к» и блока индикации «с2000-би» интегрированной системы охранно-пожарной сигнализации

Принципы построения и работы программно-аппаратных комплексов поиска устройств негласного съема информации

Время – 6 часов.

Формируемые компетенции: ОПК-4, ОПК-11, ОПК-2.1.

УЧЕБНЫЕ ВОПРОСЫ:

1. Принципы построения и характеристики программно-аппаратного комплекса радиомониторинга «Легенда».
2. Тактика применения программно-аппаратного комплекса радиомониторинга «Легенда».

СОДЕРЖАНИЕ ПРАКТИЧЕСКОГО ЗАНЯТИЯ

1. ПРИНЦИПЫ ПОСТРОЕНИЯ И ХАРАКТЕРИСТИКИ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА РАДИОМОНИТОРИНГА «ЛЕГЕНДА»

Основные понятия

Побочные электромагнитные излучения и наводки (ПЭМИН) от средств вычислительной техники являются одним из возможных каналов утечки информации. Побочные электромагнитные излучения (ПЭМИ) - это паразитные электромагнитные излучения радиодиапазона, создаваемые в окружающем пространстве устройствами, специальным образом для этого не предназначенными. Поиск и измерение ПЭМИН средств электронно-вычислительной техники вручную является трудоёмким и длительным процессом. При этом значительная часть выполняемых инженером-исследователем операций - однообразные рутинные процедуры: перестройка частоты, регистрация обнаруженных информационных ПЭМИН, запись частот и уровней этих излучений в таблицу. Поэтому автоматизация измерений ПЭМИН является важной и актуальной задачей, как в практическом, так и в теоретическом плане.

С точки зрения теории необходимо обоснованно выбрать метод автоматизации измерений, а на практике необходимо сформировать

измерительный комплекс, реализующий данный метод автоматизации измерений. К сожалению, в настоящее время наблюдаются значительные расхождения в результатах измерений, получаемых известными автоматизированными комплексами, так и между результатами, полученными квалифицированным инженером-исследователем вручную.

Задача измерения ПЭМИН

Согласно действующим нормативно-методическим документам (НМД), при проведении специсследований требуется измерять информативные ПЭМИН, т.е. такие излучения и наводки, создаваемые исследуемым техническим средством, которые содержат обрабатываемую данным техническим средством информацию. Такие излучения составляют лишь малую долю от всего спектра излучений технического средства. Все прочие излучения не должны фиксироваться. Для того чтобы выделить информационные ПЭМИН, на исследуемом техническом средстве предусматривают специальные тестовые режимы работы. Требования к тестам определяются в соответствующих ГОСТах и методиках. При поиске ПЭМИН исследователь прослушивает через головные телефоны сигналы на выходе демодулятора измерительного прибора, одновременно наблюдая осциллограммы этих сигналов. Если обнаружен сигнал, похожий на искомый тестовый сигнал, исследователь путём выключения и включения тестового режима исследуемого технического средства убеждается в том, что сигнал действительно генерируется именно этим средством и является информационным побочным излучением (наводкой). Таким образом, первым критерием для исследователя является информационная окраска искомого сигнала.

Второй, не менее важный критерий, - изменение уровня на частоте обнаруженного сигнала при включении и выключении теста на исследуемом техническом средстве. Инженер может столкнуться с трудностями при регистрации изменений уровня, если уровень ПЭМИН в тестовом режиме незначительно отличается от уровня в штатном режиме, и в этом случае, зачастую, приходится принимать решение об отнесении данного сигнала к спектру ПЭМИН, основываясь только на наличии информационной окраски.

Как известно, большинство информационных ПЭМИН представляют собой последовательность прямоугольных импульсов (пачек прямоугольных импульсов). Спектр такого сигнала описывается функцией $(\sin x)/x$ и имеет вид, показанный на рис. 1.

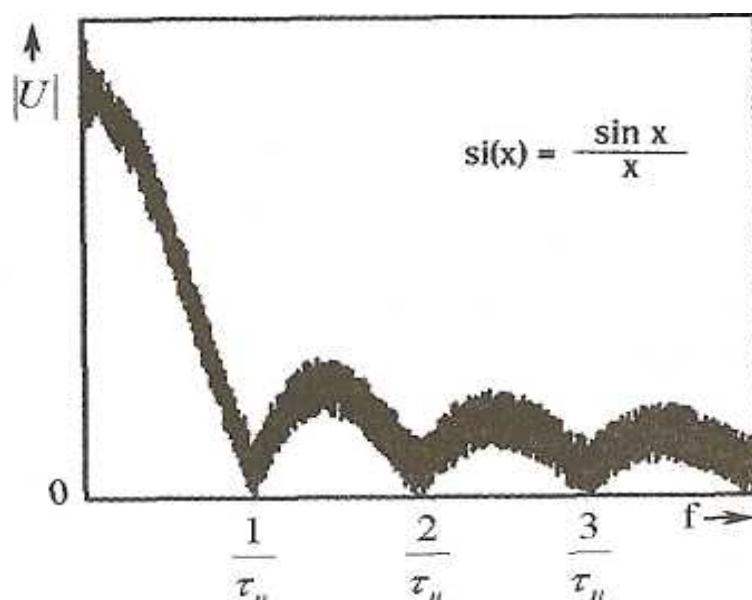


Рисунок 1 – Спектр сигнала ПЭМИН

В связи с тем, что уровень боковых составляющих сигналов, имеющих звуковую огибающую, ниже уровня центрального пика, при уровне сигнала, незначительно превышающем уровень шума, боковые составляющие могут оказаться ниже уровня шума, и звуковая огибающая не будет слышна.

Для того чтобы все же услышать звуковую огибающую, требуется подносить антенну вплотную к техническому средству, тем самым повышая отношение сигнал/шум. Для измерения же уровня сигнала антенну в соответствии с методикой следует относить на расстояние 1 м или более. Поиск информационных ПЭМИН требует от исследователя постоянной сосредоточенности, концентрации внимания. Постоянно растущий парк электронно-вычислительной техники, в том числе обрабатывающей секретную и конфиденциальную информацию, требует наращивания объемов специальных исследований.

Методы автоматизации

До недавнего времени на отечественном рынке средств автоматизации измерения ПЭМИН были представлены различные комплексы, которые так или иначе решают одну и ту же задачу, поэтому, несомненно, имеют довольно много общих черт, но есть и различия, причем весьма существенные. Чтобы прояснить эти различия, рассмотрим применяемые в комплексах методы автоматизации.

Автоматизация обнаружения гармонических составляющих тестового сигнала. Инструментальная реализация такого режима обычно приводит к тому, что автоматическая система, распознающая сигналы по их форме, работает лишь ненамного быстрее квалифицированного инженера-исследователя. Поэтому в первых комплексах данный режим не был реализован, а опознавание производится по критерию изменения уровней сигналов при включении тестового режима на исследуемом техническом средстве (так называемый «энергетический критерий»). Такой способ дает неплохие результаты: вся работа по обнаружению сводится к двум проходам сканирования

диапазона специсследования: при первом проходе запоминается картина шумов при выключенном тестовом режиме, при втором проходе исследуемое техническое средство переводится в тестовый режим, и измеряются уровни всех сигналов, превышающих запомненные шумы на заданное значение порога.

В результате инженер-исследователь получает таблицу частот и уровней сигналов (типичное количество обнаруженных составляющих - несколько сотен) и может рассчитать зоны разведдоступности. К сожалению, результаты расчета могут оказаться неверными. Дело в том, что электромагнитная обстановка имеет свойство изменяться со временем. В диапазоне от 9 кГц до 1000 МГц работают тысячи радиостанций и источников радиопомех. Некоторые из них время от времени включаются и выключаются, и если какой-то источник радиоизлучения не работал во время сканирования спектра шумов, а при втором проходе включился, его частота окажется в списке обнаруженных составляющих. Естественно, это может случайным образом изменить рассчитанные размеры зон разведдоступности. Таким образом, оператору приходится вручную проверять все обнаруженные составляющие, на что, при достаточно слабых сигналах, вновь будет уходить время. По-настоящему эффективно данный способ работает в безэховых экранированных камерах, которые ввиду своей дороговизны доступны очень немногим предприятиям. Поэтому в комплексах применено автоматическое опознавание информационных сигналов. Согласно методике инженеру-исследователю предлагается выполнить поиск какой-либо гармонической составляющей вручную или в специальном «полуавтоматическом» режиме, либо создать эталонный образ искомого сигнала при помощи редактора (генератора), либо выбрать ранее созданный образ из библиотеки, после чего комплекс автоматически обнаруживает в эфире сигналы, похожие на заданный сигнал.

Для опознавания сигналов в комплексах применяется взаимно корреляционная функция, в сочетании с Байесовским критерием минимального риска. Как отмечалось выше, это более затратный по времени способ, но и существенно более точный. Для преодоления отставания в скорости работы от комплексов, использующих «энергетический» критерий, разработчики комплексов, работающих по «информационному» критерию, используют различные приемы, такие как анализ сигнала в окрестностях частот, кратных тактовой частоте теста, измерения партий однотипных технических средств с использованием шаблонов частот. Это приводит к заметному ускорению работы без снижения точности.

Автоматизация измерения уровней сигналов. Метрологические приборы, имеющие детектор и позволяющие измерять пиковые значения уровней электромагнитных излучений, должны быть откалиброванными и проверены так, что должно быть подтверждено метрологическим сертификатом или, если прибор внесен в реестр измерительной аппаратуры Госстандарта, свидетельством о поверке. Однако получать пиковые (квазипиковые) значения непосредственно могут только те приборы, которые оснащены квазипиковым детектором. Если такого детектора нет в составе прибора, то для корректного измерения пиковых значений уровней требуется использование специальной

методики. Необходимо строго выдерживать параметры измерения, такие как время сканирования, полоса пропускания, выбор детектора, иначе при некоторых формах сигналов полученные с помощью анализатора спектра значения уровней могут отличаться от действительных пиковых значений. Следовательно, в автоматизированных комплексах, построенных на базе анализаторов спектра, должна быть реализована методика корректного измерения пиковых значений, и ее работа должна проверяться в ходе сертификационных испытаний комплекса.

Измерение наводок в сети питания, линиях и коммуникациях. Согласно действующей НМД, измерение наводок в сети питания должно осуществляться при помощи эквивалента сети или пробников напряжения. Эквивалент сети, как известно, достаточно сложное и относительно дорогостоящее устройство, однако измерения, проведенные с его помощью обычно точнее измерений, выполненных с помощью пробника напряжения. «Чистая» сеть, имитируемая эквивалентом сети, позволяет измерять создаваемые исследуемым техническим средством наводки в сеть питания, уровень которых на 4-6 дБ выше собственных шумов эквивалента сети, в то время как точность измерений, выполняемых при помощи пробника напряжения, зависит от уровней шума сети питания.

Ознакомление с ПАК для проведения специсследований «Легенда»

Программно-аппаратный комплекс «Легенда», далее по тексту «изделие», предназначен для автоматического и полуавтоматического поиска и измерения уровней побочных электромагнитных излучений и наводок (ПЭМИН), автоматического расчета размеров зон R_1 , R_2 для объектов 1, 2 и 3 категорий и требуемого затухания фильтров питания.

Технические характеристики

- 1) ПАК «Легенда» обеспечивает измерение ПЭМИН:
 - по электрической составляющей электромагнитного поля в диапазоне от 9 кГц до 1800 МГц;
 - по магнитной составляющей электромагнитного поля в диапазоне от 9 кГц до 30 МГц.
- 2) Измеряет наводки в инженерных коммуникациях от 9 кГц до 100 МГц.
- 3) Позволяет устанавливать следующие полосы пропускания – 1 кГц, 3 кГц, 9 кГц, 10 кГц, 100 кГц, 120 кГц, 300 кГц, 1 МГц, 3 МГц.
- 4) Позволяет осуществлять:
 - измерение пиковых значений уровней ПЭМИН;
 - измерение среднеквадратических значений уровней шумов на объектах информатизации;
 - автоматическое обнаружение и измерение уровней информационных ПЭМИН.
- 5) Результаты измерений, произведённых при помощи изделия, не требуют ручной проверки.
- 6) Питание изделия - от однофазной сети переменного тока 220 В $\pm$ 10%, частотой 50 Гц;
- 7) Эксплуатируется при следующих климатических условиях:

- температура окружающего воздуха от +5 до +35°C;
- относительная влажность окружающего воздуха от 45 до 80%;
- атмосферное давление от 0,86 до 1,06 кг/см кв. (от 645 до 795 мм. рт. ст.).

Состав комплекса

Измерительный прибор R&S FS300. Управляющая ПЭВМ. Комплект антенн «Альбатрос-2». Пробник напряжения измерительный Я6-122.

Устройство и работа комплекса

Изделие осуществляет автоматический поиск гармонических составляющих ПЭМИН по так называемым энергетическому и информационному критериям. При поиске ПЭМИН по энергетическому критерию обнаруживаются сигналы, уровни которых превышают уровни фоновых шумов. По информационному критерию осуществляется поиск сигналов, форма которых подобна форме заданного эталонного образа, с использованием математических методов распознавания образов. Автоматическое измерение уровней производится с использованием пикового детектора по специально разработанной методике. Автоматический расчет зон осуществляется согласно Сборнику методических рекомендаций Гостехкомиссии (ФСТЭК) России.

Программное обеспечение изделия состоит из программы управления измерительными приборами для проведения специальных исследований и программы расчёта параметров защищённости технических средств СВТ от утечки информации по техническим каналам ПЭМИН.

Программное обеспечение поставляется на компакт-дисках и эксплуатируется на ПЭВМ и с измерительным прибором, удовлетворяющих следующим требованиям:

- управляющая ПЭВМ построена на базе процессоров фирм AMD, Cytrix, IBM с тактовой частотой не ниже 100 МГц;
- объем оперативной памяти не менее 32 Мб;
- необходимый объем дискового пространства для размещения управляющей программы составляет не менее 20 Мб;
- управляющая программа функционирует под управлением операционных систем Windows 95, Windows 98, Windows ME, Windows 2000 фирмы Microsoft и более поздних версий;
- ПЭВМ комплектуется интерфейсом GPIB производства фирмы National Instruments и сконфигурирована для работы с этим интерфейсом;
- управляющая программа работает с измерительным прибором E4403B фирмы Agilent Technologies, укомплектованным встроенным GPIB (HPIB) интерфейсом.

Описание и работа составных частей

Антенная система. Комплект антенн «Альбатрос-2» (антенна рамочная активная «АГМ-30»; антенна активная дипольная «АГ-50»; антенна пассивная дипольная «АГ-1000»; антенна пассивная дипольная «АГ-2000») предназначен для измерения напряженности синусоидальных, шумовых и импульсных магнитных («АГМ-30») и электрических («АГ-50», «АГ-1000», «АГ-2000»)

полей радиопомех, в лабораторных помещениях, экранированных камерах и на открытых площадках в комплекте с измерительными приемниками, анализаторами спектра, селективными микровольтметрами любого типа, в задачах обеспечения электромагнитной совместимости радиоэлектронных средств, защиты информации, а также предельно допустимых уровней электромагнитных полей в задачах обеспечения эколого-защитных мероприятий.

Измерительный прибор R&S FS300 представляет собой прецизионный анализатор спектра с диапазоном частот от 9 кГц до 3 ГГц. Предназначен для автоматического и полуавтоматического поиска и измерения уровней побочных электромагнитных излучений и наводок (ПЭМИН).

Управляющая ПЭВМ с управляющей программой предназначены для автоматического и полуавтоматического управления измерительными приборами в процессе проведения специсследований, с целью формирования массивов исходных данных для расчета зон. Внешний вид окон программы, общий алгоритм функционирования и правила работы с ней не зависят от типа применяемого измерительного прибора.

Программа позволяет производить автоматический и полуавтоматический поиск и измерение параметров побочных электромагнитных излучений и наводок (далее ПЭМИН) и акустоэлектрических преобразований (далее АЭП).

Пробник напряжения предназначен для измерения напряжения промышленных радиопомех в электрических цепях, и представляет собой RC-фильтр верхних частот. Измерение напряжения радиопомех производится при соединении через пробник измерителя промышленных радиопомех (ИРП) с источником ИРП.

Задание для работы

- 1) Ознакомиться с назначением и принципом работы ПАК «Легенда».
- 2) Ознакомиться с внешним видом и функциональными кнопками измерительного прибора R&S FS300.
- 3) Ознакомиться с областью диаграмм, меню и функции.
- 4) Изучить порядок проведения специсследования на поиск тестового сигнала.
- 5) Изучить порядок составления протокола измерений с помощью расчетной программы.

Порядок выполнения работы

1. Изучить назначение функциональных кнопок измерительного прибора R&S FS300 (рис. 2 и рис. 3).

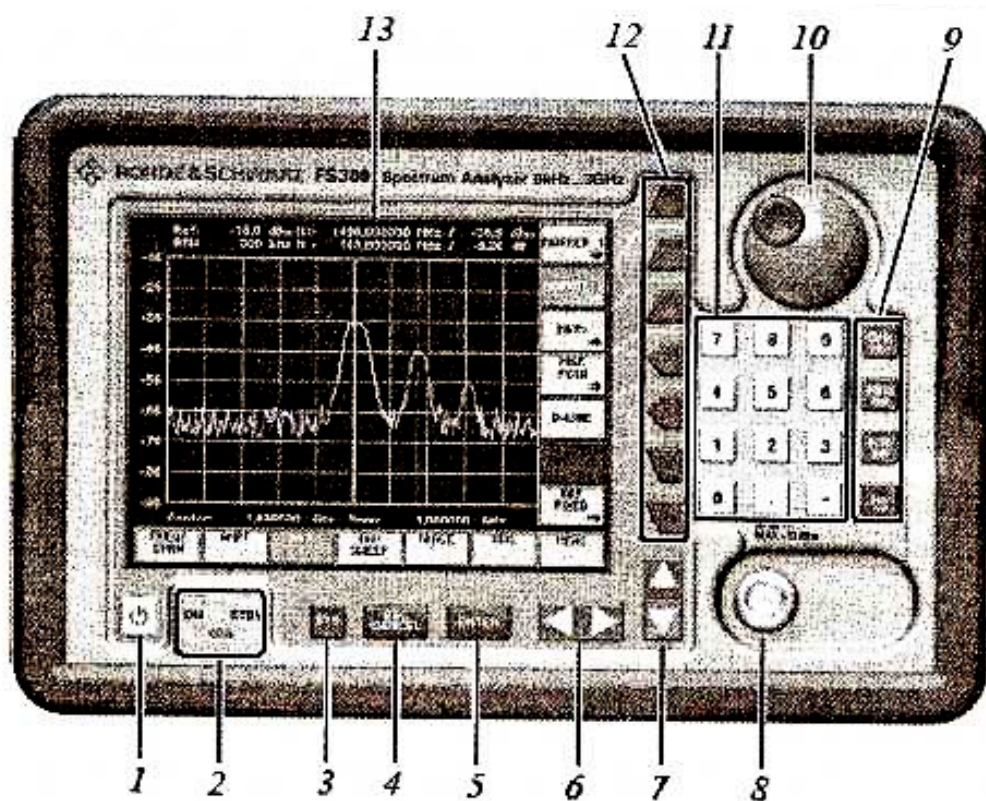


Рисунок 2 – Лицевая панель прибора:

1 - питание (Вкл/Выкл); 2 - индикатор питания (Вкл/Выкл),ожидание;
 3 - системное меню; 4 - отмена ввода операций; 5 - ввод операций;
 6 - курсор (влево-вправо); 7 - курсор (вниз-вверх); 8 - вход для подключения антенн и пробника; 9 - установка частоты; 10 - вращающаяся кнопка;
 11 - цифровое табло; 12 - функциональные кнопки; 13 – экран.

2. Подготовить изделие к использованию. Изделие устанавливается и размещается в следующем порядке:

- управляющая ПЭВМ и измерительный прибор (FS300) устанавливаются в соответствии с инструкциями по эксплуатации;
- измерительный прибор соединяется кабелем USB с компьютером.

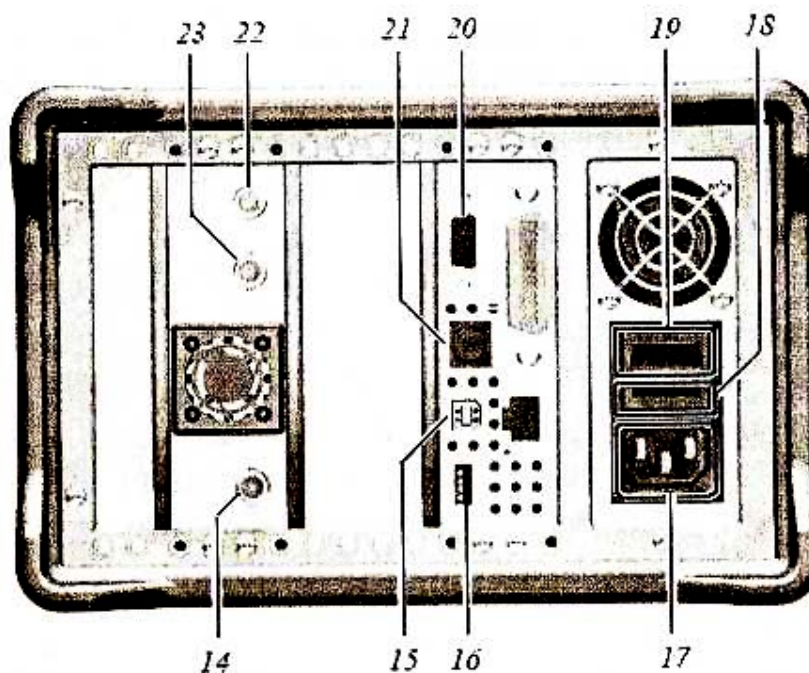


Рисунок 3 – Тыльная панель прибора:

14 — соединения для внешнего триггера; 15 - соединение через USB;
 16 - выход USB для устройств; 17 - вход для питания прибора;
 18 - предохранитель; 19 - кнопка предохранителя; 20 - соединение для монитора; 21 - соединение для клавиатуры; 22 - вход устройства; 23 - выход устройства.

3. Выполнить подготовку к работе с изделием в следующем порядке:

- включить измерительный прибор, коммутатор антенн и антенную систему в произвольном порядке;
- подключить электропитание;
- установить исследуемое техническое средство в соответствии с руководством по эксплуатации технического средства и методикой проведения СИ.

Если исследуемое техническое средство представляет собой персональную ЭВМ, работающую под управлением Windows-95/98/ME/2000 и более поздних версий, для создания тестовых режимов работы исследуемого средства следует установить на него тестовое программное обеспечение для операционной системы Windows, например, производства НПП «Гамма» (пакет программ для создания тестовых режимов работы ПЭВМ «Легенда»). В иных случаях необходимо организовать тестовый режим работы исследуемого средства в соответствии с методикой проведения специсследований.

4. Провести процедуру измерения. Для этого:

- подключите антенну (нулевая-диполь) к R&S FS300 с помощью кабеля A117.41 в разъем 8;
- подключите анализатор спектра к сети электропитания;
- нажмите кнопку включить 1;

- нажмите кнопку SYS (после загрузки);
- выберите PRESET;
- выберите FREG/SPAN с помощью курсора 6 и нажмите CENTER (центр) функционального меню и введите 200 MHz;
- выберите FREG/SPAN с помощью курсора 6 и нажмите SPAN (диапазон) функционального меню и введите 1 MHz;
- выберите MKR (маркер) с помощью курсора 6 и нажмите MARKER_1 функционального меню и нажмите PEAK функционального меню, или переместите с помощью вращающей кнопки на пик сигнала;
- нажмите кнопку SIGNAL COUNT (счет сигнала) функционального меню в MARKER_1;
- нажмите кнопку COUNT RESOL (результаты счета) функционального меню в MARKER_1;
- просмотрите полученные данные на диаграммном меню и внесите в отчет.

2. ТАКТИКА ПРИМЕНЕНИЯ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА РАДИОМОНИТОРИНГА «ЛЕГЕНДА».

1. Проведение поиска и измерения ПЭМИН при помощи управляющей программы

Запуск управляющей программы. Для запуска управляющей программы следует выбрать в меню «Пуск» соответствующий ярлык или вызвать исполняемый файл, на который ссылается данный ярлык (Легенда-управление). В результате запуска на экран управляющей ПЭВМ выводится главное окно управляющей программы (рис. 4).

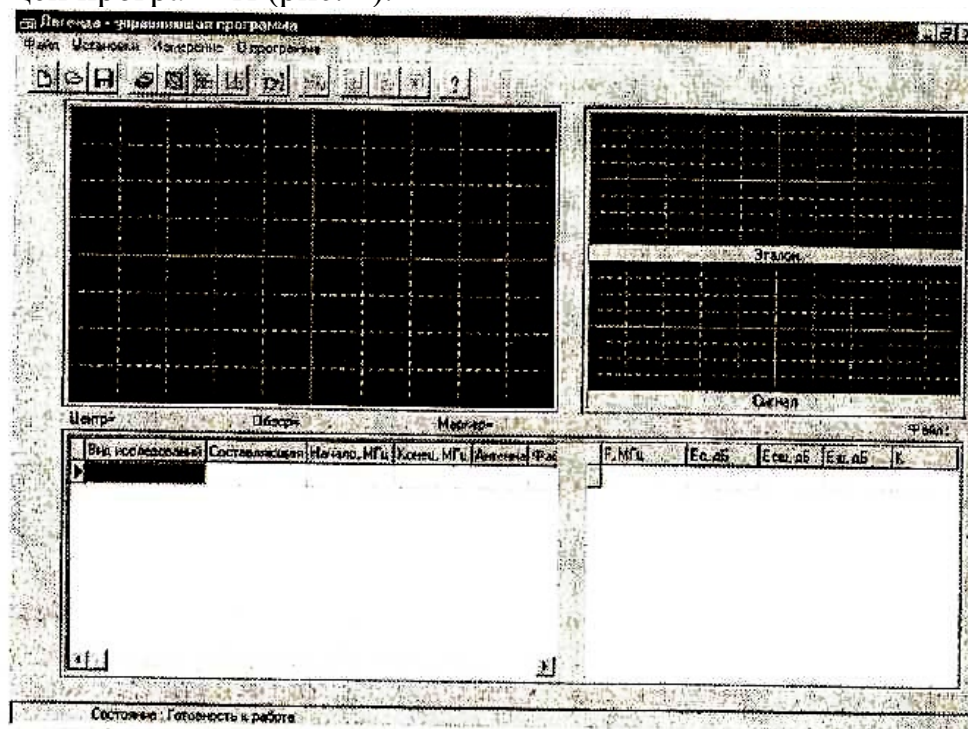


Рисунок 4 – Главное окно управляющей программы

1.1. Рекомендации по контролю электромагнитной обстановке (ЭМО)

в автоматическом режиме измерений

1) Автоматический поиск гармонических составляющих тестового сигнала по заданному эталону можно производить методом беспропускowego контроля по всему диапазону проведения специсследования, либо в окрестностях частот, кратных тактовой частоте теста. В обоих случаях, перед проведением поиска составляющих по «информационному» критерию, то есть по сходству демодулированного на данной частоте сигнала с эталоном, рекомендуется произвести предварительный контроль ЭМО при выключенном тесте на исследуемом техническом средстве. Для предварительного контроля ЭМО следует составить программу исследования, в которой указывается вид исследования, диапазон исследования, вид составляющей электромагнитного поля или наводок в линиях, используемая антенна и параметры прибора (полоса обзора, полоса пропускания, детектор, количество усреднений). Для составления программы выберите в меню главного окна программы «Установки/Программа исследований». Поверх главного окна программы откроется окно параметров исследования на странице программы исследований.

Рисунок 5 – Окно параметров исследования

2) В таблице программы исследования, расположенной в верхней части страницы, отображается программа, готовая к исполнению. По умолчанию таблица содержит программу, составленную при прошлом запуске управляющей программы. При необходимости, программу можно полностью очистить, нажав на кнопку «мусорная корзина», либо стереть любую строку программы, нажав кнопку «ножницы». Также можно воспользоваться кнопками DB-Navigator'a, расположенными непосредственно под таблицей. Каждая строка программы исследований содержит инструкции для управляющей программы для проведения тех или иных измерений на одном поддиапазоне. Если между

поддиапазонами необходимо сделать паузу для замены антенны или изменения ее конфигурации, например, после любого поддиапазона можно вставить строку с видом исследования «Пауза...». Строки таблицы редактируются непосредственно, либо в полях редактора. Отличие этих способов состоит в том, что при редактировании в полях редактора программа выполняет проверку корректности вводимых данных: проверяет соответствие диапазонов измерения выбранным антеннам, существование выбранных файлов исходных данных, корректность ввода числовых значений.

3) Для непосредственного редактирования таблицы, щелкните «мышью» по ячейке таблицы для выбора данной ячейки. Второй щелчок «мыши» переводит ячейку в режим редактирования. В ячейках, допускающих выбор из различных альтернатив (вид исследования, составляющая (электрическая), антенна, демодулятор, детектор) появляется кнопка, нажатие на которую приводит к выдаче ниспадающего списка альтернатив. В ячейках, предназначенных для ввода имени файла, появляется кнопка для обзора дисковой системы и выбора файла. Заметьте, что для правильной работы программы необходимо в каждой строке таблицы выбирать уникальное имя файла ЭМО, то есть результаты сканирования каждого диапазона должны быть сохранены в отдельном файле. В остальные ячейки значения вводятся только непосредственно.

4) Для заполнения пустой таблицы, создания новой программы, существенно отличающейся от ранее созданной, рекомендуется пользоваться полями редактирования. Для изменения существующей строки программы следует «импортировать» значения ячеек таблицы в поля редактирования, для чего нажать на кнопку «Импорт». Далее для предварительного контроля ЭМО выберите вид исследования: «Контроль ЭМО», укажите требуемую составляющую (например, электрическая) электромагнитного поля, задайте диапазон исследования и параметры прибора в соответствующих полях редактирования.

5) После завершения редактирования строки, внесите ее в таблицу, нажав кнопку «Внести в таблицу».

6) После завершения заполнения таблицы программы исследования следует нажать кнопку «Ок» окна параметров исследования и выбрать в меню главного окна программы «Измерения - Старт», либо нажать соответствующую кнопку быстрого запуска. Программа автоматически сканирует выбранный диапазон и по завершении выдает сообщение «Программа исследования завершена». При этом результаты сканирования сохранены в соответствующих выбранных файлах ЭМО для каждого диапазона (каждой строки программы) и их можно использовать для автоматического поиска составляющих тестового сигнала при включенном тесте.

1.2. Рекомендации по поиску составляющих тестового сигнала в автоматическом режиме измерений

1) Для поиска составляющих тестового сигнала следует заполнить программу исследований. Для этого достаточно заменить вид исследований во всех заполненных строках таблицы на «Измерение ПЭМИН» или «Обнаружение ПЭМИН» (если необходимо только обнаружить составляющие и не производить

дальнейших измерений), задать в каждой строке таблицы имя файла результатов (можно отдельные имена для каждой строки или одно общее имя, которое нужно указать во всех строках таблицы) и программа исследования готова к запуску.

2) При необходимости заполнения программы исследования «от нуля» следует руководствоваться следующими правилами:

- при использовании файла ЭМО необходимо задавать в точности те же диапазоны и параметры прибора, тактовая частота, что и при контроле ЭМО;

- при непосредственном редактировании таблицы, если файл ЭМО не был создан для какого-то диапазона, ячейка «Файл ЭМО» должна быть обязательно заполнена: в нее должно быть записано «не использовать» (без кавычек, строчными буквами). При редактировании таблицы с помощью полей редактирования данная фраза автоматически заносится в соответствующую ячейку, если поле «Файл ЭМО» оставлено пустым.

3) После заполнения программы исследования, следует загрузить эталон. При этом значение порогового коэффициента корреляции, сохраненное в эталоне, автоматически занесется в соответствующую ячейку таблицы программы исследований, а форма эталонного сигнала будет отображена в соответствующем дисплее главного окна управляющей программы. После загрузки эталона, выберите в меню главного окна программы «Измерения - Старт» либо нажмите соответствующую кнопку быстрого запуска. Программа начнет сканировать диапазон, выделять пики, превышающие на заданное значение уровень шумов при выключенном тесте, либо само заданное значение превышения, если файл ЭМО не использовался. Демодулированный сигнал будет сравниваться с эталоном и при превышении коэффициентом корреляции заданного порога, значение частоты будет занесено в таблицу. По завершении сканирования каждого поддиапазона, если был выбран вид исследования «Измерение ПЭМИН», производится автоматическое измерение уровней сигнала на каждой из частот обнаруженных составляющих тестового сигнала. Если был выбран режим «Обнаружение ПЭМИН, измерение уровней не производится. Если был выбран вид исследования «Измерение ПЭМИН», то по завершении сканирования всех диапазонов, выдается сообщение «Выключите тест для измерения уровней шумов» и программа выполняет необходимые действия. В конце работы выдается сообщение «Программа исследований выполнена».

4) По завершении автоматического поиска и/или измерения ПЭМИН можно проконтролировать правильность обнаружения. Для этого щелкните «мышью» по любой строке таблицы обнаруженных частот главного окна управляющей программы. На основном дисплее главного окна программы будет отображаться в реальном времени осциллограмма демодулированного сигнала на данной частоте. Включая и выключая тест на исследуемом техническом средстве, и наблюдая за изменениями формы осциллограммы, можно сделать вывод о принадлежности данного излучения к составляющим тестового сигнала. В случае ложного срабатывания процедуры распознавания, строку с ошибочно распознанным сигналом можно удалить, для чего следует нажать CTRL-DEL на клавиатуре управляющей ПЭВМ.

2. Проведение поиска и измерения ПЭМИН в полуавтоматическом

режиме измерения

2.1. Переход в полуавтоматический режим измерений

Для перехода в полуавтоматический режим измерений выберите в меню главного окна программы пункт «Измерения - Ручной режим» или нажмите соответствующую кнопку быстрого запуска. На экране управляющей ПЭВМ выводится окно полуавтоматического режима (рис. 6).

Создайте папку на рабочем столе, в которой будут сохраняться полученные данные измерения.

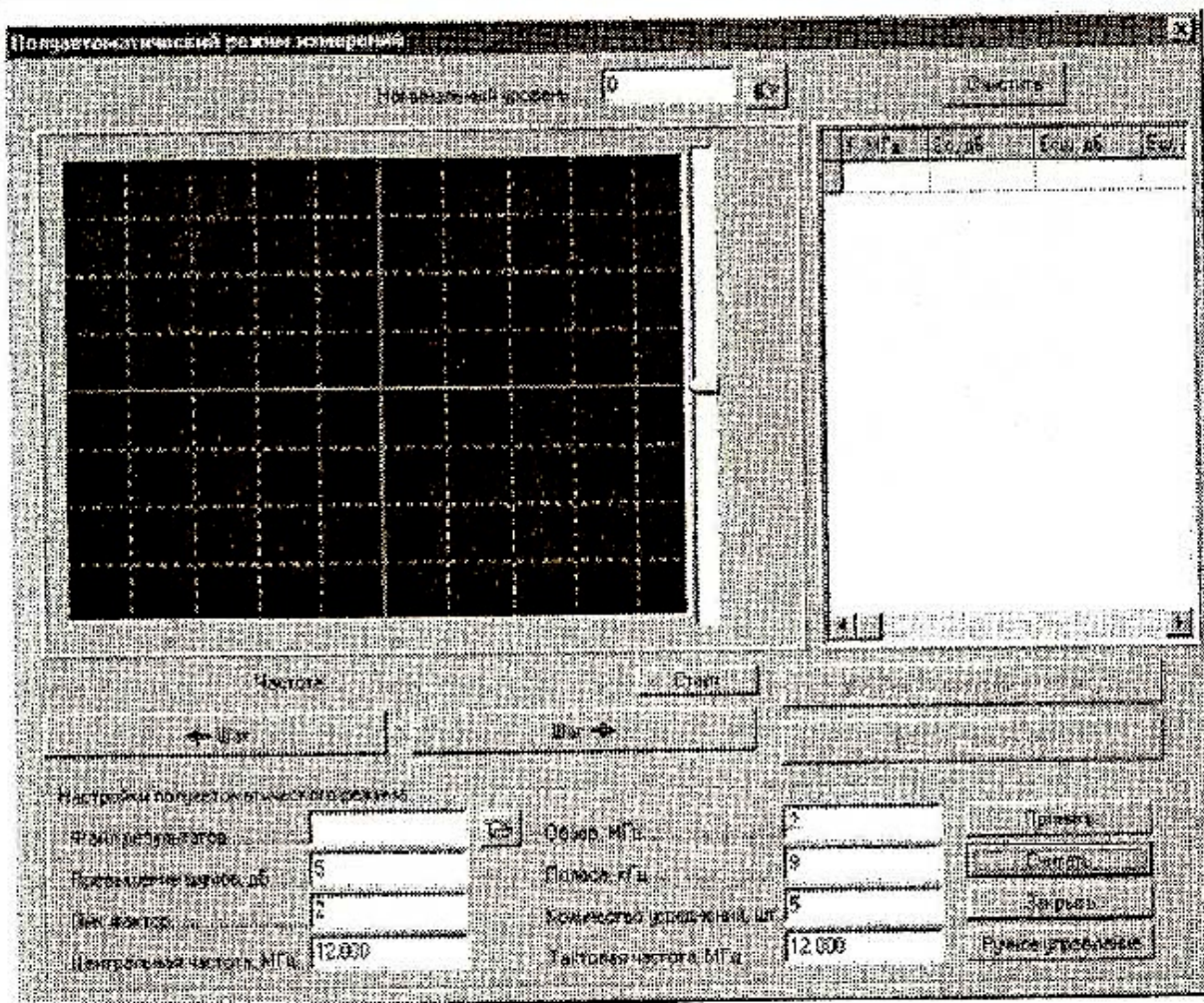


Рисунок 6 – Полуавтоматический режим измерения

2.2. Поиск тактовой частоты

Для поиска тактовой частоты при известной примерно ожидаемой тактовой частоте теста, установите в окне полуавтоматического режима измерений данную частоту в поле «Центральная частота», установите обзор, равный 2 МГц или более, установите полосу пропускания в поле «Полоса» равную 9 кГц при центральной частоте меньшей 30 МГц. Устанавливать количество усреднений трека (поле «Количество усреднений») рекомендуется не менее 5. Чем больше выбранное количество усреднений трека, тем выше точность измерения, тем выше вероятность обнаружить составляющую тестового сигнала.

После выбора параметров следует задать имя файла результатов,

непосредственно введя его в соответствующее поле, либо указав его местоположение при помощи кнопки обзора, расположенной рядом с данным полем. В файл результатов могут помещаться значения частот обнаруженных составляющих тестового сигнала. При необходимости, таблицу можно очистить, нажав кнопку «Очистить», расположенную над таблицей.

Для сканирования диапазона с выбранными исходными данными нажмите кнопку «Принять». На дисплее окна полуавтоматического режима изображается текущее усреднение трека спектра, но завершении усреднений картинка останавливается.

Для поиска гармонических составляющих тестового сигнала можно вручную проверить каждый пик трека спектра. Для этого подведите курсор «мыши» к выбранному пику, удерживая нажатой левую кнопку «мыши». При этом внизу под дисплеем отображается значение частоты, совместно с курсором «мыши» перемещается маркер желтого цвета. Настроившись на нужный пик, отпустите левую кнопку «мыши». Поверх окна полуавтоматического режима выводится окно просмотра пика (рис. 7).

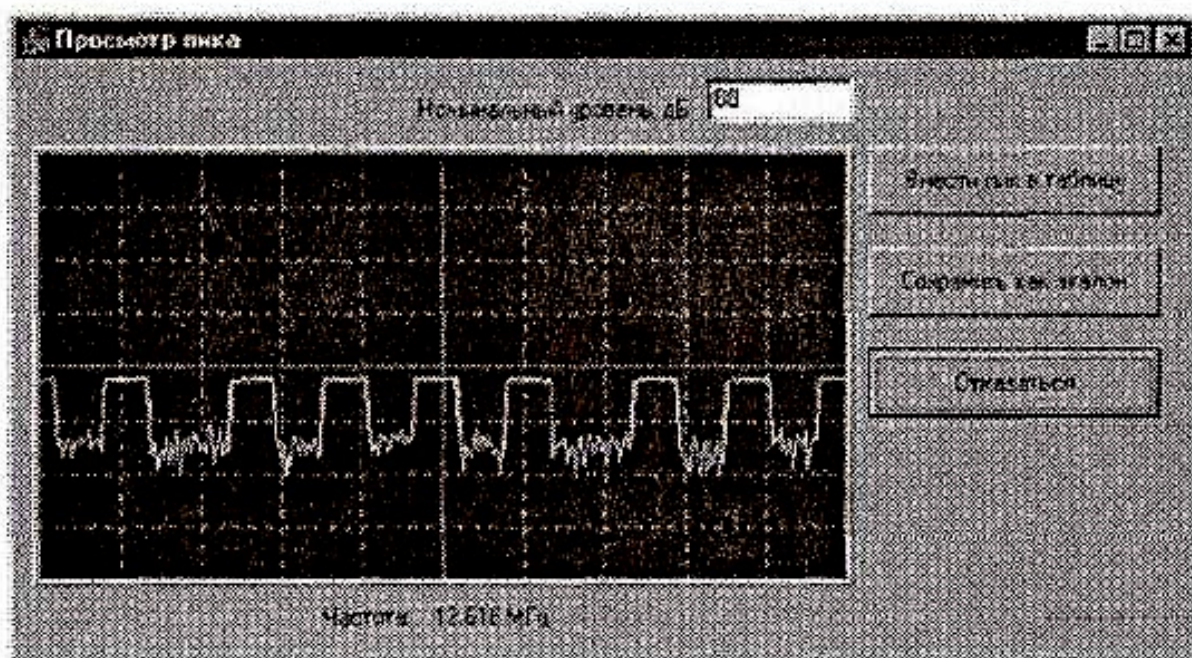


Рисунок 7 – Окно «Просмотр пика»

На дисплее этого окна отображается осциллограмма сигнала, демодулированного при помощи измерительного прибора. Включая и выключая тестовый режим работы исследуемого технического средства и, наблюдая за осциллограммой, можно установить, принадлежит ли данное излучение гармоническим составляющим тестового сигнала.

При обнаружении тестового сигнала следует сохранить его как эталон, нажав на кнопку «Сохранить как эталон» окна просмотра пика, если планируется в дальнейшем производить автоматический поиск составляющих тестового сигнала, после чего нажать кнопку «Отказаться».

Окно просмотра пика при этом закрывается. Если планируется произвести

поиск всех составляющих тестового режима вручную, следует внести частоту обнаруженной составляющей тестового сигнала в таблицу обнаруженных частот (файл результатов), нажав кнопку «Внести в таблицу». При этом окно просмотра пика закрывается, а значение частоты пика вносится в таблицу.

Возможно автоматическое занесение в таблицу значений частот пиков, превышающих заданный порог. Для этого установите требуемое превышение в поле «Превышение шумов», после чего нажмите кнопку «Внести все пики в таблицу». Превышение можно установить графически, передвигая при помощи «мыши» ползок, размещенный справа от дисплея окна полуавтоматического режима. Совместно с ползком перемещается горизонтальный маркер красного цвета.

Для повышения скорости обнаружения составляющих тестового сигнала можно перед анализом пиков на наличие информационной окраски огибающей тестового сигнала найти частоты, уровень излучения на которых снижается при выключении теста. Для этого следует задать превышение 5 дБ (можно установить иное значение превышения, но при незначительном превышении количество пиков для последующего анализа может не слишком сильно сократиться, установка же чересчур большого превышения приведет к невозможности обнаружить какой-либо пик).

Прочие параметры следует оставить теми же, что и для сканирования при включенном тесте. Также возможно с помощью кнопок «Шаг» можно перейти на другую частоту согласно выбранной тактовой частоты. Выключите тест на исследуемом техническом средстве и нажмите кнопку «Тест выключен» окна полуавтоматического режима.

На дисплее окна полуавтоматического режима отображаются в одной системе координат два графика частотного спектра: (рис. 8) синим цветом с заполнением отображается график спектра при выключенном тесте, зеленым цветом - график спектра при включенном тесте. Белым цветом с заполнением показывается превышение шумов.

Все видимые пики «зеленого» графика подлежат анализу как «подозрительные». Нажатие на кнопку «Внести все пики в таблицу» приведет к занесению в таблицу всех значений частот пиков, уровень излучения которых превышает уровень шумов при выключенном тесте на заданное значения превышения.

Если путем совместного вывода графиков спектров при включенном и выключенном тесте сложно обнаружить точки, в которых меняется уровень, можно после сканирования нажать кнопку «Старт».

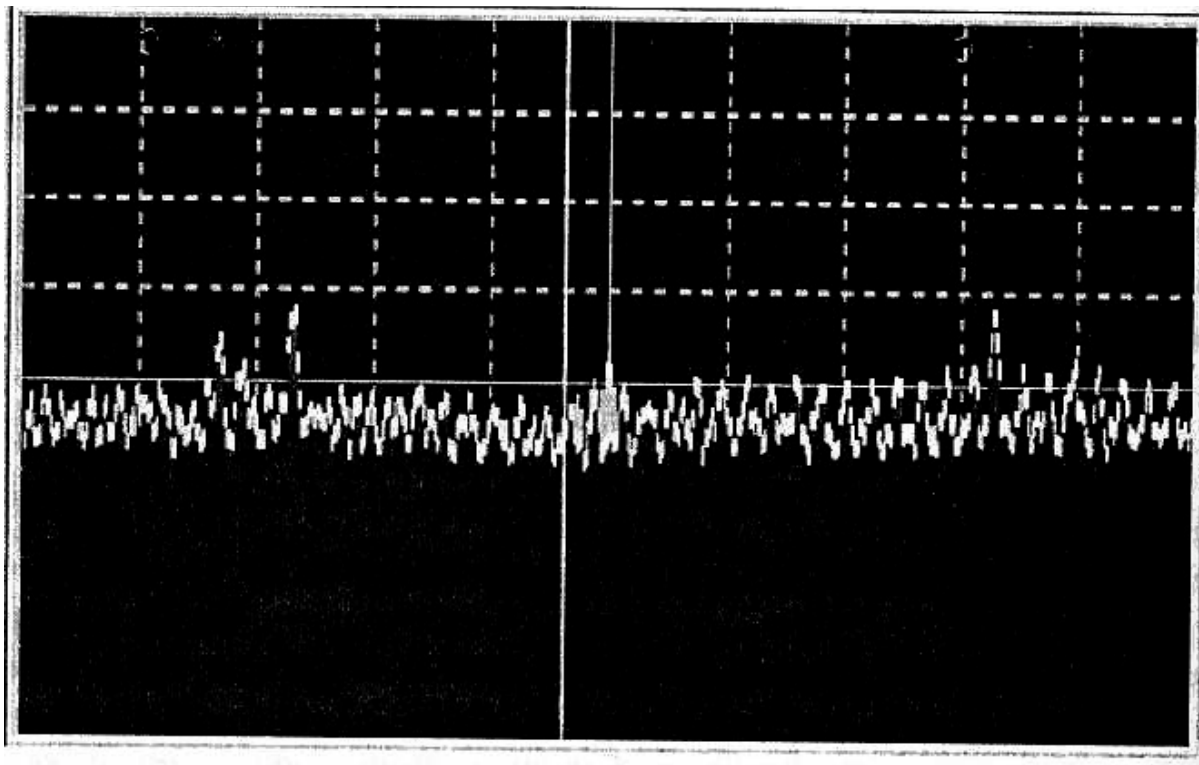


Рисунок 8 – Результаты измерений частотного спектра в дисплее окна полуавтоматического режима

При этом название кнопки меняется на «Стоп» и начинается непрерывное сканирование спектра в заданном диапазоне. Включая и выключая тест можно отследить точки, в которых происходит изменение уровня, после чего остановить сканирование, нажав кнопку «Стоп».

При обнаружении каждой очередной составляющей тестового сигнала, следует вносить значение ее частоты в таблицу для последующего измерения.

2.3. Завершение обнаружения составляющих тестового сигнала

По завершении обнаружения составляющих тестового сигнала следует нажать кнопку «Заккрыть» окна полуавтоматического режима и выбрать в меню главного окна программы «Измерения-Старт», либо нажать соответствующую кнопку быстрого запуска. При этом тест на исследуемом средстве должен быть включен. Программа произведет измерения уровней сигнала и выдаст сообщение «Выключите тест для измерения уровней шумов». Выключите тест на исследуемом техническом средстве и нажмите кнопку Ок. Программа произведет измерение уровней шумов и вычислит приведенный уровень сигнала. В дальнейшем результаты измерений можно сохранить в ASCII формате, выбрав в меню главного окна управляющей программы «Измерения-Сохранить». Сохраненный файл результатов используется в качестве исходных данных для расчетной программы.

Закройте окно полуавтоматического режима, нажав кнопку «Заккрыть». Выберите пункт меню главного окна программы «Установки-Эталоны» или нажмите соответствующую кнопку быстрого запуска. Поверх главного окна программы открывается окно параметров исследования на странице «Эталоны» (рис. 9). Загрузите эталон, сохраненный при работе в полуавтоматическом

режиме, нажав кнопку «Загрузить» окна параметров исследования.

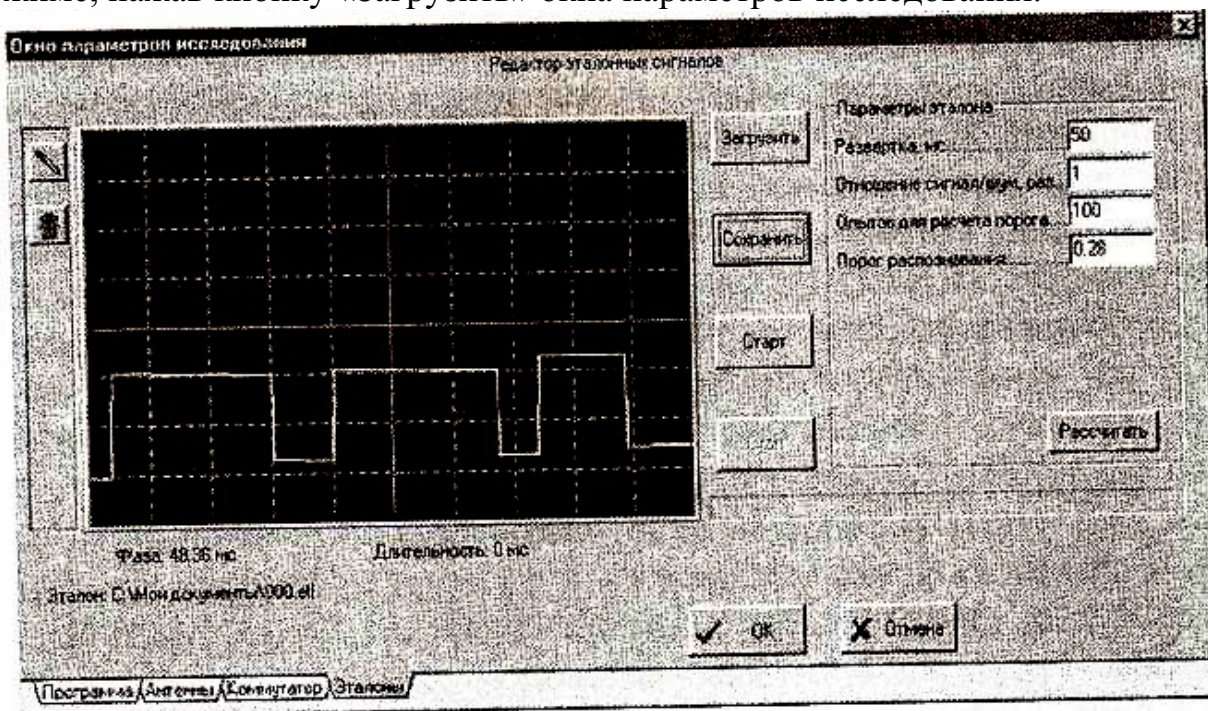


Рисунок 9 – Вид окна параметров исследования на странице «Эталон»

Форма эталонного сигнала отображается на дисплее окна параметров исследования, а пороговый коэффициент корреляции, используемый при распознавании сигнала с применением данного эталона, выводится в соответствующее поле. По умолчанию это число принято равным 0,28, однако для эталонных сигналов разной формы и степени зашумленности оптимальный пороговый коэффициент корреляции может меняться в достаточно широких пределах. Для определения оптимального порогового коэффициента корреляции по критерию Байеса можно воспользоваться встроенным «калькулятором». Задайте ожидаемое отношение сигнал/шум (требуемое отношение, при котором должно происходить устойчивое распознавание) и количество опытов для расчета порогового коэффициента корреляции (рекомендуется задавать не меньше 100 опытов, уменьшение количества опытов приводит к снижению точности расчета, увеличение ведет к увеличению времени расчета) в соответствующих полях окна параметров исследования. Нажмите кнопку «Рассчитать». По завершении расчета на экран выводится окно результатов расчета (рис. 10), на котором представлены графики зависимости вероятностей пропуска сигнала и ложного срабатывания в зависимости от выбранного порогового коэффициента корреляции и график среднего риска по Байесу.

Пороговый коэффициент корреляции, соответствующий минимуму среднего риска выбирается в качестве оптимального. При закрытии окна результатов расчета вычисленный пороговый коэффициент корреляции автоматически переносится в соответствующее поле. Оператор может принять данный порог или установить другое значение исходя из собственного опыта, после чего следует сохранить эталон, нажав кнопку «Сохранить». Сохраните эталон в созданной папке.

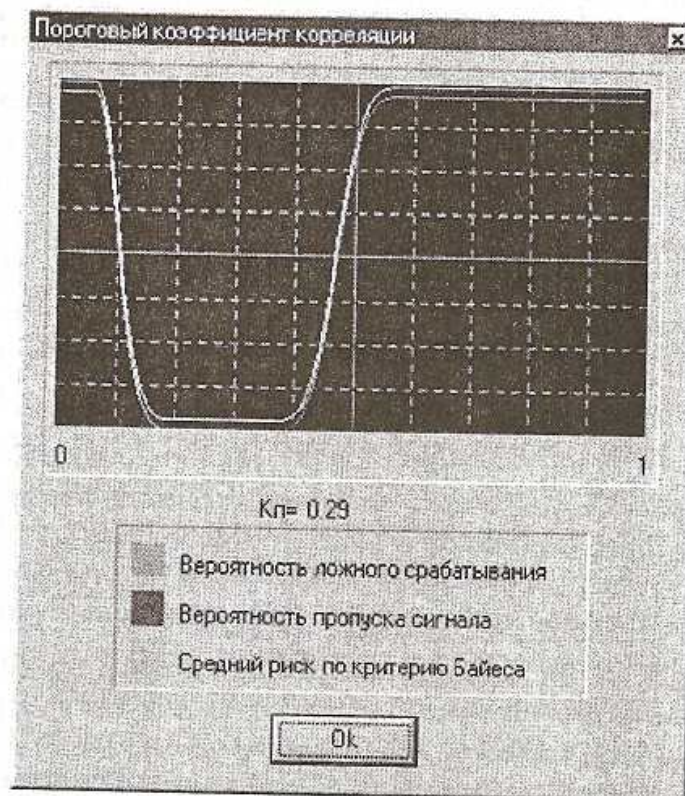


Рисунок 10 – Окно результатов расчета

3. Работа с расчетной программой

3.1. Загрузка файла данных измерений

Для того чтобы загрузить данные измерений из файла в расчетную программу нужно выбрать в меню «Файл» пункт «Открыть» (Таблица 1). Появится стандартный диалог открытия файлов Windows. Далее пользователь должен указать файл, в котором содержатся данные измерений для расчета, полученные при работе управляющей программы, и нажать кнопку «Открыть». В случае если файл имеет правильную структуру, то в поля рабочей таблицы «F, МГц», «U, дБ» и «U_{in}, дБ» загрузятся значения частоты, уровня обнаруженных компонент тестового сигнала и уровня шума.

3.2. Условие для расчета

Под «условиями для расчета» понимаются характеристики исследуемого средства, применяемого теста, измерительных приборов и условия проведения измерений, влияющих на конечные результаты работы программы:

- вид кода;
- тип кода;
- вид расчета;
- количество разрядов, в которых одновременно присутствовал единичный импульс;
- тактовая частота теста;
- длительность импульса;
- количество повторений информации за 10 с;
- расстояние от антенны до исследуемого средства;

- тип измерительной антенны (по диапазонам);
- полоса пропускания измерительного прибора (по диапазонам);
- расстояние от технического средства до границы контролируемой зоны;
- расстояние от технического средства до точки измерений затухания;
- тип линии;
- сопротивление нагрузки;
- погонное затухание;
- нормы отношения сигнал/шум.

Условия можно задать двумя способами:

1) ввести все перечисленные значения с клавиатуры (и сохранить их в виде файла на диске);

2) загрузить в программу файл с условиями для расчета.

Файлы, содержащие условия для расчета, могут подготавливаться в текстовом редакторе, либо могут быть получены в процессе работы расчетной программы.

3.3. Задание условия для расчета

Для того чтобы осуществить ввод условий с клавиатуры, следует выбрать в меню «Условия» команду «Заполнить» (таблица 1). В центре экрана появится окно, в котором последовательно задаются перечисленные выше характеристики устройства и параметры теста.

Окно задания условий имеет несколько страниц. Перемещение на следующую страницу осуществляется нажатием кнопки «далее». Кнопка «далее» на очередной странице окна ввода условий будет запрещена к нажатию до тех пор, пока все необходимые параметры не будут заданы. Отменить задание условий можно нажатием кнопки «отмена».

На первой странице («аппаратура») окна задания условий расположена таблица, в которой пользователь может выбрать (ввести) сведения об используемой при измерениях аппаратуре (см. рис. 11).

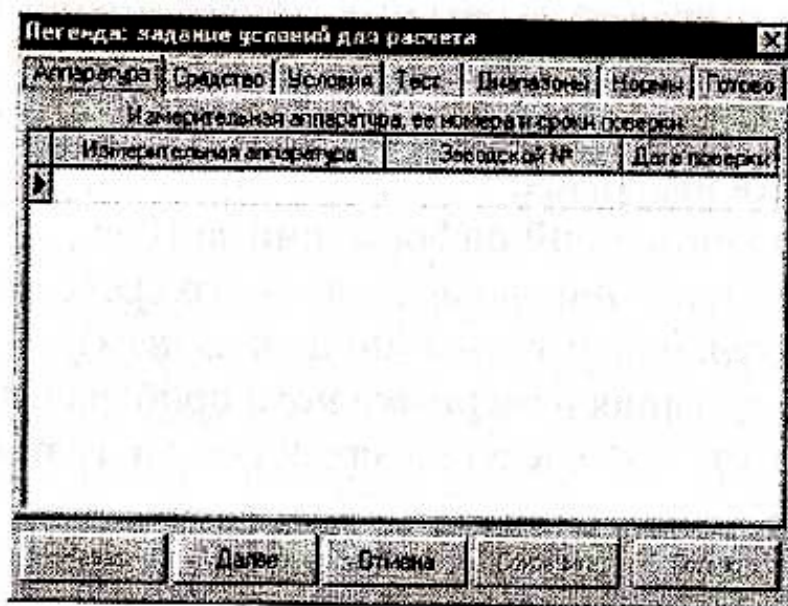


Рисунок 11 – Окно задания условий для расчета

Заполнение таблицы не является обязательным, поэтому кнопка «далее» активна, независимо от того заполнена таблица или нет.

На второй странице окна задания условий («средство», рис. 12) расположены строки ввода информации об исследуемом средстве (тип исследуемого средства и его заводской номер), ввод которой не является обязательным, а также его характеристик - тип и вид используемого кода (ввод является обязательным). Кнопка «Далее» будет запрещена до тех пор, пока строки «тип используемого кода» и «вид используемого кода» не будут заполнены. У пользователя имеется возможность, при необходимости, вернуться на предыдущую страницу условий и изменить их (кнопка «назад»).

Рисунок 12 – Вторая страница окна задания условий для расчета («Средство»)

На третьей странице окна указывается тип проводимых расчетов (см. рис. 13).

Рисунок 13 – Третья страница окна задания условий для расчета («Условия»)

При расчете зон по электрической составляющей необходимо заполнить таблицу, содержащую нижний и верхний диапазон исследуемых частот, а также расстояние от исследуемого средства до антенны и высоту подъема антенны. Данные из этой таблицы используются в дальнейшем для проведения расчета.

На четвертой странице окна задания условий (см. рис. 14) заполняются параметры тестового режима: частота теста, величина $1/t_{\text{и}}$, количество тестируемых разрядов и число повторений информации.

Рисунок 14 – Четвертая страница окна задания условий для расчета («Тест»)

При нажатии кнопки с изображением калькулятора рассчитывается и автоматически заполняется величина $1/t_{\text{и}}$ (величина лепестка). Использовать эту кнопку можно только в том случае, если импульсы, формируемые тестируемым устройством, представляют собой меандр.

При использовании строки учета повторяемости информации вводится число повторений. Если окно учета повторяемости не выбрано, то числу повторений информации автоматически присваивается значение 1.

На пятой странице (см. рис. 15) окна задания условий располагается таблица, в которую вносятся частотные диапазоны, используемые антенны и полосы пропускания приемника.

В соответствии с этой таблицей к данным измерений прибавляются антенные коэффициенты. Все строки таблицы не должны иметь пустых значений. Только в этом случае кнопка «далее» будет разрешена. На шестой странице окна задания условий вводятся нормы отношения сигнал/шум (см. рис. 16).

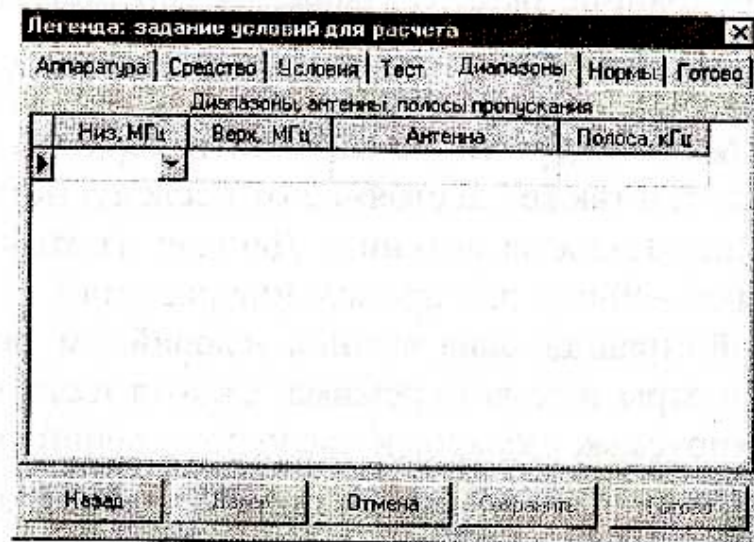


Рисунок 15 – Пятая страница окна задания условий для расчета («Диапазоны»)

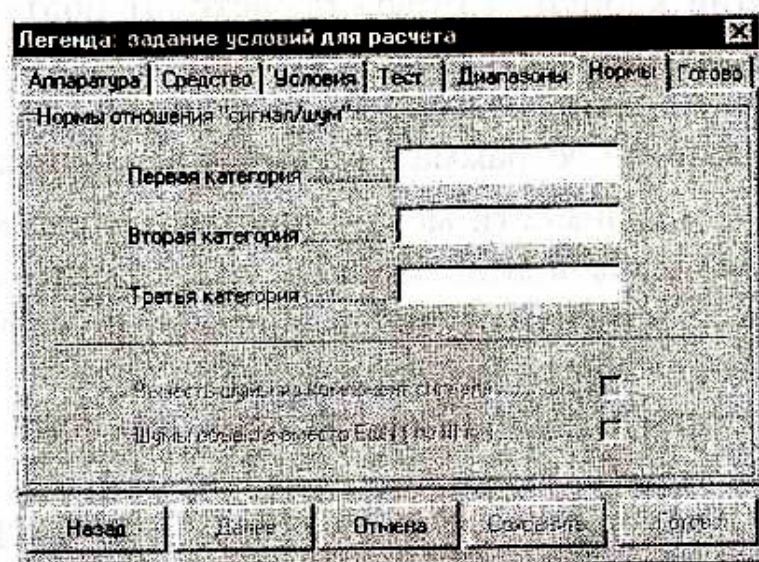


Рисунок 16 – Шестая страница окна задания условий для расчета («Нормы»)

Нормы не хранятся в программе и вводятся каждый раз при задании условий для расчета.

Так же на данной странице указывается:

- необходимо ли вычитать шумы из компонент тест-сигнала;
- заменять ли нормированные шумы на реальные (используется только при расчете минимального коэффициента защищенности, в любом другом случае флаг не активен).

На седьмой странице окна задания условий все введенные параметры отображаются в собранном виде для контроля правильности введенных условий (рис. 17).

Используя скроллер, можно просмотреть все введенные величины. Если обнаружена ошибка, то следует вернуться к неправильно введенному параметру, используя кнопку «назад». Седьмая страница является последней в окне задания

условий, и при ее достижении активизируются кнопки «готово» и «сохранить».

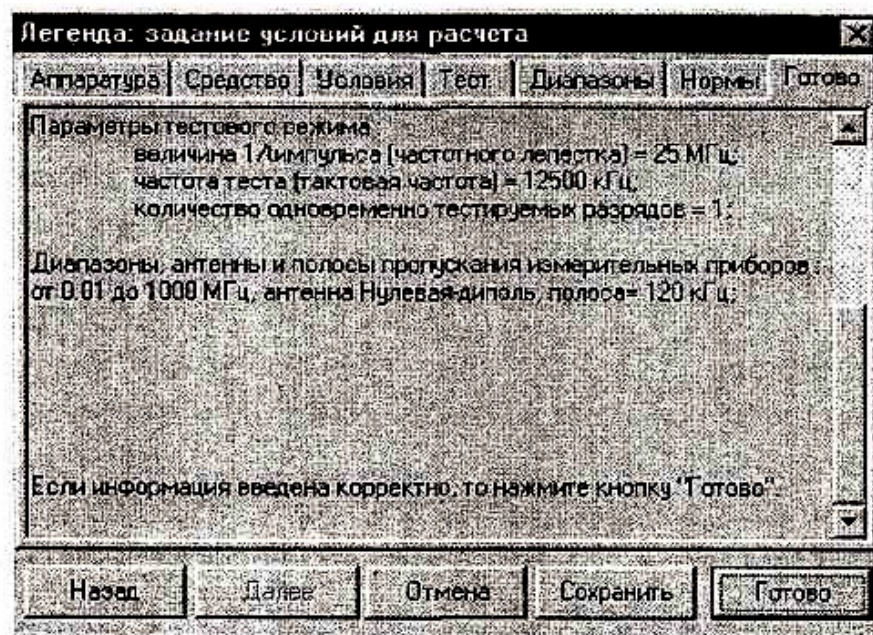


Рисунок 17 – Седьмая страница окна задания условий для расчета («Готово»)

Кнопка «сохранить» используется для сохранения всех введенных условий в виде файла на диске. При ее нажатии появляется стандартный диалог Windows с предложением сохранить файл условий.

При нажатии кнопки «готово» происходит подтверждение использования (фиксация) введенных условий в программе и добавление к исходным данным антенных коэффициентов. Условия считаются заданными, а программа - готовой к выполнению расчета.

В случае необходимости можно повторно отредактировать условия для расчета, выполнив команду «Заполнить» меню «Условия». При этом, достигнув страницы «нормы», пользователю опять потребуется ввести нормы отношения сигнал/шум.

После внесения и заполнения условий, нажмите «Измерения-Старт».

После того как программа выполнит расчет измерения, нужно сохранить результат в Microsoft Word с помощью кнопки быстрого доступа (документ Microsoft Word должен быть открыт).

Задание обучаемым для самостоятельной учебной работы при подготовке к занятию:

7. Закрепить и углубить знания, полученные на лекции, для этого изучить конспект лекций и рекомендуемую литературу:
 - [1] Технические средства и методы защиты информации. Учебное пособие для вузов / Под ред. А.П. Зайцева и А.А. Шелупанова. – М.: Горячая линия-Телеком, 2009. – С. 472 – 505.
8. Изучить методические указания к ПЗ № 1-2.

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1

**Лабораторная работа разработана
доцентом кафедры ОТЗИ Сагдеевым К.М.**

РАЗДЕЛ № 7. СПОСОБЫ И СРЕДСТВА КОНТРОЛЯ ЭФФЕКТИВНОСТИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ СРЕДСТВАМИ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И АВТОМАТИЗИРОВАННЫМИ СИСТЕМАМИ

Тема № 31. РАСЧЕТ И ОЦЕНКА ЗАЩИЩЕННОСТИ ТЕХНИЧЕСКИХ СРЕДСТВ ОТ УТЕЧКИ ИНФОРМАЦИИ ЗА СЧЕТ ПЭМИН

Практические занятия № 5-8.

Тема: Расчет и оценка защищенности технических средств от утечки информации за счет пэмин

Время – 6 часов.

Формируемые компетенции: ОПК-4, ОПК-11, ОПК-2.1.

УЧЕБНЫЕ ВОПРОСЫ:

1. Разработка программы для ПЭВМ по расчету и оценке защищенности технических средств от утечки информации за счет ПЭМИН.
2. Решение практических задач по расчету и оценке защищенности технических средств от утечки информации за счет ПЭМИН.

СОДЕРЖАНИЕ ПРАКТИЧЕСКОГО ЗАНЯТИЯ

1. РАЗРАБОТКА ПРОГРАММЫ ДЛЯ ПЭВМ ПО РАСЧЕТУ И ОЦЕНКЕ ЗАЩИЩЕННОСТИ ТЕХНИЧЕСКИХ СРЕДСТВ ОТ УТЕЧКИ ИНФОРМАЦИИ ЗА СЧЕТ ПЭМИН

Практическое задание 1. Составить в Mattcad программу для расчета оценки защищенности технических средств от утечки информации за счет ПЭМИ. Программу разработать в соответствии с ниже приведенной методикой.

Расчетная часть метода включает:

- 1) Расчет расстояний распространения информативного сигнала от ОТСС для его каждой спектральной составляющей R_2 .
- 2) Установление требуемого радиуса контролируемой зоны R_2 для ОТСС в целом.

Радиус контролируемой зоны R_2 для i -й составляющей спектра информативного сигнала определяется из условия

$$R_2 = R_i \quad (2.9)$$

где R_i рассчитывается для ближней зоны распространения сигнала.

Если $L_1 < R_i < L_2$ или $R_0 \leq L_1$, то расчет R_i проводится для промежуточной зоны, где

$$L_1 = \frac{150}{\pi \cdot f_i} \quad (2.10)$$

– расстояние от ОТСС до границы ближней и промежуточной зон, м;

$$L_2 = \frac{180}{f_i} \quad (2.11)$$

– расстояние от ОТСС до границы промежуточной и дальней зон, м;

f_i – частота спектральной составляющей информативного сигнала, МГц.

Расчеты должны быть проведены по электрической и магнитной составляющим электромагнитного поля. Если $R_i > L_2$, то расчет R_i проводится для дальней волновой зоны. За требуемый радиус контролируемой зоны принимается максимальное из всех R_2 .

Возможные расстояния R_i распространения информативного сигнала от ОТСС для каждой его спектральной составляющей рассчитываются по формуле:

$$R_i = \frac{L_i}{\sqrt[k]{\frac{k \cdot E_{\sigma_i}}{E_i}}} \text{ м.} \quad (2.12)$$

Значение P выбирается из условий:

$P = 3$ при $R_i \leq \lambda_i / 2\pi$ (ближняя зона);

$P = 2$ при $\lambda_i / 2\pi < R_i < 6 \lambda_i$ (промежуточная зона);

$P = 1$ при $R_i > 6 \lambda_i$ (дальняя волновая зона),

где $\lambda_i = 300 / f_i$ – длина волны, м.

Значение L_i выбирается из условий:

$L_i = R_o$ – для ближней зоны;

$$L_i = \begin{cases} L_1, & \text{if } L_1 > R_i \\ R_o, & \text{if } L_1 \leq R_i \end{cases} \text{ – для промежуточной зоны;}$$

$$L_i = \begin{cases} L_2, & \text{if } L_2 > R_i \\ R_o, & \text{if } L_2 \leq R_i \end{cases} \text{ – для дальней зоны.}$$

Значение E_i выбирается из условий:

$E_i = E_{ci}$ – для ближней зоны;

$$E_i = \begin{cases} E_1, & \text{if } L_1 > R_i \\ E_{ci}, & \text{if } L_1 \leq R_i \end{cases} \text{ – для промежуточной зоны;}$$

$$E_i = \begin{cases} E_2, & \text{if } L_2 > R_i \\ E_{ci}, & \text{if } L_2 \leq R_i \end{cases} \text{ – для дальней зоны.}$$

где

$$E_{1i} = E_{ci} \left(\frac{R_o}{L_{1i}} \right)^3 \quad (2.13)$$

– значение напряженности поля информативного сигнала на границе ближней и промежуточной зон;

$$E_{2_i} = \begin{cases} E_{1_i} \left(\frac{L_{1_i}}{L_{2_i}} \right)^2, & \text{if } R_o < L_{1_i} \\ E_{c_i} \left(\frac{R_o}{L_{2_i}} \right)^2, & \text{if } R_o \geq L_{1_i} \end{cases} \quad (2.14)$$

– значение напряженности поля информативного сигнала на границе промежуточной и дальней зон.

$$E_{\tilde{n}_i} = \sqrt{E_{o_i}^2 - E_{\omega_i}^2}, \text{ мкВ/м} \quad (2.15)$$

где E_{o_i} – уровень напряженности электромагнитного поля при работе ОТСС в тестируемом режиме; E_{ω_i} – уровень напряженности электромагнитного поля при выключенном ОТСС.

Значения κ выбираются из условий:

$\kappa = 1$ – для ОТСС, не имеющих в своем составе видеомониторов;

$\kappa = 0,3$ – для ОТСС, имеющих в своем составе видеомониторы.

Значения κ приведены с учетом измерения реальных шумов на объекте информатизации.

При расчете возможных расстояний распространения информативного сигнала за счет магнитной составляющей поля в формулу (2.12) подставляют значения pH_{c_i} и pH_{ω_i} .

Пример расчета. Измеренное на расстоянии 1 м от исследуемой ПЭВМ значение напряженности поля за счет ПЭМИ ее видеотракта по электрической составляющей на частоте 30 МГц составило $E_{o_i} = 40,5$ дБ за счет естественного шума 8 дБ (2,5 мкВ/м). В соответствии с формулой (2.15) $E_{c_i} = 40$ дБ (100 мкВ/м). Так как ОТСС имеет в своем составе видеомонитор, принимаем $\kappa = 0,3$. Необходимо определить требуемый радиус контролируемой зоны R_2 .

1) Пользуясь формулами (2.10) и (2.11), находим границы ближней, промежуточной и дальней зон для частоты 30 МГц:

$L_{1i} = 1,6$ м - граница ближней и промежуточной зон;

$L_{2i} = 60$ м - граница промежуточной и дальней зон.

2) Пользуясь формулой (2.12), проверяем, достаточно ли уровня $E_{c_i} = 40$ дБ, чтобы информативный сигнал от ПЭВМ распространялся за границу ближней зоны:

$$R_i = \frac{1}{\sqrt[3]{\frac{0,3 \cdot 2,5}{100}}} = 5,1 \text{ м},$$

где R_i - возможное расстояние распространения информативного сигнала в ближней зоне.

Так как $L_{1i} < R_i$, то уровня информативного сигнала достаточно для его распространения за границу ближней зоны. Пользуясь формулой (2.13), пересчитываем значение E_{c_i} на границу ближней зоны:

$$E_{li} = E_{ci} \left(\frac{R_o}{L_{li}} \right)^3 = 24,4 \text{ мкВ/м},$$

где E_{li} - значение информативного сигнала, пересчитанное на границу ближней зоны.

3) Пользуясь формулой (2.12), проверяем, достаточно ли уровня $E_{li} = 24,4$ мкВ/м, чтобы информативный сигнал от ЭВМ распространялся за границу промежуточной зоны

$$R_i = \frac{1,6}{\sqrt[2]{\frac{0,3 \cdot 2,5}{24,4}}} = 9,1 \text{ м},$$

где R_i - возможное расстояние распространения информативного сигнала в промежуточной зоне.

Так как $L_{2i} > R_i$, то информативный сигнал за границу промежуточной зоны не распространяется. Требуемый радиус контролируемой зоны R_2 определяется значением R_i и составляет 9,1 м.

Практическое задание 2. Составить в Mattcad программу для расчета оценки защищенности технических средств от утечки информации за счет наводок от ПЭМИ по соединительным линиям ВТСС. Программу разработать в соответствии с ниже приведенной методикой.

Расчетная часть метода включает:

1) Расчет значения напряжения сигнала U_{ci} в точке подсоединения измерительного пробника к линии для каждой частотной компоненты по формуле:

$$U_{ci} = 20 \cdot \lg \left(\sqrt{10^{U_{(c+\theta)_i}/10} - 10^{U_{\theta i}/10}} \right) \text{ дБ.} \quad (2.16)$$

2) Расчет показателя защищенности в точке проведения измерений для каждой из частотных компонент по формуле:

$$\ddot{I}_i = U_{ci} - U_{\theta i}, \text{ дБ} \quad (2.17)$$

3) Расчет величины коэффициента погонного затухания KPi наведенных сигналов в исследуемой линии для каждой из частот по формуле:

$$\hat{E}_{\ddot{I}_i} = \frac{20 \cdot \lg(U_{1\text{èçì}_i} / U_{2\text{èçì}_i})}{l}, \quad (2.18)$$

где $U_{1\text{изм}_i}$ - напряжение специально созданного сигнала (при помощи генератора сигналов), измеренное на частоте f_i в точке А, мкВ (рис. 2.4); $U_{2\text{изм}_i}$ - напряжение, измеренное на частоте f_i в точке Б, мкВ; l - протяженность линии ВТСС между точками А и Б, м (рисунок 2.4).

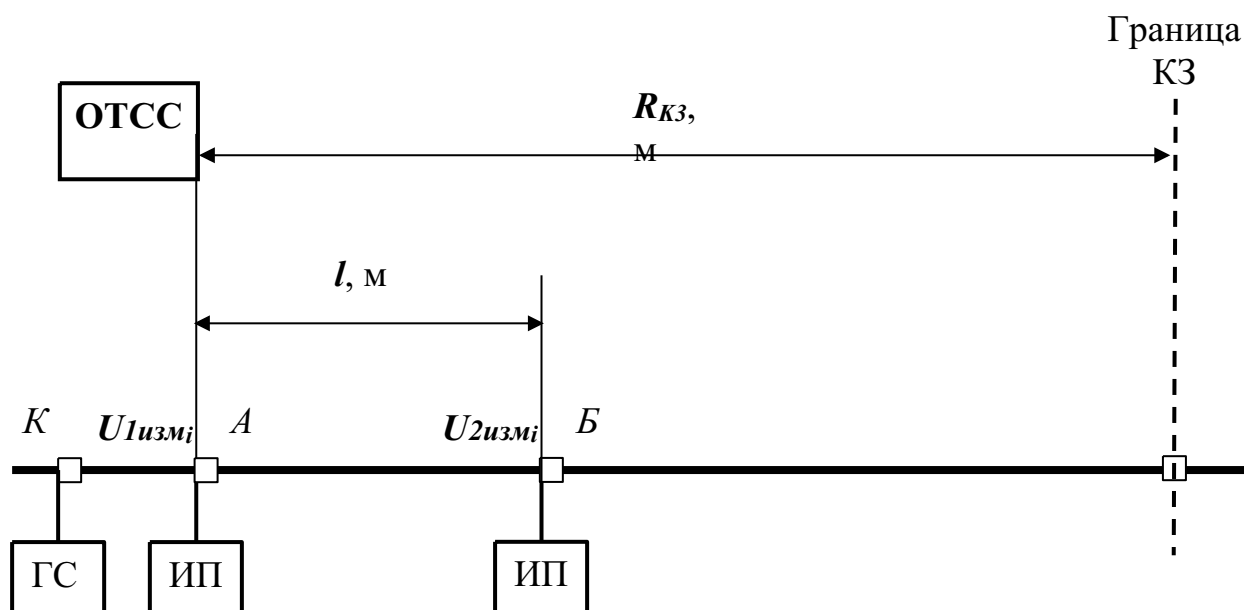


Рисунок – Схема измерения коэффициента погонного затухания.

4) Расчет максимальной длины пробега R_i исследуемой линии для каждой из частот, на которой возможно выделение информативного сигнала, для ОТСС, имеющих в своем составе видеоконтрольные устройства, при нормированном значении отношения сигнал/шум, равном 0,3, проводится по формуле:

$$R_i = \frac{\dot{I}_{i+10}}{K_{i_i}} \text{ м}, \quad (2.19)$$

а для ОТСС, не имеющих видеоконтрольных устройств, при нормированном значении отношения сигнал/шум, равном единице, проводится по формуле:

$$R_i = \frac{\dot{I}_i}{K_{i_i}} \text{ м}, \quad (2.20)$$

5) Выбор максимального из полученных значений R_i и сравнение его с пробегом линии до границы КЗ. Если пробег исследуемой линии до границы КЗ больше максимального из всех R_i , то делается вывод о защищенности информации, обрабатываемой ОТСС, от утечки за счет наводок в исследуемую линию. Если нет, то делается вывод о необходимости принятия дополнительных мер защиты.

2. РЕШЕНИЕ ПРАКТИЧЕСКИХ ЗАДАЧ ПО РАСЧЕТУ И ОЦЕНКЕ ЗАЩИЩЕННОСТИ ТЕХНИЧЕСКИХ СРЕДСТВ ОТ УТЕЧКИ ИНФОРМАЦИИ ЗА СЧЕТ ПЭМИН

Условия проведения измерений

При выполнении измерений необходимо соблюдать следующие условия:

1) Оценка защищенности должна проводиться в реальных условиях эксплуатации ОТСС.

2) Климатические условия должны соответствовать допустимым условиям работы ОТСС и применяемых средств измерений.

Рекомендуемые средства измерений

При выполнении измерений рекомендуется применять средства измерений, приведенные в таблице 3.1.

Таблица 1 – Технические характеристики применяемых средств измерений (в соответствии с ГОСТ Р 51319-99)

Наименование средств измерений	Тип	Диапазон измеряемых параметров	Основная погрешность измерения
Селективный микровольтметр	SMV-11	9кГц...30 МГц 0...125дБ	±2дБ ±1,5дБ
Наименование средств измерений	Тип	Диапазон измеряемых параметров	Основная погрешность измерения
Селективный микровольтметр	SMV-8.5	26...1000 МГц 0...125дБ	±3дБ
Комплект измерительных антенн	АИР3-2 АИР4-2	0,008...40 МГц 0,05... 1000 МГц	±1дБ ±2дБ
Осциллограф	C1-112	0...5 МГц	Не нормируется

Примечание. Вместо указанных в таблице средств измерений разрешается применять аналогичные, обеспечивающие измерение соответствующих параметров с требуемой точностью. Применяемые средства измерений должны быть исправны, поверены и иметь свидетельства (отметки в формулярах или паспортах) о поверке.

Требования безопасности выполнения работ

При проведении измерений параметров электромагнитного поля необходимо соблюдать следующие требования:

1) Лица (операторы), допущенные к выполнению работ по данной методике, должны иметь третью (до 1000 В) квалификационную группу по электробезопасности.

2) До включения приборов в сеть необходимо убедиться в исправности системы заземления.

Требования к тестовым режимам работы ОТСС

Тестовый режим должен обеспечивать:

1) Формирование продолжительной последовательности информативных сигналов.

2) Максимально возможную частоту следования информативных сигналов.

3) Идентификацию информативных тестовых сигналов на фоне других сигналов, помех и шумов.

4) Возможность измерения уровней тестовых сигналов стандартными средствами измерений.

5) Достаточное для измерений время работы ОТСС в тестируемом режиме.

Для проведения специсследований ОТСС, в состав которых входят видеомониторы, и локальных компьютерных сетей в режиме передачи данных рекомендуется применять аттестованные тестовые программы из единой базы тестов Гостехкомиссии России (ФСТЭК).

Подготовка к выполнению измерений

При подготовке к выполнению измерений проводят следующие работы:

- 1) Выбирают рекомендуемое расстояние от ОТСС до места установки антенны ИНП (см. рис. 1).
- 2) На ОТСС устанавливают тестовый режим работы.
- 3) Проводят подготовительные мероприятия в соответствии с инструкцией по эксплуатации ИНП (присоединение измерительной антенны, выдержка во включенном состоянии, калибровка и т. д.).

Порядок выполнения измерений ПЭМИ

При выполнении измерений напряженности электромагнитного поля выполняют следующие операции:

- 1) По идентификационным признакам определяют частотный спектр ПЭМИ исследуемого ОТСС, состоящий из набора спектральных составляющих $f_1, f_2, \dots, f_i, \dots, f_k$.
- 2) Определяют направления на точки возможного перехвата ПЭМИ ОТСС. Из них выбирают направление, соответствующее минимальному расстоянию до границы КЗ объекта. Таких направлений может быть выбрано одно или несколько.
- 3) В выбранном направлении измеряют напряженности 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) составляющих электромагнитного поля, создаваемых информативным сигналом на частотах спектральных составляющих f_i .
- 4) На выявленных частотах f_i измеряют уровни помех.
- 5) Результаты измерений и расчетов заносят в таблицу 2.

Обработка результатов измерений

Обработку результатов измерений выполняют в соответствии с п. 1.2 настоящей методики.

Таблица 2 – Результаты измерений и расчетов

f_i , Гц	E_i , дБ	pH_{oi} , дБ	$E_{ш_i}$, дБ	$pH_{ш_i}$, дБ	E_{ci} , мкВ/м	pH_{ci} , мкВ/м	R_i , м
f_1	E_{o1}	pH_{o1}	$E_{ш1}$	$pH_{ш1}$	E_{c1}	pH_{c1}	R_1
f_2	E_{o2}	pH_{o2}	$E_{ш2}$	$pH_{ш2}$	E_{c2}	pH_{c2}	R_2
...	...	...	...	...	...	...	...
f_i	E_{oi}	pH_{oi}	$E_{ш_i}$	$pH_{ш_i}$	E_{ci}	pH_{ci}	R_i
...	...	...	...	...	...	...	...
f_k	E_{ok}	pH_{ok}	$E_{ш_k}$	$pH_{ш_k}$	E_{ck}	pH_{ck}	R_k

Порядок выполнения измерений наводок от ПЭМИ

При выполнении измерений напряжения информативного сигнала, наведенного в токопроводящих коммуникациях, выполняются следующие

операции:

1) По идентификационным признакам определяют частотный спектр ПЭМИ. Допускается использовать частоты $f_1, f_2, \dots, f_i, \dots, f_k$ выявленные при инструментальном контроле ПЭМИ данного ОТСС.

2) Измеряют напряжение смеси обнаруженных компонент тест-сигнала и шума в соответствии с требованиями инструкций по эксплуатации применяемых средств измерения. Полосу пропускания измерительных приемников выбирают 9 кГц в диапазоне частот от 150 кГц до 30 МГц и 120 кГц в диапазоне от 30 до 250 МГц. Полученные результаты заносят в таблицу 3.4.

Примечание. Если имеется возможность подключения средств измерений к линиям на границе КЗ (в непосредственной близости) и удастся обнаружить информативный сигнал, то делается вывод о неэффективности принятых мер защиты.

3) Производят измерение уровня шума в линии на частотах обнаруженных компонент тест-сигнала при выключенном ОТСС. Полученные результаты заносят в таблицу 3.

4) Определяют коэффициент погонного затухания информативного сигнала в исследуемой линии, для чего выполняют следующее:

- собирают схему согласно рисунку 1;
- подают сигнал генератора ВЧ в исследуемую линию в точке K , отстоящей от точки A на расстоянии 1 ...3 метра. Подключение генератора в точке K рекомендуется осуществлять индуктивным способом;
- устанавливают органами управления генератора достаточный уровень выходного сигнала (уровень сигнала должен обеспечить его обнаружение в точках A и B);
- перестраивая по частоте генератор и измерительный приемник, измеряют на обнаруженных частотах напряжение генератора сигналов в точке A . Полученные результаты заносятся в таблицу 3;
- выбирают точку B проведения вторых измерений. Точку B рекомендуется выбирать на расстоянии не менее 15.. .25 м от точки A ;
- не изменяя режим работы генератора и измерительного приемника в точке B , проводят измерения, аналогичные проведенным в точке A . Полученные результаты заносят в таблицу 3.

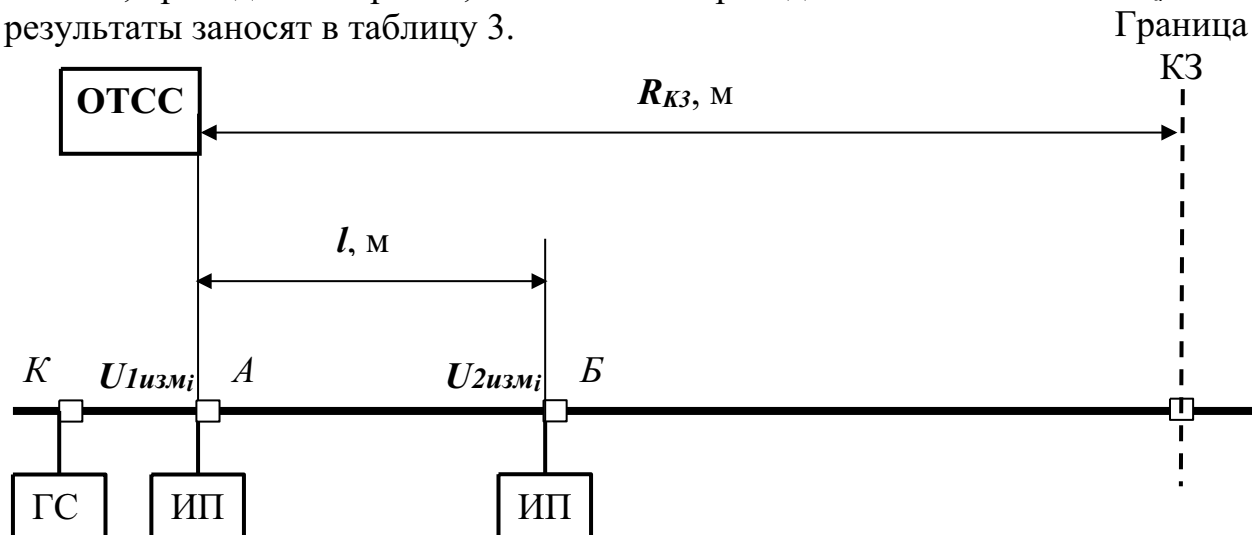


Рисунок 1 – Схема измерения коэффициента погонного затухания
Таблица 3 – Результаты измерений и расчетов

f , МГц	$U(c+u)_i$, дБ	$U_{ш_i}$, дБ	U_{c_i} , дБ	$U_{1изм_i}$, мкВ	$U_{2изм_i}$, мкВ	$KП_i$, дБ/м	R_i , м
f_1							
f_K							

Обработка и анализ результатов измерений

Объект ОТСС считается защищенным от утечки информации по линиям и коммуникациям, выходящим за пределы контролируемой зоны, если для всех частотных компонент тест-сигнала выполняется условие $R_i < R_{K3}$, где R_{K3} – реальный пробег исследуемой линии до границы контролируемой зоны.

Практическое задание 1. С помощью имеющихся средств измерения провести измерения побочных электромагнитных излучений, создаваемых ПЭВМ. Результаты измерения занести в таблицу 2.

Практическое задание 2. С помощью программы Rachtet провести оценку защищенности информации обрабатываемой ПЭВМ. Для этого результаты измерения занести в таблицу, находящуюся в верхней части рабочего окна программы Rachtet, приведенного на рис. 2. После чего в программе нажать кнопку «Расчет».

Сделать вывод по результатам измерений и расчетов об оценке защищенности информации обрабатываемой ПЭВМ.

Средства измерений | **Условные обозначения** | **Создать отчет** | **Справка**

Методика оценки защищенности конфиденциальной информации, обрабатываемой техническими средствами и системами

Расчет радиуса контролируемой зоны

Вид сверху

Схема размещения ОТСС и ИНП при проведении измерений

Введите значения f_i $E_{\theta i}$ $pH_{\theta i}$ $E_{ш_i}$ $pH_{ш_i}$ E_{c_i} pH_{c_i} $R_i(E)_м$ $R_i(H)_м$

f_i , МГц	$E_{\theta i}$, мкВ/м	$pH_{\theta i}$, мкВ/м	$E_{ш_i}$, мкВ/м	$pH_{ш_i}$, мкВ/м	E_{c_i} , мкВ/м	pH_{c_i} , мкВ/м	$R_i(E)_м$	$R_i(H)_м$

К: 1
С: 0.3

Расчет
Открыть
Сохранить

Радиус контролируемой зоны должен быть не менее ____ м

Расчет максимальной длины пробега линии

Схема измерения коэффициента погонного затухания

Введите значения f_i $U(c+u)_i$ $U_{ш_i}$ $U_{1изм_i}$ $U_{2изм_i}$

f_i , МГц	$U(c+u)_i$, дБ	$U_{ш_i}$, дБ	U_{c_i} , дБ	$U_{1изм_i}$, дБ	$U_{2изм_i}$, дБ	$KП_i$, дБ/м	R_i , м

К: 1
С: 0.3

Расчет
Открыть
Сохранить

Пробег линии до границы контролируемой зоны должен быть не менее ____ м

Рис. 2 – Рабочее окно программы Rachtet

Практическое задание 3. С помощью имеющихся средств измерения провести измерения наводок в соединительной линии ВТСС от побочных электромагнитных излучений, создаваемых ПЭВМ. Результаты измерения занести в таблицу 2.

Практическое задание 4. С помощью программы Rachet провести оценку защищенности информации обрабатываемой ПЭВМ. Для этого результаты измерения занести в таблицу, находящуюся в нижней части рабочего окна программы Rachet, приведенного на рис. 2. После чего в программе нажать кнопку «Расчет».

Сделать вывод по результатам измерений и расчетов об оценке защищенности информации обрабатываемой ПЭВМ.

**Задание обучаемым для самостоятельной учебной работы
при подготовке к занятию:**

9. Закрепить и углубить знания, полученные на лекции, для этого изучить конспект лекций и рекомендуемую литературу:
 - [1] Технические средства и методы защиты информации. Учебное пособие для вузов / Под ред. А.П. Зайцева и А.А. Шелупанова. – М.: Горячая линия-Телеком, 2009..
10. Изучить методические указания к ПЗ № 3-4.

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1

**Лабораторная работа разработана
доцентом кафедры ОТЗИ Сагдеевым К.М.**

РАЗДЕЛ № 8. СПОСОБЫ И СРЕДСТВА КОНТРОЛЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ВЫДЕЛЕННЫХ ПОМЕЩЕНИЙ ОТ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Тема № 34. РАСЧЕТ И ОЦЕНКА ЗАЩИЩЕННОСТИ ВЫДЕЛЕННОГО ПОМЕЩЕНИЯ ОТ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ
Практические занятия № 9-13.

Тема: Расчет и оценка защищенности выделенного помещения от утечки речевой информации

Время – 6 часов.

Формируемые компетенции: ОПК-4, ОПК-11, ОПК-2.1.

УЧЕБНЫЕ ВОПРОСЫ:

1. Методика расчета словесной разборчивости речи.
2. Разработка программы для ПЭВМ по расчету и оценке защищенности выделенного помещения от утечки речевой информации.
3. Решение практических задач по расчету и оценке защищенности выделенного помещения от утечки речевой информации.

СОДЕРЖАНИЕ ПРАКТИЧЕСКОГО ЗАНЯТИЯ

1. МЕТОДИКА РАСЧЕТА СЛОВЕСНОЙ РАЗБОРЧИВОСТИ РЕЧИ

Для количественной оценки качества перехваченной речевой информации наиболее часто используют показатель - словесная разборчивость речи W , под которой понимается относительное количество (в процентах) правильно понятых слов.

Проведенный анализ показал возможность ранжирования понятности перехваченной речевой информации. Из практических соображений может быть установлена некоторая шкала оценок качества перехваченного разговора:

1. Перехваченная речевая информация содержит количество правильно понятых слов, достаточное для составления подробной справки о содержании перехваченного разговора.
2. Перехваченная речевая информация содержит количество правильно понятых слов, достаточное только для составления краткой справки-аннотации, отражающей предмет, проблему, цель и общий смысл перехваченного разговора.
3. Перехваченная речевая информация содержит отдельные правильно понятые слова, позволяющие установить предмет разговора.
4. При прослушивании фонограммы перехваченного разговора нельзя установить предмет разговора.

Практический опыт показывает следующее:

- при словесной разборчивости менее 60 -70% уже невозможно составление

- подробной справки о содержании перехваченного разговора;
- при словесной разборчивости менее 40 - 60% уже невозможно составление краткой справки-аннотации;
 - при словесной разборчивости менее 20 - 40% значительно затруднено установление даже предмета ведущегося разговора;
 - при словесной разборчивости менее 10 - 20% невозможно установление предмета ведущегося разговора даже при использовании современных методов шумоочистки.

Для оценки разборчивости речи целесообразно использовать инструментально-расчетный метод, при котором числовое значение словесной разборчивости рассчитывается на основе измерения отношения уровней речевого сигнала/шума и потери (затухание) акустического речевого сигнала (или вибрационного сигнала, сопутствующего защищаемой речи), в среде распространения от источника речи до места размещения приемного акустического (вибрационного) приемника аппаратуры акустической речевой разведки.

Методика расчета словесной разборчивости речи

Словесная разборчивость речи (W) рассчитывается по формуле

$$W = \begin{cases} 1.54 \cdot R^{0.25} \cdot [1 - \exp(-11 \cdot R)] & \text{если } R < 0.15, \\ 1 - \exp\left(-\frac{11 \cdot R}{1 + 0.7 \cdot R}\right), & \text{если } R \geq 0.15 \end{cases} \quad (13)$$

где R - интегральный индекс артикуляции (понимаемости) речи.

Интегральный индекс артикуляции речи (R) определяется по формуле

$$R = \sum_{i=1}^5 r_i = \sum_{i=1}^5 p_i \cdot k_i, \quad (14)$$

где r_i – октавный (спектральный) индекс артикуляции (понимаемости) речи, то есть информационной вес i -й спектральной полосы частотного диапазона речи в ее понимаемость. Здесь и далее i -порядковый номер октавной полосы ($i=1, 2, 3, 4, 5$) со среднегеометрическими частотами $f_{cp} = 250, 500, 1000, 2000, 4000$ Гц;

k_i – весовые коэффициенты, характеризующие вероятность наличия формант в октавных полосах;

p_i – октавные коэффициенты восприятия формант слуховым аппаратом человека, представляющие собой вероятное относительное количество формантных составляющих речи, которые будут иметь уровни интенсивности выше порогового значения.

Октавный коэффициент p_i восприятия формант рассчитывается по формуле

$$r_i = \left| \gamma - \left(\frac{0.78 + 5.46 \cdot \exp\left[-4.3 \cdot 10^{-3} \cdot \{7.3 - |Q_i|\}^2\right]}{1 + 10^{0.1 \cdot |Q_i|}} \right) \right|, \quad (15)$$

где γ – индикаторная функция, показывающая, как энергетические условия разведывательного контакта, влияют на разборчивость звуков в октавных полосах

$$\gamma = \begin{cases} 0, & \text{если } Q_i \leq A_i \\ 1, & \text{если } Q_i > A_i \end{cases}, \quad (16)$$

где Q_i - октавное отношение «речевой сигнал/помеха» в месте возможного размещения акустических или вибрационных приемных датчиков аппаратуры акустической речевой разведки (в месте возможного прослушивания речи без применения технических средств - для акустического канала утечки речевой информации), дБ;

A_i - формантный параметр спектра речевого сигнала в октавной полосе, дБ;

k_i - весовой коэффициент октавной полосы частот.

Числовые значения A_i и k_i принимаются из таблицы 5.

Таблица 5

Среднегеометрические частоты октавных полос f_{cp_i} , Гц	125	250	500	1000	2000	4000	8000
Числовое значение формантного параметра спектра речевого сигнала в октавной полосе частот A_i , дБ	25	18	14	9	6	5	4
Числовое значение весового коэффициента октавной полосы частот k_i	0,01	0,03	0,12	0,20	0,30	0,26	0,07

Числовое значение Q_i определяется из энергетического соотношения

$$Q_i = L_{si} - Z_i - L_{\theta_i}, \quad (17)$$

где L_{si} – октавный уровень защищаемого речевого сигнала на выходе источника акустических сигналов, дБ. Значения L_{si} являются исходными данными для оценки защищенности речевой информации.

Z_i – потери (затухание) акустического речевого сигнала (или вибрационного сигнала, сопутствующего защищаемой речи), в среде распространения от источника речи до места размещения приемного акустического (вибрационного) приемника аппаратуры акустической речевой разведки, дБ. В качестве потери может выступать величина звукоизоляции или виброизоляции различных ограждающих конструкций, которые, как правило, определяются инструментальными методами или берутся из таблиц. В данной работе воспользуйтесь измеренными значениями, указанными в таблице 6. Потери акустического сигнала в воздушной среде, кроме того, могут быть определены расчетным путем при известных дальностях его распространения.

L_{θ_i} – уровень акустического (вибрационного) шума в i -ой октавной полосе, дБ, в месте возможного размещения акустического (вибрационного) приемника аппаратуры акустической речевой разведки (в месте возможного прослушивания речи без применения технических средств), дБ. На практике значения шума определяются инструментальными методами либо берутся из справочных таблиц.

2. РАЗРАБОТКА ПРОГРАММЫ ДЛЯ ПЭВМ ПО РАСЧЕТУ И ОЦЕНКЕ ЗАЩИЩЕННОСТИ ВЫДЕЛЕННОГО ПОМЕЩЕНИЯ ОТ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ

Для решения практических задач по расчету защищенности выделенного помещения от утечки речевой информации составить в Mathcad программу, приведенную ниже:

Начало

$i := 0 \dots 6$

Вводные исходные данные:

1) Условия распространения речевого сигнала:

- а) Открытое пространство - $\Pi 1 = 0, \Pi 2 = 0$;
- б) Помещение - $\Pi 1 = 0, \Pi 2 = 1$;
- в) Помещение - открытое пространство - $\Pi 1 = 1, \Pi 2 = 0$;
- г) Помещение - помещение - $\Pi 1 = 1, \Pi 2 = 1$.

2) Размеры защищаемого помещения, м:

- а) длина - $Dp1$; $Dp1 := 6$
- б) ширина - $Hp1$; $Hp1 := 4$
- в) высота - $Bp1$. $Bp1 := 2.5$

3) Размеры соседнего помещения, м:

- а) длина - $Dp2$; $Dp2 := 4$
- б) ширина - $Hp2$; $Hp2 := 4$
- в) высота - $Bp2$. $Bp2 := 2.5$

4) Средний коэффициент звукопоглощения звука в помещениях (0-1):

$\alpha 1 := (0.12 \ 0.13 \ 0.17 \ 0.20 \ 0.23 \ 0.25 \ 0.27)$

$\alpha 2 := (0.12 \ 0.13 \ 0.17 \ 0.20 \ 0.23 \ 0.25 \ 0.27)$

5) Средний спектральный коэффициент звукоизоляции ограждающей конструкций (ослабления речевого сигнала) в октавных полосах, дБ:

$z := (39 \ 40 \ 42 \ 48 \ 54 \ 60 \ 60)$

6) Расстояние, от источника речи до точки приема в открытом пространстве, м: $r0 := 4.5$

7) Расстояние от источника речи до контрольной точки приема на внутренней поверхности первого (защищаемого) помещения, м:

$r1 := 4$

8) Расстояние от наружной поверхности ограждающей конструкции до точки приема речевой информации в открытом пространстве, м:

$r2 := 10$

8) Расстояние от наружной поверхности ограждающей конструкции до точки приема речевой информации в соседнем помещении, м:

При использовании в качестве ТСР стетоскопа расстояние $r3$ равно 0 м, а направленного микрофона - 1 м

$r3 := 0$

9) Интегральный уровень речевого сигнала
на расстоянии 1 м от источника речи, дБ:

$$LS := 70$$

10) Средний спектральный уровень естественного шума в октавных
полосах, дБ:

$$Le := (44 \ 35 \ 29 \ 25 \ 22 \ 20 \ 19)$$

11) Наличие и вид преднамеренного шума:

$$np := 0$$

а) наличие помехи - np = 1;

б) белый шум - Ш = 0;

$$Ш := 0$$

в) розовый шум - Ш = 1;

г) шум речеподобной - Ш = 2.

12) Интегральный уровень преднамеренного шума, дБ:

$$LN := 30$$

13) Характеристика технического средства разведки в
точке приема:

а) наличие микрофона M = 1, без МКФ M = 0

$$M := 0$$

б) наличие стетоскопа St = 1

$$St := 1$$

б) V - вид = 0 - для параболического, 1 - для трубчатого

$$V := 0$$

в) диаметр отражателя параболического микрофона, м:

$$Sotr := 0.5$$

г) длина трубчатого микрофона, м

$$l_{tr} := 0.5$$

14) Использование методов шумоподавления

$$mo := 0$$

15) Октавные значения коэффициентов улучшения
отношения сигнал/шум

$$Kш := (2.0 \ 5.5 \ 5.5 \ 4.5 \ 2.25 \ 1.0 \ 0.35)$$

Постоянные исходные данные:

Коэффициент затухания звука в
воздухе

$$\beta := (0.3 \ 1.1 \ 2.8 \ 5.0 \ 9.0 \ 22.9 \ 76.6)$$

$\frac{\text{дБ}}{\text{км}}$

Среднегеометрические частоты октавных полос, Гц

$$f_{cp0,i} := 10^{\frac{3}{10} \frac{i+7}{2}}$$

Верхние и нижние частоты октавных полос, Гц:

$$f_{n0,i} := \frac{f_{cp0,i}}{\sqrt{2}}$$

$$f_{v0,i} := f_{cp0,i} \cdot \sqrt{2}$$

Расчет:

Весовые коэффициенты, характеризующие вероятность наличия формант в октавных полосах:

$$k_{l0,i} := 2.57 \cdot 10^{-8} \cdot [(f_{v0,i})^{2.4} - (f_{n0,i})^{2.4}]$$

$$k_{20,i} := 1.074 \cdot [\exp[-10^{-4} \cdot (f_{n0,i})^{1.18}] - \exp[-10^{-4} \cdot (f_{v0,i})^{1.18}]]$$

$$k_0,i := \text{if}(f_{cp0,i} > 400, k_{20,i}, k_{l0,i})$$

Формантный параметр:

$$A_{l0,i} := \frac{200}{(f_{cp0,i})^{0.43}} - 0.37$$

$$A_{20,i} := 1.37 + \frac{1000}{(f_{cp0,i})^{0.69}}$$

$$A_0,i := \text{if}(f_{cp0,i} > 1000, A_{20,i}, A_{l0,i})$$

Спектральный уровень речевого сигнала в октавных полосах, дБ:

$$L_s := (L_s - 17 \quad L_s - 4 \quad L_s - 4 \quad L_s - 9 \quad L_s - 14 \quad L_s - 17 \quad L_s - 21)$$

Расчет среднего спектрального уровня преднамеренного шума в октавных полосах дБ:

1

$$f_{spбш} := \frac{10^{\frac{LN}{10}}}{f_{v0,6} - f_{n0,0}}$$

$$L_{ш0,i} := 10 \cdot \log[f_{spбш} \cdot (f_{v0,i} - f_{n0,i})]$$

$$fspp_{\pi} := \frac{10^{\frac{LN}{10}}}{\ln\left(\frac{1}{f_{\pi 0,0}}\right) - \ln\left(\frac{1}{f_{\pi 0,6}}\right)}$$

$$L_{amp0,i} := 10 \cdot \log[fspp_{\pi} \cdot (\ln(f_{\pi 0,i}) - \ln(f_{\pi 0,i}))]$$

$$L_{amp\pi} := (LN-21 \quad LN-17 \quad LN-14 \quad LN-9 \quad LN-4 \quad LN-4 \quad LN-17)$$

$$L_{ampn0,i} := 10 \cdot \log\left(k_{0,i} \cdot 10^{\frac{LN}{10}}, 10\right)$$

$$L_{a1} := \text{if}(III > 1, L_{amp\pi}, L_{amp})$$

$$L_{a0} := \text{if}(III = 0, L_{a6}, L_{a1})$$

$$\chi := 1 \quad \phi := 1 \quad \underline{\Omega} := 2\pi \quad Kd := 1 \quad n_z := 0 \quad v := 1$$

$$P_{z0,i} := \alpha l_{0,i} \cdot \textcolor{red}{S\Omega} + \sum_{j=1}^v (A_{z0,j} \cdot n_z) \quad \textcolor{red}{P_z} = \mathbf{1}$$

$$\alpha_{cp0,i} := \frac{\textcolor{red}{P}_{z0,i}}{S\Omega} \quad B_{0,i} := \frac{\textcolor{red}{P}_{z0,i}}{1 - \alpha_{cp0,i}}$$

$$LL_{a0,i} := L_{a0,i} + 10 \cdot \log\left[\left(\left|\frac{\chi \cdot \phi}{\Omega \cdot r_l^2} + \frac{4}{Kd \cdot \textcolor{red}{B}_{0,i}}\right|\right), 10\right]$$

$$\frac{\chi \cdot \phi}{\Omega \cdot r_l^2} = 9.947 \times 10^{-3}$$

Суммарный уровень помех, дБ

$$L_{sum} := L_e + n_p \cdot \textcolor{red}{LL}_{a0}$$

Коэффициент направленного действия микрофона,
дБ:

$$K_{\text{мд}0,i} := 10 \cdot \log[1.2 \cdot 10^{-4} \cdot S_{\text{отр}} \cdot (f_{\text{ср}0,i})^2] \cdot M$$

$$K_{\text{мд}1,i} := 10 \cdot \log[6.1 \cdot 10^{-3} \cdot l_{\text{тр}} \cdot (f_{\text{ср}0,i})] \cdot M$$

$$K_{\text{мд}},i := \text{if}(V = 0, K_{\text{мд}0,i}, K_{\text{мд}1,i})$$

Уровень сигнала, распространяющегося прямой волной, в точке приема защищаемого помещения, дБ:

$$L_{\text{пр}1} := L_s - 20 \cdot \log(r_1)$$

Диффузионный уровень сигнал в точке приема в защищаемом помещении, дБ:

$$L_{\text{дл}0,i} := 10 \cdot \log \left[\frac{10^{\frac{L_{s0,i}}{10}} \cdot 4 \cdot (1 - \alpha_{0,i})}{\alpha_{0,i} \cdot S_{\text{П}}}$$

Суммарный уровень сигнала в точке приема защищаемого помещения, дБ:

$$L_{\Sigma 10,i} := 10 \cdot \log \left(10^{\frac{L_{\text{пр}10,i}}{10}} + 10^{\frac{L_{\text{дл}0,i}}{10}} \right)$$

Суммарный уровень сигнал в точке приема в соседнем помещении, дБ:

$$L_{\Sigma 20,i} := 10 \cdot \log \left[10^{0.1 \cdot (L_{\Sigma 10,i} - Z_{0,i})} + 10^{\log \left(\frac{S_{\text{пер}}}{\alpha_{20,i} \cdot S_{\text{П}2}} \right)} \right]$$

$$L_{\Sigma 2} := \text{if}(r_3 = 0, L_{\Sigma 1} - Z, \text{if}(r_3 > 1, L_{\Sigma 22}, L_{\Sigma 22} + 20 \cdot \log(r_3)))$$

Уровень сигнал, распространяющегося прямой волной, в точке приема на открытом пространстве, дБ:

$$L_o := L_s - 20 \cdot \log(r) - \frac{\beta \cdot r_o}{1000}$$

$$L_{o1} := L_{\Sigma 1} - Z - 20 \cdot \log(r_2)$$

Итоговый уровень сигнала в точке приема, дБ:

$$L\Sigma := \text{if}(\Pi1 = 1 \wedge \Pi2 = 1, L\Sigma2, \text{if}(\Pi1 = 1 \wedge \Pi2 = 0, L01, \text{if}(\Pi1 = 0 \wedge \Pi2 = 1, L\Sigma1, L0)))$$

Отношение сигнал/шум на входе акустического ПРМ, дБ:

$$q := L\Sigma + K_{\text{шд}} - L_{\text{шш}} + K_{\text{ш}}$$

Относительный уровень интенсивности формант:

$$Q := q - A \quad \text{дБ}$$

Коэффициент восприятия формант:

$$\tau_{0,i} := \text{if}(Q_{0,i} > 0, 1, 0)$$

$$r_{0,i} := \left| \tau_{0,i} - \left[\frac{0.78 + 5.46 \cdot \exp[-4.3 \cdot 10^{-3} \cdot (27.3 - |Q_{0,i}|)^2]}{1 + 10^{0.1 \cdot |Q_{0,i}|}} \right] \right| \quad +$$

Индекс артикуляции (понимаемости) звуков:

$$R := \sum_i (\tau_{0,i} \cdot k_{0,i})$$

Слоговая разборчивость речи:

$$S1 := 4 \cdot R^{1.43}$$

$$S2 := 1.1 \cdot (1 - 1.17 \cdot \exp(-2.9 \cdot R))$$

$$S3 := 1.01 \cdot (1 - 9.1 \cdot \exp(-6.9 \cdot R))$$

$$S4 := \text{if}(R \leq 0.15, S1, S2)$$

$$S := \text{if}(R > 0.7, S3, S4)$$

$$S = 1$$

Словесная разборчивость речи:

$$W1 := 1.54 \cdot R^{0.25} \cdot (1 - \exp(-11 \cdot R))$$

$$W2 := 1 - \exp\left(\frac{-11 \cdot R}{1 + 0.7 \cdot R}\right)$$

$$W := \text{if}(R < 0.15, W1, W2)$$

$$W = 1$$

Конец

3. РЕШЕНИЕ ПРАКТИЧЕСКИХ ЗАДАЧ ПО РАСЧЕТУ И ОЦЕНКЕ ЗАЩИЩЕННОСТИ ВЫДЕЛЕННОГО ПОМЕЩЕНИЯ ОТ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ

1. Исследовать зависимость словесной разборчивости речи от расстояния между источником акустического сигнала и приемником акустического сигнала для открытого пространства.

1.2 Запустить программу для расчета словесной разборчивости речи: ЛРН№1 Расчет разборчивости речи (новая 7).xmsd.

1.3. Ввести следующие исходные данные:

- формализованные параметры условий распространения речевого сигнала $\Pi 1=0$ и $\Pi 2=0$;
- интегральный уровень речевого сигнала на расстоянии 1 м от источника речи $L_s = 76$ дБ;
- средний спектральный уровень естественных шумов для тихой (сельской) местности $L_e := (44 \ 35 \ 29 \ 25 \ 22 \ 20 \ 19)$;
- формализованный параметр наличия преднамеренных помех $np = 0$;
- формализованные параметры наличия микрофона $M = 0$ и использования средств шумовой очистки $mo = 0$.

1.4. Рассчитать уровни сигнала L_o , распространяющегося прямой волной в открытом пространстве, и значения формантной R и словесной разборчивости речи W на расстояниях $ro = 1 \dots 10$ м от источника акустического сигнала.

1.5. Построить зависимости уровня сигнала L_o , формантной R и словесной разборчивости речи W от расстояния rl .

1.6. Изменить средний спектральный уровень естественных шумов, установив его для улицы с интенсивным движением $L_e := (70 \ 63 \ 58 \ 55 \ 52 \ 50 \ 49)$.

1.7. Повторить расчет значений L_o , R , W от расстояния ro и построить графики зависимостей.

2. Исследовать зависимость словесной разборчивости речи от расстояния между источником акустического сигнала и приемником акустического сигнала в выделенном помещении.

2.1. Изменить исходные данные следующим образом:

- формализованные параметры условий распространения речевого сигнала $\Pi 1=0$ и $\Pi 2=1$;
- размеры помещения $Dp1 = 12$ м, $Hp1 = 4$ м, $Bp1 = 3$ м;
- средний спектральный уровень естественных шумов для кабинета $L_e := (48 \ 40 \ 34 \ 30 \ 27 \ 25 \ 23)$.

2.2. Рассчитать уровни суммарного акустического сигнала $L\Sigma 1$ в помещении формантной R и словесной разборчивости речи W на расстояниях $ro = 1 \dots 10$ м от источника акустического сигнала.

2.3. Построить зависимости уровня сигнала $L\Sigma 1$, формантной R и словесной разборчивости речи W от расстояния rl .

2.4. Изменить средний спектральный уровень естественных шумов,

установив его шумной комнаты $L_e := (61 \ 54 \ 49 \ 45 \ 42 \ 40 \ 38)$.

2.5. Повторить расчет значений $L_{\Sigma 1}$, R , W от расстояния r_1 и построить графики зависимостей.

3. Оценить словесную разборчивость речи в каналах утечки акустической информации.

Работа проводится по вариантам, представленным в таблице.

№	Пространственные условия разведывательного контакта	Энергетические условия разведывательного контакта	Технические средства аудиоразведки
1.	1.) Подслушивание речи в кабинете руководителя (длина: 5 м, ширина: 4,5 м, высота: 2,5 м, расстояние от источника АС до стены: 2 м) из соседнего помещения (длина: 5 м ширина: 4 м высота: 2,5 м расстояние от стены до приемника АС 0,5 м)	Речь средней громкости Кирпичная кладка (0,5 кирпича) Использование методов шумоочистки: Да	Наличие микрофона: 1.) Нет 2.) Параболический микрофон (диаметр отражателя: 0,6 м)
	2.) Подслушивание речи в кабинете руководителя (длина: 5 м, ширина: 4,5 м, высота: 2,5 м, расстояние от источника АС до окна 1 м) из соседнего с помещением сквера (расстояние до приемника АС 10 м)	Громкая речь Окно (двойное остекление с воздушным промежутком «3 мм – 57 – 3 мм»): 15 дБ 20 дБ 32 дБ 41 дБ 49 дБ 46 дБ 46 дБ Использование методов шумоочистки: Да	Наличие микрофона: 1.) Параболический микрофон (диаметр отражателя: 0,85) 2.) Трубчатый микрофон (длина трубки: 0,3 м)
2.	1.) Подслушивание речи в жилом помещении многоквартирного дома (длина: 7 м ширина: 3 м высота: 2,5 м, расстояние от источника АС до стены: 1 м) из соседнего помещения (длина: 2,5 м ширина: 3,5 м высота: 2,5 м расстояние от стены до приемника АС: 0,5 м)	Тихая речь Кирпичная кладка (0,5 кирпич) Использование методов шумоочистки: Да	Наличие микрофона: 1.) Нет 2.) Трубчатый микрофон (длина трубки: 0,35 м)
	2.) Подслушивание речи в жилом помещении многоквартирного дома в спальном районе (длина: 6 м ширина: 5 м высота: 3 м, расстояние от источника АС до стены: 2 м) из близлежащей беседки (расстояние до приемника АС 15 м)	Речь средней громкости Кирпичная кладка (2 кирпича) Использование методов шумоочистки: Да	Наличие микрофона: 1.) Параболический микрофон (площадь отражателя: 0,5 м) 2.) Трубчатый микрофон (длина трубки: 0,4 м)
3.	1.) Подслушивание переговоров в кабинете университета (длина: 10 м ширина: 7,5 м высота: 3,5 м, расстояние от источника АС до металлической двери: 5 м) из соседнего кабинета (длина: 7,5 м ширина: 7,5 м высота: 3,5 м расстояние от двери до приемника АС	Громкая речь Металлическая дверь (двойная с облицовкой тамбура): 45 дБ 58 дБ 65 дБ 70 дБ 70 дБ 70 дБ 68 дБ Использование методов шумоочистки:	Наличие микрофона: 1.) Нет 2.) Трубчатый микрофон (длина трубки: 0,45 м)

№	Пространственные условия разведывательного контакта	Энергетические условия разведывательного контакта	Технические средства аудиоразведки
	0,5 м)	Нет	
	2.) Подслушивание переговоров в отделе продаж длина: 2,5 м ширина: 3,5 м высота: 2,5 м, расстояние от источника АС до окна: 1 м - с детской площадки расположенной неподалеку (расстояние до приемника АС 9 м)	Речь средней громкости Окно (двойное остекление с воздушным промежутком «3 мм – 90 – 3 мм»): 21 дБ 29 дБ 38 дБ 44 дБ 50 дБ 48 дБ 48 дБ Использование методов шумоочистки: Нет	Наличие микрофона: 1.) Параболический микрофон (площадь отражателя: 0,55 м) 2.) Трубчатый микрофон (длина трубки: 0,5 м)
4.	1.) Подслушивание переговоров в спецотделе (длина: 3 м ширина: 5 м высота: 2,5 м, расстояние от источника АС до стены 1,5 м) из соседнего помещения (длина: 4 м ширина: 5 м высота: 2,5 м расстояние от стены до приемника АС: 0,5 м)	Тихая речь Кирпичная кладка (0,5 кирпича) Использование методов шумоочистки: Нет	Наличие микрофона: 1.) Нет 2.) Трубчатый микрофон (длина трубки: 0,55 м)
	2.) Подслушивание речи в кабинете руководителя (длина: 2 м ширина: 2 м высота: 2,5 м расстояние до окна 0,5 м) из соседнего с помещением парка (расстояние до точки наблюдения 16 м)	Речь средней громкости Окно (двойное остекление с воздушным промежутком «4 мм – 57 – 4 мм»): 21 дБ 31 дБ 38 дБ 46 дБ 49 дБ 55 дБ 55 дБ Использование методов шумоочистки: Нет	Наличие микрофона: 1.) Параболический микрофон (площадь отражателя: 0,65 м) 2.) Нет
5.	1.) Подслушивание переговоров в кабинете университета (длина: 7 м ширина: 6 м высота: 3,5 м расстояние до стены: 2 м) из фойе кабинета (длина: 7,5 м ширина: 6 м высота: 3,5 м расстояние от стены до приемника АС: 0,5 м)	Громкая речь Кирпичная кладка (0,5 кирпича) Использование методов шумоочистки: Нет	Наличие микрофона: 1.) Трубчатый микрофон (длина трубки: 0,6 м) 2.) Параболический микрофон (площадь отражателя: 0,7 м)
	2.) Подслушивание речи в кабинете руководителя (длина: 6 м ширина: 3,5 м высота: 3,5 м расстояние до окна 2 м) из проходящей рядом дороги со средней интенсивностью движения (расстояние до приемника АС 12 м)	Тихая речь Окно (двойное остекление с воздушным промежутком «4 мм – 90 – 4 мм»): 25 дБ 33 дБ 41 дБ 47 дБ 48 дБ 36 дБ 36 дБ Использование	Наличие микрофона: 1.) Параболический микрофон (площадь отражателя: 0,75 м) 2.) Нет

№	Пространственные условия разведывательного контакта	Энергетические условия разведывательного контакта	Технические средства аудиоразведки
		методов шумоочистки: Да	
6.	1.) Подслушивание речи в кабинете руководителя (длина: 6 м ширина: 5 м высота: 2,8 м расстояние до двери 2 м) из коридора (длина: 10 м ширина: 3 м высота: 2 м расстояние от двери до приемника АС: 1 м)	Речь средней громкости Дверь (звукоизолирующая тяжелая): 24 дБ 36 дБ 45 дБ 51 дБ 50 дБ 49 дБ 45 дБ Использование методов шумоочистки: Да	Наличие микрофона: 1.) Нет 2.) Трубочатый микрофон (длина трубки: 0,31 м)
	2.) Подслушивание речи в кабинете руководителя (длина: 6 м ширина: 5 м высота: 2,5 м расстояние до двери 3 м) из припаркованной в центре города машины (расстояние до приемника АС 15 м)	Громкая речь Дверь (двойная с зазором не более 200 мм): 25 дБ 42 дБ 55 дБ 58 дБ 60 дБ 60 дБ 62 дБ Использование методов шумоочистки: Да	Наличие микрофона: 1.) Параболический микрофон (площадь отражателя: 0,8 м) 2.) Трубочатый микрофон (длина трубки: 0,29 м)
7.	1.) Подслушивание речи в кабинете руководителя (длина: 6 м ширина: 5,5 м высота: 3,5 м расстояние до стены: 1,5 м) из соседнего помещения (длина: 6 м ширина: 5 м высота: 3,5 м расстояние от стены до приемника АС 0,5 м)	Речь средней громкости Железобетонные плиты (40 мм) Использование методов шумоочистки: Нет	Наличие микрофона: 1.) Нет 2.) Параболический микрофон (площадь отражателя: 0,45 м)
	2.) Подслушивание переговоров в бухгалтерии (длина: 4,5 м ширина: 3,5 м высота: 2,5 м расстояние до стены: 0,5 м) мимо проходящим человеком (расстояние до приемника АС 2,5 м)	Речь средней громкости Железобетонные плиты (50 мм) Использование методов шумоочистки: Да	Наличие микрофона: 1.) Нет 2.) Трубочатый микрофон (длина трубки: 0,35 м)
8.	1.) Подслушивание переговоров в кабинете университета (длина: 9 м ширина: 6,5 м высота: 3,5 м расстояние до двери: 2 м) из соседнего кабинета (длина: 6,5 м ширина: 6,5 м высота: 3,5 м расстояние от двери до приемника АС: 0,5 м)	Речь средней громкости Дверь (звукоизолирующая облегченная): 18 дБ 30 дБ 39 дБ 42 дБ 45 дБ 43 дБ 42 дБ Использование методов шумоочистки: Нет	Наличие микрофона: 1.) Параболический микрофон (площадь отражателя: 0,5 м) 2.) Трубочатый микрофон (длина трубки: 0,33 м)
	2.) Подслушивание речи в отделе продаж длина: 3,5 м ширина: 5,5 м высота: 2,5 м расстояние до окна: 1,5 м) с детской	Громкая речь Окно (одинарное остекление толщина 3	Наличие микрофона: 1.) Нет 2.) Трубочатый

№	Пространственные условия разведывательного контакта	Энергетические условия разведывательного контакта	Технические средства аудиоразведки
	площадки расположенной неподалеку (расстояние до приемника АС 17 м)	мм): 17 дБ 17 дБ 22 дБ 28 дБ 31 дБ 32 дБ 34 дБ Использование методов шумоочистки: Нет	микрофон (длина трубки: 0,4 м)
9.	1.) Подслушивание речи в жилом помещении многоквартирного дома (длина: 6 м ширина: 4 м высота: 2,5 м расстояние до стены: 2 м) из соседнего помещения (длина: 3,5 м ширина: 2,5 м высота: 2,5 м расстояние от стены до приемника АС: 1,5 м)	Громкая речь Железобетонные плиты (100 мм) Использование методов шумоочистки: Да	Наличие микрофона: 1.) Нет 2.) Трубчатый микрофон (длина трубки: 0,44 м)
	2.) Подслушивание переговоров в жилом помещении многоквартирного дома в спальном районе (длина: 4 м ширина: 4,5 м высота: 3 м расстояние до стены: 1,5 м) из близлежащего гаража (расстояние до приемника АС 9 м)	Речь средней громкости Железобетонные плиты (160 мм) Использование методов шумоочистки: Нет	Наличие микрофона: 1.) Параболический микрофон (площадь отражателя: 0,6 м) 2.) Трубчатый микрофон (длина трубки: 0,52 м)
1	1.) Подслушивание речи в спецотделе (длина: 4 м ширина: 4 м высота: 3,5 м расстояние до стены 1,5 м) из соседнего помещения (длина: 3 м ширина: 4 м высота: 3,5 м, расстояние от стены до приемника АС: 0,5 м)	Громкая речь Шлакоблоки, отштукатуренные с двух сторон Использование методов шумоочистки: Да	Наличие микрофона: 1.) Трубчатый микрофон (длина трубки: 0,35 м) 2.) Параболический микрофон (площадь отражателя: 0,65 м)
	2.) Подслушивание речи в кабинете руководителя (длина: 4 м ширина: 2,5 м высота: 2,5 м расстояние до двери 1 м) из припаркованной в спальном районе машины (расстояние до приемника АС 20 м)	Речь средней громкости Дверь (типовая с прокладкой из пористой резины): 29 дБ 30 дБ 33 дБ 35 дБ 39 дБ 41 дБ 43 дБ Использование методов шумоочистки: Да	Наличие микрофона: 1.) Нет 2.) Параболический микрофон (площадь отражателя: 0,85)

3.1. Запустить программу для расчета словесной разборчивости речи: Прога/Wordleg.exe.

2. Для своего варианта произвести расчет словесной разборчивости речи и оценить опасность акустического канала утечки информации.

4. Исследовать эффективность маскирования речи источниками шума.

4.1. Для тех же условий разведывательного контакта, указанных в заданном варианте, произвести маскирование речи генератором белого шума

(интегральный уровень шума определяется по формуле 50 дБ минус № варианта) и рассчитать слосную разборчивость речи.

4.2. Сделать выводы об эффективности маскирования.

**Задание обучаемым для самостоятельной учебной работы
при подготовке к занятию:**

11. Закрепить и углубить знания, полученные на лекции, для этого изучить конспект лекций и рекомендуемую литературу:
 - [1] Технические средства и методы защиты информации. Учебное пособие для вузов / Под ред. А.П. Зайцева и А.А. Шелупанова. – М.: Горячая линия-Телеком, 2009..
12. Изучить методические указания к ПЗ № 5-7.

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1

**Лабораторная работа разработана
доцентом кафедры ОТЗИ Сагдеевым К.М.**

Обсуждена и одобрена на заседании
кафедры ОТЗИ Протокол
№__от____2013 г.

Ставрополь 2013 г.

РАЗДЕЛ № 9. ОРГАНИЗАЦИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Тема № 37. ДОКУМЕНТАЛЬНОЕ ОФОРМЛЕНИЕ РЕЗУЛЬТАТОВ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ ОБЪЕКТА ИНФОРМАТИЗАЦИИ ТРЕБОВАНИЯМ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Практические занятия № 14-18.

Тема: Документальное оформление результатов аттестационных испытаний объекта информатизации требованиям по безопасности информации

Время – 6 часов.

Формируемые компетенции: ОПК-4, ОПК-11, ОПК-2.1.

УЧЕБНЫЕ ВОПРОСЫ:

1. Порядок и правила документального оформления результатов аттестационных испытаний.
2. Решение практических задач по документальному оформлению результатов аттестационных испытаний.

СОДЕРЖАНИЕ ПРАКТИЧЕСКОГО ЗАНЯТИЯ

1. ПОРЯДОК И ПРАВИЛА ДОКУМЕНТАЛЬНОГО ОФОРМЛЕНИЯ РЕЗУЛЬТАТОВ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа - «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России.

Наличие на объекте информатизации действующего «Аттестата соответствия» дает право обработки информации с уровнем секретности (конфиденциальности) и на период времени, установленными в «Аттестате соответствия».

Обязательной аттестации подлежат объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров.

Аттестационные испытания по требованиям безопасности информации автоматизированной системы включают в себя:

- Экспертный анализ готовности АС к Аттестации по требованиям безопасности информации
- Разработка организационно-распорядительных документов на объект.

- Разработка и согласование Программы и методик проведения аттестационных испытаний по требованиям безопасности информации
- Проведение инструментальных измерений, специальных исследований и оценки защищенности объекта от утечки информации по каналам ПЭМИН.
- Анализ организационной структуры объекта, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, и выдача рекомендаций по применению систем и средств защиты информации на объекте.
- Установка и настройка СЗИ от НСД в соответствии с требованиями РД по защите информации от НСД, с последующими испытаниями.
- Проверка эффективности применяемых на объектах средств и систем защиты информации
- Подготовка и оформление пакета аттестационной отчетной документации
- Выдача Аттестата соответствия объекта требованиям по безопасности информации

Необходимый и достаточный пакет исходных данных документов для аттестации АС

- Распоряжение/Приказ о создании комиссии по категорированию и классификации
- Распоряжение/Приказ о назначении ответственного за эксплуатацию объекта и администратора безопасности информации
- Акт категорирования объекта информатизации
- Акт классификации объекта информатизации
- Состав технических и программных средств АС (должно быть в составе ТП)
- Схема размещения ОТСС, ВТСС и средств защиты информации (должно быть в составе ТП)
- Схема размещения объекта относительно границ контролируемой зоны(должно быть в составе ТП)
- Технический паспорт на объект информатизации
- Перечень решаемых задач
- Перечень защищаемых ресурсов АС
- Разрешительная система доступа к информационным ресурсам АС
- Схема информационных потоков (при необходимости в больших распределенных ЛВС)
- Список сотрудников лиц, имеющих право самостоятельного доступа к штатным средствам АС
- Список сотрудников лиц, имеющих право самостоятельного доступа в помещение объекта
- Описание технологического процесса обработки закрытой информации на АС
- Инструкция по антивирусной защите АС
- Инструкция пользователям АС
- Инструкция администратору безопасности АС

- Инструкция по организации парольной защиты АС
- Система защиты информации от НСД. Руководство администратора.
- Система защиты информации от НСД. Руководство пользователя.
- Лицензия РУ ФСБ на право осуществления работ с использованием сведений, составляющих ГТ

Таким образом, предоставив все перечисленные документы в соответствующие органы, вам в течение некоторого времени будет выдана аттестация объектов информатизации.

Заказчик должен быть в курсе того, что аттестация объектов информатизации проходит в несколько этапов:

- Первый этап включает в себя осмотр и исследования, при помощи которых происходит обработка закрытой информации или контроль инструментов звуковой безопасности ограждения выделенного помещения.
- Следующий этап включает в себя проведение специальных исследований объектов, которые изучают все технические средства, проводные коммуникации, средства программных информационных систем и в том числе спец проверку техсредств зарубежного производителя. По итогам проведенных мероприятий составляется протокол исследований, а также предписываются эксплуатационные действия.
- На последнем этапе аттестации объектов информатизации проводятся комплексные работы по испытанию оборудования и систем, которые входят в проверяемый объект. Мероприятия включают в себя проверку на соответствие требованиям по защите информации, а также проводят согласование итоговых результатов в УГР.

Аттестация объектов информатизации выдается Заказчику после принятия решения УГР.

2. РЕШЕНИЕ ПРАКТИЧЕСКИХ ЗАДАЧ ПО ДОКУМЕНТАЛЬНОМУ ОФОРМЛЕНИЮ РЕЗУЛЬТАТОВ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ

Практическое задание. Оформить документально результаты аттестационных испытаний компьютерного класса как объекта информатизации. Образец протокола аттестационных испытаний приведен ниже.

Закрытое акционерное общество _____

(Аттестат аккредитации №СЗИ RU. _____)

Гриф

Экз. № 1 № _____

УТВЕРЖДАЮ

Руководитель органа по аттестации
объектов информатизации _____

«_____» _____ 2005 г.

Управ ление

по Челябинской области

ул.

Объект информатизации

АВТОНОМНАЯ ПЕРСОНАЛЬНАЯ ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНАЯ МАШИНА

(№ 061208)

ПРОТОКОЛ

аттестационных испытаний объекта информатизации

на соответствие требованиям безопасности информации, по направлению

"Защита информации от несанкционированного доступа"

г. Челябинск

2005 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1.

Аттестационная комиссия ЗАО _____ (лицензии ФСБ России рег. № _____ (действительны до _____ г.), лицензия Гостехкомиссии России рег. № _____ и аттестат аккредитации органа по аттестации объектов информатизации № СЗИ RU. _____ (действительны до _____ г.)), в составе _____ провела аттестационные испытания объекта информатизации на базе автономной персональной электронно-вычислительной машины № 061208, расположенной по адресу: _____ (далее объект информатизации), на соответствие требованиям по безопасности информации по направлению «Соответствие требованиям по защите информации от НСД».

1.2. Заявитель аттестационных испытаний объекта – области. Объект информатизации принадлежит группе режима и информационной безопасности Заявителя.

1.3. Заявленная категория объекта информатизации – третья, класс защищенности автоматизированной системы от несанкционированного доступа к информации – 2А.

Состав основных технических средств и систем (ОТСС), системного и прикладного программного обеспечения, а также средств и систем защиты информации объекта информатизации приведен в Таблице 1.

Таблица 1 – Состав объекта информатизации

№ п.п.	Модель	Инв. номер	Заводской номер	Примечание
<u>Состав основных технических средств и систем</u>				
1.	Системный блок K-Systems	-		
2.	Монитор LG FLATRON F700P	-		
3.	Принтер Samsung ML-1250	-		
4.	Клавиатура Chicony	-		
5.	Манипулятор типа "мышь" K-Systems	-		
<u>Состав системного и прикладного программного обеспечения</u>				
6.	Операционная система MS Windows 2000 SP 4			
7.	Microsoft Office 2000			
8.	Asus Probe V2.22.03		-	
9.	FAR		-	свободно распространяемое ПО
10.	WinRAR 3.00		-	
<u>Состав средств и систем защиты информации</u>				
11.	Программно-аппаратный комплекс защиты информации от НЗД Secret Net 4.0			сертификат № 640 (действителен до 27.06.2005 г.)
12.	Антивирусное средство Dr WEB 4.32b			

2. РЕЗУЛЬТАТЫ ИСПЫТАНИЙ

2.1. Аттестационные испытания объекта информатизации проводились в соответствии с разделом 2 «Программы и методики проведения аттестационных испытаний...» (уч. № ____ от 25.03.2005 г.) в следующем порядке:

- анализ полноты предоставленных исходных данных, проверка их соответствия реальным условиям монтажа и эксплуатации;
- определение состава использованных для обработки информатизации технических средств, их комплектность и соответствие данным, указанным в эксплуатационной документации;
- проверка выполнения требований от утечки за счет побочных электромагнитных излучений (ПЭМИ);
- проверка выполнения требований от утечки за счет наводок на вспомогательные технические средства и системы (ВТСС);
- проверка выполнения требований от утечки информативного сигнала по цепям электропитания и заземления;
- комплексные испытания объекта, в т.ч. при возникновении внештатных ситуаций..

2.2. Анализ полноты исходных данных

2.2.1. Аттестационной комиссии были представлены следующие исходные данные и документация на объект информатизации:

Таблица 2 – Перечень документации на объект информатизации

№ п.п.	Предоставлено Заявителем	Рег. номер
1.	Приказ о подготовке к аттестации объектов вычислительной техники	
2.	Приказ о закреплении ответственных за эксплуатацию	
3.	Приказ Развернутого перечня сведений, подлежащих заскречиванию	
4.	Приказ России «О утверждении Инструкции о порядке проведения мероприятий по технической защите информации, составляющей государственную тайну, и аттестации объектов информатизации на соответствие требованиям по безопасности информации»	
5.	Приказ России «Об утверждении Инструкции по оборудованию объектов за средств охраны и их инженерно-технической укреплённости»	
6.	Приказ России «Об обеспечении безопасности деятельности»	
7.	Приказ России «Об утверждении инструкции по обеспечению режима секретности при обработке информации, содержащей сведения, составляющие государственную тайну, с использованием средств вычислительной техники в органах наркоконтроля»	
8.	Акт категорирования объекта вычислительной техники	
9.	Акт классификации автоматизированной системы по требованиям безопасности информации	
10.	Перечень защищаемых ресурсов автоматизированной системы на базе объекта вычислительной техники и уровень их конфиденциальности	
11.	Перечень ПО	
12.	Данные по уровню подготовки кадров, обеспечивающих защиту информации	
13.	Схема контролируемой зоны, утверждена начальником Управления	
14.	Руководство по защите секретной информации	
15.	Описание технологического процесса	
16.	Инструкция администратора информационной безопасности объекта вычислительной техники группы режима и информационной безопасности	
17.	Инструкция пользователя объекта вычислительной техники группы режима и информационной безопасности	
18.	Инструкция обслуживающего персонала объекта вычислительной техники группы режима и информационной безопасности	
19.	Журнал учета машинных носителей информации	
20.	Технический паспорт объекта информатизации группы режима и информационной безопасности	
21.	Заключение по результатам проведения специальной проверки технических средств иностранного производства	
22.	Предписание на эксплуатацию ПЭВМ	

23.	Сертификат соответствия на систему защиты информации от несанкционированного доступа Secret Net 4.0	
24.	Инструкция о порядке сдачи-приема под охрану режимных помещений	
25.	Инструкция по правилам пожарной безопасности для сотрудников России по Челябинской области при возникновении пожара	
26.	Инструкция по действиям сотрудников при возникновении чрезвычайных обстоятельств и план эвакуации имущества группы режима и информационной безопасности	
27.	Список лиц, имеющих право приема-сдачи помещения РСО под охрану и вскрытия с образцами подписей	
28.	Письмо из Управления ФСБ России по Челябинской области в отношении представителей иностранных государств	

Заключение: В предоставленных документах (см. 2.2.1) содержатся все необходимые исходные данные об объекте информатизации. Дополнительных документов не требуется.

2.3. Исследование технологического процесса обработки и хранения информации, анализ информационных потоков, определение состава использованных для обработки информации технических средств.

2.3.1. Согласно предоставленным Заявителем документам (см. Таблица 2) был проведен анализ технологического процесса информации реализованного в АС. Было установлено следующее:

1. АС предназначена для разработки документов с грифом «секретно», пользователи имеют одинаковые права доступа к информационным и техническим ресурсам АС.
2. Доступ исполнителей к работе на объекте осуществляется на основании приказа о назначении ответственных за эксплуатацию ОВТ (см. Таблица 2.).
3. Предполагается наличие только постоянных пользователей.
4. Помещение объекта информатизации оборудовано техническими средствами охраны.
5. Пользователи имеют право постоянного хранения файлов с секретными данными на НЖМД, в каталоге {C:\Документы\Секретно}.
6. Для хранения файлов с секретными данными могут также использоваться учтенные засекреченные установленным порядком гибкие магнитные диски "дискеты" (ГМД), устройства flash-memory.
7. Удаленные файлы, а также временные файлы на магнитных носителях уничтожаются штатными средствами системы «Secret Net 2000» версия 4.0.
8. Загрузка компьютера осуществляется по персональному имени и паролю конкретного пользователя, который хранится в персональной учетной записи пользователя в операционной системе, настройках безопасности СЗИ «Secret Net 2000» версия 4.0 и идентификаторе Touch Memory. По окончании загрузки компьютера пользователь получает установленные Администратором безопасности права доступа к устройствам, каталогам, файлам и программам АС.
9. Печать документов осуществляется специально назначенным пользователем. Печать производится на учтенных листах и регистрируется в установленном секретным делопроизводством порядке. Факт печати регистрируется вручную пользователем в «Журнале учета машинных носителей информации...».
10. В целях защиты информации от несанкционированного доступа на ПЭВМ установлена программно-аппаратная система защиты информации от НСД «Secret Net 2000» версия 4.0 (автономный вариант). Настройку системы защиты от НСД для конкретных пользователей и контроль ее работы осуществляет Администратор безопасности. Функции, права, обязанности и порядок работы на ПЭВМ Администратора безопасности и пользователей регламентируется специально разработанными инструкциями Администратору безопасности и пользователю ПЭВМ.
11. На ПЭВМ установлена операционная система Windows 2000 Professional Rus SP4. Копия лицензионной версии операционной системы, а также копии программного обеспечения системы защиты информации от НСД находятся у Администратора безопасности.
12. Для разработки документов пользователей на ПЭВМ установлен программный пакет Microsoft Office 2000.
13. Права доступа пользователей к программам, каталогам и файлам на ПЭВМ определены в документации по разрешительной системе доступа персонала к защищаемым ресурсам и реализованы средствами системы защиты от НСД «Secret Net 2000» версия 4.0.
14. Права доступа пользователей к режимам обработки информации (корректировка, просмотр, печать) утверждаются в установленном порядке.
15. Антивирусная защита осуществляется администратором с применением программных средств антивирусного контроля AVP в соответствии с «Инструкцией администратора».

Выводы: Описание технологического процесса обработки и хранения секретной информации соответствует реальной практике, принятой на рассматриваемом объекте информатизации.

2.3.2. Согласно предоставленным Заявителем документам (см. Таблица 2) была проведена проверка соответствия АС заявленному классу защищенности. Было установлено следующее:

1. Объектами доступа в АС являются:

- машинные носители информации (накопитель на жестких магнитных дисках (НЖМД – «винчестер»), накопители на гибких магнитных дисках (НГМД – дискеты 3,5"), диски CD-ROM, устройства flash-memory);
- ПЭВМ в целом, в т.ч. принтер (см. Таблица 1);
- коммуникационные порты системного блока (LPT, COM, USB-порты);
- файлы (в т.ч. временные и технологические) и каталоги с файлами, содержащие защищаемые сведения;
- распечатанные документы, содержащие защищаемые сведения;
- привод (устройство чтения) CD-ROM и дисковод (устройство чтения/записи) на 3,5" дискеты;
- каталоги (файлы) с общесистемным и прикладным программным обеспечением;
- каталог (файлы) системы защиты информации от несанкционированного доступа (СЗИ от НСД).

2. Субъектами доступа в АС являются:

- администратор информационной безопасности, осуществляющий администрирование программно-аппаратный комплекс СЗИ от НСД, а также установку и настройку прикладного и системного программного обеспечения;
- пользователи с одинаковыми правами, работающие в АС;
- обслуживающий персонал, осуществляющий техническое обслуживание средств вычислительной техники (ОТСС);

Выводы: Классификация АС выполнена в соответствии с требованиями руководящих документов. По уровню детализации и идентификации объектов доступа АС удовлетворяет требованиям руководящих документов к заявленному классу защищенности АС – 2А.

2.3.3. В качестве штатных средств доступа к информации в АС предусмотрены:

- стандартные средства операционной системы Microsoft Windows 2000 Professional;
- программы из пакета Microsoft Office 2000;
- файловый менеджер FAR;
- средства настройки и контроля функций установленного в АС программного СЗИ «Secret Net 2000» версия 4.0;
- средства настройки и контроля функций установленного антивирусного ПО Dr Web 4.32b

Выводы: По перечню штатных средств доступа АС удовлетворяет требованиям руководящих документов к заявленному классу защищенности АС – 2А.

2.3.4. На ПЭВМ установлена система «Secret Net 2000» версия 4.0 (автономный вариант) – сертификат Гостехкомиссии России № 640 от 27.06.2002 г., действительно до 27.06.2005 г. – состоящая из средства аппаратной поддержки – платы Secret Net Touch Memory Card PCI, электронного идентификатора Touch Memory и программного обеспечения для Windows NT/2000.

Сертификат прилагается в документах представленных заявителем. Обеспечиваются показатели защищенности от НСД к информации по 3 классу защищенности СВТ при условии соблюдения ограничений, приведенных в приложении к настоящему сертификату по 3 классу контроля уровня не декларированных возможностей.

Согласно представленным документам, при обработке защищаемой информации дополнительно проводятся организационно-технические мероприятия, обеспечивающие требуемый режим секретности, а также целостность и сохранность защищаемой информации.

СЗИ от НСД «Secret Net 2000» версия 4.0 установлена в необходимой комплектности в соответствии паспортом на изделие. Установка и настройка программной и аппаратной части произведена в соответствии с документацией на систему, без нарушений. По результатам настройки СЗИ от НСД «Secret Net 2000» версия 4.0 подготовлен «Формуляр на объект информатизации...».

Выводы: Применяемая сертифицированная СЗИ от НСД «Secret Net 2000» версия 4.0 удовлетворяет требованиям руководящих документов, реализует необходимые и достаточные функции, предъявляемые к АС заявленного класса защищенности – 2А.

2.3.5. Проверка разрешительной системы допуска персонала к защищаемым ресурсам АС заключалась в анализе предоставленной организационно-распорядительной документации, ее устанавливающей. Анализ документации показал, что действующими факторами разрешительной системы являются:

- размещение автоматизированного рабочего места (АРМ) в условиях контролируемого доступа – в помещении отдела по защите информации и мобилизационной работы;
- действия сотрудников (пользователей, администратора и обслуживающего персонала), имеющих доступ к автоматизированным рабочим местам (ОТСС), регламентированы специальными инструкциями;
- эксплуатация, сопровождение и контроль функционирования АС (технических и программных средств АС) осуществляется администратором АС, а при необходимости допущенным обслуживающим персоналом под контролем администратора АС;

Была проведена проверка оформленных разрешений на допуск персонала к информации определенного грифа (уровня) секретности и соответствия технологических инструкций пользователей, администратора и обслуживающего персонала установленным требованиям.

Выводы: Реализованная разрешительная система доступа сотрудников к работе на объекте информатизации удовлетворяет требованиям руководящих документов к заявленному классу защищенности АС – 2А.

2.3.6. В соответствии с действующей на объекте информатизации разрешительной системой допуска в АС средствами СЗИ от НСД «Secret Net 2000» версия 4.0 реализованы правила доступа, при которых каждый пользователь в соответствии с назначенными правилами имеет доступ:

- к средствам ОС, обеспечивающим запуск и функционирование АС;
- к средствам разработки документов;
- к средствам антивирусной защиты;
- к каталогам на НЖМД, предназначенным для хранения информации;
- к дискетам 3,5", предназначенным для хранения информации;
- портам системного блока.

СЗИ от НСД «Secret Net 2000» версия 4.0 установлена в необходимой комплектности в соответствии паспортом на изделие. Установка и настройка программной и аппаратной части произведена в соответствии с документацией на систему, без нарушений. По результатам настройки СЗИ от НСД «Secret Net 2000» версия 4.0 подготовлен «Формуляр на объект информатизации...» и «Акт установки...».

Выводы: Настройка СЗИ от НСД произведена корректно и правильно. Предоставленная документация соответствует реальной настройке СЗИ и удовлетворяет требованиям руководящих документов к заявленному классу защищенности АС – 2А.

2.4. Перечень угроз НСД АС и реализованных мер по их устранению

2.4.1 Учитывая особенности конфигурации объекта информатизации, существующего технологического процесса обработки информации и принятой разрешительной системы доступа, возможные угрозы НСД к информационным и техническим ресурсам аттестуемого объекта и принятые меры по их устранению изложены в Таблица 3.

Таблица 3 – Перечень угроз НСД в АС

№ п./п.	Тип угрозы НСД	Кто может явиться нарушителем	Способ реализации угрозы	Как устранена угроза
1.	Хищение, вывод из строя ОТСС в целом, либо носителей информации (в т.ч. бумажных)	Лица, имеющие возможность доступа в помещение с ОТСС	Вывод оборудования, не санкционированный доступ в контролируемое помещение.	Контроль доступа в помещение, физическая охрана, использование средств технической охраны.
2.	Копирование защищаемых ресурсов на неучтённые ПМД	Лица, имеющие физический доступ к ОТСС	Доступ посторонних лиц при работе легальных пользователей	Управление доступом к ресурсам средствами СЗИ от НСД. Регистрация действий пользователей средствами СЗИ от НСД. Регламентация прав и ответственности пользователей в инструкциях.
3.	Доступ к остаточной информации на НЖМД	Лица, имеющие физический доступ к ПЗВМ и НЖМД	Доступ посторонних лиц при работе легальных пользователей	Затирание остаточной информации средствами СЗИ от НСД
4.	Доступ к ресурсам ОТСС (объектам доступа) за счёт обхода СЗИ с использованием загрузки с ПМД или CD-ROM, а также путём исключения загрузки модулей и драйверов СЗИ	Лица, имеющие физический доступ к ПЗВМ	Доступ посторонних лиц при работе легальных пользователей	Запрещение загрузки с иных носителей кроме основного НЖМД, опечатывание системного блока ПЗВМ. Средствами СЗИ от НСД запрещена загрузка с внешних носителей.
5.	Нарушение целостности файлов операционной системы, СЗИ от НСД	Лица, имеющие физический доступ к ОТСС	Доступ посторонних лиц при работе легальных пользователей	Обеспечение целостности сертифицированной СЗИ от НСД
6.	Разрушение защищаемой информации компьютерными вирусами	Лица, имеющие физический доступ к ОТСС при загруженной ОС	Доступ посторонних лиц при работе легальных пользователей	Выполнение инструкции по проведению антивирусного контроля, применение программных средств защиты от вирусов.
7.	Несанкционированное ознакомление с защищаемой информацией, отображаемой на видеомониторе и распечатках.	Лица, имеющие доступ в помещение с ОТСС	Доступ посторонних лиц в помещение	Контролируемый доступ в помещение. Размещение рабочего места с монитором, исключающим возможность наблюдения информации на мониторе и распечатках, не допущенными лицами.
8.	Доступ к информации путем восстановления удалённых файлов	Лица, имеющие физический доступ к ПЗВМ	Доступ посторонних лиц при работе легальных пользователей	Затирание файлов с использованием сертифицированной СЗИ от НСД

2.4.2 Согласно представленной документации, перечисленные угрозы устраняются применением на объекте информатизации СЗИ от НСД «Secret Net 2000» версия 4.0, Антивирусной программы Dr Web 4.32b, а также организационными мерами.

Выводы: Приведенный в Таблице 3 перечень угроз информации в АС является полным и соответствует особенностям конфигурации объекта информатизации и существующего технологического процесса.

2.5 Проверка механизма идентификации и проверки подлинности (аутентификации) субъектов доступа при входе в АС.

2.5.1 Оценка реализованных правил разграничения доступа в АС проводилась по реальным возможностям (функциям) СЗИ от НСД «Secret Net 2000» версия 4.0. Установлено, что в АС реализован дискреционный и мандатный механизмы доступа к ресурсам (объектам доступа). Применяемая в АС СЗИ от НСД «Secret Net 2000» версия 4.0 предоставляет ряд возможностей по выполнению требований руководящих документов. Средства защиты активизированы и настроены согласно _____.

2.5.2 Проверка правильности идентификации субъектов и объектов доступа в АС осуществлялась путем обращения к ним (объектам) по персональному имени и паролю. Проверка проводилась штатными средствами анализа их принадлежности множеству всех зарегистрированных идентификаторов субъектов (пользователей) при обращении к объектам доступа. Данная проверка включала:

- проверку идентификации субъектов доступа при входе в АС по персональному идентификатору Touch Memory и проверку подлинности (аутентификации) предъявленных имени пользователя и пароля;
- проверку контроля доступа субъектов доступа (пользователей) к защищаемым ресурсам (объектам доступа) в соответствии с матрицей доступа;

2.5.3 При проверке идентификации и аутентификации субъектов доступа были проведены следующие действия (см. Таблица 4):

Таблица 4 – Действия по проверке идентификации и аутентификации субъектов доступа

№ п.п.	Действия по проверке	Результат проверки	Вывод по проверке
1.	Возможность загрузки системы с внешних носителей – дискиеты и/или CD диска, в обход штатных механизмов защиты	1. Попытки загрузки с внешних носителей отклоняются (игнорируются) системой защиты информации.	соответствует требованиям
2.	Запрос системой персонального идентификатора – после включения системного блока ПЭВМ	1. Запрос системой персонального идентификатора осуществляется после предварительной загрузки ядра системы. Для авторизации и дальнейшей загрузки персонального профиля пользователя с соответствующими правами доступа к информации, необходимо предъявить персональный идентификатор. 2. Без предъявления персонального идентификатора доступ к работе с информацией на ПЭВМ исключен и блокируется СЗИ от НСД.	соответствует требованиям
3.	Проверка работоспособности механизма идентификации и аутентификации в системе пользователей и Администратора АС	1. При вводе правильного имени пользователя и пароля вручную либо посредством персонального идентификатора, производится окончательная загрузка операционной системы и сконфигурированного профиля соответствующего пользователя. 2. При вводе не правильного имени пользователя и пароля выводится соответствующее сообщение и доступ ко всем ресурсам системы остается не возможным до введения корректных учетных данных (имя пользователя и пароль) 3. По достижении определенного настройками СЗИ от НСД предела неудачных попыток входа, доступ в систему блокируется для пользователя. Блокировку может снять только администратор.	соответствует требованиям
4.	Проверка надежности аутентификации	1. Установленная в АС СЗИ от НСД «Secret Net 2000» версия 4.0 автоматизированным способом осуществляет проверку количества символов в пароле пользователя. Так же, проверка осуществляется организационными мерами Администратором АС при задании (смене) пользователем пароля. 2. Пароли пользователей и Администратора АС составляют 6 и более буквенно-цифровых символов. 3. При вводе пароля на экране монитора отображение вводимых символов не производится, выводится символ «*». 4. Механизм смены пароля работоспособен. Изменение пароля производится пользователем под контролем Администратора АС, либо непосредственно администратором. 5. Требования к порядку изменения пароля отражены в инструкции Администратору АС.	соответствует требованиям

2.5.4 В соответствии с требованиями регламентирующих документов смена пароля пользователей производится не реже одного раза в шесть месяцев. Пароль может быть изменен в следующих случаях:

- по истечении срока действия;
- по требованию пользователя (но не чаще одного раза в месяц);
- по требованию Администратора АС в случае, если существуют предпосылки к раскрытию пароля (пароль стал известен другим лицам).

При изменении пароля пользователя идентификатор пользователя перезаписывается в соответствии с произведенными изменениями учетной записи.

2.5.5 В случае потери пользователем персонального идентификатора либо выходом идентификатора из строя, администратором безопасности АС создается другой идентификатор. Учетная запись пользователя не меняется.

Выводы: Реализованный в СЗИ от НСД «Secret Net 2000» версия 4.0 механизм идентификации и аутентификации пользователей и Администратора АС, а также выполненные настройки данного СЗИ от НСД (см. Таблица 4) соответствуют требованиям руководящих документов к заявленному классу защищенности АС – 2А.

2.6 Проверка механизма идентификации терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам и/или адресам

Выводы: В связи с тем, что ОТСС в своем составе не содержит терминалов, других ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ проверка механизма их идентификации не проводилась.

2.7 Проверка механизма идентификации программ, томов, каталогов, файлов, записей, полей записей

2.7.1 Была осуществлена идентификация программ путем их запуска. При запуске программ наблюдалось их соответствие заданным параметрам. Файлы программного обеспечения расположены в каталоге { C:\Programs Files\ } и { C:\Programs Files\ Microsoft Office\ }.

2.7.2 Была осуществлена идентификация каталогов, в которых должны быть размещены защищаемые файлы (файлы, содержащие закрытую информацию). Идентификация каталогов осуществлялась путем доступа (обращения) к ним штатными средствами операционной системы (при помощи программы «Проводник»). Проверка показала правильность идентификации каталогов.

2.7.3 В связи с тем, что в АС отсутствуют системы управления базами данных (СУБД), проверка механизма идентификации записей и полей записей аттестационной комиссией не проводилась.

Выводы: Реализованный в АС механизм идентификации программ, каталогов и файлов соответствует требованиям руководящих документов к заявленному классу защищенности АС – 2А.

2.8 Проверка механизма контроля доступа

2.8.1 Был проанализирован механизм контроля доступа системы защиты АС. Выяснено, что установленная в АС операционная система Windows 2000 Professional, позволяет разграничивать полномочия по доступу субъектов доступа к объектам доступа; все пользователи АС имеют одинаковый доступ к ресурсам АС: каталогам, файлам, портам, устройствам чтения (дисковод 3,5", привод CD-ROM, устройства flash-memory) и записи (дисковод 3,5", устройства flash-memory). В дополнении к штатным средствам разграничения прав доступа, разграничение прав доступа пользователей к ресурсам АС осуществляется посредством СЗИ от НСД «Secret Net 2000» версия 4.0.

СЗИ от НСД позволяет установить всем пользователям, кроме администратора, следующие полномочия на доступ к каталогам, файлам, устройствам чтения/записи на отчуждаемые машинные носители информации:

- разрешено чтение (выполнение),
- полный доступ (чтение, запись, удаление, выполнение),
- доступ запрещен.

Полномочия администратору – всегда "полный доступ".

Для пользователей разрешен доступ к портам LPT1, USB в соответствии с «Матрицей доступа...».

Права доступа к программам, кроме программ администрирования СЗИ Secret Net 2000 версия 4.0, одинаковы для всех пользователей. Запуск любых программ, кроме используемых в работе с документами, запрещен. Более подробно, правила разграниченного доступа (ПРД) описаны в «Протоколе настройки СЗИ...». Настройка механизма контроля доступа (настройка прав доступа) субъектов доступа к объектам доступа осуществляется Администратором АС с помощью специального программного обеспечения СЗИ от НСД. Данное специальное программное обеспечение доступно для запуска только Администратору АС.

2.8.2 Путем использования Анализатора уязвимостей средств защиты СВТ от НСД "НКВД" (версия 2.2 и версия 2.3, голограммы №Б _____ и №Б _____, сертификаты Гостехкомиссии № 432 и № 429 действительны до 22.02.2007 г.) была осуществлена проверка соответствия полномочий пользователей АС, настроенных атрибутов доступа на каждый защищаемый каталог, порт, привод CD-ROM и НЖМД 3,5" для всех пользователей, зарегистрированных в системе. Протоколы "НКВД" прилагаются на дискете (см Приложение 1).

2.8.3 Аналогично была осуществлена проверка полномочий доступа пользователей (установленных атрибутов доступа к каталогам) к программам. Аттестационной комиссией были признаны обоснованными и достаточными установленные атрибуты доступа к каталогам, в которых размещены файлы с программным обеспечением.

Путем запуска программного обеспечения проверена корректная работа системного и прикладного программного обеспечения.

2.8.4 Аналогично была осуществлена проверка полномочий доступа пользователей (установленных атрибутов доступа) к логическим дискам и каталогам, в которых размещены защищаемые файлы, портам, устройствам чтения/записи данных на отчуждаемые машинные носители информации (дисковод 3,5", привод CD-ROM, устройства flash-памяти). Аттестационной комиссией были признаны обоснованными и достаточными установленные атрибуты доступа к вышеуказанным ресурсам АС.

Выводы: Реализованный в АС механизм контроля доступа соответствует требованиям руководящих документов к заявленному классу защищенности АС – 2А.

2.9 Проверка механизмов управления потоками информации

2.9.1 Экспертным методом членами аттестационной комиссии было проверено соответствие присвоенных меток конфиденциальности объектам доступа (логические диски, каталоги, файлы, порты, дисковод), грифов секретности машинных носителей информации (НЖМД, дискеты 3,5", диски CD-ROM, устройства flash-памяти) и грифа секретности данных, хранимых и/или обрабатываемых и/или передаваемых данные (информацию) через объекты доступа.

Аналогично было проверено соответствие меток конфиденциальности, присвоенных пользователям и Администратору АС, с их полномочиями, необходимыми для выполнения ими технологического процесса.

2.9.2 Функционирование средств управления потоками информации было проверено путем моделирования информационных потоков в реальных условиях технологического процесса. Выполненные во время проверки действия приведены в Таблице 5.

Таблица 5 – Действия по проверке механизма управления потоками информации

№ п.п.	Действия по проверке	Результат проверки	Вывод по проверке
1.	Копирование файла (вложенного каталога) из каталога с установленной меткой конфиденциальности «конфиденциально» в каталог, метка конфиденциальности которому не присваивалась	Осуществить копирование файла (вложенного каталога) не удалось. Система выдала сообщение о не возможности скопировать файл.	соответствует требованиям
2.	Копирование файла (вложенного каталога) из каталога с установленной меткой конфиденциальности «конфиденциально» в каталог с установленной меткой конфиденциальности «конфиденциально»	Копирование осуществлено успешно без ошибок. Метка конфиденциальности не изменилась.	соответствует требованиям
3.	Копирование файла (вложенного каталога) из каталога, метка конфиденциальности которому не присваивалась в каталог, с установленной меткой конфиденциальности «конфиденциально»	Копирование осуществлено успешно без ошибок. Скопированному файлу (каталогу) система автоматически присвоила метку конфиденциальности «конфиденциально»	соответствует требованиям
4.	Копирование файла (вложенного каталога) из каталога в каталог, метка конфиденциальности которым не присваивалась	Копирование осуществлено успешно без ошибок. Скопированному файлу (каталогу) метка конфиденциальности не присваивалась.	соответствует требованиям
5.	Перенос через буфер обмена фрагмента текста из файла с установленной меткой конфиденциальности «конфиденциально» в файл, метка конфиденциальности которому не присваивалась	Осуществить перенос текста через буфер обмена не удалось. Текст в документ не скопировался.	соответствует требованиям
6.	Перенос через буфер обмена фрагмента текста из файла с установленной меткой конфиденциальности «конфиденциально» в файл с установленной меткой конфиденциальности «конфиденциально»	Перенос текста из одного файла в другой осуществлен успешно без ошибок. Метка конфиденциальности файлов не изменилась.	соответствует требованиям
7.	Перенос через буфер обмена фрагмента текста из файла, метка конфиденциальности которому не присваивалась, в файл с установленной меткой конфиденциальности «конфиденциально»	Перенос текста из одного файла в другой осуществлен успешно без ошибок.	соответствует требованиям
8.	Перенос через буфер обмена фрагмента текста из файла в файл, метка конфиденциальности которым не присваивалась	Перенос текста из одного файла в другой осуществлен успешно без ошибок	соответствует требованиям

Выводы: Реализованный в АС механизм управления потоками информации соответствует требованиям руководящих документов к заявленному классу защищенности АС – 2А.

2.10 Проверка механизма регистрации и учета

2.10.1 Был проанализирован механизм регистрации и учета событий в АС.

В настройках СЗИ Secret Net 2000 версия 4.0 предусмотрена регистрация событий.

Все виды регистрации событий для всех пользователей включены и перечислены в таблице 6:

Таблица 6 – Действия по проверке механизма управления потоками информации

Регистрация событий Windows		
Событие:	Успех	Отказ
Вход и выход	+	+
Доступ к файлам и объектам	+	+
Применение прав пользователей	+	+
Управление пользователями и группами	+	+
Изменение политики безопасности	+	+
Перезагрузка, выключение и системные события	+	+
Регистрация событий Secret Net		
События входа: Начало работы пользователя	+	
События входа: Завершение работы пользователя	+	
События входа: Запуск хранителя экрана	+	
События входа: Завершение хранителя экрана	+	
События входа: Компьютер заблокирован	+	
События входа: Компьютер разблокирован	+	
События входа: Компьютер разблокирован администратором	+	
События расширенной регистрации: Запуск программы	+	
События расширенной регистрации: Завершение контроля целостности	+	
События расширенной регистрации: Контроль целостности выполнен с исправлениями	+	
События расширенной регистрации: Ошибка при контроле целостности данных	+	
События расширенной регистрации: Удалено задание на контроль целостности	+	
События расширенной регистрации: Восстановлено значение объекта	+	
События расширенной регистрации: Изменен эталон объекта	+	
События расширенной регистрации: Изменены данные для контроля целостности	+	
События расширенной регистрации: Изменение метки конфиденциальности	+	
События расширенной регистрации: Смена пароля пользователя	+	
События расширенной регистрации: Печать конфиденциального документа	+	
События расширенной регистрации: Вывод конфиденциальной информации на внешний носитель	+	
События расширенной регистрации: Изменение конфигурации компьютера	+	

Регистрация событий осуществляется автоматически, в соответствии с заданными правилами. События заносятся в базу данных событий. Настройка механизма регистрации событий доступа осуществляется Администратором АС с помощью штатных средств операционной системы и специального программного обеспечения СЗИ от НСД. Данное специальное программное обеспечение и штатные средства доступны для запуска только Администратору АС.

2.10.2 Система регистрирует и отображает в журнале все удачные входы в АС.

Функция ведения данного журнала не может быть отключена Администратором АС.

Регистрируются следующие события: (журнал содержит поля в базе данных):

- время события,
- имя пользователя (учетная запись),
- событие
- процесс,
- объект.

При проверке осуществлялись попытки входа в АС под различными зарегистрированными учетными записями. Все входы были зарегистрированы системой и отражены в журнале.

Размер журнала – ограничен 7 днями записи информации.

2.10.3 Система регистрирует и отображает в журнале «Попытки несанкционированного входа на ПЭВМ» все особые события, возникающие при входе в АС, в том числе попытки несанкционированного доступа в АС, а также ошибки, возникающие на этапе инициализации системы защиты.

Регистрируются следующие события:

- время события,
- имя пользователя (учетная запись),
- событие
- процесс,
- объект.

Адекватность регистрации событий в журнале «Попытки несанкционированного входа на ПЭВМ» была проверена путем моделирования возможных ситуаций по доступу в АС.

Выполненные во время проверки действия приведены в Таблице 7.

Таблица 7 – Действия по проверке регистрации событий НСД

№ п.п.	Действия по проверке	Результат регистрации события	Вывод по проверке
1.	Ввод не правильного имени пользователя, пароля	Имя пользователя: <i>user1</i> Дата: <i>число и месяц</i> Время: <i>час и минуты</i> Причина прерывания входа: <i>Пароль неверен</i>	соответствует требованиям

Все входы были зарегистрированы системой и отражены в журнале.

2.10.4 Была осуществлена проверка системы регистрации и учета печати документов на бумажный носитель.

Система регистрации и учета осуществляется с помощью организационных мероприятий:

1. Пользователь имеет возможность самостоятельно отправлять документы на принтер; штатными средствами СЗИ от НСД им не запрещен доступ к порту LPT.

2. Печать (вывод документов на принтер) разрешена ответственному за вывод документов из АС сотруднику. Соответствующему пользователю разрешен доступ к порту USB, к которому подключен принтер.

Факт вывода документов на печать, дату выдачи, имя файла, гриф секретности, количество экземпляров документа, количество листов в экземпляре, отметка об уничтожении бракованных листов (если имеются бракованные листы), имя файла, с которого выполнена печать документа, регистрируется сотрудником, ответственным за вывод документов из АС.

На каждом учетном листе проставляется штамп, ручкой вписывается учетный номер документа и порядковый номер листа документа. На последнем листе каждого экземпляра указывается:

- учетный номер,
- дата печати документа,
- количество экземпляров документа и их адресаты,
- фамилия исполнителя и лица, распечатавшего данный документ.

Бракованные листы уничтожаются в порядке, установленном в секретном делопроизводстве (листы пропускаются через бумагорезательную машину, после чего оставшиеся части документа сжигаются).

2.10.5 В связи с отсутствием в АС терминалов, ЭВМ, узлов сети ЭВМ, линий (каналов) связи и внешних устройств ЭВМ проверка регистрации попыток доступа программных средств к данным объектам доступа не производилась.

2.10.6 Регистрация попыток доступа пользователей к программным средствам (их компонентам) и/или программного обеспечения к каталогам и файлам осуществляется штатными средствами и средствами установленной в АС СЗИ от НСД «Secret Net 2000» версия 4.0.

Зарегистрированные события могут быть просмотрены Администратором АС в журнале «Журнал» находящийся как в общих настройках СЗИ Secret Net 2000, так и в настройках каждого пользователя отдельно. В журнале регистрации событий операционной системы Windows 2000 Professional. Журнал настроен одинаково для всех пользователей, в нем регистрируются операции по чтению, записи, удалению, выполнению (только для исполняемых файлов) файлов и каталогов.

В параметрах регистрации указываются:

- имя пользователя,
- дата выполнения операции (число и месяц),
- время выполнения операции (час и минуты),
- объект доступа (имя файла или каталога, с указанием полного пути),
- тип доступа.
- В поле «Тип доступа» отображаются следующие действия над файлами и каталогами:
- запуск программы;
- открытие файла;
- чтение файла;
- переименование файла;
- удаление файла;
- удаление каталога;
- попытка доступа к защищенному объекту;
- попытка переименования защищенного объекта;
- попытка удаления защищенного объекта.

Была проверена работоспособность системы регистрации попыток доступа пользователей к каталогам и файлам путем моделирования работы АС, были выполнены различные действия под разными учетными именами пользователей по запуску программ, чтению и записи файла, переименование и удаление файлов, создание каталога, изменение и удаление каталога, доступ в каталог. Система регистрирует все события.

2.10.7 Была проверена регистрация изменений полномочий пользователей и статуса объектов доступа. Изменить полномочия в АС возможно только под учетной записью Администратора АС (*Администратор*). Действия Администратора АС регистрируются, результат заносится в журнал. В параметрах регистрации указываются:

- дата и время,
- учетная запись,
- учетная запись пользователя, изменение прав которого было произведено,
- выполненная операция.

2.10.8 Был проверен механизм наследования прав доступа на вновь создаваемые файлы в защищаемом каталоге { C:\Документы\Секретно }. Для этого в вышеуказанных каталогах создавались файлы и вложенные каталоги, после чего штатными средствами подсистемы управления доступом проверялись права доступа пользователей к данным созданным файлам и каталогам. Все вновь созданные файлы и вложенные каталоги имели права доступа идентичные «родительским» каталогам.

Выводы: Реализованный в АС механизм регистрации и учета событий соответствуют требованиям руководящих документов к заявленному классу защищенности АС – 2А.

2.11 Проверка системы регистрации и учета вывода файлов на отчуждаемые носители информации и учета носителей информации

2.11.1 Была осуществлена проверка системы регистрации и учета вывода файлов на диски. Регистрация и учет осуществляется с помощью организационных мероприятий:

- Пользователи не имеют возможность самостоятельно выводить документы на дискету, данное ограничение обеспечивается штатными средствами СЗИ от НСД;
- Копирование файлов на дискеты разрешено только ответственному за вывод документов из АС (Администратору безопасности). Пользователю *Администратор* разрешен доступ к НПМД, устройству flash-памяти с правами "полный доступ" к дисководу.
- В случае необходимости записать файл на дискету пользователь уведомляет о необходимости записать файл на дискету сотрудника, ответственного за вывод документов из АС.
- Сотрудник, ответственный за вывод документов из АС производит запись необходимых файлов на учетные дискеты. После окончания записи файла на дискету, при необходимости, данный файл удаляется в установленном порядке штатными средствами СЗИ от НСД.

Метка конфиденциальности, присвоенная дискете, на которую производится запись файла, соответствует грифу секретности (присвоенной метке конфиденциальности) файла.

Хранение на дискете файлов с разными метками конфиденциальности не допускается. Редактирование содержимого и/или изменение имени файла на дискете *запрещено*.

Дата копирования файла на дискету, имя файла, его размер и операция над файлом (запись, удаление и замена существующего) регистрируется в «Журнале учета машинных носителей информации...». В параметрах регистрации указывается:

- дата копирования (число, месяц и год),
- имя файла с указанием каталога (пути),
- гриф секретности,
- размер файла (определяется по данным операционной системы),
- фамилия исполнителя файла,
- операция над файлом (запись нового, удаление и замена существующего файла).

2.11.2 Была проверена разработанная в АС система учета машинных носителей информации. Машинные носители информации (накопитель на жестких магнитных дисках – «винчестер», диски CD-ROM, дискеты, устройства flash-памяти) учитываются в установленном порядке (см. журнал «Журнал учета машинных носителей...»).

Учетные в журнале носители информации маркируются. На носителе информации указывается:

- гриф секретности носителя,
- учетный номер (по журналу),

- наименование организации.

2.11.3 В нерабочее время машинные носители информации хранятся в отделе по защите информации и мобилизационной работы организации. Выдача носителей производится в установленном порядке, факты выдачи пользователям регистрируются в карточке «Учета выдачи носителя...».

В журнале регистрируются следующие параметры:

- вид машинного носителя,
- условное наименование записанной информации,
- заводской номер носителя,
- место хранения,
- ответственный за хранение,
- отметка об уничтожении (по факту уничтожения носителя).

Решение о выводе носителя из эксплуатации принимается начальником отдела защиты информации. Вывод из эксплуатации осуществляется следующим порядком:

1. Администратор АС в присутствии сотрудника отдела по защите информации и мобилизационной работы производит форматирование накопителя (для НЖМД или дискеты) – только при работоспособности накопителя.
2. Несколько ударами тяжелым предметом производится механическое повреждение носителя. Оставшиеся части носителя сжигаются в установленном порядке в отделе по защите информации и мобилизационной работы.
3. По факту уничтожения носителя составляется соответствующий акт и делается отметка в журнале.

В целях гарантированной сохранности файлов на дискете информация одновременно копируется на две дискеты. «Карточка учета ...» заполняется одна на две дискеты. Любые операции на одной дискете дублируются на другой. В случае выхода одной дискеты из строя данные с другой дискеты копируются на две новые дискеты (учтенные в установленном порядке), а дискета выводится из эксплуатации в установленном порядке.

2.11.4 Был проверен порядок ведения учета машинных носителей. Дискеты и НЖМД, участвующие в работе АС зарегистрированы и учтены в журнале, пользователи ознакомлены и выполняют требования инструкций в части работы с машинными носителями.

Выводы: Реализованная в АС система регистрации и учета вывода файлов на отчуждаемые носители информации и учета носителей информации соответствуют требованиям руководящих документов к заявленному классу защищенности АС – 2А.

2.12.1 Очистке подлежат следующие устройства памяти:

- микросхемы оперативной памяти (ОЗУ),
- файл подкачки операционной системы (создается на НЖМД),
- временные файлы, создаваемые системным и прикладным программным обеспечением,

2.12.2 Данные, хранящиеся в микросхемах ОЗУ (в т.ч. буфере обмена принтера), после выключения питания (перезагрузки) системного блока и/или принтера уничтожаются.

Файл подкачки создается операционной системой во время работы программного обеспечения. Уничтожение файла подкачки производится с помощью штатных средств СЗИ от НСД «Secret Net 2000» версия 4.0 при выключении питания (перезагрузке) системного блока в нормальном режиме или перед загрузкой операционной системы при аварийном завершении работы.

2.12.3 Очистка данных, удаляемых с НЖМД, производится с помощью штатного средства гарантированного уничтожения, входящего в СЗИ от НСД «Secret Net 2000» версия 4.0. Проверка работоспособности механизма гарантированного уничтожения была осуществлена путем использования "Программы поиска и гарантированного уничтожения информации на дисках Tertier" (версия 2.0, голограмма № _____, сертификат Гостехкомиссии №710, действителен до 14.01.2006 г.). С этой целью на диске в каталоге C:\Test был создан файл test.txt, в который была записана строка «_____» в качестве шаблона для поиска. После чего была запущена программа Tertier для определения адреса искомой строки на жестком диске. Искомая строка была найдена в единственном экземпляре, что отражено в протоколе (a:\report\tertier\found.txt – прилагается на дискете). Далее файл test.txt был удален штатными средствами (shift-del), и снова запущена программа Tertier. Искомая строка не была обнаружена по известному адресу, что говорит о гарантированном затирании данных. Из протокола (a:\report\tertier\found_in_report.txt – прилагается на дискете) видно, что искомая строка обнаружена по другому адресу, что объясняется ее наличием в предыдущем протоколе (found.txt). Гарантированная очистка осуществляется путем записи в секторы НЖМД, в которых размещались удаленные данные, последовательности "0". Не смотря на это понижение грифа секретности НЖМД организационно-распорядительными документами, принятыми в АС, запрещается.

2.12.4 Очистка накопителя на гибких магнитных дисках (дискеты 3,5") осуществляется путем двукратного его форматирования с ключом /u. При этом понижение грифа секретности накопителя (использование для хранения файлов, содержащих не секретную информацию и/или служебную информацию) организационно - распорядительными документами, принятыми в АС, запрещается.

Выводы: Реализованная в АС система очистки памяти и внешних накопителей информации соответствуют требованиям руководящих документов к заявленному классу защищенности АС – 2А.

2.13 Проверка механизма сигнализации попыток нарушения защиты

2.13.1 В связи с тем, что рассматриваемая АС создана на базе автономной ПЗВМ, система защиты информации АС не предусматривает специального механизма сигнализации попыток нарушения защиты (например, вывод сообщения о факте НСД в режиме реального времени на рабочее место Администратора АС). Все сигнальные сообщения получает текущий пользователь.

2.13.2 В качестве альтернативы механизму сигнализации попыток нарушения защиты, можно принять регистрацию событий НСД, которые отражаются в журнале и еженедельно анализируются Администратором АС.

Выводы: Реализованный в АС механизм сигнализации попыток нарушения защиты соответствуют требованиям руководящих документов к заявленному классу защищенности АС – 2А.

2.14 Проверка механизма обеспечения целостности программных средств

2.14.1 Механизм обеспечения целостности реализуется с помощью подсистемы целостности файлов и модуля контроля целостности запускаемых задач СЗИ от НСД «Secret Net 2000» версия 4.0.

2.14.2 Подсистема целостности файлов обеспечивает автоматический контроль изменения или удаления файлов системы защиты. Контроль целостности файлов обеспечивается во время загрузки операционной системы.

Для контроля целостности файлов используется механизм подсчета контрольных сумм. С каждым файлом сопоставляется некоторое число, позволяющее анализировать целостность файла. При этом анализируются следующие изменения:

- удаление файлов,
- изменение длины файлов,
- изменение начала и конца файла (секторов файла на НЖМД),

Таблица 8 – Перечень каталогов и файлов, целостность которых контролируется в АС

№ п.п.	Контролируемые каталоги	Контролируемые файлы	Примечание
1.	C:\Program files\infosec	*.exe, *.dll	проверке подлежат файлы, размещенные в контролируемом каталоге и во вложенных в него каталогах

Изменение целостности контролируемых файлов регистрируется системой и отображается в «Журнале». В параметрах регистрации указывается:

- объект контроля, целостность которого была изменена (каталог и файл),
- время контроля (дата и время),
- событие

2.14.3 Модуль контроля целостности запускаемых задач обеспечивает контроль целостности запускаемой программы или исполняемого модуля в момент запуска. Проверка осуществляется СЗИ от НСД автоматически на основе предварительно просчитанной контрольной суммы файла. В случае выявления изменения файла запуск блокируется и производится запись в «Журнал». Восстановить возможность запуска возможно путем восстановления исходного файла или пересчитать его контрольную сумму.

Управление модулем контроля целостности запускаемых задач осуществляет только Администратор АС. В случае необходимости установки в АС дополнительного программного обеспечения Администратор АС устанавливает (инсталлирует) программные файлы, вносит данные программные файлы в список "защищаемых файлов", целостность которых проверяется в дальнейшем.

Таблица 9 – Перечень каталогов, в которых размещены исполняемые файлы, подлежащие контролю целостности

№ п.п.	Контролируемые каталоги	Контролируемые файлы	Примечание
1.	C:\Program Files\Microsoft Office	*.com, *.exe, *.dll, *.vxd, *.sys	проверке подлежат файлы, размещенные в контролируемом каталоге и во вложенных в него каталогах
2.	C:\WINNT\		

Для осуществления возможности периодического контроля целостности программной среды в дальнейшем было произведено контрольное суммирование всех папок и файлов жесткого диска (состоящего из логического диска C:) с помощью "Программы контроля состояния сертифицированных программных средств защиты информации ФИКС" версии 2.0.1 (годограмма № А _____, сертификат Гостехкомиссии № 913, действителен до 27.05.2007 г.) и выпущены соответствующие протоколы. По причине большого объема данные протоколы прилагаются в виде файлов на дискете (см. Приложение 1).

2.14.4 В АС отсутствуют средства разработки программного обеспечения, модификации объектного кода программ, а также других средств с помощью которых возможно изменение кода программ с целью изменения их алгоритма работы. Предусмотренные в пакете Microsoft Office 2000 Professional (Word 2000 Professional и Excel 2000 Professional) средства разработки макрокоманд ("макросов") и редактор Visual Basic в АС не установлены (не инсталлированы). Пользователь не имеет возможности их самостоятельной установки.

Выводы: Реализованные в АС меры обеспечения целостности программных средств соответствуют требованиям руководящих документов к заявленному классу защищенности АС – 2А.

2.15 Проверка системы физической охраны ОТСС и носителей информации

2.15.1 ОТСС размещены в специально выделенном помещении отдела по защите информации и мобилизационной работы организации. Помещение (комната), в которой установлены ОТСС, предназначено для работы с документами с грифом "секретно" и "Для служебного пользования". После окончания работы (в нерабочее время) машинные носители информации и документы, содержащие секретные сведения, сдаются пользователями в отдел по защите информации и мобилизационной работы.

2.15.2 Доступ лиц в помещение ограничен, в помещении (в соответствии с утвержденным списком) могут находиться только допущенные сотрудники, форма допуска допущенных в помещение лиц – третья.

2.15.3 Пропускной режим на территорию предприятия регламентируется инструкцией о пропускном режиме. Требования инструкции соответствуют реальным условиям функционирования объекта. Порядок сдачи помещения объекта под охрану и снятия с охраны отражен в специальной инструкции. Ее требования обоснованы для конкретных условий и выполняются пользователями.

Выводы: Реализованная на объекте система физической Охраны ОТСС и носителей информации соответствует требованиям и может быть признана удовлетворительной для объектов вычислительной техники третьей категории и АС класса 2А.

2.16 Проверка наличия в АС администратора

2.16.1 В аттестуемой АС присутствует Администратор АС, действующий на основании приказа генерального директора и инструкции.

2.16.2 Администратор АС знает организационно-распорядительную документацию на объект информатизации, имеет опыт и навыки настройки (администрирования) системного и прикладного программного обеспечения, программной и аппаратной части СЗИ от НСД «Secret Net 2000» версия 4.0.

Выводы: Знания и навыки Администратора АС соответствуют требованиям руководящих документов, он в состоянии проводить работы по настройке системы защиты информации и контролю выполнения организационно-распорядительных документов на объекте вычислительной техники третьей категории и АС класса 2А.

2.17 Проверка механизма периодического тестирования и восстановления средств и систем защиты информации от НСД

2.17.1 Проверялось наличие организационно-распорядительной документации, предписывающей периодичность и порядок тестирования всех функций СЗИ от НСД. Осуществлялась проверка возможности периодического тестирования СЗИ путем анализа применяемых разработчиком средств контроля целостности компонентов системного программного обеспечения, реализующих функции СЗИ от НСД и наборов данных, используемых этими средствами.

2.17.2 Периодичность проведения тестирования – не реже одного раза в год.

2.17.3 Средствами восстановления СЗИ от НСД в АС являются дистрибутивы (инсталляционные файлы) с системным и прикладным программным обеспечением. Копии дистрибутивов хранятся на дисках CD-R отдельно для обеспечения возможной полной замены (переустановки) программного обеспечения в случае каких-либо отказов (сбоев) или нарушений в работе технических средств АС.

Выводы: В АС периодичность и порядок тестирования, средства восстановления СЗИ от НСД удовлетворяют требованиям руководящих документов к заявленному классу защищенности АС – 2А.

2.18 Проверка сертификатов соответствия на применяемые средства и системы защиты информации от НСД

2.18.1 В АС установлена сертифицированная система защиты информации от несанкционированного доступа Secret Net 2000 версия 4.0 (автономный вариант) (Сертификат Гостехкомиссии России № 640 от 27.06.2002 г., действительно до 27.06.2005 г.).

Данный сертификат удостоверяет, что система защиты информации от НСД «Secret Net 2000» версия 4.0, разработанная и производимая ЗАО Научно-инженерное предприятие «ИНФОРМЗАЩИТА» (г. Москва) функционирующая под управлением ОС Windows NT 4.0 SP3-SP6, Windows 2000, является программно-аппаратным средством защиты от несанкционированного доступа к информации и соответствует требованиям руководящих документов Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации по 3 классу защищенности при условии соблюдения ограничений, приведенных в приложении к настоящему сертификату, «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей» по 3 уровню контроля.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ООО «Центр безопасности информации» (аттестат аккредитации испытательной лаборатории от 23.05.97 № СЗИ RU.117.608.025) – техническое заключение от 20.06.2002г., и экспертное заключение Гостехкомиссии России от 26.06.2002г.

2.18.2 Аттестационной комиссии была предоставлена копия сертификата, подтвержденная голографической наклейкой (А 13987). Сертификат действующий – срок его окончания 27.06.2005 г.

Выводы: Установленная в АС система защиты информации от несанкционированного доступа «Secret Net 2000» версия 4.0 имеет сертификат Гостехкомиссии России, которым подтверждаются требования руководящих документов к заявленному классу защищенности АС – 2А. При установке выполнены дополнительные требования к порядку эксплуатации АС, приведенные в технических условиях на СЗИ от НСД.

2.19 Проверка АС на отсутствие компьютерных вирусов

2.19.1 Была проведена проверка программного обеспечения на отсутствие компьютерных вирусов. Проверка была выполнена с помощью антивирусного программного обеспечения Dr Web 4.23b. По результатам проверки компьютерных вирусов не обнаружено.

2.19.2 Был проанализирован предполагаемый порядок проверки АС на отсутствие компьютерных вирусов. Проверка осуществляется:

- постоянно в режиме "монитор" (программа запускается в памяти АС при загрузке операционной системы) при работе пользователей и Администратора АС;
- периодически в режиме "сканер" (программа запускается пользователем) по мере необходимости, при обнаружении в режиме "монитор" компьютерных вирусов (подозрения на вирусы);
- при проведении Администратором АС ежемесячных регламентных проверок и обновлению антивирусных баз данных.

Выводы: Принятые в АС меры по защите информации от компьютерных вирусов являются обоснованными и могут быть признаны достаточными для заявленного класса защищенности АС – 2А.

Результаты аттестационных испытаний представлены в виде протоколов программ Фикс 3.0, НКВД 2.2, 2.3, Terrier 2.0 и прилагаются к данному протоколу на дискете в самораспаковывающемся rar-архиве. (см. Приложение 1).

1. Дискета с файлом report.exe, report.r00. Уч. №№ 19дсп, 20дсп.

ВЫВОДЫ АТТЕСТАЦИОННОЙ КОМИССИИ

По результатам аттестационных испытаний комиссия считает, что автоматизированная система объекта информатизации на базе автономной персональной ЭВМ (№ 026091-001) отвечает требованиям руководящих документов к заявленному классу защищенности АС – 2А.

Члены комиссии:

ПЕРЕЧЕНЬ ОРГАНИЗАЦИОННО - РАСПОРЯДИТЕЛЬНЫХ И НОРМАТИВНЫХ ДОКУМЕНТОВ, НА которые имеются ссылки

1. Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР). Решение Гостехкомиссии России от 23.5.1997 г., № 55.
2. Инструкция по обеспечению режима секретности в Министерствах, ведомствах, на предприятиях, в учреждениях и организациях СССР, Утверждена Постановлением Совета Министров СССР от 12.05.1987 г. № 556-126.
3. Руководящий документ Гостехкомиссии России. Защита от НСД к информации. Термины и определения.
4. Руководящий документ Гостехкомиссии России. Концепция защиты средств вычислительной техники и автоматизированных систем от НСД к информации.
5. Руководящий документ Гостехкомиссии России. Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации.
6. Руководящий документ Гостехкомиссии России. Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности информации.
7. Руководящий документ Гостехкомиссии России. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники.
8. Руководящий документ Гостехкомиссии России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей. Приказ Председателя Гостехкомиссии России от 4.6.1999 г., № 114.

№ ____ дсп

Экз. № 1 на 26 л.

Исп. и отп. б/ч

11.11.2004 г.

Задание обучаемым для самостоятельной учебной работы при подготовке к занятию:

13. Закрепить и углубить знания, полученные на лекции, для этого изучить конспект лекций и рекомендуемую литературу:
 - [1] Технические средства и методы защиты информации. Учебное пособие для вузов / Под ред. А.П. Зайцева и А.А. Шелупанова. – М.: Горячая линия-Телеком, 2013..
14. Изучить методические указания к ПЗ № 8-9.

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1

**Лабораторная работа разработана
доцентом кафедры ОТЗИ Сагдеевым К.М.**

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для обучающихся по организации и проведению самостоятельной работы
по дисциплине «Техническая защита информации»

для студентов направления подготовки
10.03.01 «Информационная безопасность»

Направленность (профиль):
«Организация и технологии защиты информации (по отрасли или в сфере профессиональной
деятельности)»

Ставрополь
2026

СОДЕРЖАНИЕ

Введение	157
1. Общая характеристика самостоятельной работы студента	161
2. Технологическая карта самостоятельной работы студента	162
3. Самостоятельное изучение тем лекций	163
4. Паспорт фонда оценочных средств для проверки самостоятельной работы.....	163
5. Список рекомендуемой литературы.....	178

Введение

1. Цель и задачи освоения дисциплины (модуля)

«Техническая защита информации» является формированием набора общекультурных и профессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность». Формируемые в рамках дисциплины компетенции способствуют решению профессиональных задач по защите информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях, а также приобретение набора общекультурных и общепрофессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ОПК-4 Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности;	ИД-3ОПК-4 Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	в совершенстве анализирует физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности
ОПК-11 Способен проводить эксперименты по заданной методике и обработку их результатов;	ИД-1ОПК-11 Показывает понимание сущности проведения экспериментов по заданной методике и обработку их результатов	-формулирует сущность проведения экспериментов по заданной методике и обработку их результатов; -выделяет целесообразные методики для проведения экспериментов; -демонстрирует уверенное использование процедур обработки результатов проведенных экспериментов
	ИД-2ОПК-11 Демонстрирует способность к реализации проведения экспериментов по заданной методике и обработку их результатов	-демонстрирует способность и проведения экспериментов по заданной методике и обработку их результатов; -уверенно выбирает заданные методики

		проведения экспериментов; -применяет методы обработки результатов экспериментов
ОПК-2.1 Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба;	ИД-1ОПК-2.1 Показывает понимание сущности анализа функционального процесса объекта защиты и его информационных составляющих	-демонстрирует понимание сущности анализа функционального процесса объекта защиты и его информационных составляющих; -формулирует сущность анализа функционального процесса объекта защиты и его информационных составляющих; -оперирует понятиями процесса анализа функционального процесса объекта защиты и его информационных составляющих
	ИД-2ОПК-2.1 Выявляет возможные источники информационных угроз, их возможные цели, пути реализации и предполагаемый ущерб	-выделяет возможные источники информационных угроз, их возможные цели, пути реализации и предполагаемый ущерб; -анализирует возможные источники информационных угроз, их возможные цели, пути реализации и предполагаемый ущерб; -оперирует понятиями возможных источников информационных угроз, их возможными целями, путями реализации;

1. Общая характеристика самостоятельной работы студента

Основными видами учебной работы по достижению результатов освоения дисциплины являются лекции, лабораторные и практические работы и самостоятельная работа студентов (СРС).

На лекциях раскрываются основные положения и понятия курса, формируются знания в области технической защиты информации. На лабораторных и практических работах формируются умения и навыки, необходимые для решения задач профессиональной деятельности.

Приступая к изучению учебной дисциплины, необходимо ознакомиться с учебной программой, получить в библиотеке рекомендованные учебные пособия, а также получить у ведущего преподавателя в электронном виде конспекты лекций, методические рекомендации к лабораторным и практическим работам и тестовые, завести новую тетрадь для конспектирования лекций и выполнения лабораторных и практических работ.

Для изучения дисциплины предлагается список основной и дополнительной литературы. Основная литература предназначена для обязательного изучения, дополнительная – поможет более глубоко освоить отдельные вопросы, подготовить исследовательские задания и выполнить задания для самостоятельной работы.

В ходе лекционных занятий студент обязан осуществлять конспектирование учебного материала, особое внимание, обращая на категории, формулировки, раскрывающие содержание тех или иных понятий, физических явлений, процессов, эффектов. В рабочих конспектах желательно оставлять поля, на которых следует делать пометки из рекомендованной литературы, дополнять материал прослушанной лекции, формулировать научные выводы и практические рекомендации. Студент имеет право задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Самостоятельная работа студентов над материалом учебной дисциплины является неотъемлемой частью учебного процесса и должна предполагать углубление знания учебного материала, излагаемого на аудиторных занятиях, и приобретение дополнительных знаний по отдельным вопросам самостоятельно.

Основными видами самостоятельной работы курсантов по учебной дисциплине являются:

- самостоятельное изучение учебного материала по заданным темам;
- подготовка к лабораторным работам, оформление отчета по выполненному лабораторному и практическому занятию и подготовка к собеседованию по результатам работы.

Основными методами самостоятельной работы студентов являются:

- 1) для овладения знаниями:
 - чтение текста (конспекта лекций, учебника, дополнительной литературы) и конспектирование текста;
 - работа с нормативными документами;
 - поиск информации в Интернет;
- 2) для закрепления и систематизации знаний:
 - работа с конспектом лекции (обработка текста);
 - повторная работа над учебным материалом (учебника, дополнительной литературы, слайдами);
 - составление плана и тезисов ответа или графическое изображение структуры ответа;
 - составление таблиц для систематизации учебного материала;
 - изучение нормативных документов;

- ответы на контрольные вопросы;
- 3) для формирования умений:
 - подготовка к лабораторным и практическим занятиям;
 - решение задач и практических заданий;
 - подготовка отчетов по лабораторным и практическим занятиям;
 - рефлексивный анализ профессиональных умений.

В случае пропуска учебного занятия студент может воспользоваться содержанием различных блоков учебно-методического комплекса (лекции, лабораторные и практические занятия, контрольные вопросы и тесты) для самоподготовки и освоения темы. Для самоконтроля необходимо использовать вопросы и задания, предлагаемые к лабораторным и практическим занятиям, а также варианты тестовых заданий.

2. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций, индикатора(ов)	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе		
			СРС	Контактная работа с преподавателем	Всего
5 семестр					
ОПК-4 ИД-3 ОПК-11 ИД-1 ОПК-11 ИД-2 ОПК-2.1 ИД-1 ОПК-2.1 ИД-2	Подготовка к лабораторной работе	Собеседование	1.00	2.00	3.00
ОПК-4 ИД-3 ОПК-11 ИД-1 ОПК-11 ИД-2 ОПК-2.1 ИД-1 ОПК-2.1 ИД-2	Подготовка к лекции	Конспект	1.00	2.00	3.00
ОПК-4 ИД-3 ОПК-11 ИД-1 ОПК-11 ИД-2 ОПК-2.1 ИД-1 ОПК-2.1 ИД-2	Подготовка доклада	Доклад	1.00	2.00	3.00
ОПК-4 ИД-3 ОПК-11 ИД-1 ОПК-11 ИД-2 ОПК-2.1 ИД-1 ОПК-2.1 ИД-2	Самостоятельное изучение литературы	Конспект	1.00	2.00	3.00
ОПК-4 ИД-3 ОПК-11 ИД-1 ОПК-11 ИД-2 ОПК-2.1 ИД-1 ОПК-2.1 ИД-2	Самостоятельное выполнение заданий по заданным темам.	Конспект. Письменный отчет	1.00	2.00	3.00

ОПК-4 ИД-3 ОПК-11 ИД-1 ОПК-11 ИД-2 ОПК-2.1 ИД-1 ОПК-2.1 ИД-2	Подготовка к практическому занятию	Собеседование	1.00	2.00	3.00
Итого за 5 семестр			6.00	12.00	18.00
Итого			6.00	12.00	18.00

1. Порядок выполнения самостоятельной работы

3.1 Методические рекомендации по изучению теоретического материала

Комплексное изучение предлагаемой студентам учебной дисциплины «Техническая защита информации» предполагает овладение материалами лекций, учебников, программы, творческую работу студентов в ходе проведения практических занятий, а также систематическое выполнение заданий для самостоятельной работы.

В ходе лекций раскрываются основные вопросы в рамках рассматриваемых тем, делаются акценты на наиболее сложные и интересные положения изучаемого материала, которые должны быть приняты студентами во внимание. Материалы лекций являются основой для подготовки студентов к практическим занятиям.

Работа с конспектом лекций

Просмотрите конспект сразу после занятий. Отметьте материал конспекта лекций, который вызывает затруднения для понимания. Попробуйте найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь на текущей консультации или на ближайшей лекции за помощью к преподавателю.

Каждую неделю отводите время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам и тестам.

Выполнение практических занятий по дисциплине «Техническая защита информации»

На первом занятии получите у преподавателя задания по курсу, планы подготовки к практическим занятиям. Обзаведитесь всем необходимым методическим обеспечением.

Перед практическими занятиями изучите теорию вопроса, предполагаемого к исследованию, ознакомьтесь с опытом других исследователей в этом направлении.

Целью практических занятий является:

- закрепление методов приложения теории к решению практических задач анализа и синтеза психологического знания;
- проверка уровня понимания студентами вопросов, рассмотренных на лекциях и по учебной литературе, степени и качества усвоения материала;
- обучение навыкам освоения методики эксперимента и работы с нормативно-справочной литературой;
- восполнение пробелов в пройденной теоретической части курса и оказание помощи в его усвоении.

3.2 Методические рекомендации по написанию и оформлению доклада

1. Общие положения

1.1. Доклад, как вид самостоятельной работы в учебном процессе, способствует формированию навыков исследовательской работы, расширяет познавательные интересы, учит критически мыслить.

1.2. При написании доклада по заданной теме студент составляет план, подбирает основные источники.

1.3. В процессе работы с источниками систематизирует полученные сведения, делает выводы и обобщения.

1.4. К докладу по крупной теме могут привлекать несколько студентов, между которыми распределяются вопросы выступления.

2. Выбор темы доклада

2.1. Тематика доклада обычно определяется преподавателем, но в определении темы инициативу может проявить и студент.

2.2. Прежде чем выбрать тему доклада, автору необходимо выявить свой интерес, определить, над какой проблемой он хотел бы поработать, более глубоко ее изучить.

3. Этапы работы над докладом

3.1. Формулирование темы, причем она должна быть не только актуальной по своему значению, но и оригинальной, интересной по содержанию.

3.2. Подбор и изучение основных источников по теме (как правильно, при разработке доклада используется не менее 8-10 различных источников).

3.3. Составление списка использованных источников.

3.4. Обработка и систематизация информации

3.5. Разработка плана доклада.

3.6. Написание доклада.

3.7. Публичное выступление с результатами исследования.

4. Структура доклада:

- титульный лист

- оглавление (в нем последовательно излагаются названия пунктов доклада, указываются страницы, с которых начинается каждый пункт);

- введение (формулирует суть исследуемой проблемы, обосновывается выбор темы, определяются ее значимость и актуальность, указываются цель и задачи доклада, дается характеристика используемой литературы);

- основная часть (каждый раздел ее, доказательно раскрывая отдельную проблему или одну из ее сторон, логически является продолжением предыдущего; в основной части могут быть представлены таблицы, графики, схемы);

- заключение (подводятся итоги или дается обобщенный вывод по теме доклада, предлагаются рекомендации);

- список использованных источников

5. Структура и содержание доклада

5.1. Введение - это вступительная часть научно-исследовательской работы. Автор должен приложить все усилия, чтобы в этом небольшом по объему разделе показать актуальность темы, раскрыть практическую значимость ее, определить цели и задачи эксперимента или его фрагмента.

5.2. Основная часть. В ней раскрывается содержание доклада.

Как правило, основная часть состоит из теоретического и практического разделов. В теоретическом разделе раскрываются история и теория исследуемой проблемы, дается критический анализ литературы и показываются позиции автора. В практическом разделе излагаются методы, ход, и результаты самостоятельно проведенного эксперимента или фрагмента.

В основной части могут быть также представлены схемы, диаграммы, таблицы, рисунки и т.д.

5.3. В заключении содержатся итоги работы, выводы, к которым пришел автор, и рекомендации. Заключение должно быть кратким, обязательным и соответствовать поставленным задачам.

5.4. Список использованных источников представляет собой перечень использованных книг, статей, фамилии авторов приводятся в алфавитном порядке, при этом все источники даются под общей нумерацией литературы. В исходных данных источника указываются фамилия и инициалы автора, название работы, место и год издания.

5.5. Приложение к докладу оформляются на отдельных листах, причем каждое должно иметь свой тематический заголовок и номер, который пишется в правом верхнем углу, например: «Приложение 1»

6. Требования к оформлению доклада

6.1. Объем доклада может колебаться в пределах 5-15 печатных страниц; все приложения к работе не входят в ее объем.

6.2. Доклад должен быть выполнен грамотно, с соблюдением культуры изложения.

6.3. Обязательно должны иметься ссылки на используемую литературу.

6.4. Должна быть соблюдена последовательность написания библиографического аппарата.

7. Критерии оценки доклада

- актуальность темы исследования;
- соответствие содержания теме;
- глубина проработки материала; правильность и полнота использования источников;
- соответствие оформления доклада стандартам.

По усмотрению преподавателя доклады могут быть представлены на семинарах, научно-практических конференциях, а также использоваться как зачетные работы по пройденным темам.

3.3 Методические рекомендации по конспектированию первоисточников

Изучение и анализ литературных источников является обязательным видом самостоятельной работы студентов. Изучение литературы по избранной теме имеет своей задачей проследить характер постановки и решения определенной проблемы различными авторами, аргументацию их выводов и обобщений, провести анализ и систематизировать полученный материал на основе собственного осмысления с целью выяснения современного состояния вопроса.

Проработка отобранного материала обязательно должна идти с одновременным ведением записей прочитанного и своих замечаний. Запись может иметь как форму конспекта, так и выписок, а также картотеку положений, тезисов, идей, методик, что в дальнейшем облегчит классификацию и систематизацию полученного материала. Такого рода записи являются лучшим способом накопления и первичной обработки материала, одной из обязательных форм организации умственного труда.

Планом удобно пользоваться при подготовке к устному выступлению по выбранной теме. Каждый пункт плана должен раскрывать одну из сторон избранной темы, а весь план должен охватывать ее целиком.

Тезисы предполагают сжатое изложение основных положений текста в форме утверждения или отрицания. Они являются более совершенной формой записей и представляют основу для дискуссии. К тому же их легко запомнить.

Конспектирование – процесс мысленной переработки и письменной фиксации информации, в виде краткого изложения основного содержания, смысла какого-либо текста.

Результат конспектирования – запись, позволяющая конспектирующему немедленно или через некоторый срок с нужной полнотой восстановить полученную информацию. Конспект в переводе с латыни означает «обзор». По существу его и составлять надо как обзор, содержащий основные мысли текста без подробностей и второстепенных деталей. Конспект носит индивидуализированный характер: он рассчитан на самого автора и поэтому может оказаться малопонятным для других.

Для того чтобы осуществлять этот вид работы, в каждом конкретном случае необходимо грамотно решить следующие задачи:

1. Сориентироваться в общей композиции текста (уметь определить вступление, основную часть, заключение).
2. Увидеть логико-смысловую канву сообщения, понять систему изложения автором информации в целом, а также ход развития каждой отдельной мысли.
3. Выявить «ключевые» мысли, т. е. основные смысловые вехи, на которые «нанизано» все содержание текста.

4. Определить детализирующую информацию.
5. Лаконично сформулировать основную информацию, не перенося на письмо все целиком и дословно.

Во всяком научном тексте содержится информация 2-х видов: основная и вспомогательная. Основной является информация, имеющая наиболее существенное значение для раскрытия содержания темы или вопроса. К ней относятся: определения научных понятий, формулировки законов, теоретических принципов и т. д. Назначение вспомогательной информации – помочь читателю лучше усвоить предлагаемый материал. К этому типу информации относятся разного рода комментарии. Основную – записываем как можно полнее, вспомогательную, как правило, опускаем. Содержание конспектирования составляет переработка основной информации в целях ее обобщения и сокращения. Обобщить – значит представить ее в более общей, схематической форме, в виде тезисов, выводов, отдельных заголовков, изложения основных результатов и т. п. Читая, мы интуитивно используем некоторые слова и фразы в качестве опорных. Такие опорные слова и фразы называются ключевыми. Ключевые слова и фразы несут основную смысловую и эмоциональную нагрузку содержания текста.

Выбор ключевых слов – это первый этап смыслового свертывания, смыслового сжатия материала.

Важными требованиями к конспекту являются наглядность и обозримость записей и такое их расположение, которое давало бы возможность уяснить логические связи и иерархию понятий.

По форме конспекты подразделяются на формализованные и графические.

1. Формализованные (все записи вносятся в заранее подготовленные таблицы).

Это удобно, во-первых, при конспектировании материалов, когда перечень характеристик описываемых предметов или явлений более или менее постоянен, во-вторых, при подготовке единого конспекта по нескольким источникам. Особенно если есть необходимость сравнения отдельных данных. Разновидностью формализованного конспекта является запись, составленная в форме ответов на заранее подготовленные вопросы, обеспечивающие исчерпывающие характеристики однотипных предметов или явлений.

2. Графические (элементы конспектируемой работы располагаются в таком виде, при котором видна иерархия понятий и взаимосвязь между ними).

По каждой работе может быть не один, а несколько графических конспектов, отображающих книгу в целом и отдельные ее части. Ведение графического конспекта – наиболее совершенный способ изображения внутренней структуры книги, а сам этот процесс помогает усвоению ее содержания.

Можно выделить следующие основные **типы конспектов: плановый, текстуальный, сводный, тематический.**

Плановый – легко получить с помощью предварительно сделанного плана произведения, каждому вопросу плана отвечает определенная часть конспекта:

а) вопросно-ответный (на пункты плана, выраженные в вопросительной форме, конспект дает точные ответы);

б) схематичный плановый конспект (отражает логическую структуру и взаимосвязь отдельных положений).

Текстуальный – это конспект, созданный в основном из цитат.

Сводный конспект – сочетает выписки, цитаты, иногда тезисы; часть его текста может быть снабжена планом.

Тематический – дает более или менее исчерпывающий ответ (в зависимости из числа привлеченных источников и другого материала, например, своих же записей) на поставленный вопрос – тему: обзорный; хронологический.

Роль конспекта – чисто учебная: он помогает зафиксировать основные понятия и

положения первичного текста и в нужный момент их воспроизвести, например, при написании реферата или подготовке к экзамену.

Способы конспектирования.

- **Тезисы** – это кратко сформулированные основные мысли, положения изучаемого материала. Тезисы лаконично выражают суть читаемого, дают возможность раскрыть содержание. Приступая к освоению записи в виде тезисов, полезно в самом тексте отмечать места, наиболее четко формулирующие основную мысль, которую автор доказывает (если, конечно, это не библиотечная книга). Часто такой отбор облегчается шрифтовым выделением, сделанным в самом тексте.

- **Линейно-последовательная запись текста.** При конспектировании линейно – последовательным способом целесообразно использование плакатно-оформительских средств, которые включают в себя следующие:

- сдвиг текста конспекта по горизонтали, по вертикали;
- выделение жирным (или другим) шрифтом особо значимых слов;
- использование различных цветов;
- подчеркивание;
- заключение в рамку главной информации.

- **Способ «вопросов – ответов».** Он заключается в том, что, поделив страницу тетради пополам вертикальной чертой, конспектирующий в левой части страницы самостоятельно формулирует вопросы или проблемы, затронутые в данном тексте, а в правой части дает ответы на них.

Одна из модификаций способа «вопросов – ответов» - таблица, где место вопроса занимает формулировка проблемы, поднятой автором (лектором), а место ответа – решение данной проблемы. Иногда в таблице могут появиться и дополнительные графы: например, «мое мнение» и т. п.

- **Схема с фрагментами** – способ конспектирования, позволяющий ярче выявить структуру текста, - при этом фрагменты текста (опорные слова, словосочетания, пояснения всякого рода) в сочетании с графикой помогают созданию рационально - лаконичного конспекта.

- **Простая схема** – способ конспектирования, близкий к схеме с фрагментами, объяснений к которой конспектирующий не пишет, но должен уметь давать их устно. Этот способ требует высокой квалификации конспектирующего. В противном случае такой конспект нельзя будет использовать.

- **Параллельный способ** конспектирования. Конспект оформляется на двух листах параллельно или один лист делится вертикальной чертой пополам и записи делаются в правой и в левой части листа.

Однако лучше использовать разные способы конспектирования для записи одного и того же материала.

Комбинированный конспект – вершина овладения рациональным конспектированием. При этом умело используются все перечисленные способы, сочетая их в одном конспекте (один из видов конспекта свободно перетекает в другой в зависимости от конспектируемого текста, от желания и умения конспектирующего). Именно при комбинированном конспекте более всего проявляется уровень подготовки и индивидуальность студента.

Принципы составления конспекта прочитанного.

1. Записать все выходные данные источника: автор, название, год и место издания. Если текст взят из периодического издания (газеты или журнала), то записать его название, год, месяц, номер, число, место издания.

2. Выделить поля слева или справа, можно с обеих сторон. Слева на полях отмечаются страницы оригинала, структурные разделы статьи или книги (названия параграфов, подзаголовки и т. п.), формулируются основные проблемы. Справа – способы фиксации прочитанной информации.

Один из видов чтения – углубленное – предполагает глубокое усвоение прочитанного и часто сохранение информации в целях последующего обращения к ней. Эффективность такого чтения повышается, если прочитанное зафиксировано не только в памяти, но и на бумаге. Психологи утверждают, что записанное лучше и полнее усваивается, прочнее откладывается в памяти. Установлено, что если прочитать 1000 слов и затем записать 50, подытоживающих прочитанное, то коэффициент усвоения будет выше, чем, если прочитать 10000 слов, не записав ни одного. Кроме того, при записи прочитанного формируется навык свертыwania информации. И, наконец, чередование чтения и записывания уменьшает усталость, повышает работоспособность и производительность умственного труда.

1. Резюмирование.

Резюме – краткий итог прочитанного, содержащий его оценку. Резюме характеризует основные выводы книги, главные итоги.

Выбор языковых средств для построения резюме-выводов подчинен основной задаче свертыwania информации: минимум языковых средств – максимум информации. Это обычно одно – три четких, кратких, выразительных предложения, раскрывающих, по мнению автора, самую суть описываемого объекта.

2. Аннотация.

Аннотация – краткая обобщенная характеристика печатной работы (книги, статьи), включающая иногда и его оценку. Это наикратчайшее изложение содержания первичного документа, дающее общее представление о теме.

Основное ее назначение – дать некоторое представление о книге (статье, научной работе) с тем, чтобы рекомендовать ее определенному кругу читателей или воспользоваться своими записями при выполнении работы исследовательского, реферативного характера. Поэтому аннотации не требуются изложения содержания произведения, в ней лишь перечисляются вопросы, которые освещены в первоисточнике (содержание этих вопросов не раскрывается). Аннотация отвечает на вопрос: «О чем говорится в первичном тексте?», дает представление только о главной теме и перечне вопросов, затрагиваемых в тексте первоисточника.

Текст аннотации не стандартизирован. В научной литературе можно встретить различные требования к составлению аннотаций. Например, текст справочной аннотации может включать следующие сведения:

- тип и название аннотируемого документа (монография, диссертация, сборник, статья и т. п.)
- задачи, поставленные автором аннотируемого документа
- метод, которым пользовался автор (эксперимент, сравнительный анализ, компиляция других источников)
- принадлежность автора к определенной научной школе или направлению
- структуру аннотируемого документа
- предмет и тему произведения, основные положения и выводы автора
- характеристику вспомогательных иллюстративных материалов, дополнений, приложений, справочного аппарата, включая указатели и библиографию.

4.1 Вопросы для проверки уровня обученности

1. Государственная система защиты информации. Основные направления защиты информации.
2. Цели и задачи защиты информации от утечки информации по техническим каналам.
3. Объекты технической защиты информации.
4. Нормативные документы по технической защите информации.
5. Объект информатизации (определение и характеристика).
6. Характеристика основных технических средств и систем (ОТСС).
7. Характеристика вспомогательных технических средств и систем (ВТСС).
8. Структура и состав технического канала утечки информации.
9. Классификация технических каналов утечки информации.
10. Основные показатели технических каналов утечки информации.
11. Концепция технической защиты информации.
12. Общие принципы технической защиты информации.
13. Принципы построения системы защиты информации.
14. Классификация направлений и методов защиты.
15. Характеристика методов скрытия информации.
16. Понятия информации.
17. Свойства информации, как предмета технической защиты.
18. Характеристика информационных технологий как предмет защиты.
19. Характеристика информационных процессов в автоматизированных информационных системах.
20. Структура и схема информационного процесса передачи информации.
21. Виды информации в автоматизированных информационных системах.
22. Машинное представление информации.
23. Физическое представление информации в автоматизированных информационных системах.
24. Виды сообщений в информационно-телекоммуникационных системах.
25. Классификация сигналов.
26. Сравнительная характеристика аналоговых и дискретных сигналов.
27. Временное и спектральное представление сигналов.
28. Принципы записи информации на носители в виде физических полей.
29. Виды модуляции. Характеристика аналоговых видов модуляции.
30. Виды модуляции. Характеристика импульсных видов модуляции (манипуляции).
31. Принципы передачи и считывания информации с носителей в виде физических полей.
32. Особенности современных автоматизированных информационных системах как объектов защиты.

33. Уязвимость основных структурно-функциональных элементов распределенных АИС.
34. Определения угроз безопасности информации АИС и субъектов информационных отношений.
35. Источники угроз безопасности АИС, их классификация.
36. Основные непреднамеренные искусственные угрозы АИС.
37. Основные преднамеренные искусственные угрозы АИС.
38. Доступ к информации, условия разведывательного контакта.
39. Способы и каналы несанкционированного доступа к информации.
40. Опасные случайные сигналы и их источники.
41. Классификация акустоэлектрических преобразователей.
42. Акустоэлектрические преобразователи как источники опасных сигналов.
43. Паразитные связи и наводки как источники опасных сигналов.
44. Низкочастотные и высокочастотные излучения технических средств.
45. Классификация и характеристика видов технической разведки.
46. Классификация и характеристика технических средств разведки.
47. Возможности (показатели) технической разведки и ее средств.
48. Общая характеристика радиоэлектронных технических каналов утечки информации.
49. Классификация радиоэлектронных технических каналов утечки информации.
50. Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений.
51. Структура и характеристика электромагнитного технического канала утечки информации.
52. Характеристика и демаскирующие признаки сигналов ПЭМИ от средств вычислительной техники.
53. Условия возникновения электромагнитного канала утечки информации. Характеристика опасной зоной 2 (R2).
54. Перехват побочных электромагнитных излучений СВТ средствами разведки ПЭМИН.
55. Технические каналы утечки информации, возникающие за счет наводок побочных электромагнитных излучений.
56. Структура и характеристика электрического технического канала утечки информации.
57. Условия возникновения электрического канала утечки информации. Характеристика опасных зон 1 (r1).
58. Перехват наведенных информационных сигналов средствами разведки ПЭМИН.
59. Технический канал утечки информации, создаваемый путем высокочастотного облучения ТСПИ.
60. Классификация аппаратных закладок, внедряемых в средства вычислительной техники.
61. Технический канал утечки информации, создаваемый путем внедрения в ТСПИ электронных устройств негласного получения информации.

62. Характеристика электронных устройств перехвата информации, внедряемых в средства вычислительной техники.
63. Аппаратные кейлоггеры.
64. Способы перехвата информации, обрабатываемой ТСПИ.
65. Общая характеристика речевого сигнала. Линейные характеристики акустического поля.
66. Общая характеристика речевого сигнала. Энергетические характеристики акустического поля.
67. Общая характеристика речевого сигнала. Фонетические характеристики речи.
68. Выделенные помещения.
69. Классификация способов перехвата акустической (речевой) информации.
70. Схема и характеристика прямого акустического канала перехвата речевой информации.
71. Схемы каналов перехвата речевой информации с использованием микрофонов и диктофонов.
72. Схемы каналов перехвата речевой информации с использованием закладных устройств с передачей информации по каналам связи.
73. Схема перехвата речевой информации с использованием устройств типа «телефонное ухо» с передачей информации по телефонной линии на низкой частоте.
74. Принципы построения акустических закладок.
75. Эндовибраторы.
76. Акустовибрационные технические каналы утечки информации.
77. Схемы каналов перехвата речевой информации с использованием стетоскопов.
78. Акустооптические (лазерные) технические каналы утечки информации.
79. Принцип действия лазерной акустической системы разведки.
80. Акустоэлектрический (параметрический) технический канал утечки информации.
81. Схема пассивного акустоэлектрического канала утечки речевой информации.
82. Схема канала перехвата речевой информации методом высокочастотного навязывания.
83. Схема подключения аппаратуры высокочастотного навязывания к телефонной линии.
84. Акустоэлектромагнитный (параметрический) технический канал утечки информации.
85. Схема пассивного акустоэлектромагнитного канала утечки речевой информации.
86. Средства акустической разведки и их технические характеристики. Акустические приемники.
87. Классификация, принципы работы и характеристики микрофонов.
88. Средства акустической разведки и их технические характеристики. Закладные устройства.
89. Характеристика каналов проводной связи как объектов защиты.
90. Способы перехвата информации, передаваемой по каналам проводной связи.

91. Схема перехвата информации, передаваемой по телефонному каналу.
92. Схемы подключения закладных устройств к телефонной линии.
93. Перехват данных, передаваемых по телефонной линии в сети Интернет.
94. Способы перехвата информации, передаваемой по каналам радиосвязи.
95. Структура и характеристика комплекса средств перехвата информации, передаваемой по радиоканалу.
96. Характеристика сетей подвижной радиосвязи общего пользования как объектов защиты.
97. Перехват информации в сетях сотовой и транкинговой связи.
98. Перехват информации, передаваемой с использованием радиотелефонов.
99. Перехват информации, передаваемой в сетях беспроводного доступа.
100. Классификация методов и средств защиты информации от утечки по техническим каналам.
101. Технические мероприятия защиты информации от утечки за счет ПЭМИН с использованием пассивных средств.
102. Технические мероприятия защиты информации от утечки за счет ПЭМИН с использованием активных средств.
103. Методы и средства защиты информации, обрабатываемой ТСПИ, от утечки по техническим каналам за счет ПЭМИН.
104. Способы предотвращения утечки информации через ПЭМИН от СВТ.
105. Способы экранирования, их характеристики.
106. Требования к различным видам экранов.
107. Экранирование технических средств.
108. Экранирование соединительных линий.
109. Экранирование помещений.
110. Заземление технических средств. Схемы заземления.
111. Основные требования, предъявляемые к системе заземления.
112. Заземление технических средств. Сопротивление заземления.
113. Заземление технических средств. Характеристика средств заземления.
114. Фильтрация информационных сигналов.
115. Разделительные трансформаторы.
116. Помехоподавляющие фильтры.
117. Принципы построения и работы помехоподавляющих фильтров.
118. Пространственное зашумление ПЭМИ.
119. Линейное зашумление информационных наводок от ПЭМИ.
120. Принципы работы генераторов шума.
121. Порядок проведения контроля эффективности защиты ВТСС.
122. Состав и основные требования к аппаратуре контроля при контроле ВТСС на подверженность акустоэлектрическим преобразованиям.
123. Схема измерительной установки при контроле ВТСС на подверженность акустоэлектрическим преобразованиям.
124. Порядок проведения проверки ВТСС на подверженность акустоэлектрическим преобразованиям.
125. Состав и основные требования к аппаратуре контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН.

126. Порядок проведения контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН.
127. Сканирующие приемники (принцип работы, основные характеристики).
128. Детекторы поля (принцип работы, основные характеристики).
129. Нелинейные локаторы (принцип работы, основные характеристики).
130. Порядок организации защиты информации на объектах информатизации.
131. Предварительное специальное обследование объекта информатизации.
132. Аналитическое обоснование необходимости создания системы технической защиты информации на защищаемом объекте (СТЗИ) (содержание, порядок проведения).
133. Замысел создания СТЗИ. Техническое задание на разработку СТЗИ объекта информатизации.
134. Организация аттестации объекта информатизации по требованиям безопасности информации.
135. Перечень документов, предоставляемых Заявителем для проведения аттестации объекта информатизации.
136. Порядок проведения аттестации объекта информатизации по требованиям безопасности информации.
137. Заключение по результатам аттестационной проверки объекта информатизации.
138. Аттестат соответствия объекта информатизации.

4.2 Комплект разноуровневых задач

1. Тема 4. Исследование сигнальных демаскирующих признаков радиоэлектронных средств.

Типовые задачи (всего 14 заданий):

Задания реконструктивного уровня:

21) Составить и отладить программу методики расчета вероятности обнаружения в «Mathcad Professional».

22) Исследовать зависимость вероятности обнаружения РЭС от мощности излучения.

23) Исследовать зависимость вероятности обнаружения РЭС от КНД приемной антенны.

24) Исследовать зависимость вероятности обнаружения РЭС от длины волны.

25) Исследовать зависимость вероятности обнаружения РЭС от вероятности ложной тревоги.

26) Составить и отладить программу расчета дальности обнаружения РЭС в «Mathcad Professional».

27) Исследовать зависимость дальности обнаружения РЭС от мощности шума.

28) Смоделировать и исследовать сигнальные демаскирующие признаки амплитудно-модулированных сигналов.

29) Смоделировать и исследовать сигнальные демаскирующие признаки

частотно-модулированных сигналов.

30)Смоделировать и исследовать сигнальные демаскирующие признаки квадратурного амплитудно-модулированного сигнала.

31)Смоделировать и исследовать сигнальные демаскирующие признаки амплитудно-манипулированных сигналов.

32)Смоделировать и исследовать сигнальные демаскирующие признаки частотно-манипулированных сигналов.

33)Смоделировать и исследовать сигнальные демаскирующие признаки фазово-манипулированных сигналов.

Задания творческого уровня:

34)Смоделировать и исследовать сигнальные демаскирующие признаки GMSK сигнала.

Тема 5. Исследование источников опасных сигналов.

Типовые задачи (всего 8 заданий):

Задания реконструктивного уровня:

35)Собрать схему и провести исследования зависимости величины опасного сигнала акустоэлектрического преобразователя от площади диффузора акустоэлектрического преобразователя (динамика).

36)Собрать схему и провести исследования зависимости величины опасного сигнала акустоэлектрического преобразователя от интенсивности входного акустического сигнала.

37)Собрать схему и провести исследования зависимости величины опасного сигнала акустоэлектрического преобразователя от расстояния между источником акустического сигнала и акустоэлектрическим преобразователем.

38)Собрать схему и провести исследования зависимости величины опасного сигнала акустоэлектрического преобразователя от угла прихода звуковой волны.

39)Собрать схему и провести исследования зависимости величины опасного сигнала акустоэлектрического преобразователя от величины электрического сопротивления акустоэлектрического преобразователя.

Задания творческого уровня:

40)Смоделировать и исследовать эффект паразитной генерации на транзисторном усилителе.

41)Смоделировать и исследовать эффект паразитной генерации на операционном усилителе.

42)Смоделировать и исследовать эффект паразитной генерации на логических элементах.

Тема 8. Моделирование и исследование технических каналов утечки информации, возникающих за счет побочных электромагнитных излучений и наводок.

Типовые задачи (всего 8 заданий):

Задания реконструктивного уровня:

43)Смоделировать электромагнитный технический канал утечки информации, возникающий за счёт ПЭМИ от СВТ, в программе EWB.

44) Исследовать эквивалентную электрическую схему замещения электромагнитного ТКУИ, возникающего за счёт ПЭМИ от СВТ.

45) Смоделировать электромагнитный технический канал утечки информации, возникающий за счёт ПЭМИ при передаче цифрового видеосигнала.

46) Исследовать электромагнитный технический канал утечки информации, возникающий за счёт ПЭМИ при передаче цифрового видеосигнала.

Задания творческого уровня:

47) Смоделировать и провести исследование электрического канала утечки информации, возникающего путем наводки информационного сигнала в линию электропитания ТСПИ за счет гальванической паразитной связи.

48) Смоделировать и провести исследование электрического канала утечки информации, возникающего путем наводки информационного сигнала в соединительную линию ВТСС за счет емкостной паразитной связи.

49) Смоделировать и провести исследование электрического канала утечки информации, возникающего путем наводки информационного сигнала в цепь заземления ТСПИ за счет индуктивной паразитной связи.

50) Смоделировать и провести исследование электрического канала утечки информации, возникающего путем наводки от высокочастотного ПЭМИ информационного сигнала в посторонних проводниках.

Тема 12. Исследование способов и принципов построения и работы технических средств подслушивания акустической (речевой) информации.

Типовые задачи (всего 8 заданий):

Задания реконструктивного уровня:

51) Смоделировать в программе «Electronics Workbench» простейшую схему стетоскопа.

52) Исследовать амплитудно-частотную характеристику стетоскопа.

53) Провести анализ выходного сигнала усилителя стетоскопа на наличие нелинейных искажений.

54) Провести анализ влияния фильтра нижних частот на качество работы стетоскопа.

55) Смоделировать в программе «Electronics Workbench» простейшую схему радиозакладного устройства, формирующего амплитудно-модулированные сигналы.

56) Смоделировать в программе «Electronics Workbench» простейшую схему радиозакладного устройства, формирующего частотно-модулированные сигналы.

57) Исследовать принципы работы радиозакладного устройства, формирующего амплитудно-модулированные сигналы.

58) Исследовать принципы работы радиозакладного устройства, формирующего частотно-модулированные сигналы.

Тема 13. Исследование акустического канала утечки информации, создаваемого способом высокочастотного навязывания.

Типовые задачи (всего 8 заданий):

Задания реконструктивного уровня:

59) Смоделировать в программе EWB процесс паразитной модуляции на

нелинейном элементе – диоде.

60) Исследовать процесс паразитной модуляции на нелинейном элементе – диоде.

61) Смоделировать в программе EWB процесс паразитной модуляции на конденсаторном микрофоне.

62) Исследовать процесс паразитной модуляции на конденсаторном микрофоне.

63) Смоделировать в программе EWB модель телефонного аппарата.

Задания творческого уровня:

64) Смоделировать в программе EWB систему высокочастотного навязывания.

65) Создать в программе EWB модель процесса высокочастотного навязывания.

66) Исследовать в программе EWB процесс высокочастотного навязывания.

Тема 17. Исследование принципов построения и работы средств экранирования, фильтрации информационных сигналов и генерации шума для энергетического скрывания ПЭМИН.

Типовые задачи (всего 16 заданий):

Задания реконструктивного уровня:

67) Смоделировать в программе EWB эквивалентную схему замещения процесса экранирования электромагнитного излучения.

68) Исследовать в программе EWB эквивалентную схему замещения процесса экранирования электромагнитного излучения.

69) Смоделировать и исследовать в программе EWB эквивалентную схему электрического экранирования провода.

70) Смоделировать и исследовать в программе EWB эквивалентную схему магнитного экранирования провода.

71) Смоделировать и исследовать в программе EWB эквивалентную схему полного электромагнитного экранирования провода.

72) Рассчитать и смоделировать в программе EWB эквивалентные схемы замещения фильтров нижних частот с Т-образными и П-образными структурами.

73) Провести исследование амплитудно-частотных характеристик фильтров нижних частот с Т-образными и П-образными структурами, определить их полосы пропускания.

74) Рассчитать и смоделировать в программе EWB эквивалентные схемы замещения фильтров высоких частот с Т-образными и П-образными структурами.

75) Провести исследование амплитудно-частотных характеристик фильтров высоких частот с Т-образными и П-образными структурами, определить их полосы пропускания.

76) Рассчитать и смоделировать в программе EWB эквивалентные схемы замещения полосовых пропускающих фильтров с Т-образными и П-образными структурами.

77) Провести исследование амплитудно-частотных характеристик полосовых пропускающих фильтров с Т-образными и П-образными структурами, определить их полосы пропускания.

78) Рассчитать и смоделировать в программе EWB эквивалентные схемы замещения полосовых загораживающих фильтров с Т-образными и П-образными структурами.

79) Провести исследование амплитудно-частотных характеристик полосовых загораживающих фильтров с Т-образными и П-образными структурами, определить их полосы пропускания.

80) Собрать лабораторную установку для энергетического подавления электромагнитных излучений с помощью генератора шума ГШ-1000М.

81) Провести исследование способа зашумления радиозакладок при помощи генератора шума «ГШ – 1000М».

82) Смоделировать в программе EWB эквивалентную схему замещения генератора шума и провести исследование принципов его работы.

Тема 19. Исследование звукопоглощающих и звукоизоляционных характеристик материалов, применяемых для звукоизоляции выделенных помещений.

Типовые задачи (всего 4 задания):

Задания реконструктивного уровня:

83) Собрать лабораторную установку для исследования звукопоглощающих свойств материалов.

84) Провести исследования звукопоглощающих свойств материалов

85) Собрать лабораторную установку для исследования звукоизоляционных свойств инженерных конструкций.

86) Провести исследования звукоизоляционных свойств инженерных конструкций.

Тема 21. Исследование способов и средств защиты речевой информации в телефонных линиях.

Типовые задачи (всего 16 заданий):

Задания реконструктивного уровня:

87) Смоделировать в программе EWB амплитудный диодный ограничитель для защиты телефонного аппарата.

88) Провести исследование принципа работы амплитудного диодного ограничителя для защиты телефонного аппарата.

89) Смоделировать в программе EWB схему защиты звонковой цепи телефонного аппарата.

90) Провести исследование схемы защиты звонковой цепи телефонного аппарата.

91) Смоделировать в программе EWB схему защиты цепи микрофона телефонного аппарата.

92) Провести исследование схемы защиты цепи микрофона в телефонном аппарате.

93) Смоделировать в программе EWB схему фильтрации опасных сигналов для защиты телефонной линии.

94) Провести исследование схемы фильтрации опасных сигналов для защиты телефонной линии.

95) Смоделировать в программе EWB комбинированную схему защиты

телефонного аппарата.

96) Провести исследование комбинированной схемы защиты телефонного аппарата.

Задания творческого уровня:

97) Смоделировать в программе EWB эквивалентную схему замещения кабельного радара в режиме измерения неоднородностей, создаваемых при подключении резистивной нагрузки.

98) Провести исследование эквивалентной схемы замещения кабельного радара в режиме измерения неоднородностей, создаваемых при подключении резистивной нагрузки.

99) Смоделировать в программе EWB эквивалентную схему замещения кабельного радара в режиме измерения неоднородностей, создаваемых при подключении последовательной емкостной или параллельной индуктивной нагрузки.

100) Провести исследование эквивалентной схемы замещения кабельного радара в режиме измерения неоднородностей, создаваемых при подключении последовательной емкостной или параллельной индуктивной нагрузки.

101) Смоделировать в программе EWB эквивалентную схему замещения кабельного радара в режиме измерения неоднородностей, создаваемых при подключении параллельной емкостной или последовательной индуктивной нагрузки.

102) Провести исследование эквивалентной схемы замещения кабельного радара в режиме измерения неоднородностей, создаваемых при подключении параллельной емкостной или последовательной индуктивной нагрузки.

Тема 23. Исследование принципов построения и работы аналоговых скремблеров речевого сигнала.

Типовые задачи (всего 4 задания):

Задания реконструктивного уровня:

103) Провести в программе «WAV Scrambler» исследование принципов работы скремблера в режиме временной инверсии.

104) Провести в программе «WAV Scrambler» исследование принципов работы скремблера в режиме частотной инверсии.

105) Провести в программе «WAV Scrambler» исследование принципов работы скремблера в режиме временного скремблирования.

106) Провести в программе «WAV Scrambler» исследование принципов работы скремблера в режиме частотного скремблирования.

Тема 27. Исследование принципов построения и работы средств выявления электронных устройств перехвата информации: детекторов поля, сканирующих приемников и нелинейных локаторов.

Типовые задачи (всего 12 заданий):

Задания творческого уровня:

107) Смоделировать в программе EWB принципиальную схему индикатора (детектора) электромагнитного поля.

108) Провести в программе EWB исследование принципиальной схемы индикатора (детектора) электромагнитного поля в режиме индикации.

109) Провести в программе EWB исследование принципиальной схемы индикатора (детектора) электромагнитного поля в режиме акустической завязки.

110) Разработать алгоритм поиска (локализации) устройств негласного перехвата информации с помощью детектора поля.

111) Смоделировать в программе EWB упрощенную функциональную схему сканирующего приемника.

112) Провести в программе EWB исследование принципов работы сканирующего приемника.

113) Разработать алгоритм обнаружения устройств негласного перехвата информации с помощью сканирующего приемника.

114) Смоделировать в программе EWB принципиальную схему замещения нелинейного локатора для обнаружения р-п-перехода.

115) Провести в программе EWB исследование принципов работы нелинейного локатора в режиме обнаружения р-п-перехода.

116) Смоделировать в программе EWB принципиальную схему замещения нелинейного локатора для обнаружения МОМ-диода (коррозийной нелинейности).

117) Провести в программе EWB исследование принципов работы нелинейного локатора в режиме обнаружения МОМ-диода (коррозийной нелинейности).

118) Разработать алгоритм поиска (локализации) устройств негласного перехвата информации с помощью нелинейного локатора.

4.3 Вопросы для защиты заданий по практическим занятиям

Практические занятия 1 – 4. Тема 28. Принципы построения и работы программно-аппаратных комплексов поиска устройств негласного съема информации.

1) Назначение и принцип работы ПАК «Легенда».

2) Предназначение функциональных кнопок измерительного прибора R&S FS300.

3) Порядок подготовки изделия к использованию.

4) Порядок работы с областью диаграмм, меню и функции интерфейса специализированного программного обеспечения.

5) Порядок проведения специальных исследований на поиск тестового сигнала.

6) Порядок составления протокола измерений с помощью расчетной программы.

7) Порядок поиска и измерения ПЭМИН при помощи управляющей программы.

8) Порядок контроля электромагнитной обстановке (ЭМО) в автоматическом режиме измерений.

9) Порядок поиска составляющих тестового сигнала в автоматическом режиме измерений.

10) Порядок поиска и измерения ПЭМИН в полуавтоматическом режиме измерения.

Практические занятия 5-8. Тема 31. Расчет и оценка защищенности технических средств от утечки информации за счет ПЭМИН.

11) Методика расчета и оценки защищенности технических средств от утечки информации за счет ПЭМИ.

12) Методика расчета и оценки защищенности технических средств от утечки информации за счет наводок от ПЭМИ по соединительным линиям ВТСС

13) Порядок проведения измерений побочных электромагнитных излучений, создаваемых ПЭВМ, с помощью имеющихся средств измерения.

14) Порядок оценки защищенности информации обрабатываемой ПЭВМ от ее утечки по электромагнитному каналу с помощью программы Ratchet.

15) Порядок проведения измерений наводок в соединительной линии ВТСС от побочных электромагнитных излучений, создаваемых ПЭВМ, с помощью имеющихся средств измерения.

16) Порядок оценки защищенности информации обрабатываемой ПЭВМ от ее утечки по электрическому каналу с помощью программы Ratchet.

Практические занятия 9-13. Тема 34. Расчет и оценка защищенности выделенного помещения от утечки речевой информации.

17) Показатель и критерии количественной оценки качества перехваченной речевой информации.

18) Методика расчета словесной разборчивости речи.

19) Порядок разработки программы для ПЭВМ по расчету и оценке защищенности выделенного помещения от утечки речевой информации

20) Порядок исследования зависимости словесной разборчивости речи от расстояния между источником акустического сигнала и приемником акустического сигнала для открытого пространства.

21) Порядок исследования зависимости словесной разборчивости речи от расстояния между источником акустического сигнала и приемником акустического сигнала в выделенном помещении.

22) Порядок оценки словесной разборчивости речи в каналах утечки акустической информации.

23) Порядок исследования эффективности маскирования речи источниками шума.

Практические занятия 14-18. Тема 34. Расчет и оценка защищенности

выделенного помещения от утечки речевой информации.

24) Перечень аттестационных испытаний автоматизированной системы по требованиям безопасности информации.

25) Состав пакета исходных данных документов для аттестации автоматизированной системы.

26) Состав аттестационной комиссии.

27) Порядок документального оформления результатов аттестационных испытаний.

28) Перечень разделов протокола аттестационных испытаний объекта информатизации.

29) Содержание разделов протокола аттестационных испытаний объекта информатизации.

30) Реквизиты протокола аттестационных испытаний объекта информатизации.

5. Список рекомендуемой литературы

5.1.1. Основная литература

– Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: учеб. пособие для студентов вузов. Под ред. Зайцева А.П. и Шелупанова А.А.. Изд. 4-е испр. и доп. – М.: Горячая линия-Телеком, 2013.

– Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. – М.: НПЦ «Аналитика», 2013.

– Методы и средства инженерно-технической защиты информации: учебное пособие [Электронный ресурс]/ В.И. Аверченков, М.Ю. Рытов, А.В. Кувиклин, Т.Р. Гайнулин. – 2-е изд., стер. – М.: Флинта, 2014. – URL:<http://biblioclub.ru/index.php?page=book&id=93275>

5.1.2. Дополнительная литература

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

– Торокин А.А. Инженерно-техническая защита информации: Учебное пособие. – М.: «Гелиос АРВ», 2013. – 960 с.

– Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки по информации техническим каналам: Учеб. пособие. – М.: Горячая линия – Телеком, 2013.

– Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г. Защита информации в телекоммуникационных системах. – К.: «МК-Пресс», 2013.

– Меньшаков Ю.К. Теоретические основы технических разведок.- М.: МГТУ им. Н.Э.Баумана, 2013.

5.1.3. Методическая литература

– Электронный курс лекций:

– Электронные методические рекомендации по выполнению лабораторных работ.

– Электронные методические рекомендации к практическим занятиям.

– Очков В.Ф. Mathcad 14 для студентов и инженеров. Русская версия. – СПб.: БХВ-Петербург, 2013. – 512 с.

– Черных И.В. Simulink: среда создания инженерных приложений. – М.: Диалог-МИФИ, 2013. – 496 с.

– Серебряков А.С. Электротехника и электроника. Лабораторный практикум на Electronics Workbench и Multisim. – М.: Высшая школа, 2013. – 336 с.

– Кардашев Г.А. Цифровая электроника на персональном компьютере. Electronics Workbench и Micro-Cap. – М.: Горячая Линия - Телеком, 2014. – 312 с.

5.1.4. Интернет-ресурсы

– сайт Федеральной службы по техническому и экспортному контролю. – www.fstec.ru;

– сайт Федеральной служба безопасности Российской Федерации. – www.fsb.ru.

5.1.5. Программное обеспечение

- специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам;

- программа тестового контроля «Iren»;

- математический программный редактор «Mathcad Professional 14»;

- программный редактор «Electronics Workbench 5.12».

- Обучающие программы (симуляторы): электронная программная модель «Спецтехника»; электронная программная модель скремблера «Scrambler»; электронная программная модель прибора «ПСЧ-5»; электронная программная модель «Нелинейный локатор NR-m»; электронная расчетная программа «Методика оценки защищенности конфиденциальной информации, обрабатываемой техническими средствами и системами».

5.2. Материально-техническое обеспечение дисциплины